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

KÜBİK REZİDÜLER

DOKTORA TEZİ

Dilek NAMLI

Balıkesir, Kasım-2001

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

KÜBİK REZİDÜLER

DOKTORA TEZİ

Dilek NAMLI

Tez Danışmanı : Doç. Dr. İsmail Naci CANGÜL

Sınav Tarihi : 12.11.2001

Jüri Üyeleri : Prof. Dr. Musa ERDEM (BAÜ)
Doç. Dr. İ. Naci CANGÜL (Danışman-UÜ)
Yrd. Doç. Dr. Osman BİZİM (UÜ)
Yrd. Doç. Dr. Basri ÇELİK (UÜ)
Yrd. Doç. Dr. Hülya GÜR (BAÜ)

Balıkesir, Kasım-2001

ÖZET

KÜBİK REZİDÜLER

Dilek NAMLI

Balıkesir Üniversitesi, Fen Bilimleri Enstitüsü,
Matematik Eğitimi Ana Bilim Dalı

Doktora Tezi / Tez Danışmanı: Doç. Dr. İsmail Naci CANGÜL

Balıkesir, 2001

Bu tezin amacı kuadratik rezidüler için literatürde geniş bir şekilde yer alan sonuçları, kübik rezidüler için elde etmek ve bunlar yardımıyla üçüncü dereceden denklemlerin çözümleri ile ilgili yöntemler ortaya koymaktır.

Bu çalışma yedi bölümden oluşmaktadır. Birinci bölümde daha sonraki bölümlerde gerekli olacak bazı önbilgiler hatırlatılmıştır.

İkinci bölümde kübik denklemlerin tarihçesi ve bunları çözme amacıyla ortaya atılmış olan yöntemler verilmiştir.

Üçüncü bölümde kuadratik rezidüler ile ilgili sonuçlar bir araya getirilmiş, dördüncü bölümde ise kübik rezidüler ele alınmıştır. Bu bölümde $D=\mathbf{Z}[\omega]$ halkasındaki asallar sınıflandırılmış, ve kübik rezidü kavramı ele alınmıştır. Çeşitli formüller elde edilmiş, değişik asal sayı tipleri için kübik rezidü karakterinin nasıl hesaplanacağı belirlenmiştir. Kübik İndirgeme Yasası verilmiştir.

Beşinci bölümde özel bazı kübik denklemlerin çözümünde kübik rezidülerden nasıl faydalanılabileceği ile ilgili sonuçlar elde edilmiştir. Dördüncü ve beşinci bölümdeki tüm sonuçlar orijinaldir.

Altıncı bölüm, kübik denklemlerin yaklaşık köklerini bulma ile ilgili yöntem lere ayrılmıştır.

Yedinci ve son bölümde ise tezde neler yapıldığı belirtilmiştir.

Anahtar kelimeler: Kuadratik rezidü, Kübik rezidü, Rasyonel asal,Kompleks asal, 1.tip asal, İndeks.

ABSTRACT

CUBIC RESIDUES

Dilek NAMLI

Balıkesir University, Institute of Science,
Department of Mathematics Education

Ph. D. Thesis/ Supervisor: Doç. Dr. İsmail Naci CANGÜL
Balıkesir, 2001

The aim of this thesis is to determine the methods for calculating cubic residues and the methods used in solving cubic equations by means of cubic residues, similarly to the ones given in literature for quadratic residues.

This work consists of seven chapters. In the first chapter some preliminary information used in succeding chapters are given.

In the second chapter the history of cubic equations and the methods given for solving these are mentioned.

In the third chapter, results for quadratic residues are collected. In the fourth chapter cubic residues are investigated. In this chapter, first, the primes in the ring $D=\mathbf{Z}[\omega]$ are classified, and then the notion of cubic residue is introduced. Several formulae are obtained to calculate cubic residue character for several types of primes in $\mathbf{Z}[\omega]$. Cubic reciprocity law is given.

In the fifth chapter, some results concerning the solutions of some specific cubic equations by means of cubic residues are given. All results in chapters fourth and fifth are original.

The approximation methods for finding the roots of a given cubic equation are recalled.

At the final chapter, the conclusion and summary of what has been done at the thesis is given.

KEY WORDS: Quadratic residue, Cubic residue, rational prime, complex prime, primary prime, İndex.

İÇİNDEKİLER

ÖNSÖZ

Öncelikle çalışmalarım sırasında beni destekleyip güdüleyen, deneyimleriyle yönlendiren ve pozitif yaklaşımıyla güçlükler karşısında da rahatlamamı sağlayan danışman hocam Doç. Dr. İsmail Naci CANGÜL'e, yine her zaman her konuda destek olarak yanımda olduğunu hissettiren hocam Prof. Dr. Turgut BAŞKAN' a, her zaman olduğu gibi tezimin yazım aşamasında da yardımlarını esirgemeyen Recep ŞAHİN'e ve çalışmalarım süresince emeği geçen başta Ayşen KARAMETE olmak üzere tüm Matematik ve Matematik Eğitimi Bölümündeki arkadaşlarıma sonsuz teşekkürler ediyorum.

Ayrıca dostça yaklaşımlarından dolayı Uludağ Üniversitesi Fen Fakültesi Matematik Bölümündeki tüm hocalarıma ve arkadaşlarıma bu vesileyle teşekkür ediyorum.

Çocuklarının eğitimi için güç koşullarda bile hiç bir fedakarlıktan kaçınmayan sevgili anneme, babama ve her zaman ve her konuda yanımda olduğunu hissettiğim kardeşim İpek' e içten teşekkürlerimi sunuyorum.

Ve hayatıma girdiği andan itibaren bana hep mutluluk veren, herşeyi paylaştığım sevgili, güzel eşim sana ne diyebilirim ki her zaman, her yerde olduğu gibi tezimi hazırlarken de yanımda olduğun için teşekkürler...

Kasım, 2001 Dilek NAMLI

1. GİRİŞ

Kübik denklemlerin çözülebilmesi problemi yaklaşık 4000 yıldır çalışılmaktadır. Özellikle Tartaglia, Cardano, Viéte tarafından bazı metodlar geliştirilmiştir. Bu tezde, bu çalışmalar ve ek olarak bu denklemlerin yaklaşık çözümleri ile ilgili sonuçlar verilmiştir.

Kuadratik rezidü kavramı matematiğin bir çok alanında karşımıza çıkmaktadır. Örneğin, ikinci derece denklemlerin belli bir modda çözümleri, bazı grupların altgruplarının bulunması ve ilkel köklerin bulunması bunların başlıcalarıdır.

Kübik rezidü kavramı, Gauss tarafından ele alınmış olup G.Eisenstein tarafından bazı sonuçlar elde edilmiştir. Özellikle Kübik İndirgeme Yasası bunlar arasındadır. Bu tezde kübik rezidü kavramıyla ilgili literatürde bulunan az sayıda sonuç bir araya getirilmiş ve bunların daha ayrıntılı ele alınmasıyla çok sayıda sonuç elde edilmiştir.

Kübik rezidüleri çalışırken birimin ilkel kökü olan $\omega = \frac{-1+\sqrt{-3}}{2}$ elemanının tamsayılara katılmasıyla elde edilen $\mathbf{Z}[\omega] = \{a + b\omega | a, b \in \mathbf{Z}\}$ halkası kullanılmaktadır. Bu halkadaki asal sayılar ile ilgili literatürde olmayan sınıflandırma teoremleri elde edilmiş ve $\mathbf{Z}[\omega]$ nın bir U.F.D.olduğu belirtilmiştir.

Kübik rezidü karakteri, kuadratik rezidüler için varolan Legendre sembolüne benzer olarak tanımlanmaktadır. Aslında ω nın $p \equiv 1 \ (3)$ olduğunda $\mathbf{Z}_p$ nin bir elemanı olarak düşünülebileceği ispatlandığından, $p \equiv 1 \ (3)$ olduğunda $\mathbf{Z}[\omega]$ nın tüm elemanlarını $\mathbf{Z}_p$ de düşünebiliriz. Bu sayede, modun $a+b\omega$ gibi bir kompleks sayı olması durumunda yine bir tamsayı modu gibi düşünülebileceği gösterilmiştir.

Kübik rezidü karakterinin hesaplanması ile ilgili çeşitli sonuçlar elde edilmiştir. Kübik rezidülerin, kübik denklemlerin belli bir modda çözülebilmesi problemiyle ilişkisi ortaya konulmuştur.

1.1 Lineer Kongrüans Denklemleri

Burada lineer kongrüansların çözülebilme koşullarından bahsedeceğiz.

1.1.1Tanım: $n \in \mathbf{N}$ olsun. Bu durumda $\varphi(n)$ ile gösterilen ve

$$\varphi(n) = \#\left\{k \in Z^+ \middle| (k,n) = 1,\ 1 \le k < n\right\}$$

şeklinde tanımlanan fonksiyona Euler-φ fonksiyonu denir.

Özel olarak n asal olduğunda $\varphi(n) = n - 1$ olur.

1.1.2 Tanım: $a, b \in \mathbf{Z}$ ve m, a'yı bölmeyen bir sayı olmak üzere

$$ax \equiv b \ (m)$$

şeklindeki denklemlere lineer kongrüans denklem denir.

1.1.3 Teorem: (a,m)=1 ise $ax \equiv b \ (m)$ kongrüansının bir tek çözümü vardır,[1].□

1.1.4 Teorem: (a,m)=1 olmak üzere $ax \equiv b \ (m)$ lineer kongrüansının çözümü

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

dir, [1].□

1.1.5 Teorem: (a,m)=d olmak üzere $ax \equiv b \ (m)$ lineer kongrüansının çözümünün olması için gerek ve yeter şart $d \mid b$ olmasıdır. Bu durumda tam d tane çözüm vardır, [2].□

1.1.6 Teorem: $ax+by\equiv c\ (m)$ lineer kongrüansının çözümünün olması için gerek ve yeter şart $d=(a,b,m)\mid c$ olmasıdır, [1].□

1.1.7 Teorem(Polinomlar İçin Lagrange Teoremi): p bir asal sayı ve a_n p modunda sıfıra denk değilse,

$$P(x)=a_n x^n+a_{n-1}x^{n-1}+\ldots+a_0\equiv 0\,(p)$$

kongrüansının köklerinin sayısı en fazla n tanedir, [1].□

1.1.8 Teorem(Fermat' ın Küçük Teoremi): p asal ve (a,p)=1 ise

$$a^{p-1}\equiv 1\ (p)$$

dir.□

Euler, bu sonucu tüm doğal sayılara genelleştirmiştir:

1.1.9 Teorem (Euler Teoremi): $(a,m)=1$ ise

$$a^{\varphi(m)}\equiv 1\ (m)$$

dir.□

1.2 Z_n de Birimler

p asal ise $ab\equiv 0\ (p)$ iken $a\equiv 0$ veya $b\equiv 0\ (p)$ dir. Bu sayede $\mathbf{Z}_p$ nin aritmetiği, **Z** ninkine benzerlik gösterir. Ancak bu özellik mod bileşik sayı iken geçerli olmaz. Eğer $n=a.b$, $1<a<n$ ise $a.b\equiv 0\ (n)$ olması durumunda a ve b n modunda sıfıra denk olmayabilir. Bu gibi problemler sebebiyle asal moddan birleşik moda geçerken daha dikkatli olmak gereklidir.

Örneğin, Fermat'ın Küçük Teoremindeki p asalını n birleşik sayısı ile değiştirirsek $a^{n-1}\equiv 1\ (n)$ genelde doğru olmayabilir. Bu durumda Euler teoremindeki gibi a'nın $\varphi(n)$ inci kuvvetini almak gerekir. Yani $a^{\varphi(n)}\equiv 1\ (n)$ dir.

1.2.1 Tanım: $\bar{a} \in \mathbf{Z}_n$ in çarpmaya göre bir tersi, $\bar{a}.\bar{b} = \bar{1}$ olacak şekildeki bir $\bar{b} \in \mathbf{Z}_n$ dir. $\mathbf{Z}_n$ de çarpmaya göre tersi olan bir elemana birim (unit) denir ve $\mathbf{Z}_n$ deki birimlerin kümesi $\mathcal{U}_n$ ile gösterilir.

1.2.2 Yardımcı Teorem: $\bar{a} \in \mathbf{Z}_n$ in birim olması için gerek ve yeter şart (a,n)=1 olmasıdır.

İspat: $\bar{a}$ bir birimse $\bar{a}.\bar{b} = \bar{1}$, yani a.b≡1 (n) olacak şekilde bir $b \in \mathbf{Z}_n$ vardır. O halde ab=1+qn, $q \in \mathbf{Z}$ yazabiliriz. Bu durumda, a ve n yi aynı anda bölen bir sayı, 1' i de bölecektir. O halde (a,n)=1 olmalıdır.

Tersine (a,n)=1 ise $1 = ax + ny$ olacak şekilde $x,y \in \mathbf{Z}$ vardır. O halde ax≡1(n), yani $\bar{x}$, $\bar{a}$ nin çarpmaya göre tersidir.□

1.2.3 Örnek: $\mathbf{Z}_8$ deki birimler $\bar{1}$, $\bar{3}$, $\bar{5}$ ve $\bar{7}$ dir. Çünkü $\bar{1}.\bar{1}=\bar{1}$, $\bar{3}.\bar{3}=\bar{1}$ ve $\bar{7}.\bar{7}=\bar{1}$ dir, yani her biri kendisinin tersidir. $\mathbf{Z}_9$ da ise 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 tersidirler. $\mathcal{U}_9=\{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\}$ dir. Dikkat edilirse $|\mathcal{U}_n| = \varphi(n)$ dir.

1.2.4 Tanım: $g \in \mathbf{Z}$ olsun. $\bar{g}$, $\mathcal{U}_n$ yi üretiyorsa g ye n modunda bir ilkel kök denir. Bu durumda g nin 0 ile n-1 arasındaki tüm kuvvetleri farklıdır ve $\mathcal{U}_n$ deki tüm elemanları verir.

1.2.5 Örnek: mod 5 te $\bar{2}$ ve $\bar{3}$ ilkel köklerdir. Çünkü $\mathcal{U}_5=\{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ ve

$\bar{1}^2 = \bar{1}$,

$\bar{2}^1 = \bar{2}, \bar{2}^2 = \bar{4}, \bar{2}^3 = \bar{3}, \bar{2}^4 = \bar{1}$,

$\bar{3}^1 = \bar{3}, \bar{3}^2 = \bar{4}, \bar{3}^3 = \bar{2}, \bar{3}^4 = \bar{1}$,

$\bar{4}^1 = \bar{4}, \bar{4}^2 = \bar{1}$

dir.

1.3 İndeks Kuralları ile Lineer Kongrüansların Çözümleri

1.3.1 Tanım: g, $\mathbf{Z}_m$ de bir ilkel kök olsun. Eğer (a,m)=1 iken $0 \le k \le \varphi(m)-1$ ve $g^k \equiv a\,(m)$ olacak şekilde bir k tamsayısı varsa, k ya a nın indeksi denir ve k=I(a) ile gösterilir.

İndeks fonksiyonunun özellikleri, logaritma fonksiyonuna benzerlikler gösterir:

1) $I(a.b) \equiv I(a) + I(b) \quad (\varphi(m))$

2) $I(a^n) \equiv n.I(a) \quad (\varphi(m)),\ n \ge 1$ için

3) $I(1) = 0,\ I(g) = 1$

4) $I(-1) = \varphi(m)/2,\quad m > 2$ ise

5) g', $\mathbf{Z}_m$ de g den farklı bir ilkel kök ise $I_g(a) \equiv I_g(g').I_{g'}(a) \quad (\varphi(m))$

6) $(a,b)=1$ ise $I(a/b) \equiv I(a) - I(b)\ (\varphi(m))$

İndeks fonksiyonu, $ax \equiv b\ (c)$ şeklindeki lineer kongrüansları çözmek için çok kullanışlıdır.

Örneğin; $5x \equiv 3\ (13)$ lineer kongrüansını düşünelim. p=13 asal olduğundan $\mathcal{U}_{13}=\{1,2,3,4,5,6,7,8,9,10,11,12\}$ dir. $\varphi(\varphi(13)) = \varphi(12) = 4$ tane ilkel kök vardır. $12=2^2.3$ olduğundan, mod 13 teki ikinci ve üçüncü dereceden rezidüleri bulacağız. İkinci dereceden rezidüler; 1, 3, 4, 9, 10, 12 ve üçüncü dereceden rezidüler; 1, 5, 8 ve 12 dir. Geriye 2, 6, 7, 11 olmak üzere dört eleman kalır, bunlar ilkel köklerdir. Bunlardan birini seçelim. Mesela $g = 2$ olsun ve indeks tablosunu oluşturalım:

a	2	4	8	3	6	12	11	9	5	10	7	1
I(a)	1	2	3	4	5	6	7	8	9	10	11	12

Şimdi tekrar $5x \equiv 3\ (13)$ kongrüansına dönelim.

$I(5x) \equiv I(3)\ (\varphi(13))$

$I(5)+I(x)\equiv I(3)$ (12)

dir. ve tablodan faydalanarak,

$9+I(x)\equiv 4$ (12)

$I(x)\equiv 7$ (12) ve $x\equiv 11$ (13)

bulunur.

1.4 Diğer Sonuçlar

1.4.1 Tanım: Eğer bir f polinomunun en büyük dereceli teriminin katsayısı 1 ise f ye monik polinom denir.

1.4.2 Tanım: $f(X)=a_nX^n+a_{n-1}X^{n-1}+\ldots+a_0$

şeklindeki bir polinomda, $a_{n-1}=0$ ise bu polinoma indirgenmiş polinom denir.

1.4.3 Yardımcı Teorem: Eğer $f(X)=a_nX^n+a_{n-1}X^{n-1}+\ldots+a_0$ ise X yerine $x-\frac{a_{n-1}}{n}$ yazılarak $\tilde{f}(x)=f\left(x-a_{n-1}/n\right)$ indirgenmiş polinomu elde edilir. Üstelik eğer u, $\tilde{f}(x)$ in bir kökü ise, $u-\frac{a_{n-1}}{n}$, f(X) in bir köküdür.□

Genel kübik denklem; $A,B,C,D\in\mathbf{R}$ veya $\mathbf{C}$ ve $A\neq 0$ olmak üzere

$$Ax^3+Bx^2+Cx+D=0 \qquad (1.1)$$

şeklindedir. (1.1) denklemi A ile bölünürse, $\frac{B}{A}=b$, $\frac{C}{A}=c$ ve $\frac{D}{A}=d$ olmak üzere,

$$x^3+bx^2+cx+d=0 \qquad (1.2)$$

üçüncü derece monik polinomu elde edilir. Bir kübik denklemdeki ikinci derece terimin yokedilebileceğini 1.4.3 yardımcı teoreminden biliyoruz. Gerçekten, (1.2) denkleminde $x=y+k$ yazılırsa,

$$(y+k)^3+b(y+k)^2+c(y+k)+d=0$$

$$y^3+(3k+b)y^2+(3k^2+2bk+c)y+k^3+bk^2+ck+d=0$$

denklemi elde edilir ki, bu denklemde y^2 li terimin yokedilmesi için $k=-\frac{b}{3}$ seçilmelidir. Dolayısıyla, eğer (1.2) denkleminde $x=y-\frac{b}{3}$ yazılırsa ikinci dereceden terimi olmayan, üçüncü dereceden $x^3+mx+n=0$ denklemi elde edilir.

1.4.4 Tanım: n>1 tamsayısının kendisinden ve 1 den başka pozitif böleni yoksa bu sayıya asal sayı denir. Rasyonel asal sayı denildiğinde de bu şekildeki asal sayıları anlayacağız.

Rasyonel asal sayılar ile ilgili aşağıdaki iyi bilinen sonuç bu çalışmada sıkça kullanılacaktır.

1.4.5 Teorem: a, b∈**Z** olmak üzere $p=a^2-ab+b^2$ şeklindeki tüm rasyonel asallar 6 modunda 1'e denktir.

1.4.6 Tanım: $\omega=\frac{-1+\sqrt{-3}}{2}$ olmak üzere $\pi=a+b\omega$ sayısı, c+dω ve e+fω şeklindeki birimden farklı iki sayının çarpımı olarak yazılamıyorsa π ye kompleks asal sayı denir.

1.4.7 Teorem(Euler Kriteri): $p\equiv 1\ (k)$ bir asal sayı ve k>2 bir tamsayı olsun. $x^k\equiv a\ (p)$ kongrüansının çözülebilmesi için gerek ve yeter şart $a^{\frac{p-1}{k}}\equiv 1\ (p)$ olmasıdır.

2. KÜBİK DENKLEMLERİN ÇÖZÜM YÖNTEMLERİ

Kübik denklemler, Babilliler (M.Ö 2000) zamanından beri çalışılmaktadır. Her ne kadar kökleri hesaplamak için kullandıkları yöntem, tam olarak açık olmasa da Babilliler kübik kökleri tablolar yaparak hesapladılar. Neugebauer'e göre bir iterasyon metodu kullandıklarına dair güçlü deliller vardır. Babilliler karekökler, kareler, küpler ve üstelik $x^3 + x^2$ ler için de tablolar yapmışlardır. Neugebauer'e göre, $x^3 + bx^2 + cx + d$ polinomunu basitleştirmek için, ardışık yerine koyma yöntemleri uyguladıklarına ilişkin de güçlü deliller vardır.

Çin'de de yüksek dereceli denklemlerin köklerinin yaklaşık değerleri için çözüm yöntemleri uzun zamandır biliniyordu. Jiuzhang'ın önemli problemlerinden biri, bir küpkökü bulabilmek ve yazabilmekti. Çin'de, üçten daha yüksek dereceli sayısal denklemler için ilk olarak M.S.1245 civarında Q.I.N.Jiushao tarafından çalışmalar yapıldı.

Araplar da bazı kübik denklemleri cebirsel olarak çözdüler ve geometrik yorumunu verdiler. Bunu bir denklem için Tabit ibn Qorra (836-901) ve al-hasan ibn al-haitham (965-1039) yaptı. Umar al-Khayyami (Omar Khayyam) (1048-1125) genel kübik denklemleri çözmek için konik bölgeleri kullandı. Khayyami,

$$x^3 + Bx = C \qquad (2.1)$$

şeklindeki özel kübik denklemleri aşağıdaki gibi çözmüştür:

$$B = p^2 \text{ ve } C = p^2 q$$

olmak üzere, (2.1) denklemi

$$x^3 + p^2 x = p^2 q \qquad (2.2)$$

şeklinde yazılır. $x^2 = py$ denklemi ile bir parabol ve $x^2 + y^2 = qx$ denklemi ile bir çember çizilirse, (2.1) denkleminin pozitif bir çözümü bu iki eğrinin arakesitidir.

Örneğin; $x^3+4x=16$ alınırsa, burada $B=p^2$ ve $C=p^2q$ olduğundan $p=2$ ve $q=4$ bulunur. Buradan $x^2=2y$ parabolü ile $x^2+y^2=4x$, yani $(x-2)^2+y^2=4$ çemberi elde edilir. Dikkat edilirse $x=2, y=2$ ve $x=0, y=0$ her iki eğri denklemini de sağlar. Pozitif çözüm, her iki denklemin ortak çözümü olduğundan $x=2$, $x^3+4x=16$ nın çözümüdür.

Kübik denklemlerin çözümü konusunda Leonardo Pisano Fibonacci (1170-1250), matematikçileri harekete geçirmede önemli bir rol oynamış ve önemli çalışmalar yapmıştır. $x^3+2x^2+10x=20$ denklemine ondalık notasyonda, yani yaklaşık bir çözüm bulmuştur.

Batılı matematikçiler literatüründe, ilk kez Gerardi kübik denklemler için yanlış da olsa genel çözümler vermiştir:

$ax^3=bx+N$ denkleminin çözümünün, $x=\sqrt{\frac{N}{a}+\left(\frac{b}{2a}\right)^2}+2a$ olduğunu iddia etti. Dikkat edilirse, bulduğu çözüm aslında $ax^2=bx+N$ ikinci derece denkleminin çözümüdür. Çözümünü kontrol etmediği için çözüm tekniklerinin hatalı sonuçlar verdiğini kabul etmedi. Aslında, Gerardi' nin kuralları, problemleri ve hatta hatalı formülleri 1340'lardan Pacioli' nin zamanına kadar kullanılmıştı.

Scipione dal Ferro (1465-1526) nun 1500-1515 arasında ve muhtemelen 1504' te, $ax^3+bx=c$ kübik denkleminin çözümünde başarılı olduğu bilinir. dal Ferro sadece $x^3+mx=n$ şeklindeki kübik denklemlerin çözülebileceğine inandı, gerçekte bunun tüm kübik denklemlerin çözülebilmesini gerektirdiğini biliyoruz. dal Ferro' nun, $x^3+mx=n$ denkleminin çözümü şu şekildedir:

$(a-b)^3+3ab(a-b)=a^3-b^3$ olduğundan m=3ab ve n=a^3-b^3 denirse x=a-b, $x^3+mx=n$ nin bir çözümü olacaktır. a^3-b^3=n, $a^3-\left(\frac{m}{3a}\right)^3=n$ şeklinde yazılıp düzenlendiğinde ise $a^6-na^3-\frac{m^3}{27}=0$, yani a^3' e göre ikinci derece denklemi elde

edilir ve sonuç olarak; $x=\sqrt[3]{\frac{n}{2}+\sqrt{\frac{n^2}{4}+\frac{m^3}{27}}}-\sqrt[3]{\sqrt{\frac{n^2}{4}+\frac{m^3}{27}}-\frac{n}{2}}$ bulunur. dal Ferro, bu kübik denklemi çözdükten sonra, öğrencisi Antonio Fiore bu çözümü, 1526' da tam Ferro' nun ölümünden önce açıkladı. O zamana kadar dal Ferro, çalışmasını tamamen gizli tutmuştu.

1530' da bir matematik yarışmasında, Brescia' dan Tonioni da Coi isimli bir matematikçi Fiore'e meydan okudu. Fiore tarafından ileri sürülen problemler, doğal olarak kübik denklemlerdi. Da Coi bu problemleri çözmeyi başaramadı ve yardım almak için Tartaglia' ya başvurdu. Kübik denklemleri çözebildiği hakkındaki söylentileri işitmesine rağmen, Fiore Tartaglia' ya meydan okudu.

Tartaglia' nın kübik denklemleri çözme yöntemi şu şekildedir:

$x=p^{\frac{1}{3}}+q^{\frac{1}{3}}$ seçelim. O zaman $x^3=p+3p^{\frac{2}{3}}q^{\frac{1}{3}}+3p^{\frac{1}{3}}q^{\frac{2}{3}}+q=p+3(pq)^{\frac{1}{3}}\left(p^{\frac{1}{3}}+q^{\frac{1}{3}}\right)+q$

bulunur ve $x=p^{\frac{1}{3}}+q^{\frac{1}{3}}$ olduğundan, $x^3=p+3(pq)^{\frac{1}{3}}x+q$ olur. Böylece, $x^3-3(pq)^{\frac{1}{3}}x-(p+q)=0$ olur. Burada, $c=-(pq)^{1/3}$ ve d=-(p+q) denirse;

$$x^3+3cx+d=0 \qquad (2.3)$$

elde edilir. Buradan, $dp=-p^2-pq$, yani $p^2+dp-c^3=0$ bulunur ki, bu denklemin çözümü $p=\frac{-d+\sqrt{d^2+4c^3}}{2}$ dir. $q^{1/3}=-\frac{c}{p^{1/3}}$ olduğu dikkate alınırsa, (2.3) ün çözümü;

$$x=\sqrt[3]{\frac{-d+\sqrt{d^2+4c^3}}{2}}-\frac{c}{\sqrt[3]{\frac{-d+\sqrt{d^2+4c^3}}{2}}}$$

şeklinde bulunur.

Şimdi Ferro ve Tartaglia' nın metodlarını bir örnekle açıklayalım:

$x^3+9x=6$ denklemini alalım. x=a-b yi denklemde yerine yazalım. $(a-b)^3+9(a-b)=6$ ve $a^3-b^3-3ab(a-b)+9(a-b)=6$ dır. ab=3 diyelim. O

zaman $a^3 - b^3 = 6$ olur. Burada, $a^3 = p$ ve $b^3 = q$ dersek, p-q=6 ve ab=3 olduğundan, pq=27 olur. p-q=6 ise $pq - q^2 = 6q$ olacağından ve pq=27 olduğundan $q^2 + 6q - 27 = 0$ ikinci derece denklemi elde edilir. Buradan q=3, p=9 bulunur. O halde, $x^3 + 9x = 6$ denkleminin çözümü,

$$x=a-b=\sqrt[3]{p}-\sqrt[3]{q}=\sqrt[3]{9}-\sqrt[3]{3}$$

şeklinde bulunur.

Cardano, Tartaglia' nın başarısını duydu ve bulduklarını kendisiyle paylaşmasını rica etti. Bunun üzerine Tartaglia metodunu bir şiirde gizleyerek yolladı. Cardano bu şiirsel açıklamayı anlamadı ve Tartaglia' dan daha fazla yardım istedi. Sonra Cardano, cebir üzerine ilk Latin çalışmayı yaptı ve 1545' te çalışmasını "Ars Magna" isimli kitapta yayınladı. Önce, $x^3 + 6x = 20$ denkleminin çözümünü gösterdi. $x^3 + mx = n$ denkleminde, m ve n pozitif sayılar, t-u=n ve $tu = \left(\frac{m}{3}\right)^3$ olmak üzere, $x = \sqrt[3]{t} - \sqrt[3]{u}$ olduğunu iddia etti. Sadeleştirmelerden sonra ortaya çıkan ikinci derece denklemi çözerek, $t = \sqrt{\left(\frac{n}{2}\right)^2 + \left(\frac{m}{3}\right)^3} + \frac{n}{2}$ ve $u = \sqrt{\left(\frac{n}{2}\right)^2 + \left(\frac{m}{3}\right)^3} - \frac{n}{2}$ elde etti ve böylece x değerini buldu. Cardano bu metodunu geometrik olarak yorumladı.

Cardano; henüz negatif bir sayının karekökünü alamadığı için, formülünü bazı kübik denklemlere uyguladığında negatif sayıların karekökü ile karşılaşınca biraz şaşırdı. Ancak daha sonra, Raphael Bombelli (1526-1573), sanal sayılar ile ilgili tanımlamalar yaptı ve dal Ferro/Tartaglia metodunu kullanarak üçüncü derece denklemlerin çözümünü genelleştirdi.

Ars Magna' dan sonra, matematikçilerin çoğu üçüncü ve dördüncü derece denklemlerin çözümleri için farklı yöntemler ileri sürdüler. Bu matematikçiler arasında François Viéte (1540-1603), Thomas Harriot (1560-1621), René Descartes (1596-1650), Ehrenfried Walter von Tschirnhauss (1651-1708) ve Leonhard Euler (1707-1783) i sayabiliriz.

1591' de Viéte, $q^2 < p^2$ olduğunda

$$x^3 = 3px + 2q \qquad (2.4)$$

kübik denklemi için aşağıdaki çözümü önerdi:

x=kcosz

olsun. O zaman (2.4) denklemi,

$$k^3 \cos^3 z - 3pk \cos z = 2q \qquad (2.5)$$

şekline gelir. Burada k^2=4p yazılır ve $\cos 3z = 4\cos^3 z - 3\cos z$ olduğu dikkate alınırsa (2.5) eşitliğinden $kp\cos 3z = 2q$ elde edilir. Yani; $\cos 3z = \frac{2q}{kp} = \frac{2q}{p.2\sqrt{p}} = \frac{q}{p^{3/2}}$ olur. Böylece (2.4) denkleminin bir çözümü, $x = 2\sqrt{p}\cos\left(\frac{1}{3}\arccos\frac{q}{p^{3/2}}\right)$ dir. Diğer çözümler de buna bağlı olarak bulunur.

Gottfried Wilhelm von Leibnitz (1646-1695), dal Ferro' nun formüllerini doğrulamayı denedi. Cebirsel bir ispat verdi ve bu ispatı Mart 1673' te Christian Huygens (1629-1695)' a gönderdiği bir mektupla belgeledi.

Alexandre Théophile Vandermonde (1735-1796) ve Joseph-Louis Lagrange (1646-1716) birbirlerinden bağımsız olarak kübik denklemlerin çözümü için yöntemler verdiler.

3. KUADRATİK REZİDÜLER

Bu bölümde amaç, kuadratik kongrüans denklemlerinin çözümlerini bulmaktır. Bunu belirlemede en çok kullanılan yöntem bir sayının verilen bir modülde tam kare olarak ifade edilip edilemeyeceğinin belirlenmesidir. Bu da "Kuadratik Rezidüler" başlığı altında incelenir ve sayılar teorisinin en önemli konularından biridir.

3.1 Kuadratik Kongrüanslar

İkinci derece denklemlerin çözümünde olduğu gibi, ikinci derece kongrüansların çözümünde de köklerin bulunması önemlidir. a, b, c$\in$**R** veya **C** olmak üzere

$$ax^2 + bx + c = 0 \qquad (3.1)$$

denkleminin köklerini veren $x = \frac{-b \mp \sqrt{b^2 - 4ac}}{2a}$ bağıntısını ele alalım. Bu $\bar{a}, \bar{b}, \bar{c} \in \mathbf{Z}_n$ durumuna uygulanırsa $\overline{2a}$ ile bölmeyi, yani $\overline{2a}$ nın tersinin olduğunu garantilemek gerekir. O halde $\overline{2a}$ mod n de bir birim olmalıdır. Bu durumda $\frac{1}{\overline{2a}} \in \mathbf{Z}_n$ olur.

Şimdi n tek ve $\bar{a} \in \mathcal{U}_n$ olsun. O zaman $\overline{4a} \in \mathcal{U}_n$ olup (3.1) denklemi,

$$4a^2x^2 + 4abx + 4ac = 0 \qquad (3.2)$$

şekline dönüşür.

$$(2ax + b)^2 = 4a^2x^2 + 4abx + b^2$$

olduğundan (3.2) denklemi

$$(2ax + b)^2 = b^2 - 4ac$$

olur. O halde b^2-4ac nin $\mathbf{Z}_n$ deki tüm kareköklerini bulabilirsek, 2ax+b=s veya denk olarak $x=\frac{-b+s}{2a}$ olacak şekildeki tüm $x\in\mathbf{Z}_n$ çözümlerini de bulabiliriz. Normalde iki tane olan kareköker bazen yanıltıcı bir şekilde farklı sayıda olabilir. Örneğin $\mathbf{Z}_{15}$ te $\bar{1}$ ve $\bar{4}$ nin her birinin dörder tane karekökü vardır. $\bar{1}$ in kareköklerinin ∓ 1 ve ∓ 4, $\bar{4}$ nin kareköklerinin de ∓ 2 ve ∓ 7 olduğu açıktır.

3.2 Kuadratik Rezidülerin Grubu

3.2.1 Tanım: Bir $\bar{a}\in\mathcal{U}_n$ verilsin. Eğer $\bar{a}=\bar{s}^2$ olacak şekilde bir $\bar{s}\in\mathcal{U}_n$ varsa $\bar{a}$ ya mod n de bir kuadratik rezidü denilir ve bu şekildeki kuadratik rezidülerin kümesi Q_n ile gösterilir.

3.2.2 Örnek: Küçük n ler için $\mathcal{U}_n$ deki tüm sayıların kareleri alınarak Q_n belirlenebilir. Örneğin n=7 için $1^2=1, 2^2=4, 3^2\equiv 2, 4^2\equiv 2, 5^2\equiv 4, 6^2\equiv 1\ (7)$ olduğundan $Q_7=\{\bar{1},\bar{2},\bar{4}\}$ tür. n=8 için $\mathcal{U}_8=\{1,3,5,7\}$ ve $1^2=1, 3^2\equiv 1, 5^2\equiv 1, 7^2\equiv 1$ olup $Q_8=\{\bar{1}\}$ dir.

3.2.3 Yardımcı Teorem: k, n sayısını bölen farklı asalların sayısı olsun. $\bar{a}\in Q_n$ ise $\bar{t}^2=\bar{a}$ olacak şekildeki $\bar{t}\in\mathcal{U}_n$ lerin sayısı

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

şeklindedir, [1].□

3.2.4 Teorem: $|Q_n|=\varphi(n)/N$ dir.

İspat: Herhangi bir n sayısı için $\mathcal{U}_n$ nin $\varphi(n)$ tane elemanı (birim) vardır. $\bar{s}\in\mathcal{U}_n$ birimi bir $\bar{a}\in Q_n$ karesine sahiptir. 3.2.3 gereği her bir $\bar{a}\in Q_n$, $\mathcal{U}_n$ de N tane kareköke sahiptir. O halde,

$$|Q_n| = \varphi(n)/N$$

dir.

3.2.5 Örnek: n=8 ise $Q_8 = \{\bar{1}\}$, yani $|Q_8| = 1$ dir. Gerçekten, $\varphi(8)=4$ olup $N = 2^{1+1} = 2^2 = 4$ ve $|Q(8)|=4/4=1$ dir.

3.3 Legendre Sembolü

Burada verilen bir $\bar{a} \in \mathcal{U}_n$ biriminin bir kuadratik rezidü olup olmadığını belirleyeceğiz. Modun asal olması durumunda işlem kolaydır. $n = 2$ ise $Q_2 = \{\bar{1}\}$ dir ve bir kuadratik rezidüdür. O halde $n = p$ nin tek asal olması durumuyla başlayalım.

3.3.1 Tanım: p tek asal sayısı için bir a tamsayısının Legendre sembolü

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & , p \mid a \text{ ise} \\ 1 & , a \in Q_p \text{ ise} \\ -1 & , a \in Q_p \text{ değil ise} \end{cases}$$

şeklindedir.

3.3.2 Örnek: p=7 ise

$$\left(\frac{a}{7}\right) = \begin{cases} 0 & , a \equiv 0\,(7) \text{ ise} \\ 1 & , a \equiv 1, 2 \text{ veya } 4\,(7) \text{ ise} \\ -1 & , a \equiv 3, 5 \text{ veya } 6\,(7) \text{ ise} \end{cases}$$

dir.

3.3.3 Sonuç: p tek asal ve g, p modunda bir ilkel kök ise

$$\left(\frac{g^i}{p}\right) = (-1)^i$$

dir.

İspat: Hem $\left(\frac{g^i}{p}\right)$, hem de $(-1)^i$ ya $+1$ dir ya da -1 dir. $\left(\frac{g^i}{p}\right)=1$ olması için gerek ve yeter şart i nin çift sayı olmasıdır. Bu aynı zamanda $(-1)^i$ nin de $+1$ olması için gerek ve yeter şarttır.□

3.3.4 Teorem: p tek asal ise $\forall a,b\in\mathbf{Z}$ için

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

dir.

İspat: p| a veya p| b ise iki tarafta sıfırdır. O halde $a,b\in\mathcal{U}_p$ alabiliriz. p asal olduğundan $\mathcal{U}_p=\{\bar{1},\bar{2},...,\overline{p-1}\}$ dir. g ilkel kök olmak üzere $a=g^i$ ve $b=g^j$ yazabiliriz. Öyleyse $a.b=g^{i+j}$ dir. 3.3.3 gereği,

$$\left(\frac{ab}{p}\right)=(-1)^{i+j}=(-1)^i.(-1)^j=\left(\frac{a}{p}\right).\left(\frac{b}{p}\right)$$

olur.□

3.3.5 Örnek: p=17 olsun. $\left(\frac{1}{17}\right)=+1$ dir. Çünkü $\bar{1}=\bar{1}^2$ dir. Aynı zamanda $-1\equiv 4^2\ (17)$ olup $\left(\frac{-1}{17}\right)=+1$ dir. O halde $\forall\bar{a}\in\mathcal{U}_p$ için $\left(\frac{a}{17}\right)=\left(\frac{-a}{17}\right)$ dir, yani $\bar{a}\in Q_{17}\Leftrightarrow\overline{-a}\in Q_{17}$ dir. Mesela $13\in Q_{17}\Leftrightarrow -13\equiv 2^2\in Q_{17}$ dir.

3.3.6 Uyarı: Genelde $\left(\frac{-a}{p}\right)$ ile $-\left(\frac{a}{p}\right)$ farklı olabilir. Örneğin; $\left(\frac{-1}{17}\right)=+1$ dir, ancak $-\left(\frac{1}{17}\right)=-1$ dir.

3.3.7 Sonuç: $a_1,a_2,...,a_k\in\mathbf{Z}$ için

$$\left(\frac{a_1.a_2...a_k}{p}\right)=\left(\frac{a_1}{p}\right)...\left(\frac{a_k}{p}\right)$$

dir.

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

İspat: Legendre sembolünün tanımından görülür.□

3.3.9 Teorem (Euler Kriteri): p tek asal sayı ise $\forall a \in \mathbf{Z}$ için

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

dir.

İspat: $p \nmid a$ ise aşikardır. O halde $\bar{a} \in \mathcal{U}_p$ olsun. O halde g ilkel kök olmak üzere $a = g^i$ yazılabilir. $h = g^{(p-1)/2}$ tanımlayalım. $h^2 = g^{p-1} \equiv 1\,(p)$ olur. O zaman $h \equiv \mp 1\,(p)$ dir. g ilkel kök olup, mertebesi $\varphi(p) = p\text{-}1$ dir. $p-1 > \frac{p-1}{2}$ ve p-1 en küçük mertebe olduğu için $g^{(p-1)/2} \equiv 1\ (p)$ olamaz. O halde $h \equiv 1\ (p)$ olamaz, yani $h \equiv -1\ (p)$ dir. O halde,

$$a^{(p-1)/2} = (g^i)^{(p-1)/2} = \left(g^{(p-1)/2}\right)^i = h^i \equiv (-1)^i = \left(\frac{g^i}{p}\right) = \left(\frac{a}{p}\right)\ (p)$$

olur.□

3.3.10 Sonuç: p tek asal olsun. $-1 \in Q_p$ olması için gerek ve yeter şart $p \equiv 1\ (4)$ olmasıdır.

İspat: Euler Kriterinde $a = -1$ alınırsa

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

olup ancak $\frac{p-1}{2}$ çift iken $\left(\frac{-1}{p}\right) = +1$ olur. Bu ise $k \in \mathbf{Z}$ olmak üzere $\frac{p-1}{2} = 2k$ iken, yani $p \equiv 1(4)$ iken doğrudur.□

3.3.11 Uyarı: $-1 \in Q_p$ oluşu $\forall a \in \mathbf{Z}$ için $\left(\frac{-a}{p}\right) = \left(\frac{a}{p}\right)$ oluşunu gerektirir.

3.3.12 Teorem: p modundaki kuadratik rezidülerin sayısı, kuadratik rezidü olmayanların sayısına eşittir.

İspat: a bir kuadratik rezidü ise Legendre sembolünün tanımı gereği $\left(\frac{a}{p}\right)=1$ dir. O halde Euler Kriteri gereği $a^{(p-1).2} \equiv 1(p)$ yazabiliriz. Bu denkliğin Polinomlar için Lagrange Teoremi gereği $\frac{p-1}{2}$ tane çözümü vardır. Yani $\frac{p-1}{2}$ tane kuadratik rezidü vardır. Dolayısıyla kuadratik rezidü olmayanların sayısı $p-1-\frac{p-1}{2}=\frac{p-1}{2}$ dir.□

3.3.13 Teorem: İki kuadratik rezidünün ve iki kuadratik rezidü olmayan elemanın çarpımı bir kuadratik rezidü, bir kuadratik rezidü ile kuadratik rezidü olmayanın çarpımı ise bir kuadratik rezidü olmayan elemandır.

İspat: Legendre sembolünün tanımından görülür.□

3.3.14 Uyarı: mod p deki kalan sınıfları $\bar{0},\bar{1},...,\overline{p-1}$ olup $\mathcal{U}_p=\left\{\bar{1},\bar{2},...,\overline{p-1}\right\}$ dir. $\mathcal{U}_p$ yi bazen iki altkümeye ayırmak yararlı olacaktır:

$$P=\left\{1,2,...,\frac{p-1}{2}\right\} \text{ ve } N=\left\{-1,-2,...,-\frac{p-1}{2}\right\}$$

olsun.

Örneğin; p=19 ise $P=\{1,2,...,9\}$ ve $N=\{-1,-2,...,-9\}$ dur. $\forall a\in\mathcal{U}_p$ için $aP=\{ax|x\in P\}=\left\{a,2a,...,\frac{p-1}{2}a\right\}\subset\mathcal{U}_p$ tanımlayalım. Örneğin; N=-1.P dir. Bu tanımlamadan faydalanarak kuadratik rezidüler için Gauss tarafından verilmiş olan bir testi verebiliriz.

3.3.15 Teorem: p tek asal sayı, $\bar{a}\in\mathcal{U}_p$ olsun. $\mu=|aP\cap N|$ olmak üzere

$$\left(\frac{a}{p}\right)=(-1)^{\mu}$$

dür, [1].□

3.3.16 Örnek: p=19, $\bar{a}=\overline{11}$ olsun. $11P=\{-8,3,-5,6,-2,9,1,-7,4\}$ olup –8, -5, -2 ve $-7\in N$ dir. O zaman $\mu=4$ tür. Dolayısıyla $\left(\frac{11}{19}\right)=(-1)^4=1$ dir. Gerçekten de $11\equiv 7^2\ (19)$ dur.

3.3.17 Sonuç: p tek asal ise

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

dir. Denk olarak, $2\in Q_p$ olması için gerek ve yeter şart $p\equiv\mp 1\ (8)$ olmasıdır.

İspat: 3.3.15 de $a=2$ alınırsa $aP=2P=\{2,4,6,\ldots,p-1\}$ olur. İlk olarak $p\equiv 1\ (4)$ olduğunu varsayalım. Bu durumda, $2P=\left\{2,4,6,\ldots,\frac{p-1}{2},\frac{p+3}{2},\ldots,p-1\right\}$ olur. Buradaki $\frac{p-1}{2}$ tane elemanın yarısı, yani $\frac{p-1}{4}$ tanesi P de, diğer $\frac{p-1}{4}$ tanesi de N dedir. Öyleyse $|2P\cap N|=\frac{p-1}{4}$ tür. 3.3.15 gereği;

$$\left(\frac{2}{p}\right)=(-1)^{(p-1)/4}=\left((-1)^{(p-1)/4}\right)^{(p+1)/2}\quad\left(\frac{p+1}{2}\text{ tek sayıdır}\right)$$

$$=(-1)^{(p^2-1)/8}\text{ olur.}$$

İkinci olarak $p\equiv 3\equiv -1\ (4)$ olsun. Bu durumda,

$$2P=\left\{2,4,6,\ldots,\frac{p-3}{2},\frac{p+1}{2},\ldots,p-1\right\}$$

olup ilk $\frac{p-3}{4}$ eleman 2,4, ... , $\frac{p-3}{2}\in P$ dir ve geriye kalan $\frac{p+1}{4}$ eleman $\frac{p+1}{2}$, ... , $p-1\in N$ dir. Böylece $\mu=\frac{p+1}{4}$ olur ve buradan,

$$\left(\frac{2}{p}\right)=(-1)^{(p+1)/4}=\left((-1)^{(p+1)/4}\right)^{(p-1)/2}\quad\left(\frac{p-1}{2}\text{ tek sayıdır}\right)$$

$$=(-1)^{(p^2-1)/8}$$

bulunur.

Teoremin ikinci kısmı için ise, $2 \in Q_p$ olsun. O zaman, $\left(\frac{2}{p}\right) = 1$ olur. Bu ise birinci kısımdan dolayı, $\frac{p^2-1}{8}$ in çift olmasını gerektirir. O halde 16, p^2-1'i, yani (p-1).(p+1) i bölmelidir. O halde 8, ya p-1'i ya da p+1'i böler. Yani $p \equiv \mp 1$ (8) olur. Tersi de benzer şekilde görülür.□

3.3.18 Örnek: mod 7, 17, 23, 31, ... için 2 bir kuadratik rezidüdür. 3, 5, 11, 13, 19, ... modlarında ise 2 kuadratik rezidü değildir.

3.4 Kuadratik İndirgeme Kuralı

Bir a tamsayısının bir p modunda kuadratik rezidü olup olmadığını anlayabilmek için $\left(\frac{a}{p}\right)$ sayısını hesaplamamız gerekir. Bunu da tüm a tamsayıları için bulmak yerine, yukarıdaki sonuçlar gereği sadece üç özel durumda yani (-1/p), (2/p) ve q tek asal sayı olmak üzere (q/p) durumlarında bulmak yeterli olacaktır.

3.4.1 Teorem (Gauss'un Kuadratik İndirgeme Kuralı): p ve q farklı tek asal sayılar ise

$$\left(\frac{q}{p}\right) = \begin{cases} -\left(\frac{p}{q}\right) & ; p \equiv q \equiv 3\,(4) \text{ ise} \\ \left(\frac{p}{q}\right) & ; \text{aksi halde} \end{cases}$$

dir.

Denk olarak;

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)\cdot 4}$$

olarak da bilinir, [1].□

3.4.2 Örnek: i) $\left(\frac{15}{7}\right)=\left(\frac{3}{7}\right).\left(\frac{5}{7}\right)=(-1).(-1)=+1$ dir.

ii) $\left(\frac{41}{73}\right)=\left(\frac{73}{41}\right).(-1)^{(73-1)(41-1)\cdot 4}$

$$=\left(\frac{32}{41}\right)(-1)^{72.10}=\left(\frac{2}{41}\right)^{5}=\left(\frac{2}{41}\right)=+1$$

(41≡1(8) olduğundan)

Gerçekten, $41\equiv 625=25^2$ (73) tür.

iii) $\left(\frac{83}{103}\right)=\left(\frac{103}{83}\right).(-1)^{(103-1)(83-1)\cdot 4}$

$$=\left(\frac{103}{83}\right).(-1)^{51.41}=(-1).\left(\frac{20}{83}\right)=(-1).\left(\frac{4}{83}\right).\left(\frac{5}{83}\right)$$

$$=(-1).\left(\frac{2}{83}\right)^{2}\left(\frac{83}{5}\right)(-1)^{(83-1)(5-1)/4}$$

$$=(-1).1.\left(\frac{83}{5}\right)$$

$$=(-1).\left(\frac{3}{5}\right)=(-1).\left(\frac{5}{3}\right)(-1)^{(5-1)(3-1)/4}$$

$$=(-1).\left(\frac{2}{3}\right)=(-1).(-1)^{\frac{9-1}{8}}=1$$

dir.

4. KÜBİK REZİDÜLER

4.1 Giriş

3. Bölümde $x^2 \equiv a\,(p)$ denkliğinin hangi p asalları için çözülebileceğinden bahsedildi. Bu bölümde $x^3 \equiv a\,(p)$ denkliğinin çözülebilme koşulları incelenecektir.

Gauss meşhur "Theorie der biquadratischen Reste I, II" makalelerinin girişinde, kuadratik rezidüler teorisinde yapılacak daha fazla hiçbir şeyin kalmadığını, ancak kübik ve dördüncü derece rezidüler teorisinin çok daha zor olduğunu iddia eder.

Bu bölümde, $\omega = (-1+\sqrt{-3})/2$ birimin 3.dereceden kökü ve $\mathbf{Z}$ tamsayılar kümesi olmak üzere, $\mathbf{Z}[\omega]=\{a+b\omega \mid a,b \in \mathbf{Z}\}$ halkasında çalışacağız ve $\mathbf{Z}[\omega]$ yı D ile göstereceğiz. $\alpha = a+b\omega$ sayılarına Eisenstein tamsayıları denir ve Kübik İndirgeme konusundaki çalışmalarda Eisenstein tarafından kullanılmıştır.

4.1.1 Tanım: $\alpha=a+b\omega \in D$ ise α nın normu $\alpha\,\bar{\alpha}$ şeklinde tanımlanır ve $N\alpha$ ile gösterilir.

4.1.2 Teorem: $\alpha=a+b\omega \in D$ nın normu $N\alpha=a^2-ab+b^2$ dir.

İspat: $\alpha=a+b\omega \in D$ olsun. O zaman $N\alpha=\alpha\,\bar{\alpha}$ olduğunu biliyoruz.

$$\begin{aligned} N\alpha = \alpha\,\bar{\alpha} &= (a+b\omega)\overline{(a+b\omega)} \\ &= (a+b\omega)(a+b\,\bar{\omega}) \\ &= a^2+ab\bar{\omega}+ab\omega+b^2\omega\bar{\omega} \\ &= a^2+ab(\bar{\omega}+\omega)+b^2.1 \\ &= a^2-ab+b^2 \end{aligned}$$

dir (Burada $\omega = \frac{-1+\sqrt{-3}}{2}$ olduğundan, $\omega\bar{\omega} = |\omega|^2 = 1$ dir ve $\bar{\omega}+\omega = 2\mathrm{Re}\,\omega$ olacağından $\bar{\omega}+\omega = 2.\frac{-1}{2} = -1$ olur.).

4.1.3 Sonuç: $N\alpha$ pozitif bir tamsayıdır.

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

İspat : $N\alpha=1$ olsun. $N\alpha=\alpha\bar{\alpha}=1$ dir. $\bar{\alpha} \in D$ olduğundan α bir birimdir.

$\alpha \in D$ birim ise $\alpha\beta=1$ olacak şekilde bir $\beta \in D$ vardır. Böylece $N(\alpha\beta)=1$ ve buradan

$$N(\alpha\beta)=N\alpha\, N\beta=1$$

olur ki $N\alpha$ ve $N\beta$ pozitif tamsayılar olduğundan $N\alpha=1$ dir.

$\alpha=a+b\omega$ bir birim olsun. O zaman $N\alpha=1$ dir. Yani

$$a^2 - ab + b^2 = 1 \qquad (4.1)$$

dir. (4.1) denklemini 4 ile çarparsak

$$4a^2 - 4ab + 4b^2 = 4$$

yani,

$$(2a-b)^2 + 3b^2 = 4$$

elde edilir. Burada iki durum söz konusudur.

i) $(2a-b) = \mp 1$ ve $b = \mp 1$

ii) $(2a-b) = \mp 2$ ve $b = 0$

Önce (i) durumunu ele alalım:

a) $2a-b=1$ ve $b=1$ ise $a=1$ bulunur ve $\alpha = 1+\omega$ olur.

b) $2a-b=1$ ve $b=-1$ ise $a=0$ bulunur ve $\alpha = -\omega$ olur.

c) $2a-b=-1$ ve $b=1$ ise $a=0$ bulunur ve $\alpha = \omega$ olur.

d) $2a-b=-1$ ve $b=-1$ ise $a=-1$ bulunur ve $\alpha = -1-\omega$ olur.

$\omega^3 = 1$ olduğundan $\omega^3 - 1 = 0$ ve $\omega^3 - 1 = (\omega-1)(\omega^2+\omega+1) = 0$ olacağından $\omega^2+\omega+1=0$ dır. Böylece, $\omega^2 = -1-\omega$ dır. Yani (a) durumunda $\alpha = -\omega^2$ ve (d) durumunda da $\alpha = \omega^2$ olur.

Şimdi (ii) durumunu inceleyelim. Bu durumda da,

$2a-b=2$ ve $b=0$ ise $a=1$ ve $\alpha=1$ bulunur.

$2a-b=-2$ ve $b=0$ ise $a=-1$ ve $\alpha=-1$ bulunur.□

4.1.5 Tanım: $u\in D$ bir birim olmak üzere $\alpha=\beta u$ olacak şekildeki α ve β sayılarına denktir (associate) denir ve $\alpha\sim\beta$ ile gösterilir.

4.1.6 Teorem: $p\equiv 1(3)$ bir asal sayı olsun. $\omega=\dfrac{-1+\sqrt{-3}}{2}$ sayısı $\mathbf{Z}_p$ nin bir elemanıdır.

İspat: Önce $\sqrt{-3}\in\mathbf{Z}_p$ olduğunu gösterelim. Yani $-3\equiv k^2(p)$ olacak şekilde bir $k>0$ tamsayısının varlığını göstermek istiyoruz. Bunun için $\left(\dfrac{-3}{p}\right)=+1$ olduğunu göstermemiz gerekir. Burada $\left(\dfrac{\bullet}{\bullet}\right)$ Legendre sembolünü göstermektedir.

$$\left(\frac{-3}{p}\right)=\left(\frac{-1}{p}\right).\left(\frac{3}{p}\right)$$

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

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

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

Burada $p>2$ asal olup $p-1$ çifttir ve ayrıca $p\equiv 1$ (3) olduğundan $\left(\dfrac{p}{3}\right)=\left(\dfrac{1}{3}\right)=+1$ dir.

Böylece $\left(\dfrac{-3}{p}\right)=1$ olur.

İkinci olarak, $(2,p)=1$ olduğunu ve bu durumda 2 nin mod p de çarpmaya göre bir t tersine sahip olduğunu biliyoruz. Öyleyse $\sqrt{-3}\in\mathbf{Z}_p$ olduğundan $-1+\sqrt{-3}\in\mathbf{Z}_p$ ve böylece $\dfrac{1}{2}(-1+\sqrt{-3})\equiv t.(-1+\sqrt{-3})\in\mathbf{Z}_p$ olur.□

4.1.7 Sonuç: $p \equiv 1\ (3)$ asal iken ω^2 elemanı da $\mathbf{Z}_p$ nin bir elemanıdır.

4.1.8 Örnek: 7 modunda $\omega = \frac{-1+\sqrt{-3}}{2} \equiv \frac{-1+\sqrt{4}}{2} = \frac{1}{2} \equiv \frac{8}{2} \equiv 4\ (7)$.olur.

$\omega^2 = -1-\omega$ olduğundan $\omega^2 \equiv -5 \equiv 2\ (7)$ yani $\omega, \omega^2 \in \mathbf{Z}_7$ dir.

13 modunda, $\omega = \frac{-1+\sqrt{-3}}{2} \equiv \frac{-1+\sqrt{36}}{2} \equiv \frac{18}{2} \equiv 9\,(13)$ ve $\omega^2 \equiv 3\ (13)$ olup $\omega, \omega^2 \in \mathbf{Z}_{13}$ bulunur.

4.1.9 Uyarı: 3 modunda 1' e denk olmayan asallar için ω, $\omega^2 \in \mathbf{Z}_p$ olmaz. Örneğin, p=5 için $\sqrt{-3} \in \mathbf{Z}_5$ değildir. Gerçekten de $-3+5k$ sayıları 2 ve 7 ile biteceğinden bir tam kare olamaz. Ancak bu bir kısıtlama değildir. Çünkü ilerde göreceğimiz gibi D de normu 3 modunda 2 ye denk olan kompleks asal yoktur.

4.2 D deki Asallar

4.2.1 Tanım: $\pi = a+b\omega \in D$ olsun. $c+d\omega$ ve $e+f\omega$ birimden farklı olmak üzere $\pi = (c+d\omega)(e+f\omega)$ olacak şekilde c, d, e, f tamsayıları bulunamıyorsa π ye D de asaldır denir. Değilse π ye D de birleşik sayı denir.

İlk olarak **Z** deki rasyonel asallardan hangileri D de asaldır sorusunun cevabını arayacağız.

4.2.2 Teorem: p rasyonel ise $Np = p^2$ dir.

İspat: Tanımdan görülür.□

4.2.3 Teorem: p rasyonel asalı D de asal değilse birimden farklı tam 2 çarpanı vardır. Bu çarpanlardan her birinin normu p dir.

İspat: p bir rasyonel asal olup D de asal değilse en az iki tane çarpanı vardır. Bu çarpanlara $a_1, a_2, \ldots, a_n$ dersek

$$Np = Na_1.Na_2. \ldots .Na_n$$

ve

$$Np = p^2$$

olduğundan

$$p^2 = Na_1.Na_2. \ldots .Na_n$$

elde edilir. O halde sağdaki sayılardan sadece biri p^2 diğerleri 1, ya da ikisi p, diğerleri 1 olmak zorundadır. İlk durumda normu 1 olmayan (yani birimden farklı) sadece bir çarpan olduğundan, p nin D de asal olduğu sonucu çıkar, ki bu bir çelişkidir. O halde iki çarpan olmalıdır ve bu çarpanların normu p dir.□

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

İspat: $p \equiv 1(3)$ rasyonel asal ise, $p \equiv 1(6)$ yazabiliriz. 6 modunda 1 e denk olan asalların ise $p = a^2 - ab + b^2$ şeklinde olduğunu biliyoruz.

$$\begin{aligned} p &= a^2 - ab + b^2 \\ &= a^2 - ab + b^2(-\omega + \omega + 1) \\ &= a^2 - ab - \omega b^2 + \omega b^2 + b^2 \\ &= a^2 - ab - \omega b^2 + b^2(1 + \omega) \\ &= a^2 - ab - \omega b^2 - b^2\omega^2 \\ &= a^2 - ab - \omega b^2 - b^2\omega^2 + ab\omega - ab\omega \\ &= (a + b\omega)(a - b - b\omega) \end{aligned}$$

yazılabilir. Burada $c = a - b$ ve $d = -b$ denirse $p = (a + b\omega).(c + d\omega)$ olur. Dikkat edilirse $N(a+b\omega) = N(c+d\omega) = a^2 - ab + b^2 = p$ olur. Bu nedenle $a+b\omega$ ve $c+d\omega$ birim değildir. O halde p D de asal değildir.□

4.2.5 Uyarı: $p=(a+b\omega)(c+d\omega)$ yazılabiliyorsa,

$$Np = p^2 = N(a + b\omega).N(c + d\omega)$$

dır. 4.2.3 Teorem gereği,

$$N(a + b\omega) = p \text{ ve } N(c + d\omega) = p$$

olmak zorundadır.

$$N(a + b\omega) = a^2 - ab + b^2 = p$$

olduğundan c+dω nın normu da a^2-ab+b^2 olmalıdır. Bu koşulu sağladığı için 4.2.4 Teoremde $c=a-b$ ve $d=-b$ alabiliriz. p nin başka şekillerde de çarpanlara ayrılabileceği açıktır.□

Son olarak $p=3$ ise,

$$3=(2+\omega)(1-\omega)$$

yazılabilir. O halde 3, D de asal değildir. Tüm bunların sonucu olarak, aşağıdaki teorem elde edilir.

4.2.6 Teorem: p rasyonel asal sayı olsun. p nin D de asal olması için gerek ve yeter şart $p\equiv 2\ (3)$ olmasıdır.

İspat: p rasyonel asalı D de de asal olsun ve $p\equiv 2\ (3)$ olmasın. O zaman ya $p\equiv 1\ (3)$ ya da $p=3$ tür. Ancak bu iki durumda da p nin D de asal olamayacağını göstermiştik. O halde bu p nin D de asal oluşu ile çelişir. Yani $p\equiv 2\ (3)$ tür.

$p\equiv 2\ (3)$ olsun. O zaman $p\equiv 2,5\ (6)$ olur. Tersine p nin D de asal olmadığın varsayalım.

$$p=(a+b\omega)(c+d\omega)$$

olacak şekilde D nin birimden farklı $a+b\omega$, $c+d\omega$ elemanları vardır.

$$p^2=Np=N(a+b\omega).N(c+d\omega)$$

olacağından

$$N(a+b\omega)=N(c+d\omega)=p$$

yani $a^2-ab+b^2=c^2-cd+d^2=p$ olmalıdır. Halbuki p asal olup a^2-ab+b^2 şeklinde ifade edilebilen tüm asallar 6 modunda bire denk olduğundan bu $p\equiv 2\ (3)$ ile çelişir. O halde p D de asaldır.□

Böylece, D deki rasyonel asalları belirlemiş olduk. Şimdi de, D deki kompleks asalları belirleyelim.

Burada $\pi=a+b\omega\in D$, $b\neq 0$ olacaktır. İlk olarak π nin normu 3 olsun. Yani

$$a^2-ab+b^2=3$$

olsun. O halde,

$$4a^2-4ab+4b^2=12$$

$$(2a-b)^2+3b^2=12 \qquad (4.2)$$

olur.

(4.2) denkleminin, tüm tamsayı çözümleri bulunduğunda, bu özellikteki tüm π sayılarının $1-\omega$, $-1+\omega$, $1+2\omega$, $-1-2\omega$, $2+\omega$ ve $-2-\omega$ olduğu kolayca hesaplanabilir. Bunlar aslında $1-\omega$ nin (veya herhangi birinin) denkleridir.

4.2.7 Teorem: Normu 3 olan tüm sayılar D de asaldır.

İspat: $1-\omega$ nin D de asal olduğunu gösterirsek diğer 5 eleman da $1-\omega$ nın birimle çarpımı olduğundan asal olur.

Tersine $1-\omega$ D de asal olmasın. O zaman,

$$1-\omega=(a+b\omega).(c+d\omega)$$

şeklinde birimden farklı iki elemanın çarpımı olarak yazılabilir. Buradan,

$$N(1-\omega)=N(a+b\omega).N(c+d\omega)$$

$$3=N(a+b\omega).N(c+d\omega)$$

elde edilir. 4.1.3 Sonuç gereği sağdaki çarpanlar birer pozitif tamsayı olduğundan biri 1 olmalıdır. Yani karşılık gelen eleman D de birimdir. Bu ise $a+b\omega$ ve $c+d\omega$ nın birimden farklı oluşu ile çelişir. Yani $1-\omega$ D de asaldır. O halde normu 3 olan tüm elemanlar D de asaldır.□

Şimdi 3 modunda normu 2 olan sayıların asallığını inceleyelim:

4.2.8 Teorem: D de normu $N\pi\equiv 2\ (3)$ olan hiçbir $\pi=a+b\omega\in D$ asalı yoktur.

İspat: $a\equiv 0\ (3)$ ve $b\equiv 1\ (3)$; $a\equiv 1\ (3)$ ve $b\equiv 0\ (3)$; $a\equiv b\equiv 1\ (3)$; $a\equiv b\equiv 2\ (3)$; $a\equiv 2\ (3)$ ve $b\equiv 0\ (3)$; $a\equiv 0\ (3)$ ve $b\equiv 2\ (3)$ durumlarında, $N\pi\equiv 1\ (3)$ olmaktadır. Ayrıca $a\equiv b\equiv 0(3)$; $a\equiv 2\ (3)$ ve $b\equiv 1\ (3)$ ve son olarak, $a\equiv 1\ (3)$ ve $b\equiv 2\ (3)$ durumlarında da $N\pi\equiv 0\ (3)$ olduğundan mod 3 te mümkün olan tüm dokuz durumda da $N\pi\equiv 2\ (3)$ elde edilemez.□

4.2.9 Teorem: $k > 1$ olsun. D de normu $3k$ olan hiçbir asal yoktur.

İspat: 4.2.8 Teorem gereği, $\pi=a+b\omega$ nın normu 3 modunda sıfıra denk ise üç ihtimal vardır :

i) $a \equiv 0 \equiv b$ (3) : Bu durumda $\pi = a+b\omega$, 3 ün katı olacağından asal değildir.

ii) $a \equiv 2$ (3), $b \equiv 1$ (3) : Burada $a=3k+2$, $b=3m+1$, $k, m \in Z$ alınırsa

$$N(a+b\omega) = 3[3k^2+3k-3km+3m^2+1]$$

olur. D de normu 3 olan elemanların varlığını biliyoruz (Aynı zamanda bu 6 eleman asaldır). Göstermemiz gereken D de normu, $3k^2+3k-3km+3m^2+1$ olan bir elemanın var olduğudur. D de normu 6 modunda 1 e denk olan elemanların mevcut olduğunu biliyoruz. O halde $3(k^2+k-km+m^2)+1$ deki $k^2+k-km+m^2$ ifadesinin çift olduğunu gösterirsek, $a+b\omega$ yı normu 3 ve normu 6 modunda 1 e denk olan iki elemanın çarpımı olarak yazabilmiş oluruz, ki bu $a+b\omega$ nın asal olmadığını gösterir.

a) k ve m tek ise

b) k ve m çift ise

c) k tek ve m çift ise

basit bir işlem ile $k^2+k-km+m^2$ nin çift olduğu görülür.

d) k çift ve m tek ise $a=3k+2$ ve $b=3m+1$ çift olacağından $2 \mid \pi$ olup π asal olamaz.

iii) $a \equiv 1$ (3), $b \equiv 2$ (3) durumu da ii) ye benzer şekilde gösterilir.

O halde D de normu 3 ün katı olan hiçbir asal sayı yoktur (normu 3 olanlar hariç).□

4.2.10 Teorem: p rasyonel asal ve $N\pi = p \equiv 1$ (3) ise π D de asaldır.

İspat: Tersine π D de asal olmasın. O halde $a+b\omega$, $c+d\omega$ D de birimden farklı elemanlar olmak üzere $\pi = (a+b\omega)(c+d\omega)$ yazılabilir. Böylece

$$p = N\pi = N(a+b\omega).N(c+d\omega)$$

olup $N(a+b\omega) = 1$ veya $N(c+d\omega) = 1$ olmalıdır. Bu ise $a+b\omega$ ve $c+d\omega$ nın birimden farklı oluşu ile çelişir. Üstelik $N\pi \equiv 1$ (3)tür. Gerçekten $\pi = (a+b\omega)(c+d\omega)$ daki $a+b\omega$ nın birim olduğunu varsayalım ($c+d\omega$ için de aynı ispat yapılabilir). O halde $p=N\pi=N(c+d\omega)$ olacağından $c+d\omega$ normu 6 modunda 1' e denk olan bir sayıdır. □

O halde D de üç tip asal olduğu açıktır:

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) şeklindeki tüm rasyonel asallar

ve

3) $\pi = 1-\omega$ nın denkleri

D de asaldır.

4.2.11 Tanım: a) 1) deki asallardan $a\equiv 2$ (3) ve $b\equiv 0$ (3) olanlarla sıkça karşılacağız. $b=0$ özel halinde ise 2) deki rasyonel asallar elde edilir. Bu iki tür asala 1.tip asallar (primary primes) denir.

b) 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)

şeklindedir. Bunlara da 2.tip asallar (secondary primes) diyeceğiz.

c) $1-\omega$ nın denklerine de 3.tip asallar diyeceğiz.

4.2.12 Uyarı: **Z** deki bazı asalların D de asal olmadıklarına dikkat edilmelidir. Örneğin

$$7=(3+\omega)(2-\omega)$$

ve

$$19=(5+3\omega)(2-3\omega)$$

olup 7 ve 19, D de asal değildir. Bunlar 3 modunda bire denk olan rasyonel asallardır.

4.2.13 Örnek: a) Normu 7 olan $2+3\omega$, normu 13 olan $-1+3\omega$ ve normu 19 olan $5+3\omega$, 1.tip asallardır. Aynı zamanda 2, 5, 11, 17, ... gibi rasyonel asallarda D de 1.tip asallardır.

b) Normu 7 olan $1+3\omega$, normu 13 olan $3+4\omega$ ve normu 19 olan $2+5\omega$, 2.tip asallara örnektir.

c) 3. tip asallar toplam 6 tane olup $1-\omega$, $-1+\omega$, $1+2\omega$, $-1-2\omega$, $2+\omega$ ve $-2-\omega$ dir.

D deki sıfır veya birim olmayan her bir elemanın D deki asalların çarpımı olarak bir tek şekilde ifade edilebileceği bilinmektedir. Dolayısıyla D bir U.F.D dir.

4.2.14 Teorem: π, D de asal ise p rasyonel asal olmak üzere $N\pi = p$ veya $N\pi = p^2$ dir.

İspat: $N\pi = n > 1$ denilirse $\pi\bar{\pi} = n$ yazabiliriz. n rasyonel asal sayıların bir çarpımıdır. Böylece bir p rasyonel asalı için $\pi \mid p$ olur ve $\gamma \in D$ olmak üzere $p = \pi\gamma$ yazabiliriz. O halde $N(\pi\gamma) = Np$ ve buradan $N\pi\, N\gamma = p^2$ olur. Böylece ya $N\pi = p^2$ ya da $N\pi = p$ dir.□

4.2.15 Sonuç: 1) π, 1. tip asal ise, π kompleks asal iken $N\pi = p \equiv 1$ (3), π rasyonel asal iken $N\pi = p^2 \equiv 1$ (3) olacak şekilde bir p rasyonel asalı mevcuttur.

2) π, 2. tip asal ise $N\pi = p \equiv 1$ (3) olacak şekilde bir p rasyonel asalı mevcuttur.

3) π, 3. tip asal ise $N\pi = 3$ olup asaldır.

4.2.16 Teorem: p rasyonel asal ve $\pi \in D$ olmak üzere $N\pi = p$ ise π, D de asaldır. Yani normu rasyonel asal olan her eleman D de asaldır.

İspat: π nin D de asal olmadığını varsayalım. O halde, $N\alpha$, $N\beta > 1$ olmak üzere $\pi = \alpha\beta$ yazabiliriz. Buradan $p = N\pi = N\alpha.N\beta$ olur. Ancak p, **Z** de asal olduğundan bu doğru değildir. O halde π, D de asaldır.□

Bu teoremin tersi doğru değildir. Çünkü örneğin $a = 0$, $b \equiv 2$ (3) şeklindeki $\pi = a + b\omega$ elemanları D de 2.tip asal olup $N\pi = b^2$ bir rasyonel asal değildir. Yani D de normu asal olmayan asallar da vardır. (Hatta bunların normu 4.2.14 gereği p rasyonel asal olmak üzere p^2 dir.)

4.2.17 Teorem: $\pi \in D$ asal ise onun denkleri de D de asaldır ve $N\pi = p$ ise π nin denklerinin normları da p ye eşittir.

İspat: $\pi = a + b\omega$ olsun. π asal ise $N\pi = a^2 - ab + b^2 = p$ rasyonel asaldır.

i) $1.\pi$ için $N(1.\pi) = N(1).N(\pi) = 1.p = p$ dir.

ii) $-1.\pi$ için $N(-1.\pi) = N(-1).N(\pi) = 1.p = p$ dir.

iii) $\omega.\pi$ için $N(\omega.\pi) = N(\omega).N(\pi)$ dir.

$$\omega = \frac{-1+\sqrt{-3}}{2} \text{ ve } N\omega = \omega.\bar{\omega} = 1 \text{ olduğundan, } N(\omega.\pi) = 1.p = p \text{ olur.}$$

iv) $-\omega.\pi$ için $N(-\omega.\pi) = N(-\omega).N(\pi) = p$ dir.

v) $\omega^2\pi$ için $N(\omega^2.\pi)=N(\omega^2).N(\pi)$ dir ve $\omega^2=-1-\omega=\frac{1-\sqrt{-3}}{2}$ olduğundan

$N(\omega^2)=1$ olur ve $N(\omega^2.\pi)=p$ dir.

vi) $-\omega^2\pi$ için $N(-\omega^2.\pi)=N(-\omega^2).N(\pi)=p$ olur.

i), ii), iii), ,iv), v), vi) gereği D deki bir π asalının denkleri de D de asaldır.□

Şimdi $p\equiv 1$ (3) rasyonel asal ve $N\pi=p$ olmak üzere $\pi=a+b\omega$ şeklindeki asalları belirleyeceğiz.

$p\equiv 1$ (3) rasyonel asalları ile çalışacağımızdan, $p\equiv 1$ (3) yerine $p\equiv 1$ (6) alarak, asal olmayan sayıların bir kısmını elemiş olacağız.

4.2.18 Teorem: $p\equiv 1$ (6) rasyonel asal olsun. Eğer p-1 sayısı ardışık iki sayının çarpımı olarak yazılabiliyorsa, yani $p-1=6k=n(n+1)$ ise o zaman $\pi=n+(n+1)\omega$ ve $\lambda=1+(n+1)\omega$ nın denkleri D de asaldır.

İspat: $p\equiv 1$ (6) **Z** de asal ve $p-1=6k=n(n+1)$ olsun. Bu durumda $p=n^2+n+1$ dir. $N\pi=n^2-n(n+1)+(n+1)^2=n^2+n+1=p$ ve p rasyonel asal olduğundan π, D de asaldır. 4.2.17 Teorem gereği π nin denkleri de D de asaldır.

$N\lambda=1^2=1.(n+1)+(n+1)^2=n^2+n+1=p$ ve yine p rasyonel asal olduğundan λ ve 4.2.17 Teorem gereği denkleri de D de asaldır.

4.2.19 Teorem: $p\equiv 1$ (6) rasyonel asal olsun. Eğer p-1 ardışık iki sayının çarpımı değil, fakat $\frac{p-1}{3}$ ardışık iki sayının çarpımı ise, yani $n>0$ olmak üzere $\frac{p-1}{3}=n(n+1)$ ise $m=n+1$ için, $\pi=n+(m+n)\omega$ ve $\lambda=m+(m+n)\omega$ nın denkleri de D de asaldır.

İspat: $p\equiv 1$ (6) rasyonel asal olsun. $\frac{p-1}{3}=n(n+1)$ olduğundan $p=3n^2+3n+1$ dir.

$\pi=n+(m+n)\omega$ olduğunda

$N\pi=n^2-(m+n)n+(m+n)^2$

$= n^2-(n+1+n)n+(n+1+n)^2$

$=3n^2+3n+1=p$

olur ve p rasyonel asal olduğundan π ve 4.2.17 Teorem gereği π nin denkleri de D de asaldır.

$\lambda=m+(m+n)\omega$ ise

$N\lambda = m^2-m(m+n)+(m+n)^2$

$=(n+1)^2-(n+1)(n+1+n)+(n+1+n)^2$

$=3n^2+3n+1=p$

olur ve böylece λ ile 4.2.17 Teorem gereği λ nın denkleri de D de asaldır.□

4.2.20 İddia: $p\equiv 1$ (6) rasyonel asal ise her p için D de tam 12 tane π asalı vardır.

4.2.21 Örnek: $p=13\equiv 1$ (6) olsun. $p-1=12$ ve $12=3.4$ ardışık 2 sayının çarpımı olarak yazılabiliyor. O halde 4.2.18 Teorem gereği $\pi=3+4\omega$, $\lambda=1+4\omega$ ve 4.2.17 Teorem gereği denkleri D de asaldır. Gerçekten, $\pi=3+4\omega$ nın normu $N\pi=\pi\bar{\pi}=a^2-ab+b^2$ olduğundan, $N\pi=9-3.4+16=13$ olur ve dolayısıyla π, D de asaldır. $\lambda=1+4\omega$ nın normu, $N\lambda=1-1.4+16$ olduğundan, λ da D de asaldır. Denkleri de 4.2.17 Teorem gereği D de asaldır.

4.2.22 Örnek: $p=19\equiv 1$ (6) olsun. $p-1=18$ ve 18 ardışık 2 sayının çarpımı değildir. $\frac{p-1}{3}=6$ ve $6=2.3$ ardışık iki sayının çarpımı olarak yazılabiliyor. Öyleyse 4.2.19 Teorem gereği $\pi=2+5\omega$ ve $\lambda=3+5\omega$ D de asaldır. Gerçekten $N\pi=4-10+25=19$ ve $N\lambda=9-15+25=19$ olduğundan π ve λ D de asaldır. Denkleri de 4.2.17 Teorem gereği D de asaldır.

4.3 Kübik Rezidü Karakteri

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

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

şeklinde tanımlanır. Burada $\alpha^{(N\pi-1)/3}$ π modunda 1, ω veya ω^2 ye denktir. Bu karakter kübik rezidü teorisinde, Legendre sembolünün kuadratik rezidü teorisindeki görevini yapar. Literatürde $\left(\frac{\alpha}{\pi}\right)_3$ yerine bazen $\chi_\pi(\alpha)$ da kullanılır.

4.3.2 Tanım: $\left(\frac{\alpha}{\pi}\right)_3 = 1$ ise α ya π modunda bir kübik rezidü, aksi halde kübik rezidü olmayan (non-rezidü) denir.

$p \equiv 1 \ (3)$ iken $\frac{p+1}{3}$ tane birbirinden farklı kübik rezidü ve $\frac{2p-1}{3}$ tane kübik rezidü olmayan, $q \equiv 2 \ (3)$ iken tam q tane birbirinden farklı kübik rezidü vardır.

4.3.3 Sonuç: İki kübik rezidünün ve farklı türdeki kübik rezidü olmayan (ω ve 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 veya ω^2 ve ω^2) çarpımı bir kübik rezidü olmayandır.

Bu durumun kuadratik rezidülerden farklı olduğuna dikkat edilmelidir.

İspat: Kübik rezidü karakterinin tanımından görülür.□

4.3.4 Teorem: π D de asal ve $N\pi = p$ olsun. $x^3 \equiv a \ (p)$ çözülebilir ise $x^3 \equiv a \ (\pi)$ çözülebilirdir.

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

4.3.5 Uyarı: 4.3.4 gereği, uygulamada π modu yerine $N\pi = p$ modu alınabilir.

4.3.6 Örnek: $\left(\frac{5+7\omega}{1+3\omega}\right)_3 = ?$

$N\pi = 1\text{-}3+9 = 7$ ve $N\alpha = 25\text{-}35+49 = 39$ dur. O halde;

$$\left(\frac{5+7\omega}{1+3\omega}\right)_3 = 39^{\frac{7-1}{3}}$$

$$= 39^2 \ (7)$$

$$\equiv 4^2 \ (7)$$

$$\equiv 2 \ (7)$$

elde edilir.

$\omega^2 \equiv 2 \ (7)$ olduğundan

$$\left(\frac{5+7\omega}{1+3\omega}\right)_3 = \omega^2$$

dir. O halde $5+7\omega$ $1+3\omega$ modunda bir kübik rezidü değildir.

4.3.7 Örnek: $\alpha = 2+4\omega$, $\pi = 3+4\omega$ olsun. $\left(\frac{\alpha}{\pi}\right)_3 = ?$

$N(3+4\omega) = 13$ ve $N(2+4\omega) = 4\text{-}8+16 = 12$ olduğundan

$$\left(\frac{2+4\omega}{3+4\omega}\right)_3 \equiv 12^{\frac{13-1}{3}} \ (13)$$

$$\equiv (-1)^4 \ (13)$$

$$\equiv 1 \ (13)$$

olur. O halde $2+4\omega$, $3+4\omega$ modunda bir kübik rezidüdür.

4.3.8 Örnek: $\alpha = 5+8\omega$ ve $\pi = 1+3\omega$ olsun. $N(\alpha) = 49$ ve $N(\pi) = 7$ dir. $7 \mid 49$ olduğundan tanım gereği $\left(\frac{\alpha}{\pi}\right)_3 = 0$ dır. Gerçekten,

$$\left(\frac{5+8\omega}{1+3\omega}\right)_3 = 49^{\frac{7-1}{3}}$$

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

$\equiv 0\ (7)$

bulunur.

4.3.9 Teorem: i) $\left(\frac{\alpha\beta}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3$

ii) $\alpha \equiv \beta\ (\pi)$ ise $\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3$

dir.

İspat: i) $\left(\frac{\alpha\beta}{\pi}\right)_3 \equiv (\alpha\beta)^{(N\pi-1)/3} \equiv \alpha^{(N\pi-1)/3}.\beta^{(N\pi-1)/3} \equiv \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3$

olur.

ii) $\alpha \equiv \beta\ (\pi)$ ise $\left(\frac{\alpha}{\pi}\right)_3 = \alpha^{(N\pi-1)/3} \equiv \beta^{(N\pi-1)/3} \equiv \left(\frac{\beta}{\pi}\right)_3\ (\pi)$

olur.□

4.3.10 Teorem: i) $\overline{\left(\frac{\alpha}{\pi}\right)_3} = \left(\frac{\alpha}{\pi}\right)_3^2 = \left(\frac{\alpha^2}{\pi}\right)_3$

ve

ii) $\overline{\left(\frac{\alpha}{\pi}\right)_3} = \left(\frac{\bar{\alpha}}{\bar{\pi}}\right)_3$

dir.

İspat: Kübik rezidü karakterinin tanımında $\left(\frac{\alpha}{\pi}\right)_3$, 1, ω veya ω^2 ye eşittir ve bu sayıların her birinin karesi eşleniğine eşittir. $N\bar{\pi}=N\pi$ olacağı da, göz önüne alınırsa i) ve ii) görülür.□

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

İspat: π asal ise, $p \equiv 1\ (3)$ rasyonel asal olmak üzere $N\pi = p$ dir. $p \equiv 1\ (3)$ ise $p = 3k+1$, $k \in \mathbf{Z}$ dir ve p asal olduğundan k çift sayıdır. O zaman

$$\left(\frac{-1}{\pi}\right)_3 = (-1)^{(N\pi-1)/3}$$

olduğundan, $N\pi-1 = p-1 = 3k+1-1 = 3k$ ve dolayısıyla

$$\left(\frac{-1}{\pi}\right)_3 = (-1)^{\frac{3k}{3}} = (-1)^k$$

olur. k çift sayı olduğundan,

$$\left(\frac{-1}{\pi}\right)_3 = 1$$

olur.

Eğer $q \equiv 2\ (3)$ ve q rasyonel asal ise q D de asaldır. $Nq = q.\bar{q} = q^2$ olduğundan $Nq-1 = q^2-1$ dir. $q \equiv 2\ (3)$ ve asal olduğundan q tek sayıdır. O zaman Nq-1 çift sayıdır ve dolayısıyla $\frac{Nq-1}{3}$ bir çift sayıdır. O halde $\left(\frac{-1}{q}\right)_3 \equiv (-1)^{(Nq-1)/3} = 1$

olur. □

4.3.12 Uyarı: -1 in her π modundaki kübik karakterinin 1 olacağı, $(-1)^3 = -1$ olduğundan da görülür.

$p \equiv 1\ (3)$ asal ve $N\pi = p$ olmak üzere $a^{\frac{p-1}{3}} \equiv 1,\ \omega,\ \omega^2\ (p)$ olduğunu biliyoruz. Yani $\mathbf{Z}_p$-{0} ın elemanlarının $\frac{p-1}{3}$. kuvvetleri, 4.1.6 Teorem gereği 1, ω, ω^2 ye $\mathbf{Z}_p$ de denk olan elemanlardır. Dolayısıyla p-1 tane elemanı, 3 grupta toplamış oluyoruz. Her bir grupta $\frac{p-1}{3}$ eleman vardır.

$K_p = \{k \mid k,\ p$ modunda sıfırdan farklı bir $\frac{p-1}{3}$. rezidü $\}$

şeklinde tanımlayalım. Yani K_p, $\mathbf{Z}_p$-{0} daki elemanların $\frac{p-1}{3}$. kuvvetlerinin p modundaki değerlerinden oluşmaktadır.

4.3.13 Teorem: K_p, $\mathbf{Z}_p$ deki çarpma işlemine göre bir gruptur ve aslında $\mathbf{Z}_p^*$ ın bir alt grubudur.

İspat : $K_p = \{1, \omega, \omega^2\}$ alabiliriz.

i) $\forall a,b,c \in K_p$ için $a(bc)=(ab)c$ olduğu görülüyor.

ii) 1, K_p nin birim elemanıdır.

iii) $1.1=1$, $\omega.\omega^2=1$ olduğundan 1 in tersi 1, ω nin tersi ω^2 ve ω^2 nin tersi de ω dir.

i), ii) ve iii) den K_p çarpma işlemi altında bir gruptur.

Şimdi $\forall a,b \in K_p$ nin $a\,b^{-1} \in \mathbf{Z}_p^*$ olduğunu gösterelim.

$$1.\omega^{-1} = 1.\omega^2 = \omega^2 \in \mathbf{Z}_p^*, \qquad 1.(\omega^2)^{-1} = 1.\omega = \omega \in \mathbf{Z}_p^*,$$

$$\omega.\omega^{-1} = \omega.\omega^2 \equiv 1 \in \mathbf{Z}_p^*, \qquad \omega.(\omega^2)^{-1} = \omega.\omega = \omega^2 \in \mathbf{Z}_p^*,$$

$$1.1^{-1} = 1.1 = 1 \in \mathbf{Z}_p^* \quad \text{ve} \quad \omega^2.(\omega^2)^{-1} = \omega^3 \in \mathbf{Z}_p^*$$

dır. □

4.3.14 Örnek: K_7 ve K_{13} ü oluşturalım. $p=7$ ve $\frac{p-1}{3}=2$ dir. 7 modunda $1^2 \equiv 1$, $2^2 \equiv 4$, $3^2 \equiv 2$, $4^2 \equiv 2$, $5^2 \equiv 4$, $6^2 \equiv 1$ ve $\omega \equiv 4\ (7)$, $\omega^2 \equiv 2\ (7)$ olduğundan

$$K_7 = \{1,2,4\} = \{1, \omega, \omega^2\}$$

Şimdi $p=13$ olsun. $\frac{p-1}{3}=4$ olur. 13 modunda, $1^4 \equiv 1$, $2^4 \equiv 3$, $3^4 \equiv 3$, $4^4 \equiv 9$, $5^4 \equiv 1$, $6^4 \equiv 9$, $7^4 \equiv 9$, $8^4 \equiv 1$, $9^4 \equiv 9$, $10^4 \equiv 3$, $11^4 \equiv 3$, $12^4 \equiv 1$ ve $\omega \equiv 9\ (13)$, $\omega^2 \equiv 3\ (13)$ olduğundan

$$K_{13} = \{1,3,9\} = \{1, \omega, \omega^2\}$$

olur.

4.3.15 Uyarı: $p \equiv 1\ (3)$ asal olduğunda $\frac{p-1}{3} = \frac{3k+1-1}{3} = k$ olur. p asal olduğundan, k çift sayı olmalıdır. Dolayısıyla $\frac{p-1}{3}$ çifttir. O halde a, $\frac{p-1}{3}$. kuvvet ise, -a da $\frac{p-1}{3}$. kuvvettir. □

Şimdi "Kübik İndirgeme Yasası"nı vereceğiz. Bu teorem ilk kez G. Eisenstein tarafından ispatlanmıştır.

4.3.16 Teorem (Kübik İndirgeme Yasası): π_1 ve π_2 1. tip, $N\pi_1, N\pi_2 \neq 3$ ve $N\pi_1 \neq N\pi_2$ olsun. O zaman

$$\left(\frac{\pi_1}{\pi_2}\right)_3 = \left(\frac{\pi_2}{\pi_1}\right)_3$$

tür, [3].□

4.3.17 Teorem: Eğer $\pi = a+b\omega$ ve $\pi \equiv 2$ (3) ise $\left(\frac{\omega}{\pi}\right)_3 = \omega^{(a+b+1)/3}$ tür, [4].□

4.3.18 Teorem: Eğer $\pi = a+b\omega$ ve $\pi \equiv 2$ (3) ise $\left(\frac{1-\omega}{\pi}\right)_3 = \omega^{2(a+1)/3}$ tür, [4].□

4.3.19 Teorem: π, 1.tip rasyonel asal ise $\left(\frac{2}{\pi}\right)_3 = 1$ dir. Yani $\pi = q > 2$ 1.tip rasyonel asal olmak üzere, 2 her q modunda bir kübik rezidüdür.

İspat: $\pi = q$ rasyonel asal olsun. $q = 2$ olamaz, çünkü o zaman $2 \mid 2$ ve $\left(\frac{2}{q}\right)_3 = 0$ olur. $q \equiv 2$ (3) rasyonel asal iken q modunda q tane kübik rezidünün olduğunu yani q modunda her a sayısının kübik rezidü olduğunu biliyoruz. Dolayısıyla 2, mod q da kübik rezidüdür.□

4.3.20 Teorem: $\pi = a+b\omega$, 1.tip kompleks asal ise $x^3 \equiv 2$ (π) nin çözülebilmesi için gerek ve yeter şart $\pi \equiv 1$ (2), yani $a \equiv 1$ (2) ve $b \equiv 0$ (2) olmasıdır.

İspat: $x^3 \equiv 2$ (π) çözülebilir olsun. O zaman, $\left(\frac{2}{\pi}\right)_3 = 1$ olur. 2 ve π nin ikisi de 1.tip asal olduğundan, Kübik İndirgeme Yasası gereği $\left(\frac{2}{\pi}\right)_3 = \left(\frac{\pi}{2}\right)_3$ yazabiliriz.

$\left(\frac{\pi}{2}\right)_3 \equiv \pi^{(N(2)-1)/3}\ (2)$ ve $N(2)=2^2=4$ olduğundan, $\left(\frac{\pi}{2}\right)_3 \equiv \pi\ (2)$ dir. Dolayısıyla, $\left(\frac{\pi}{2}\right)_3 = 1$ olması için $\left(\frac{\pi}{2}\right)_3 \equiv \pi \equiv 1\ (2)$ olması gerekir. Tersi de benzer şekilde görülür.□

4.3.21 Örnek: $x^3 \equiv 2\ (5+6\omega)$ denkliği çözülebilir midir?

$\pi = 5+6\omega$ hem 1.tip yani $\pi \equiv 2\ (3)$ ve hem de $\pi \equiv 1\ (2)$ şeklinde olduğundan, 4.3.20 gereği $\left(\frac{2}{5+6\omega}\right)_3 = 1$, yani $x^3 \equiv 2\ (5+6\omega)$ denkliği çözülebilirdir. Gerçekten 4.3.16 kullanılarak,

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

$$\equiv 1+0\omega\ \ (2)$$

$$\equiv 1\ \ (2)$$

bulunur.

Gauss, $p \equiv 1\ (3)$ ise $4p = A^2 + 27B^2$ olacak şekilde A ve B tamsayılarının varolduğunu ve bu A, B tamsayılarının işaretleri hariç bir tek şekilde belirlenebileceğini gösterdi.

4.3.22 Teorem: $\pi = a+b\omega$, 1.tip asal ve $N\pi = p = a^2 - ab + b^2$ olsun. $p \equiv 1\ (3)$ ise $x^3 \equiv 2\ (p)$ nin çözülebilmesi için gerek ve yeter şart $p = C^2 + 27D^2$ olacak şekilde C ve D tamsayılarının bulunabilmesidir.

İspat: $x^3 \equiv 2\ (p)$ çözülebilirse, o zaman $x^3 \equiv 2\ (\pi)$ çözülebilir ve 4.3.16 gereği $\pi \equiv 1\ (2)$ dir. $p = a^2 - ab + b^2$ ise $4p = 4a^2 - 4ab + 4b^2 = (2a-b)^2 + 3b^2$ olur. Burada $2a-b = A$, $\frac{b}{3} = B$ denirse, a tek ve b çift olduğundan A ve B çifttir. O halde $D = \frac{B}{2}$ ve $C = \frac{A}{2}$ yazılabilir ve böylece $p = C^2 + 27D^2$ elde edilir.

Şimdi $p = C^2 + 27D^2$ olacak şekilde C ve D tamsayılarının varolduğunu kabul edelim. O zaman, $4p = (2C)^2 + 27(2D)^2$ olur. Buradan, $B = \mp 2D$ bulunur. yani B ve dolayısıyla b çifttir. O halde $\pi = a+b\omega \equiv 1\,(2)$ elde edilir ($a \equiv 0$ (2) olamaz, çünkü o zaman $\pi \equiv 0$ (2) olur.) ve 4.3.20 den sonuç görülür.□

4.3.23 Örnek: $p = 19$ alalım. p sayısı $C^2 + 27D^2$ şeklinde yazılamayacağından, $x^3 \equiv 2\,(19)$ çözülemez. Gerçekten $\left(\frac{2}{19}\right)_3 = 2^{(N(19)-1)/3} = 2^{120} \equiv 11\ (19)$ ve $\omega \equiv 11\ (19)$ olduğundan $\left(\frac{2}{19}\right)_3 \equiv \omega\ (19)$ elde edilir.

Şimdi de $N\pi = 19$ olan, $\pi = 5+3\omega$ 1.tip asalını alalım.

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

ve

$$1+\omega = -\omega^2 \equiv (-1).\omega^2\,(2)$$
$$\equiv 1.\omega^2\,(2)$$

olduğundan

$$\left(\frac{2}{5+3\omega}\right)_3 = \omega^2\,(2)$$

elde edilir ve bu nedenle $x^3 \equiv 2\,(5+3\omega)$ çözülemez.

Buna karşılık $p = 31$ sayısı $2^2 + 27.1 = 31$ şeklinde yazılabildiğinden $x^3 \equiv 2\,(31)$ çözülebilirdir. Gerçekten

$$\left(\frac{2}{31}\right)_3 = 2^{(N(31)-1)/3} = 2^{320} \equiv 1\ (31)$$

olduğundan, $x^3 \equiv 2\,(31)$ denkliği çözülebilirdir ve $x \equiv 4\ (31)$ olacağı kolayca görülebilir. Buradan diğer kökler $x\omega \equiv 20\ (31)$ ve $x\omega^2 \equiv 7\ (31)$ olarak bulunur.

Şimdi $N\pi = 31$ olan, $\pi = 5+6\omega$ 1.tip asalını alalım.

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

olur ve böylece 2, 5+6ω modunda bir kübik rezidüdür.

$p \equiv 1 \ (3)$ iken $\omega \in Z_p$ olduğundan biz, D deki $\pi = a+b\omega$ asal modundaki kübik rezidülerden çok p modundakilerle ilgileneceğiz. $k>1$ tamsayı olmak üzere $p=3k$ iken ve $p \equiv 2 \ (3)$ iken D de normu p olan hiçbir $\pi = a+b\omega$ asalı bulunmadığından ve kübik rezidü kavramı $N\pi \neq 3$ iken tanımlı olduğundan herhangi bir kısıtlama söz konusu değildir.

4.3.24 Tanım: $x^3 \equiv a \ (p)$ olacak şekilde bir $x \in \mathbf{Z}$ varsa $a \in \mathbf{Z}$ ye p modunda bir kübik rezidü denir.

4.3.25 Uyarı: Dikkat edilirse 4.3.7 Örnekte $x^3 \equiv 2+4\omega \ (3+4\omega)$ dır. Gerçekten normlarını düşünürsek $Nx=4$, $N(2+4\omega)=12$ ve $N(3+4\omega)=13$ olduğundan $4^3 \equiv 12 \ (13)$ olur.

4.3.26 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.

İspat: Bu teorem Euler Kriterinin $k=3$ için özel halidir.□

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

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

4.3.28 Örnekler : 1) $\left(\frac{9}{7}\right)_3 \equiv \left(\frac{2}{7}\right)_3 = 2^{\frac{7-1}{3}} = 2^2 = 4 \ (7)$

$\omega^2 \equiv 4\ (7)$ olduğundan $\left(\frac{9}{7}\right)_3 = \omega^2$ dir ve bu nedenle 9, mod 7 de kübik rezidü değildir.

2) $\left(\frac{15}{7}\right)_3 \equiv \left(\frac{1}{7}\right)_3 \equiv 1^{\frac{7-1}{3}} \equiv 1^2 \equiv 1\ (7)$, dolayısıyla 15, mod 7 de bir kübik rezidüdür. Yani $x^3 \equiv 15\ (7)$ denkliği çözülebilirdir. Gerçekten, $x^3 \equiv 15 \equiv 1\ (7)$, $x=1$, $x=\omega$ ve $x=\omega^2$ bu denkliğin kökleridir. $\omega = \frac{-1+\sqrt{-3}}{2} \equiv 4\ (7)$ ve $\omega^2 \equiv 2\ (7)$ olduğundan bu denkliğin kökleri $x\equiv 1\ (7)$, $x\equiv 4\ (7)$ ve $x\equiv 2\ (7)$ dir.

3) $x^3 \equiv 41\ (73)$ çözülebilir mi?

$$\left(\frac{41}{73}\right)_3 \equiv 41^{\frac{73-1}{3}} \equiv 41^{24}\ (73)$$

$$41^{24} \equiv (41^2)^{12} \equiv 2^{12} \equiv 8\ (73)$$

$\omega \equiv 8\ (73)$ olduğundan $\left(\frac{41}{73}\right)_3 = \omega$ dır ve dolayısıyla $x^3 \equiv 41\ (73)$ çözülemez.

4.3.29 Teorem : $q \equiv 2\ (3)$ asal ve a, $(a,q)=1$ olacak şekilde pozitif bir tamsayı ise a mod q da bir kübik rezidüdür.

İspat: $q \equiv 2\ (3)$ bir asal ve a, $(a,q)=1$ olacak şekilde pozitif bir tamsayı olsun. $q \equiv 2\ (3)$ ise $q=3k+2$, $k \in \mathbf{Z}$ yazabiliriz. Bu durumda

$$Nq = q.\bar{q} = (3k+2)(3k+2) = 9k^2+12k+4 \text{ ve}$$

$$\frac{Nq-1}{3} = 3k^2+4k+1$$

tür. $(a,q)=1$ olmak üzere

$$a^{(Nq-1)/3} = a^{3k^2+4k+1}$$

dir. Fermat'ın küçük teoremi gereği,

$$a^{q-1} \equiv 1\ (q)$$

olduğunu biliyoruz. O halde

$$a^{q-1} = a^{3k+2-1} = a^{3k+1} \equiv 1\ (q)$$

olur. Böylece;

$$a^{(Nq-1)/3} = a^{3k^2+4k+1} = a^{(3k+1)(k+1)}$$

$$(a^{3k+1})^{k+1} \equiv 1^{k+1} \equiv 1\ (q)$$

olur.

4.3.30 Sonuç: Eğer $q \equiv 2\ (3)$ asal ise mod q da birbirinden farklı tam q tane kübik rezidü vardır. Yani $\mathbf{Z}_q$ nun tüm elemanları kübik rezidüdür.

İspat: $q \equiv 2\ (3)$ ise $\{1, 2, ..., q-1\}$ kümesinden bir a elemanını ve $\{0, 1, ..., q-2\}$ kümesinden de bir k sayısını, g ilkel kök olmak üzere,

$$g^k \equiv a\ (p)$$

olacak şekilde seçelim. $(3, q-1) = 1$ olduğundan,

$$3x' + (q-1)y' = 1$$

olacak şekilde x', y' tamsayıları bulunabilir. O halde $x = x'k$ ve $y = y'k$ tamsayıları için,

$$3x + (q-1)y = k$$

şeklinde yazabiliriz. Bu durumda $g^{p-1} \equiv 1\ (p)$ oluşu kullanılırsa,

$$a \equiv g^k = g^{3x+(q-1)y} = (g^x)^3 . (g^{q-1})^y \equiv (g^x)^3\ (q)$$

olur. Yani a, q modunda bir küptür. Ayrıca $0 \equiv 0^3\ (p)$ olduğu bilindiğinden, p modunda farklı tam q tane küp olduğu sonucu bulunur.

4.3.31 Örnek: $p = 11$ olsun. $0 \equiv 0^3$, $1 \equiv 1^3$, $2 \equiv 7^3$, $3 \equiv 9^3$, $4 \equiv 5^3$, $5 \equiv 3^3$, $6 \equiv 8^3$, $7 \equiv 6^3$, $8 \equiv 2^3$, $9 \equiv 4^3$, $10 \equiv 10^3\ (11)$ dir ve $\mathbf{Z}_{11}$ deki tüm sayılar kübik rezidüdür.

4.3.32 Teorem : $p \equiv 1\ (3)$ rasyonel asal ise p modundaki farklı kübik rezidülerin sayısı $\frac{p+2}{3}$ tür.

İspat: $p \equiv 1\ (3)$ ise $\{3, 6, 9, ..., p-1\}$ kümesinin her bir k elemanı $t \in \mathbf{Z}$ olmak üzere 3t şeklindedir. O halde,

$$g^k = g^{3t} = (g^t)^3$$

olup bir küptür. g ilkel kök olduğu için, bunların hepsi farklıdır. O zaman p modunda en azından $\frac{p-1}{3}$ tane sıfırdan farklı küp vardır. Bu özellikteki her bir $a \equiv b^3$ (p) küpü, Fermat'ın küçük teoremi gereği,

$$a^{\frac{p-1}{3}} = b^{p-1} \equiv 1 \ (p)$$

yazılabilir. Polinomlar İçin Lagrange Teoremi gereği,

$$x^{\frac{p-1}{3}} - 1 \equiv 0 \ (p)$$

denkliğinin en çok $\frac{p-1}{3}$ kökü olduğundan, $\frac{p-1}{3}$ sayısı aynı zamanda p modundaki küplerin toplam sayısı için bir üst sınırdır. O halde tam $\frac{p-1}{3}$ tane sıfır olmayan küp vardır. Sıfırı da sayarsak, p modunda $\frac{p-1}{3}+1 = \frac{p+2}{3}$ tane küp vardır.□

4.3.33 Teorem: p tek asal sayı ise $-a \equiv a$ olması için gerek ve yeter şart $a \equiv 0$ (p) olmasıdır.

İspat: $a \equiv -a$ (p) $\Leftrightarrow 2a \equiv 0$ (p) ve (2,p)=1 olduğundan $a \equiv 0$ (p) dir.

4.3.34 Sonuç: $\mathbf{Z_p}$ deki kübik rezidüler:

$0^3, 1^3, 2^3, 3^3, \ldots, \left(\frac{p-1}{2}\right)^3, \left(\frac{p+1}{2}\right)^3, \ldots, (p-1)^3$ dür ve burada $(p-1)^3 \equiv -1$ (p) dir.

4.3.35 Sonuç: Bir a tamsayısının $\mathbf{Z_p}$ de kübik rezidü olması için gerek ve yeter şart –a nın $\mathbf{Z_p}$ de kübik rezidü olmasıdır.

İspat: $x^3 \equiv k$ (p) nin bir çözümü $x \equiv a$ (p) ise $a^3 \equiv k$ (p) dir.

$$(-a)^3 = -a^3 \equiv -k \ (p) \Leftrightarrow a^3 \equiv k \ (p)$$

olduğundan $x \equiv -a$ (p) da $x^3 \equiv k$ (p) nin bir çözümüdür.

4.3.36 Teorem: $q \equiv 2$ (3) asal olsun. $x^3 \equiv a$ (q) denkliğini sağlayan kübik rezidülerin toplamı q modunda sıfıra denktir.

İspat: $q\equiv 2$ (3) iken tüm kübik rezidüler farklıdır ve bunlar 0, 1, 2, ..., q-1 dir. Toplamları ise,

$$0+1+2+...+q-1=\frac{(q-1).q}{2}=\frac{q-1}{2}.q$$

dir.

q asal ve $q\neq 2$ olduğundan q-1 çift sayıdır. O halde $k\in\mathbf{Z}$ olmak üzere, $q-1=2k$ yazabiliriz. Bu durumda,

$$\frac{q-1}{2}=\frac{2k}{2}=k\in\mathbf{Z}$$

yani, $\frac{q-1}{2}\in\mathbf{Z}$ olur. O zaman,

$$0+1+2+...+q-1=\frac{q-1}{2}.q=k.q=0 \pmod q$$

olur.□

4.3.37 Teorem: $p\equiv 1$ (3) asal olsun. $x^3\equiv a$ (p) denkliğini sağlayan kübik rezidülerin toplamı p modunda sıfıra denktir.

İspat: $p\equiv 1$ (3) asal iken $\frac{p+2}{3}$ tane farklı kübik rezidü bulunduğunu görmüştük. $p\equiv 1$ (3) ise $k\in\mathbf{Z}$ olmak üzere $p=3k+1$ yazabiliriz ve p asal olduğundan burada k çift sayıdır. $\frac{p+2}{3}=\frac{3k+1+2}{3}=k+1$ ve dolayısıyla $\frac{p+2}{3}$ tek sayıdır. Kübik rezidülerden biri sıfırdır. $a_0=0$ olsun. O zaman $\frac{p+2}{3}-1=\frac{p-1}{3}$ farklı kübik rezidü vardır. Üstelik a, $\mathbf{Z}_p$ de kübik rezidü ise, –a nın da kübik rezidü olduğunu biliyoruz. Bu durumda kübik rezidülerin toplamı,

$$a_0+a_1+...+a_{\frac{p-1}{3}}=a_0+(a_1+a_2+...+a_{\frac{p-1}{6}})+(-a_1-a_2-...-a_{\frac{p-1}{6}})$$

$$\equiv 0\ (p)$$

dir.□

4.3.38 Teorem: $x^3\equiv a$ (m) denkliğinin çözümlerinden biri x ise diğerleri $x\omega$ ve $x\omega^2$ dir.

İspat: $x^3 \equiv 1\ (m)$ nin çözümlerini $x \equiv 1,\ x\omega \equiv 1.\omega,\ x\omega^2 \equiv 1.\omega^2\ (m)$, şeklinde düşünürsek, $a \neq 1$ için de $x^3 \equiv a\ (m)$ nin çözümlerinden biri $x_1 \equiv x$ ise $x_2 \equiv x.\omega$ ve $x_3 \equiv x.\omega^2\ (m)$ olur. Gerçekten de x çözüm olduğundan

$$x_2^3 = (x\omega)^3 = x^3\omega^3 \equiv x^3 \equiv a(m)$$

ve benzer şekilde $x_3^3 \equiv a\ (m)$ bulunur.□

4.3.39 Teorem: $x^3 \equiv a\ (m)$ denkliğinin çözümlerinin toplamı, m modunda sıfıra denktir.

İspat: x_1, $x^3 \equiv a\ (m)$ nin çözümlerinden biri olsun. Bu durumda $x_2 \equiv x_1\omega$ ve $x_3 \equiv x_1\omega^2$ olduğundan

$$\begin{aligned} x_1 + x_2 + x_3 &= x_1 + x_1\omega + x_1\omega^2 \\ &= x_1 + x_1\omega + x_1(-1-\omega) \\ &= 0 \end{aligned}$$

bulunur.□

4.4 İndeks Kuralları ile Kübik Rezidüleri Belirleme

Burada $x^3 \equiv a\ (p)$ şeklindeki kübik kongrüansları 1.bölümde verilen indeks kurallarını kullanarak çözeceğiz.

4.4.1 Teorem: p bir asal sayı, $a \in \mathbf{Z}_p$ sıfır olmayan bir eleman ve $d=(3,p-1)$ olsun. $x^3 \equiv a\ (p)$ kongrüansının çözülebilmesi için gerek ve yeter şart $d \mid I(a)$ olmasıdır.

İspat: $x^3 \equiv a\ (p)$ kongrüansı yerine denk olarak,

$$3.I(x) \equiv I(a)\ (p-1)$$

yazılabileceğini biliyoruz. Bu bir lineer kongrüansdır ve sadece $(3,p-1)=d \mid I(a)$ durumunda çözülebilir.□

Burada iki durum söz konusudur. $d=(3,p-1)$ olduğundan $d=1$ ya da $d=3$ olabilir.

d=1 ise p-1, 3 ile bölünemeyeceğinden k∈**Z** için p-1≠3k, yani p 3 modunda 1'e denk değildir. O halde ya p≡2 (3) ya da p=3 tür. Yani bu iki halde kongrüans çözülebilirdir. Yani her a elemanı bir kübik rezidüdür.

d=3 ise p-1, 3 ile bölünebileceğinden k∈**Z** için p-1=3k, yani p≡1 (3) olur. Bu durumda tam $\frac{p+2}{3}$ tane kübik rezidü olduğunu ve a nın bunlardan biri olması durumunda kongrüansın çözülebileceğini biliyoruz. Sonuç olarak aşağıdaki teoremi verebiliriz:

4.4.2 Teorem: p bir asal sayı ve (3,p-1) =1 olsun. O zaman $x^3 \equiv a\,(p)$ kongrüansı her $a \in \mathbf{Z}_p$ için çözülebilir.

İspat: (3,p-1)=1 olduğunda p≡2 (3) ya da p=3 olacağını biliyoruz. p=3 ise $\mathbf{Z}_3$ te $0^3=0$, $1^3=1$, $2^3 \equiv 2\,(3)$ yani her a∈$\mathbf{Z}_3$ bir kübik rezidüdür. p≡2 (3) ise p modunda, p tane farklı kübik rezidü bulunduğundan her $a \in Z_p$ bir kübik rezidüdür.

4.4.3 Örnek: p=7 alalım. $\mathcal{U}_7=\{1,2,3,4,5,6\}$ ve 3 ve 5 ilkel köklerdir. g=3 alıp, indeks tablosunu oluşturursak,

a	3	2	6	4	5	1
I(a)	1	2	3	4	5	6

bulunur. d=(3,6) olduğundan d=3 tür. O halde $x^3 \equiv a\,(7)$ kongrüansı 3| I(a) durumunda çözülebileceğinden I(a)=6 veya I(a)=3, yani tablodan a=1 veya a=6 dır. Dolayısıyla mod 7 de sadece 1 ve 6 kübik rezidüdür. Gerçekten; $x^3 \equiv 1\,(7)$ nin çözümü; 3.I(x)≡I(1) (φ(6)) kongrüansının çözümüdür. Tablodan değerler bulunup yerine yazılırsa,

3.I(x)≡6 (6)

3.I(x)≡0 (6)

I(x)≡0 (2)

bulunur. Böylece I(x)≡2,4,0 (6) ve buradan sırasıyla x≡2,4,1 (7) olur.

Şimdi, $x^3 \equiv 6\,(7)$ yi düşünelim. 3.I(x)≡I(6) (6) kongrüansı için tablodan değerler bulunup yerine yazılırsa,

3.I(x)≡3 (6)

I(x)≡1 (2)

bulunur. Buradan I(x)≡1,3,5 (6) ve böylece x≡3,6,5 (7) bulunur. Her iki durumda da kökler toplamının sıfır olduğuna dikkat ediniz.

4.4.4 Örnekler: 1) $x^3 \equiv 10\,(37)$ çözülebilir midir?

$$\left(\frac{10}{37}\right)_3 = \left(\frac{2}{37}\right)_3 \cdot \left(\frac{5}{37}\right)_3 \equiv 2^{\frac{37^2-1}{3}} .5^{\frac{37^2-1}{3}} \ (37)$$

$$\equiv 10.26\ (37)$$

$$\equiv 260\ (37)$$

$$\equiv 1\ (37)$$

olduğundan $x^3 \equiv 10\,(37)$ çözülebilirdir.

2) 6, 19 modunda bir kübik rezidü müdür?

$$\left(\frac{6}{19}\right)_3 = \left(\frac{2}{19}\right)_3 \cdot \left(\frac{3}{19}\right)_3 \equiv 2^{\frac{19^2-1}{3}} .3^{\frac{19^2-1}{3}} \ (19)$$

$$\equiv 2^{120}.3^{120}$$

$$\equiv 11.11\ (19)$$

$$\equiv 7\ (19)$$

bulunur. $\omega^2 \equiv 7\,(19)$ olduğundan, $\left(\frac{6}{19}\right)_3 = \omega^2$ olur ve bu nedenle 6, 19 modunda bir kübik rezidü değildir.

3) $x^3 \equiv 2+2\omega\ \ (5+6\omega)$ kongrüansı çözülebilir midir?

N(2+2ω)=4 ve N(5+6ω)=31

olduğundan

$$\left(\frac{2+2\omega}{5+6\omega}\right)_3 \equiv 4^{\frac{31-1}{3}} = 4^{10}$$

$$\equiv 1\ (31)$$

bulunur. Bu nedenle $x^3 \equiv 2+2\omega\ (5+6\omega)$ kongrüansı çözülebilirdir.

4) $x^3 \equiv 8\,(13)$ kongrüansının çözümünü bulunuz.

$\left(\frac{8}{13}\right)_3 = \left(\frac{2}{13}\right)_3^3$ yazılabilir. $\left(\frac{2}{13}\right)_3$ ün 1, ω ya da ω^2 ye eşit olacağını biliyoruz. Bu üç durumda da, $\left(\frac{8}{13}\right)_3$ 1' denk olacaktır ($1^3=1$, $\omega^3=1$ ve $\left(\omega^2\right)^3 = 1$ dir.). O halde $x^3 \equiv 8\,(13)$ çözülebilirdir.

Şimdi bu denkliği, indeks yöntemiyle çözelim: Burada $p=13$ ve $\mathcal{U}_{13}=\{1,2,3,4,5,6,7,8,9,10,11,12\}$ dir. $\varphi(\varphi(13))=\varphi(12)=4$ tane ilkel kök vardır. Burada $12=2^2.3$ tür. O halde 13 modundaki kuadratik rezidüler 1,3,4,9,10,12 ve kübik rezidüler 1,5,8,12 dir. Geriye 2,6,7 ve 11 olmak üzere 4 eleman kalır. Bunlar ilkel köklerdir. $g=2$ seçelim ve indeks tablosunu oluşturalım:

a	2	4	8	3	6	12	11	9	5	10	7	1
I(a)	1	2	3	4	5	6	7	8	9	10	11	12

$p=13$ olduğundan, $d=(3,13-1)=3$ tür. $d=3$ durumunda, $x^3 \equiv a\,(p)$ denkliği sadece $3 \mid I(a)$ olduğunda çözülebileceğinden, $I(8)=3$ olup $x^3 \equiv 8\,(13)$ denkliği çözülebilirdir. O halde

$x^3 \equiv 8\,(13)$ ise

$3.I(x) \equiv I(8)\ (\varphi(13))$

yazabiliriz. Şimdi tablodan değerleri bulup yazalım.

$3.I(x) \equiv 3\ (12)$

$I(x) \equiv 1\ (4)$

$I(x) \equiv 1,5,9\ (12)$

ve

$x \equiv 2,6,5\ (13)$

bulunur.

5) $x^3 \equiv 24\,(73)$ kongrüansının çözümünü bulunuz.

$$\left(\frac{24}{73}\right)_3 = \left(\frac{2^3.3}{73}\right)_3 = \left(\frac{2}{73}\right)_3^3 . \left(\frac{3}{73}\right)_3$$

yazabiliriz. Burada $\left(\frac{2}{73}\right)_3^3 \equiv 1\ (73)$ olacaktır. O halde $\left(\frac{3}{73}\right)_3$ ü bulmak yeterlidir.

$$\left(\frac{3}{73}\right)_3 \equiv 3^{(73-1)/3} \equiv 1\,(73)$$

tür. Dolayısıyla,

$$\left(\frac{24}{73}\right)_3 \equiv 1\,(73)$$

olduğundan $x^3 \equiv 24\,(73)$ çözülebilirdir.

Şimdi bu kongrüansı indeks yöntemiyle çözelim:

$p=73$ olduğundan, $d=(3,73-1)=3$ tür. $d=3$ durumunda, $x^3 \equiv a\,(73)$ denkliği sadece $3 \mid I(a)$ olduğunda çözülebileceğinden, Ek A daki $p=73$ için indeks tablosuna bakılırsa $I(24)=30$ olduğundan $x^3 \equiv 24\,(73)$ denkliğinin çözülebileceği görülür.

$x^3 \equiv 24\,(73)$ ise

$3.I(x) \equiv I(24)\ (\varphi(73))$

yazabiliriz. Şimdi tablodan değerleri bulup yazalım.

$3.I(x) \equiv 30\ (72)$

$I(x) \equiv 10\ (24)$

ve

$x \equiv 50\ (73)$

bulunur. $\omega \equiv 8\ (73)$ ve $\omega^2 \equiv 64\ (73)$ olduğundan 4.3.38 gereği diğer kökler,

$x\omega \equiv 50.8 \equiv 35\ (73)$

ve

$x\omega^2 \equiv 50.64 \equiv 61\ (73)$

tür. Bu kökler $I(x) \equiv 10,34,58\ (72)$ denkliğinden de bulunabilir.

6) $x^3 \equiv 37\,(83)$ kongrüansının çözümünü bulunuz.

$83 \equiv 2(3)$ olduğundan 4.3.29 gereği $37 \in \mathbf{Z}_{83}$ bir kübik rezidüdür. Yani bu kongrüans çözülebilirdir.

$$x^3 \equiv 37\,(83) \text{ ise}$$

$$3.I(x) \equiv I(37)\ (\varphi(83))$$

yazabiliriz. Şimdi Ek A daki $p = 83$ için verilen indeks tablosundan değerleri bulup yerine yazalım.

$$3.I(x) \equiv 20\ (82)$$

$$3.I(x) \equiv 102\ (82)$$

$$I(x) \equiv 34\ (82)$$

ve

$$x \equiv 59\ (83)$$

bulunur. $d = 1$ olduğundan tek çözüm vardır. Zaten ω ve ω^2 nin $p \equiv 2\ (3)$ iken $\mathbf{Z}_p$ de olmadığını da biliyoruz.

5. KÜBİK DENKLEMLER İLE KÜBİK REZİDÜLER ARASINDAKİ İLİŞKİ

5.1 Giriş

Bu bölümde genel kübik denklemlerin kübik rezidüler yardımıyla tamsayı çözümlerini arayacağız.

Önce a, b, c, d$\in$**Z** olmak üzere

$$ax^3+bx^2+cx+d=0 \tag{5.1}$$

denkleminde $b=0$ özel halini alalım. O zaman (5.1) denklemi

$$ax^3+cx+d=0 \tag{5.2}$$

olacaktır. Burada $a \mid c$ ve $a \mid d$ durumunda (5.2) denklemini

$$x^3 \equiv -\frac{d}{a} \quad \left(\frac{c}{a}\right) \tag{5.3}$$

şeklinde kongrüans denklemi olarak düşünebiliriz. Bu durumda (5.3) kongrüansında

$r=-\frac{d}{a}$ ve $s=\frac{c}{a}$ denirse

$$x^3 \equiv r \quad (s)$$

yazılabilir. O halde $x^3 \equiv r \pmod{s}$ çözülebilirse, yani $\left(\frac{s}{r}\right)_3=+1$ ise, $ax^3+cx+d=0$ denklemi de çözülebilirdir.

İkinci olarak (5.1) denkleminde $a=1$ ve $b=0$ özel halini düşünelim. Bu durumda (5.1) denklemi

$$x^3+cx+d=0 \tag{5.4}$$

şeklinde olur. Bu durumda ise $x^3 \equiv d \pmod{c}$ çözülebilirse, yani $\left(\frac{d}{c}\right)_3=+1$ ise, $x^3+cx+d=0$ denklemi de çözülebilirdir.

Şimdi (5.1) denkleminde b≠0 olduğunu düşünelim. x yerine $y-\frac{b}{3a}$ yazılırsa, (5.1) denklemi

$$y^3+ry+s=0 \qquad (5.5)$$

denklemine dönüşür ve burada $r=\frac{c-b^2}{3a}$ ve $s=\frac{9abc-27a^2d+2b^3}{27a^2}$ dir.

$r, s\in\mathbf{Z}^+$ ise (5.5) denklemi

$$y^3\equiv s \ (r)$$

haline gelir. Eğer $y^3\equiv s \ (r)$ kongrüansı çözülebilirse, yani $\left(\frac{s}{r}\right)_3=+1$ ise, (5.1) denklemi de çözülebilirdir.

r bir tamsayı fakat s tamsayı değilse s bir rasyonel sayı olacaktır. $p,q\in\mathbf{Z}, q\neq 0$ ve $(p,q)=1$ olmak üzere $s=\frac{p}{q}$ diyelim. $s\in\mathbf{Z}_r$ olması için gerek ve yeter şart $s=\frac{p}{q}=p.\frac{1}{q}=p.t$ olacak şekilde q nun r modunda bir t tersinin mevcut olmasıdır. Bu ise $(q,r)=1$ iken mümkündür.

Son olarak r bir tamsayı değilse,

$$y^3\equiv s \ (r)$$

anlamsızdır.

5.1.1 Örnekler: 1) $2x^3+10x+4\equiv 0$ (p) kongrüansını uygun bir p modunda çözünüz.

$2x^3+10x+4=x^3+5x+2=0$ dir. Buradan

$$x^3\equiv -2 \ (5)$$

yazabiliriz. O halde p≡5 modunda çözüm arayabiliriz.

$$x^3\equiv 3 \ (5) \qquad (5.6)$$

dir. $\left(\frac{3}{5}\right)_3 = 3^{(N(5)-1)/3} = 3^8 \equiv 1 \ (5)$ olduğundan, (5.6) kongrüansı çözülebilirdir.

Şimdi bu kongrüansı çözelim.

$x^3 \equiv 3 \ (5)$

$3I(x) \equiv I(3) \ (\varphi(5))$

dir. İndeks tablolarından değerler bulunup yazılırsa

$3I(x) \equiv 3 \ (4)$

$I(x) \equiv 1 \ (4)$

$x \equiv 2 \ (5)$

bulunur. $x \equiv 2 \ (5)$ değeri 5 modunda $2x^3 + 10x + 4 = 0$ denkleminin de çözümüdür.

2) $x^3 + 14x - 1 \equiv 0 \ (p)$ kongrüansını uygun bir p modunda çözünüz.

$x^3 \equiv 1 \ (14)$

yazılabilir. $p \equiv 2 \ (3)$ olduğundan, 4.3.29 Teorem gereği bu kongrüans ve denk olarak

$x^3 + 14x - 1 \equiv 0 \ (14)$

çözülebilirdir.

Şimdi $x^3 \equiv 1 \ (14)$ kongrüansını çözelim.

$x^3 \equiv 1 \ (14)$

$3I(x) \equiv I(1) \ (\varphi(14))$

dir. İndeks tablolarından değerler bulunup yazılırsa

$3I(x) \equiv 6 \ (6)$

$I(x) \equiv 2 \ (2)$

$I(x) \equiv 0,2,4 \ (6)$

ve buradan

$x \equiv 1,9,11 \ (14)$

bulunur. Bu x değerleri $\mathbf{Z}_{14}$ te $x^3+14x-1=0$ denkleminin de çözümleridir.

3) $4x^3+6x^2+6x+7\equiv 0$ (p) kongrüansını uygun bir p modunda çözünüz.

Önce denklemi 4 ile bölelim. O zaman

$$x^3+\frac{3}{2}x^2+\frac{3}{2}x+\frac{7}{4}=0$$

elde edilir. Şimdi son denklemde x yerine $y-\frac{1}{2}$ yazalım.

$$y^3+\frac{3}{4}y+\frac{5}{4}=0$$

bulunur. Buradan

$$4y^3+3y=-5$$

ve böylece

$4y^3\equiv -5$ (3) yani

$y^3\equiv 1$ (3)

yazabiliriz.

Şimdi $y^3\equiv 1$ (3) kongrüansını çözelim.

$3.I(y)\equiv I(1)$ $(\varphi(3))$

$3.I(y)\equiv 2$ (2)

$3.I(y)\equiv 0$ (2)

$I(y)\equiv 0\equiv 2$ (2)

$y\equiv 1$ (3)

bulunur. O halde $x=y-\frac{1}{2}$ olduğundan $x=\frac{1}{2}\equiv 2$ (3) olur ve dikkat edilirse bu değer

$\mathbf{Z}_3$ te $4x^3+6x^2+6x+7=0$ denkleminin de çözümdür.

6. KÜBİK DENKLEMLERİN YAKLAŞIK ÇÖZÜMLERİ

Bu bölümde, kübik denklemlerin yaklaşık çözümlerini veren sayısal yöntemlerden bahsedeceğiz.

Bu yöntemlerin hepsinde önce verilen fonksiyonun kökünün içinde olduğu bir [a,b] aralığı seçmek gerekir. f(x) fonksiyonu [a,b] aralığında sürekli ve $f(a).f(b)<0$ ise bu aralıkta $f(x)=0$ denkleminin en az bir kökü vardır. Üstelik f(x) [a,b] de monoton ise, denklemin bu aralıkta tam bir tane kökü vardır. $f'(x)\geq 0$ iken, $f(a).f(b)<0$ ise f(x) in kökü [a,b] dedir. Aksi halde bu aralıkta kök yoktur.

6.1 Sabit Nokta İterasyonu:

Bu yöntem kısaca $f(x)=0$ denkleminden x' i çekerek aşağıda belirtilen özelliklere sahip olan bir g(x) fonksiyonu yazabilmek olarak özetlenebilir.

1) g(x) ve $g'(x)$ seçilen aralıkta sürekli,

2) Aralığın her noktası için $|g'(x)|<1$,

oluyorsa aralıkta rastgele seçilmiş olan bir x_0 başlangıç değeri ile sabit nokta iterasyonunda köke yaklaşılır.

Kübik denklemlere yöntemi uygularsak, $x^3+mx=n$ denklemini düşünmeliyiz. Bu denklemden seçilecek g fonksiyonu ya $g(x)=\frac{-x^3+n}{m}$ ya da $g(x)=\sqrt[3]{n-mx}$ şeklinde olacaktır.

6.2 Newton-Raphson Yöntemi:

Bu yöntem seçilen aralıkta fonksiyona teğet çizilmesiyle köke yaklaşma yöntemidir. Bu özelliğinden dolayı teğet yöntemi olarak da bilinir. f(x) in türevinin kolayca hesaplanabildiği durumlarda kullanılan bir yöntemdir.

Köke yaklaşık değerler kümesi olan [a,b] aralığında $f(x), f'(x), f''(x)$ var, sürekli ve gerçek kök olan α noktasında $f(\alpha)\neq 0$ olsun. Eğer ilk yaklaşım değeri olan x_0, [a,b] aralığında seçilmiş ise

$$x_{i+1} = x_i - \frac{f(x_i)}{f'(x_i)}$$

formülü bizi gerçek köke yaklaştırır.

6.3 Kiriş Yöntemi:

Bu yöntem, Newton –Raphson yöntemine benzerlikler gösterir. Burada, köke yaklaşmak için,

$$x_{i+1} = \frac{x_{i-1}f(x_i) - x_i f(x_{i-1})}{f(x_i) - f(x_{i-1})}$$

formülü kullanılır.

6.4 Teğet-Kiriş Yöntemi:

Teğet ve Kiriş yöntemlerinin birlikte kullanıldığı bir yöntemdir. Burada da verilen fonksiyonun kökünün bulunduğu, ve sürekli olduğu [a,b] aralığı belirlendikten sonra,

$$b_{n+1} = b_n - \frac{f(b_n)}{f'(b_n)} \qquad (6.2)$$

$$b_{n+1} = \frac{b_n f(a_n) - a_n f(b_n)}{f(a_n) - f(b_n)} \qquad (6.3)$$

formülleri kullanılarak köke yaklaşılır.

$f(a).f(b)<0$ ise

1) $f(a).f''(a) < 0$ ise bu durumda, b noktasında teğet yöntemi, yani (6.2), a noktasında ise kiriş yöntemi, yani (6.3) uygulanır.

2) $f(a).f''(a) > 0$ bu durumda, b noktasında kiriş yöntemi, yani (6.3), a noktasında ise teğet yöntemi, yani (6.2) uygulanır.

6.5 Yarılama Yöntemi:

Kiriş yöntemine benzer, ancak kiriş yöntemine göre köke yaklaşmada daha yavaş çalışır.

Bu yöntemde, $m = \frac{a_i + b_i}{2}$ olmak üzere, $f(a_i).f(m) < 0$ ise kök $[a_i, m]$ aralığındadır. Aksi halde kök, $[m, b_i]$ aralığındadır. Bu algoritma, istenen adım kadar uygulanarak köke yaklaşılır.

6.6 Örnek: $f(x)=x^3-5x+3$ denklemini alalım ve tüm yöntemleri bu fonksiyona uygulayarak köke yaklaşalım.

$x=0$ için $f(0)=3$ ve $x=1$ için $f(1)=-1$ ve bu durumda $f(0).f(1)<0$ olduğundan $[0,1]$ aralığını seçebiliriz.

İlk olarak $g(x) = \frac{x^3+3}{5}$ seçerek Sabit Nokta İterasyonu yöntemini uygulayalım:

1) $g'(x) = \frac{3x^2}{5}$ olup g ve g′ fonksiyonları süreklidir.

2) Dikkat edilirse, $\forall x \in [0,1]$ için $|g'(x)| < 1$ olduğu görülür.

O halde g fonksiyonunu seçimimiz doğru demektir. Şimdi iterasyonu uygulayabiliriz.

$$x_0 = 0$$

$$x_1 = g(x_0) = 0.6$$

$$x_2 = g(x_1) = 0.6432$$

bulunur.

İkinci olarak Newton-Raphson yöntemini uygulayalım:

$$x_{i+1} = x_i - \frac{f(x_i)}{f'(x_i)}$$

ve

$$f'(x) = 3x^2 - 5$$

olduğundan,

$$x_0 = 0$$

$$x_1 = x_0 - \frac{f(x_0)}{f'(x_0)} = 0 - \frac{3}{-5} = 0.6$$

$$x_2 = x_1 - \frac{f(x_1)}{f'(x_1)} = 0.6 - \frac{0.1296}{3.92} = 0.56693$$

bulunur.

Üçüncü olarak ta, kiriş yöntemini uygulayalım:

$$x_{i+1} = \frac{x_{i-1}f(x_i) - x_i f(x_{i-1})}{f(x_i) - f(x_{i-1})}$$

olduğundan,

$$x_2 = \frac{x_0 f(x_1) - x_1 f(x_0)}{f(x_1) - f(x_0)} = \frac{0f(1) - 1f(0)}{f(1) - f(0)} = \frac{-3}{-1-3} = 0.75$$

bulunur.

Şimdi de, teğet-kiriş yöntemini uygulayalım:
$f''(x) = 6x$ olduğundan $f(0).f''(0) = 0$ olur. Bu yöntemi uygulayabilmemiz için $f(a).f''(a)$ sıfırdan küçük ya da büyük olmalıydı. Seçtiğimiz aralığı değiştirirsek sorunu çözmüş oluruz. $a=1$ ve $b=2$ seçelim. Bu durumda $f(1)=-1$, $f(2)=1$ ve $f(1).f(2)<0$ olduğundan [1,2] aralığında da kök vardır. Şimdi tekrar yöntemimize dönelim. $f(1)f''(1) = -6 < 0$ dır. O halde, $b=2$ noktasında teğet $a=1$ noktasında kiriş yöntemlerini birlikte uygulayacağız.

$$b_2 = b_1 - \frac{f(b_1)}{f'(b_1)} = 2 - \frac{1}{7} = 1.8528$$

$$a_2 = \frac{b_1 f(a_1) - a_1 f(b_1)}{f(a_1) - f(b_1)} = \frac{2f(1) - 1f(2)}{f(1) - f(2)} = \frac{3}{2} = 1.5$$

bulunur. Böylece kökün bulunduğu [1,2] aralığı, [1.5,1.8528] şeklinde daraldı. Adım sayısını arttırdığımızda, a_n b_n e çakışık çıkacaktır. Bu durumda bulunan $a_n = b_n$ değeri verilen fonksiyonun köküdür.

Son olarak $f(x)=x^3-5x+3$ fonksiyonuna yarılama yöntemini uygulayalım:
Bu fonksiyonun [0,1] aralığında kökü olduğunu biliyoruz. O halde

$$m = \frac{a_0 + b_0}{2} = \frac{0+1}{2} = 0.5$$

ve

$$f(0.5) = 0.625$$

olup $f(0.5).f(1)<0$ olduğundan denklemin kökü [0.5,1] aralığındadır. Yöntemi bir adım daha uygularsak,

$$m = \frac{a_1 + b_1}{2} = \frac{0.5+1}{2} = 0.75$$

ve

$$f(0.75) = -0.328125$$

olup $f(0.5).f(0.75)<0$ olduğundan denklemin kökü [0.5,0.75] aralığındadır.

Tüm yöntemlerde adım sayısı arttırıldıkça köke daha fazla yaklaşılacaktır.

7. SONUÇLAR

Bu çalışmada, kuadratik rezidüler için bilinen sonuçları kübik rezidülerde elde etmek ve kübik rezidüler yardımıyla üçüncü derece denklemlerin çözümleri ile ilgili yöntem belirlemek amaçlanmıştır. $\mathbf{Z}[\omega]$ nın yapısı ve kübik rezidüler ile ilgili pek çok sonuç elde edilmiştir. Bazı kübik denklemler kongrüans şeklinde yazılarak bu denklemlerin $\mathbf{Z}_m$ de köklerinin bulunabilme şartları belirtilmiş, indeks yöntemiyle denklemlerin çözülebileceği gösterilmiş ve örnekler verilmiştir.

Bundan sonraki araştırmalarımızda, bazı kübik denklemler için belirlenen çözüm koşulları, genel kübik denklemler için geliştirilip, indeks yöntemiyle genel kübik denklemlerin çözümleri aranacaktır. Ayrıca kübik rezidülerin diğer uygulama alanları belirlenecektir.

EK A p<100 OLAN ASAL SAYILAR İÇİN İNDEKS TABLOLARI

p=3 için:

a	2	1
I(a)	1	2

p=5 için:

a	2	4	3	1
I(a)	1	2	3	4

p=7 için:

a	3	2	6	4	5	1
I(a)	1	2	3	4	5	6

p=11 için:

a	2	4	8	5	10	9	7	3	6	1
I(a)	1	2	3	4	5	6	7	8	9	10

p=13 için:

a	2	4	8	3	6	12	11	9	5	10	7	1
I(a)	1	2	3	4	5	6	7	8	9	10	11	12

p=17 için:

a	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1
I(a)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

p=19 için:

a	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
I(a)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18

p=23 için:

a	5	2	10	4	20	8	17	16	11	9	22	18	21	13	19	3	15	6	7	12	14	1
I(a)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22

p=29 için:

a	2	4	8	16	3	6	12	24	19	9	18	7	14	28	27	25	21	13	26	23	17	5
a	10	20	11	22	15	1																
I(a)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
I(a)	23	24	25	26	27	28																

p=31 için:

a	3	9	27	19	26	16	17	20	29	25	13	8	24	10	30	28	22	4	12	5	15	14
a	11	2	6	18	23	7	21	1														
I(a)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
I(a)	23	24	25	26	27	28	29	30														

p=37 için:

a	2	4	8	16	32	27	17	34	31	25	13	26	15	30	23	9	18	36	33	33	29	21
a	5	10	20	3	6	12	24	11	22	7	14	28	19	1								
I(a)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
I(a)	23	24	25	26	27	28	29	30	31	32	33	34	35	36								

p=41 için:

a	6	36	11	25	27	39	29	10	19	32	28	4	24	21	3	18	26	33	34	40	35	5
a	30	16	14	2	12	31	22	9	13	37	17	20	38	23	15	8	7	1				
I(a)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
I(a)	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40				

p=43 için:

a	3	9	27	38	28	41	37	25	32	10	30	4	12	36	22	23	26	35	19	14	42	40
a	34	16	5	15	2	6	18	11	33	13	39	31	7	21	20	17	8	24	29	1		
I(a)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
I(a)	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42		

p=47 için:

a	5	25	31	14	23	21	11	8	40	12	13	18	43	27	41	17	38	2	10	3	15	28
a	46	42	22	16	33	24	26	36	39	7	35	34	29	4	20	6	30	9	45	37	44	32
a	19	1																				
I(a)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
I(a)	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
I(a)	45	46																				

p=53 için:

a	2	4	8	16	32	11	22	44	35	17	34	15	30	7	14	28	3	6	12	24	48	43
a	33	13	26	52	51	49	45	37	21	42	31	9	18	36	19	38	23	46	39	25	50	47
a	41	29	5	10	20	40	27	1														
I(a)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
I(a)	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
I(a)	45	46	47	48	49	50	51	52														

p=59 için:

a	2	4	8	16	32	51	10	20	40	21	42	25	50	41	23	46	33	7	14	28	56	53
a	47	35	11	22	44	29	58	57	55	51	43	27	54	49	39	19	38	17	34	9	18	36
a	13	26	52	45	31	3	6	12	24	48	37	15	30	1								
I(a)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
I(a)	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
I(a)	45	46	47	48	49	50	51	52	53	54	55	56	57	58								

p=61 için:

a	2	4	8	16	32	3	6	12	24	48	35	9	18	36	11	22	44	27	54	47	33	5
a	10	20	40	19	38	15	30	60	59	57	53	45	29	58	55	49	37	13	26	52	43	25
a	50	39	17	34	7	14	28	56	51	41	21	42	23	46	31	1						
I(a)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
I(a)	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
I(a)	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60						

p=67 için:

a	2	4	8	16	32	64	61	55	43	19	38	9	18	36	5	10	20	40	13	26	52	37
a	7	14	28	56	45	23	46	25	50	33	66	65	63	59	51	35	3	6	12	24	48	29
a	58	49	31	62	57	47	27	54	41	15	30	60	53	39	11	22	44	21	42	17	34	1
I(a)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
I(a)	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
I(a)	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66

p=71 için:

a	7	49	59	58	51	2	14	27	47	45	31	4	28	54	23	19	62	8	56	37	46	38
a	53	16	41	3	21	5	35	32	11	6	42	10	70	64	22	12	13	20	69	57	44	24
a	26	40	67	43	17	48	52	9	63	15	34	25	33	18	55	30	68	50	66	36	39	60
a	65	29	61	1																		
I(a)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
I(a)	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
I(a)	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66
I(a)	67	68	69	70																		

p=73 için:

a	5	25	52	41	59	3	15	2	10	50	31	9	45	6	30	4	20	27	62	18	17	12
a	60	8	40	54	51	36	34	24	47	16	7	35	29	72	68	48	21	32	14	70	58	71
a	63	23	42	64	28	67	43	69	53	46	11	55	56	61	13	65	33	19	22	37	39	49
a	26	57	66	38	44	1																
I(a)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
I(a)	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
I(a)	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66
I(a)	67	68	69	70	71	72																

p=79 için:

a	3	9	27	2	6	18	54	4	12	36	29	8	24	72	58	16	48	65	37	32	17	51
a	74	64	34	23	69	49	68	46	59	19	57	13	39	38	35	26	78	76	70	52	77	73
a	61	25	75	67	43	50	71	55	7	21	63	31	14	42	47	62	28	5	15	45	56	10
a	30	11	33	20	60	22	66	40	41	44	53	1										
I(a)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
I(a)	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
I(a)	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66
I(a)	67	68	69	70	71	72	73	74	75	76	77	78										

p=83 için:

a	2	4	8	16	32	64	45	7	14	28	56	29	58	33	66	49	15	30	60	37	74	65
a	47	11	22	44	5	10	20	40	80	77	71	59	35	70	57	31	62	41	82	81	79	75
a	67	51	19	38	76	69	55	27	54	25	50	17	34	68	53	23	46	9	18	36	72	61
a	39	78	73	63	43	3	6	12	24	48	13	26	52	21	42	1						
I(a)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
I(a)	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
I(a)	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66
I(a)	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82						

p=89 için:

a	3	9	27	81	65	17	51	64	14	42	37	22	66	20	60	2	6	18	54	73	41	34
a	13	39	28	84	74	44	43	40	31	4	12	36	19	57	82	68	26	78	56	79	59	88
a	86	80	62	8	24	72	38	25	75	47	52	67	23	69	29	87	83	71	35	16	48	55
a	76	50	61	5	15	45	46	49	58	85	77	53	70	32	7	21	63	11	33	10	30	1
I(a)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
I(a)	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
I(a)	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66
I(a)	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88

p=97 için:

a	5	25	28	43	21	8	40	6	30	53	71	64	29	48	46	36	83	27	38	93	77	94
a	82	22	13	65	34	73	74	79	7	35	78	2	10	50	56	86	42	16	80	12	60	9
a	45	31	58	96	92	72	69	54	76	89	57	91	67	44	26	33	68	49	51	61	14	70
a	59	4	20	3	15	75	84	32	63	24	23	18	90	62	19	95	87	47	41	11	55	81
a	17	85	37	88	52	66	39	1														
I(a)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
I(a)	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
I(a)	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66
I(a)	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88
I(a)	89	90	91	92	93	94	95	96														

EK B ASAL OLMAYAN n≤20 SAYILARI İÇİN İNDEKS TABLOLARI

n=4 için:

a	3	1
I(a)	1	2
I(a)	3	

n=6 için

a	5	1
I(a)	1	2
I(a)	3	4
I(a)	5	

n=9 için

a	2	4	8	7	5	1
I(a)	1	2	3	4	5	6
I(a)	7	8				

n=10 için

a	3	9	7	1
I(a)	1	2	3	4
I(a)	5	6	7	8
I(a)	9			

n=14 için

a	3	9	13	11	5	1
I(a)	1	2	3	4	5	6
I(a)	7	8	9	10	11	12
I(a)	13					

NOT: n=8, 12, 15, 16, 20 için ilkel kök bulunamadığından indeks tabloları elde edilemez.

n=18 için

a	5	7	17	13	11	1
I(a)	1	2	3	4	5	6
I(a)	7	8	9	10	11	12
I(a)	13	14	15	16	17	

EK C D DEKİ $N\pi=p<500$ ve $p\equiv 1$ (3) ŞEKLİNDEKİ $\pi=a+b\omega$ ASALLARI

p=7	p=13	p=19	p=31	p=37
1+3ω	1+4ω	2+5ω	1+6ω	3+7ω
2+3ω	3+4ω	3+5ω	5+6ω	4+7ω
3+ω	4+ω	5+2ω	6+ω	7+3ω
3+2ω	4+3ω	5+3ω	6+5ω	7+4ω
-1-3ω	-1-4ω	-2-5ω	-1-6ω	-3-7ω
-2-3ω	-3-4ω	-3-5ω	-5-6ω	-4-7ω
-3-ω	-4-ω	-5-2ω	-6-ω	-7-3ω
-3-2ω	-4-3ω	-5-3ω	-6-5ω	-7-4ω
2-ω	3-ω	2-3ω	5-ω	3-4ω
-2+ω	-3+ω	-2+3ω	-5+ω	-3+4ω
1-2ω	1-3ω	3-2ω	1-5ω	4-3ω
-1+2ω	-1+3ω	-3+2ω	-1+5ω	-4+3ω

p=43	p=61	p=67	p=73	p=79
6+7ω	4+9ω	2+9ω	1+9ω	3+10ω
7+6ω	5+9ω	7+9ω	8+9ω	7+10ω
7+ω	9+4ω	9+7ω	9+ω	10+3ω
1+7ω	9+5ω	9+2ω	9+8ω	10+7ω
-6-7ω	-4-9ω	-2-9ω	-1-9ω	-3-10ω
-7-6ω	-5-9ω	-7-9ω	-8-9ω	-7-10ω
-7-ω	-9-4ω	-9-7ω	-9-ω	-10-3ω
-1-7ω	-9-5ω	-9-2ω	-9-8ω	-10-7ω
6-ω	4-5ω	2-7ω	8-ω	7-3ω
-6+ω	-4+5ω	-2+7ω	-8+ω	-7+3ω
1-6ω	5-4ω	7-2ω	1-8ω	3-7ω
-1+6ω	-5+4ω	-7+2ω	-1+8ω	-3+7ω

p=97	p=103	p=109	p=127	p=139
11+3ω	2+11ω	5+12ω	6+13ω	10+13ω
11+8ω	9+11ω	7+12ω	7+13ω	3+13ω
3+11ω	11+2ω	12+5ω	13+6ω	13+10ω
8+11ω	11+9ω	12+7ω	13+7ω	13+3ω
-11-3ω	-2-11ω	-5-12ω	-6-13ω	-10-13ω
-11-8ω	-9-11ω	-7-12ω	-7-13ω	-3-13ω
-3-11ω	-11-2ω	-12-5ω	-13-6ω	-13-10ω
-8-11ω	-11-9ω	-12-7ω	-13-7ω	-13-3ω
3-8ω	9-2ω	7-5ω	7-6ω	10-3ω
-3+8ω	-9+2ω	-7+5ω	-7+6ω	-10+3ω
8-3ω	2-9ω	5-7ω	6-7ω	3-10ω
-8+3ω	-2+9ω	-5+7ω	-6+7ω	-3+10ω

p=151	p=157	p=163	p=181	p=193
5+14ω	1+13ω	3+14ω	4+15ω	7+16ω
9+14ω	12+13ω	11+14ω	11+15ω	9+16ω
14+5ω	13+ω	14+3ω	15+4ω	16+7ω
14+9ω	13+12ω	14+11ω	15+11ω	16+9ω
-5-14ω	-1-13ω	-3-14ω	-4-15ω	-7-16ω
-9-14ω	-12-13ω	-11-14ω	-11-15ω	-9-16ω
-14-5ω	-13-ω	-14-3ω	-15-4ω	-16-7ω
-14-9ω	-13-12ω	-14-11ω	-15-11ω	-16-9ω
9-5ω	12-ω	11-3ω	11-4ω	9-7ω
-9+5ω	-12+ω	-11+3ω	-11+4ω	-9+7ω
5-9ω	1-12ω	3-11ω	4-11ω	7-9ω
-5+9ω	-1+12ω	-3+11ω	-4+11ω	-7+9ω

p=199	p=211	p=223	p=229	p=241
13+15ω	1+15ω	6+17ω	5+17ω	1+16ω
2+15ω	14+15ω	11+17ω	12+17ω	15+16ω
15+13ω	15+ω	17+6ω	17+5ω	16+ω
15+2ω	15+14ω	17+11ω	17+12ω	16+15ω
-13-15ω	-1-15ω	-6-17ω	-5-17ω	-1-16ω
-2-15ω	-14-15ω	-11-17ω	-12-17ω	-15-16ω
-15-13ω	-15-ω	-17-6ω	-17-5ω	-16-ω
-15-2ω	-15-14ω	-17-11ω	-17-12ω	-16-15ω
13-2ω	14-ω	11-6ω	12-5ω	15-ω
-13+2ω	-14+ω	-11+6ω	-12+5ω	-15+ω
2-13ω	1-14ω	6-11ω	5-12ω	1-15ω
-2+13ω	-1+14ω	-6+11ω	-5+12ω	-1+15ω

p=271	p=277	p=283	p=307	p=313
10+19ω	7+19ω	6+19ω	1+18ω	3+19ω
9+19ω	12+19ω	13+19ω	17+18ω	16+19ω
19+10ω	19+7ω	19+6ω	18+ω	19+3ω
19+9ω	19+12ω	19+13ω	18+17ω	19+16ω
-10-19ω	-7-19ω	-6-19ω	-1-18ω	-3-19ω
-9-19ω	-12-19ω	-13-19ω	-17-18ω	-16-19ω
-19-10ω	-19-7ω	-19-6ω	-18-ω	-19-3ω
-19-9ω	-19-12ω	-19-13ω	-18-17ω	-19-16ω
10-9ω	12-7ω	13-6ω	17-ω	16-3ω
-10+9ω	-12+7ω	-13+6ω	-17+ω	-16+3ω
9-10ω	7-12ω	6-13ω	1-17ω	3-16ω
-9+10ω	-7+12ω	-6+13ω	-1+17ω	-3+16ω

p=331	p=337	p=349	p=367	p=373
10+21ω	8+21ω	3+20ω	9+22ω	4+21ω
11+21ω	13+21ω	17+20ω	13+22ω	17+21ω
21+10ω	21+8ω	20+3ω	22+9ω	21+4ω
21+11ω	21+13ω	20+17ω	22+13ω	21+17ω
-10-21ω	-8-21ω	-3-20ω	-9-22ω	-4-21ω
-11-21ω	-13-21ω	-17-20ω	-13-22ω	-17-21ω
-21-10ω	-21-8ω	-20-3ω	-22-9ω	-21-4ω
-21-11ω	-21-13ω	-20-17ω	-22-13ω	-21-17ω
10-11ω	13-8ω	17-3ω	13-9ω	17-4ω
-10+11ω	-13+8ω	-17+3ω	-13+9ω	-17+4ω
11-10ω	8-13ω	3-17ω	9-13ω	4-17ω
-11+10ω	-8+13ω	-3+17ω	-9+13ω	-4+17ω

p=379	p=397	p=409	p=421	p=433
15+22ω	11+23ω	8+23ω	1+21ω	11+24ω
7+22ω	12+23ω	15+23ω	20+21ω	13+24ω
22+15ω	23+11ω	23+8ω	21+ω	24+11ω
22+7ω	23+12ω	23+15ω	21+20ω	24+13ω
-15-22ω	-11-23ω	-8-23ω	-1-21ω	-11-24ω
-7-22ω	-12-23ω	-15-23ω	-20-21ω	-13-24ω
-22-15ω	-23-11ω	-23-8ω	-21-ω	-24-11ω
-22-7ω	-23-12ω	-23-15ω	-21-20ω	-24-13ω
15-7ω	12-11ω	15-8ω	20-ω	13-11ω
-15+7ω	-12+11ω	-15+8ω	-20+ω	-13+11ω
7-15ω	11-12ω	8-15ω	1-20ω	11-13ω
-7+15ω	-11+12ω	-8+15ω	-1+20ω	-11+13ω

p=439	p=457	p=463	p=487	p=499
18+23ω	17+24ω	1+22ω	2+23ω	7+25ω
5+23ω	7+24ω	21+22ω	21+23ω	18+25ω
23+18ω	24+17ω	22+ω	23+2ω	25+7ω
23+5ω	24+7ω	22+21ω	23+21ω	25+18ω
-18-23ω	-17-24ω	-1-22ω	-2-23ω	-7-25ω
-5-23ω	-7-24ω	-21-22ω	-21-23ω	-18-25ω
-23-18ω	-24-17ω	-22-ω	-23-2ω	-25-7ω
-23-5ω	-24-7ω	-22-21ω	-23-21ω	-25-18ω
18-5ω	17-7ω	21-ω	21-2ω	18-7ω
-18+5ω	-17+7ω	-21+ω	-21+2ω	-18+7ω
5-18ω	7-17ω	1-21ω	2-21ω	7-18ω
-5+18ω	-7+17ω	-1+21ω	-2+21ω	-7+18ω

KAYNAKÇA

[1] Jones, G.A., Jones J.M., Elemantary Number Theory, Springer-Verlag, Newyork , (1998), S.37-140

[2] Leveque, W.J., Fundamentals of Number Theory, Dover Publications, Newyork, (1997), s.47-93, 97-120, 270-273

[3] Ireland, K., Rosen, M., A Classical Introduction to Modern Number Theory, Springer-Verlag, Newyork, (1982), s.108-121

[4] Sun, Z.H., "On the theory of cubic residues and nonresidues", *Acta Arithmetica J.*, 4 (1998), s.291-335

[5] Stark, H.M., An Introduction to Number Theory, Cambridge, London, (1979), s.51-117

[6] Tall, D.O., Stewart I.N., Algebraic Number Theory, Mathematics Institute University of Warwick Coventry, Second Edition, (1987), s.38-65, 231-252

[7] Türker, E.S.,Can, E.,Bilgisayar Uygulamalı Sayısal Analiz Yöntemleri, Değişim Yayınları, Adapazarı, (1997), s.41-72

[8] Flath, D.E., Introduction to Number Theory, A.Wiley-İnterscience Publication, (1989), s.63-104

[9] Williams, K.S., "Cubic Nonresidues (mod p)", *Delta J.*, 6, (1976), s.23-28

[10] Williams, K.S., "On Euler's Criterion for Cubic Nonresidues ", *Proceeding of Amer.Math.Soc.*, 49, (1975), s.277-283

[11] Magnusson, C., The History of Cubic Equations, Thesis, Miduniversity, Sweden, (1998).

[12] Filaseta,M., Lecture Notes on Number Theory,
http://www.math.sc.edu/~filaseta/

[13] Bayraktar, M., Soyut Cebir ve Sayılar Teorisi, Uludağ Üniversitesi Fen-Edb. Fakültesi Yayınları, Bursa, (1997), 2.baskı, s.46-79