ÖZET

Yüksek Lisans Tezi

GAUSS TAMSAYILARI HALKASINDA KONGRÜANS DENKLEMERİNİN ÇÖZÜMLERİ VE 4. DERECEDEN KALANLAR ÜZERİNE

Kevser AKTAŞ

Selçuk Üniversitesi Fen Bilimleri Enstitüsü

İlköğretim Anabilim Dalı

Matematik Öğretmenliği Programı

Danışman : Prof.Dr. Hasan ŞENAY

2008, 37 Sayfa

Juri : Prof. Dr. Hasan ŞENAY

Prof. Dr. Durmuş BOZKURT

Yard. Doç. Dr. Ahmet CİHANGİR

Bu çalışmada Gauss tamsayılarının özellikleri yardımıyla Elemanter Legendre Sembolünün 4. dereceden Legendre sembolüne genişlemesini inceledik. 4. dereceden Legendre sembolünün özelliklerini inceledik. Buradan 4. dereceden kalanlar teoremine ulaştık.

Gauss tamsayılar halkasında P_k kümelerinin varlığı için bir kriter oluşturarak bazı genişlemeyen P_k kümelerinin var olduğunu gösterdik. Ayrıca Gauss asallarından faydalanılarak nasıl P_4 kümelerinin yazılabileceğini gösterdik.

Anahtar Kelimeler: Gauss Tamsayıları, Legendre Sembolü, P_k Cümleleri.

ABSTRACT

Master Thesis

ON THE SOLUTIONS OF CONGRUENCE EQUATIONS IN THE GAUSSIAN INTEGERS RING AND BIQUADRATIC RESIDUES

Kevser AKTAŞ

Selçuk University

Graduate School of Natural and Applied Sciences

Department of Education

Supervisor : Prof.Dr. Hasan ŞENAY

2008, 37 Pages

Jury : Prof. Dr. Hasan ŞENAY

Prof. Dr. Durmuş BOZKURT

Assist. Prof. Dr. Ahmet CİHANGİR

In this study, using properties of Gaussian Integers, we investigated the extention of Elementary Legendre Symbol to the biquadratic. We considered the properties of the biquadratic Legendre symbol. Then we obtained the biquadratic residue theorem.

In this study we formed a criter for the existence of P_k Sets in Gaussian Integers Ring and we showed the existence of some nonextendanble P_k Sets. In addition to this, using Gaussian Integers we showed that how to write P_4 Sets.

Key Words : Gaussian Integers, Legendre Symbol, P_k Sets.

ÖNSÖZ

Bu çalışma Selçuk Üniversitesi Eğitim Fakültesi Ortaöğretim Fen ve Matematik Alanlar Eğitimi Ortaöğretim Matematik Eğitimi Anabilim Dalı Öğretim Üyesi Prof. Dr. Hasan ŞENAY yönetiminde yapılarak Selçuk Üniversitesi Fen Bilimleri Enstitüsü'ne Yüksek Lisans Tezi olarak sunulmuştur.

Çalışmamdaki yardımlarından dolayı saygıdeğer hocam Prof. Dr. Hasan ŞENAY'a ve bana destek veren TÜBİTAK'a teşekkürlerimi ve saygılarımı sunarım.

İÇİNDEKİLER

ÖZET i
ABSTRACT ii
ÖNSÖZ iii
İÇİNDEKİLER iv
1. GİRİŞ 1
2. ÖN BİLGİLER 2
2.1. Sonlu Cisimlerin Temel Özellikleri 2
2.2. Çarpanlanabilir Karakterler 4
2.3. $\mathbb{Z}[i]$ Halkasının Bazı Özellikleri 5
3. TEORİK ESASLAR 14
3.1. Dördüncü Dereceden Kalanlar 14
3.2. 4. Dereceden Kalan Sembolü 18
4. $\mathbb{Z}[i]$ DE P_k KÜMELERİNİN VARLIĞI 32
5. SONUÇLAR 36
6. KAYNAKLAR 37

1. GİRİŞ

David COX yılındaki kitabında, benzer şekilde 4. dereceden kalanlar için Legendre sembolünü tanımlayıp, p asalının $x, y \in \mathbb{Z}$ için $p = x^2 + 64y^2$ biçiminde temsil edilebilmesi için gerek ve yeter koşul $p \equiv 1 \pmod 4$ ve 2 nin, p modülüne göre bir 4. dereceden kalan olması gerektiğini ifade etmiştir.[1]

Fethi ÇALLIALP kitabında , $\mathbb{Z}[i]$ Gauss Tamsayılar halkasının genel özelliklerinden bahsetmiştir.[2]

Andrej DUJELLA makalesinde tamsayılar ile yazılabilen 4 elemanlı P_k kümelerinin Gauss tamsayılarına nasıl genişlediğini gösterdi. b tek veya $a \equiv b \equiv 2 \pmod 4$ ise, bu şekilde 4 elemanlı bir P_{a+bi} kümesi yazılamayacağını söylemiştir. Eğer 4 elemanlı bir P_{a+bi} kümesi ve $a+bi$ yukarıdaki formda olmayıp $a+bi \notin \{2, -2, 1+2i, -1-2i, 4i, -4i\}$ ise, o halde en azından bir tane 4 elemanlı bir P_{a+bi} kümesi varlığını gösterdi. $\mathbb{Z}$ ve $\mathbb{Z}[i]$ de , 4 elemanlı P_k kümelerinin iki kare farkı şeklinde temsil edilen elemanların kümesi olduğunu gösterdi.[3]

H. FLANDERS makalesinde, $\mathbb{Z}[i]$ de kalanlı bölme teoreminin geçerli olduğunu belirtmiştir.[4]

Kenneth IRELAND ve Michael ROSEN kitabında, $\mathbb{Z}[i]$ nin asalları ile ilgili bilgi verip Legendre sembolünün 4. dereceden kalanlara genişletmesini göstermiştir. 4. dereceden kalanlar teoremi üzerinde durmuştur.[5]

Kenan KAYGISIZ makalesinde bazı genişletilemeyen P_k kümeleri üzerinde çalışmıştır.[6]

Hasan ŞENAY kitabında, $\mathbb{Z}[i]$ Gauss tamsayılar halkasının özellikleri ve asalların karakterizasyonu ile ilgili çalışmalara yer vermiştir.[7]

2. ÖN BİLGİLER

Bu bölümde çalışmamızın konusunun temeli olan $\mathbb{Z}[i]$ Gauss tamsayılar halkasının temel özellikleri ile bunların kullanılmasında yardımcı olacak diğer bilgileri vereceğiz.

2.1. Sonlu Cisimlerin Temel Özellikleri

F, q elemanlı bir sonlu cisim olsun. O zaman F nin çarpımsal alt grubu olan F^* nın $q-1$ tane elemanı vardır. Böylece $\forall \alpha \in F^*$, $x^{q-1}=1$ eşitliğini sağlar. (Burada 1, F nin çarpımsal birimini temsil edip, bildiğimiz anlamda tamsayı 1 değildir.) F nin her elemanı $x^q = x$ eşitliğini sağlar.

Önerme 2.1.1.

$$x^q - x = \prod_{\alpha \in F} (x-\alpha)$$

İspat: Her iki polinom da $F[x]$ in elemanları olarak düşünülür.

$\forall \alpha \in F$ nın, $x^q - x$ in bir kökü olduğunu biliyoruz. F nin q tane elemanı olduğundan ve $x^q - x$ in derecesi q olduğundan $\prod_{\alpha \in F}(x-\alpha)$ nın derecesi de q dur. O halde, $x^q - x = \prod_{\alpha \in F}(x-\alpha)$ dır (Ireland ve Rosen 1990).

Sonuç 2.1.1. *K bir cisim olmak üzere $F \subset K$ olsun. Bir $\alpha \in K$ nın F nin içinde olması için gerek ve yeter şart $\alpha^q = \alpha$ olmasıdır* (Ireland ve Rosen 1990).

İspat: $\alpha^q = \alpha$ olması için gerek ve yeter şart α nın $x^q - x$ in kökü olmasıdır. Buradan, Önerme 2.1.1. gereği, $x^q - x$ in köklerinin tam olarak F nin elemanları olduğuna ilgi çekilmelidir.

Sonuç 2.1.2. *Eğer $f(x)$, $x^q - x$ i bölüyorsa, o halde d, $f(x)$ in derecesi olmak üzere, $f(x)$ in d tane farklı kökü vardır* (Ireland ve Rosen 1990).

İspat: $f(x)g(x)=x^q-x$ olsun. $g(x)$ in mertebesi $q-d$ dir. Eğer $f(x)$ in d farklı kökten daha az kökü varsa, cebirden bilindiğine göre, $f(x)g(x)$, $d+(q-d)=q$ farklı kökten daha az köke sahip olacaktır. Buradan $f(x)$ in d tane kökü vardır.

Teorem 2.1.1. (Lagrange Teoremi) *p asal, $a_0 \not\equiv 0 \pmod p$ ve $f(x)=\sum_{k=0}^{n} a_k x^{n-k}$ biçiminde bir polinom ise, $f(x)\equiv 0 \pmod p$ kongrüansının en fazla n tane kökü vardır* (Şenay 2007).

Teorem 2.1.2. *Sonlu bir cismin çarpımsal grubu devirlidir* (Ireland ve Rosen 1990).

İspat: Bu teorem "$U(\mathbb{Z}/p\mathbb{Z})$ devirli bir gruptur." teoreminin genelleştirilmesidir. İspatı aynıdır. Eğer, $d \mid q-1$ ise, $x^d-1 \mid x^{q-1}-1$ dir ve Sonuç 2.1.2. den x^d-1 in d farklı kökü vardı. Böylece F^* ın alt grubu, d. dereceden (mertebeden) $x^d=1$ i sağlayan elemanları içerir. $\psi(d)$, d. dereceden F^* ın elemanlarının sayısıdır. O halde,

$$\sum_{c \mid d} \psi(c) = d$$

Mobius ters çevirme formülü ile,

$$\psi(d) = \sum \mu(c)\frac{d}{c} = \varphi(d)$$

olur.

Özel olarak, $q=2$ olmadıkça, $\psi(q-1)=\varphi(q-1)>1$ dir.

F^* ın devirli olma durumu F sonlu olduğunda şu durumu gösterir.

Eğer $m \in \mathbb{Z}^+$ ilkel köklere sahip ve $(a,m)=1$ ise, a nın m modülüne göre $n.$ dereceden kalan olması için gerek ve yeter şart $a^{\varphi(m)/d} \equiv 1 \pmod m$ $\left(d=(n,\varphi(m))\right)$ olması da göz önüne alarak bunun kısmi genelleştirmesini verir.

Önerme 2.1.2. $\alpha \in F^*$ *olsun. O halde,* $x^n = \alpha$ *nın çözümlerinin olması için gerek ve yeter şart* $\alpha^{(q-1)/d} = 1$ *dir* $\left(d = (n, q-1)\right)$ (Ireland ve Rosen 1990).

Eğer çözümler mevcutsa, tam olarak d tane çözüm vardır.

İspat: γ, F^*ın üreteci olsun. $\alpha = \gamma^a$ ve $x = \gamma^y$ olsun. O halde, $x^n = \alpha$ eşitliği $ny \equiv a\left(\mathrm{mod}(q-1)\right)$ kongrüansına denktir.

Şimdi $n \mid q-1$ ve $(n, q-1) = 1$ iken nasıl durumların oluşacağını gözlemleyelim.

Eğer $n \mid q-1$ ise, o zaman F^*ın $n.$ kuvvetten $\dfrac{q-1}{n}$ tane elemanı vardır ve eğer α, $n.$ kuvvettense o halde $x^n = \alpha$ eşitliğinin tam olarak n tane çözümü vardır.

Eğer $(n, q-1) = 1$ ise, $n.$ kuvvetten her eleman tektir. Örneğin, $\alpha \in F^*$ için, $x^n = \alpha$ nın sadece bir çözümü vardır.

Sonuç 2.1.3. $\alpha \in \left(\mathbb{Z}[i]/\pi\mathbb{Z}[i]\right)^*$ *olsun. O halde* $x^4 = \alpha$ *nın çözümlerinin olması için gerek ve yeter şart* $\alpha^{(N(\pi)-1)/d} = 1$ *dir.* $\left(d = \left(4, N(\pi)-1\right)\right)$

Not 2.1.1. $\mathbb{Z}/p\mathbb{Z} = F_p$ sonlu cisimdir.

2.2. Çarpanlanabilir Karakterler

F_p üzerinde çarpanlanabilir bir karakter, F_p^*dan sıfırdan farklı kompleks sayılara bir χ dönüşümü,

$$\chi(ab) = \chi(a)\chi(b)\ , \quad \left(\forall a, b \in F_p^*\right)$$

şeklindedir.

Eğer p modülüne göre a kalan sınıfının bir fonksiyonu gözüyle bakılırsa, $\left(\dfrac{a}{p}\right)$ elemanter Legendre sembolü çarpanlanabilir karaktere bir örnektir.

Önerme 2.2.1. χ çarpanlanabilir karakter ve $a \in F_p^*$ olsun. O halde,

1) $\chi(1) = 1$

2) $\chi(a)$, birimin $(p-1)$. köküdür.

3) $\chi\left(a^{-1}\right)=\chi(a)^{-1}=\overline{\chi(a)}$

dir (Ireland ve Rosen 1990).

2.3. $\mathbb{Z}[i]$ Halkasının Bazı Özellikleri

Şimdi $\mathbb{Z}[i]$ halkasının çalışmamıza konu olan özelliklerini ele alabiliriz.

Tanım 2.3.1. Herhangi a , $b\in\mathbb{Z}$ ve $i=\sqrt{-1}$ olmak üzere $a+bi$ biçimindeki bütün sayılara *Gauss Tamsayıları* denir. Bu tür sayıların cümlesini $\mathbb{Z}[i]$ ile göstereceğiz. Yani, $i=\sqrt{-1}$ olmak üzere,

$$\mathbb{Z}[i]=\left\{a+bi \middle| a,b\in\mathbb{Z}\right\}$$

dır.

Tanım 2.3.2. $a,b\in\mathbb{Z}$ olmak üzere $\alpha=a+bi\in\mathbb{Z}[i]$ sayısının *eşleniği* $a-bi$ şeklinde tanımlanıp $\bar{\alpha}$ ile gösterilir. Bir $\alpha=a+bi\in\mathbb{Z}[i]$ sayısının *normu* $N(a+bi)=\alpha\bar{\alpha}=a^2+b^2\in\mathbb{Z}$ dır.

Önerme 2.3.1. *Norm fonksiyonun şu özellikleri vardır* (Şenay 2007).

1) $\forall\alpha\in\mathbb{Z}[i]$ için $N(\alpha)\geq 0$

2) $N(\alpha)=0\Leftrightarrow\alpha=0$

3) $\forall\alpha,\beta\in\mathbb{Z}[i]$ için $N(\alpha\cdot\beta)=N(\alpha)\cdot N(\beta)$ dır.

4) $\alpha=a+bi\in\mathbb{Z}[i]$,$\beta=c+di$ $(a,b,c,d\in\mathbb{Z})$ olmak üzere,

- **a)** $\overline{\alpha\beta}=\bar{\alpha}\bar{\beta}$
- **b)** $\overline{(\alpha+\beta)}=\bar{\alpha}+\bar{\beta}$

dır.

İspat: $\alpha=a+bi\in\mathbb{Z}[i]$, $(a,b\in\mathbb{Z})$ olmak üzere,

1) $\mathrm{N}(\alpha)=\alpha\cdot\bar{\alpha}=(a+bi)\cdot(a-bi)=a^2+b^2\geq 0$ dır.

2) $\Rightarrow$: $N(\alpha)=a^2+b^2=0$ ise,

$a^2=-b^2$ olur. Böyle bir durum ancak $a=b=0$ olması ile mümkün olacağından $\alpha=0+0i=0$ dır.

$\Leftarrow$: $\alpha=0$ ise,

$$\alpha=a+bi=0 \Rightarrow a=-bi$$

$$N(\alpha)=a^2+b^2=(-bi)^2+b^2$$

$$=-b^2+b^2$$

$$=0$$

3) $\forall \alpha,\beta \in \mathbb{Z}[i]$ için, $\alpha=a+bi$, $\beta=c+di$ olacak şekilde $a,b,c,d \in \mathbb{Z}$ olsun.

$$N(\alpha\cdot\beta)=N\left((a+bi)\cdot(c+di)\right)$$

$$=N\left(ac+adi+bci+bdi^2\right)$$

$$=N\left((ac-bd)+(ad+bc)i\right)$$

$$=(ac-bd)^2+(ad+bc)^2$$

$$=a^2c^2-2abcd+b^2d^2+a^2d^2+2abcd+b^2c^2$$

$$=a^2\left(c^2+d^2\right)+b^2\left(c^2+d^2\right)$$

$$=N(a+bi)\cdot N(c+di)$$

$$=N(\alpha)\cdot N(\beta)$$

4) a) $\overline{\alpha\beta}=\overline{(a+bi)(c+di)}=\overline{(ac+adi+bci-bd)}$

$$=\overline{(ac-bd)+(ad+bc)i}$$

$$=(ac-bd)-(ad+bc)i$$

$$=ac-bd-adi-bci$$

$$=a(c-di)-bi(c-di)$$

$$=(a-bi)(c-di) \quad =\overline{(a+bi)}\,\overline{(c+di)}=\bar{\alpha}\bar{\beta}$$

b) $\overline{(\alpha+\beta)}=\overline{(a+bi+c+di)}$

$$=\overline{(a+c+(b+d)i)} \quad =a+c-(b+d)i$$

$$=a+c-bi-di$$

$$= (a - bi) + (c - di)$$
$$= \overline{(a + bi)} + \overline{(c + di)} = \overline{\alpha} + \overline{\beta}$$

Tanım 2.3.2. $\forall \alpha \in \mathbb{Z}[i]$ için, $u \mid \alpha$ olacak şekilde bir u tamsayısı varsa buna $\mathbb{Z}[i]$ *nin bir tersinir elemanı* denir.

Önerme 2.3.2. $\alpha \in \mathbb{Z}[i]$ *nin tersinir olması için gerek ve yeter şart* $N(\alpha) = 1$ *olmasıdır. Şu halde tersinir elamanlar* ∓ 1 , $\mp i$ *lerdir* (Çallıalp 1999).

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

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

Tersine olarak, $\alpha = a + bi \in \mathbb{Z}[i]$ için, $N(\alpha) = 1 = \alpha \cdot \overline{\alpha}$ ise,

$\frac{1}{\alpha} = \overline{\alpha} = a - bi \in \mathbb{Z}[i]$ bulunur.

$N(\alpha) = a^2 + b^2 = 1 \Leftrightarrow a = \mp 1$, $b = 0$ veya $a = 0$, b= ∓ 1 anlamını taşıdığından $\mathbb{Z}[i]$ deki tersinir elemanların ∓ 1 , $\mp i$ olduğu anlaşılır.

Tanım 2.3.3. u , $\mathbb{Z}[i]$ nin herhangi bir tersinir elemanı olmak üzere, herhangi $\alpha, \beta \in \mathbb{Z}[i]$ elemanları için $\alpha = u \cdot \beta$ eşitliği geçerli ise α ve β elemanlarına *ilgili elemanlar* denir ve bu durum $\alpha \approx \beta$ şeklinde gösterilir.

Tanım 2.3.4. $\alpha \in \mathbb{Z}[i]$ elemanına eğer α nın $\mathbb{Z}[i]$ deki her böleni ya kendisinin bir ilgilisi yada bir tersinir eleman ise *indirgenemez* denir.

Tanım 2.3.5. $\mathbb{Z}[i]$ nin tersinir olmayan sıfırdan farklı bir π tamsayısına; herhangi $\alpha, \beta \in \mathbb{Z}[i]$ tamsayıları için, $\pi \mid \alpha\beta$ olması ya $\pi \mid \alpha$ veya $\pi \mid \beta$ olmasını gerektiriyorsa *asal eleman* denir.

Not 2.3.1. Bundan sonra $\mathbb{Z}$ nin asallarına rasyonel asal diyeceğiz.

Teorem 2.3.1. *$\mathbb{Z}[i]$ nin, 0 ve tersinir olmayan her elemanı sonlu sayıda indirgenemez elemanlarının çarpımı biçimindedir.*

Tanım 2.3.6. Bir $\mathbb{Z}[i]$ halkasına, her $\alpha \in \mathbb{Z}[i]$ tamsayısının sonlu sayıda indirgenemez elemanların çarpımı olarak temsili, çarpanlarının sırasının ve indirgenemez elemanlarının ilgilileri ile değişimi dışında tek türlü ise, *tek çarpanlama bölgesi* denir.

Teorem 2.3.2. *Bir bölgede çarpanlara ayrılışın tek olmasının gerek ve yeter koşulu her indirgenemez elemanın asal olmasıdır* (Şenay 2007).

Not 1.3.2. Yukarıdaki teoreme göre $\mathbb{Z}[i]$ nin her indirgenemez elemanı aynı zamanda bir asal elemandır.

Tanım 2.3.7. İkisi birden sıfır olmayan $\alpha, \beta \in \mathbb{Z}[i]$ elemanları için aşağıdaki iki koşulu sağlayan bir $\delta \in \mathbb{Z}[i]$ tamsayısına α, β tamsayılarının *en büyük ortak böleni* denir.

(1) $\delta | \alpha$ ve $\delta | \beta$,

(2) α, β nın her δ_1 ortak böleni için $\delta_1 | \delta$.

Not 2.3.3. Herhangi $\alpha, \beta \in \mathbb{Z}[i]$ tamsayılarının (eğer mevcutsa) bir en büyük ortak böleni ile ilgili olan tamsayının da α, β nın keza bir en büyük ortak böleni olduğuna ilgi çekilmelidir. Böylece α, β nın yukarıdaki koşulları gerçekleyen bir en büyük ortak böleninin tek biçimde belirtilmediği açık olup, bunu (α, β) ile göstereceğiz. O halde ilgili olanları dışında (α, β) tek bir biçimde belirtilmiştir.

Teorem 2.3.3. *Eğer $\alpha, \beta \in \mathbb{Z}[i]$ nin en büyük ortak böleni δ ise, herhangi $\lambda, \mu \in \mathbb{Z}[i]$ tamsayıları için $\delta = \lambda\alpha + \mu\beta$ olur* (Flanders 1985).

İspat. Verilen $\alpha, \beta \in \mathbb{Z}[i]$ tamsayıları ile $\mathbb{Z}[i]$ halkasındaki bütün tamsayı değerleri serbestçe alabilen λ, μ sayıları için $|N(\alpha\lambda + \beta\mu)|$ biçimindeki pozitif tamsayıların

oluşturduğu cümleyi göz önüne alalım. İyi sıralama ilkesine göre bu cümlenin bir en küçük $0<|N(\delta_1)|$ elemanı vardır. Burada $\lambda,\mu\in\mathbb{Z}[i]$ olmak üzere $\delta_1=\alpha\lambda+\beta\mu$ olduğuna ilgi çekilmelidir. Bölünebilmenin lineerlik özeliği gereği α ve β nın her $2=(a+bi)(c+di)$ ortak böleni için $\rho|\delta_1$ olur. Bundan başka $\delta_1|\alpha$ ve $\delta_1|\beta$ dır. Gerçekten böyle olmasaydı $\alpha=\delta_1\kappa+\delta_2$ ve $0\le|N(\delta_2)|<|N(\delta_1)|$ olacak biçimde $\delta_2,\kappa\in\mathbb{Z}[i]$ elemanları bulunacaktı. Böylece $\delta_1=\alpha\lambda+\beta\mu$ ve $\alpha=\delta_1\kappa+\delta_2$ eşitliklerinden $\delta_2=(1-\lambda\kappa)\alpha+(-\kappa\mu)\beta$ bulunur ki, bu δ_1 in $0<|N(\delta_1)|$ koşulu ile $\mathbb{Z}[i]$ nin en küçük elemanı olduğu kabulü ile çelişir. O halde π ve sonuçta $\delta_2=0$ olur. Benzer biçimde $u=-i\Rightarrow\pi=x+yi=-i\overline{\pi}=-y-xi\Rightarrow x=-y\Rightarrow p=2x^2$ olduğu da gösterilir. Öte yandan $\alpha,\beta\in\mathbb{Z}[i]$ nin en büyük ortak böleni δ olduğundan $\alpha=\delta\tau$ ve $\beta=\delta\omega$ olacak biçimde $\tau,\omega\in\mathbb{Z}[i]$ sayıları vardır. Buradan

$$\delta_1=\lambda\alpha+\mu\beta=\lambda\tau\delta+\mu\omega\delta=(\lambda\tau+\mu\omega)\delta,$$

ve sonuçta $\delta|\delta_1$ ayrıca δ hipoteze göre $\alpha,\beta\in\mathbb{Z}[i]$ nin en büyük ortak böleni olduğundan tanım gereği $\delta_1|\delta$ elde edilir ki, δ ve δ_1 ilgili ve sonuçta Tanım 2.3.7. gereği $\delta\in\mathbb{Z}[i]$ α,β nın en büyük ortak böleni olur.

Not 2.3.4. Gauss tamsayılar halkasının bir Öklid bölgesi olduğunu göstermek için öncelikle $\mathbb{Z}[i]$ de kalanlı bölme teoreminin geçerli olup olmadığını inceleyelim.

Teorem 2.3.4. (**$\mathbb{Z}[i]$ de Kalanlı Bölme Teoremi**) *$\forall\alpha,\beta\in\mathbb{Z}[i]$ ve $\beta\neq0$ için, $\alpha=\beta\gamma+\delta$ olacak şekilde $\exists\gamma,\delta\in\mathbb{Z}[i]$ ve $N(\alpha)<N(\beta)$ dır* (Flanders 1985).

İspat: Kompleks düzlemi, köşelerinin koordinatları tamsayılar olan karelere ayıralım. Böylece herhangi bir kompleks sayı, Bu karelerden birinin üzerine veya içine düşer. Ayrıca, karelerin köşeleri de $\mathbb{Z}[i]$ nin elemanlarıdırlar. $\alpha,\beta\in\mathbb{Z}[i],\beta\neq0$ ise $\frac{\alpha}{\beta}$ sayısının üzerine veya içine düştüğü kareyi ve $\frac{\alpha}{\beta}$ ya en yakın olan bu karenin γ köşesini düşünelim. Açıktır ki, $\frac{\alpha}{\beta}$ nın γ ya olan uzaklığı, karenin köşe uzunluğu olan $\sqrt{2}$ nin yarısından küçük veya eşit olur. Şu halde,

$$\left|\frac{\alpha}{\beta}-\gamma\right| \le \frac{\sqrt{2}}{2} \Rightarrow \left|\frac{\alpha}{\beta}-\gamma\right|^2 \le \frac{1}{2} < 1$$

Buradan $\alpha = \beta\gamma + \delta$ elde edilir.

Tanım 2.3.8. Eğer $\mathbb{Z}[i]$ halkasının $\alpha \neq 0$ ve β gibi herhangi elemanları için $\beta = \alpha\kappa + \rho$ ve $0 \le N(\rho) < N(\alpha)$ olacak biçimde $\kappa, \rho \in \mathbb{Z}[i]$ tamsayıları varsa $\mathbb{Q}(\sqrt{-1})$ cismine bir *Öklid Bölgesi* veya tam olarak *norm için Öklid Bölgesi* denir.

Teorem 2.3.5. $\mathbb{Z}[i]$ *bir Öklid bölgesidir* (Şenay 2007).

$\mathbb{Z}[i]$ nin bir Öklid bölgesi olduğunu aşağıdaki gözlemle de görebiliriz.

Gözlem: $\alpha = a + bi \in \mathbb{Z}[i]$ ve sıfırdan farklı $\gamma = c + di \in \mathbb{Z}[i]$ olmak üzere, $\frac{\alpha}{\gamma} = r + si$ olacak şekilde $r, s \in \mathbb{R}$ olsun. $|r-m| \le \frac{1}{2}$ ve $|s-n| \le \frac{1}{2}$ olacak şekilde $m, n \in \mathbb{Z}$ alarak, $\delta = (m+ni) \in \mathbb{Z}[i]$ elemanı oluşturalım. Buradan,

$$N(r+si-m-ni)$$

$$= N(r-m+(s-n)i)$$

$p = \alpha - \gamma\delta$ olsun. $p = a+bi-(c+di)\cdot(m+ni)$

$$= a+bi-(cm+cni+dmi-dn)$$

$$= a+bi-cm-cni-dmi+dn$$

$$= a-cm+dn+(b-cn-dm)i \in \mathbb{Z}[i] \text{ ve,}$$

Ya $p = 0$ ya da $N(p) = N\left(\gamma\left(\frac{\alpha}{\gamma}-\gamma\right)\right)$

$$= N(\gamma)\cdot N\left(\frac{\alpha}{\gamma}-\gamma\right)$$

$$\le \frac{1}{2}N(\gamma) < N(\gamma)$$

O halde $\mathbb{Z}[i]$ bir Öklid bölgesidir.

Tanım 2.3.9. Bir $\mathbb{Z}[i]$ Öklid bölgesinde herhangi α,β tamsayılarının en büyük ortak böleni $\mathbb{Z}[i]$ nın tersinir bir elemanı ise α,β tamsayılarına *aralarında asal* denir.

Not 2.3.5. Bir en büyük ortak bölenle ilgili olan herhangi bir tamsayı da en büyük ortak bölen ve 1 herhangi bir tersinir elemanla ilgili olduğundan α,β aralarında asal ise $(\alpha,\beta)=1$ kabul edebiliriz.

Sonuç 2.3.1. *Eğer* $(\alpha,\beta)=1$ *ise,* $\lambda\alpha+\mu\beta=1$ *olacak şekilde* $\lambda,\mu\in\mathbb{Z}[i]$ *tamsayıları vardır.*

Şimdi her Öklid bölgesinin bir tek çarpanlama bölgesi olduğunu gösterebiliriz.

Teorem 2.3.6. *Her Öklid bölgesi bir tek çarpanlama bölgesidir* (Şenay 2007).

İspat. Teorem 2.3.2. gereği $\mathbb{Z}[i]$ nin her indirgenemez elemanının bir asal eleman olduğunu kanıtlamamız yeterlidir. Buna göre π, $\mathbb{Z}[i]$ nin indirgenemez bir elemanı olmak üzere herhangi $\alpha,\beta\in\mathbb{Z}[i]$ için $\pi\mid\alpha\beta$ ancak $\pi\nmid\alpha$ olduğunu varsayalım. O zaman $(\alpha,\pi)=1$ ve Sonuç 2.3.1. e göre $\lambda\alpha+\mu\pi=1$ olacak şekilde $\lambda,\mu\in\mathbb{Z}[i]$ tamsayıları vardır. Şimdi bu eşitliğin her iki yanını β ile çarparsak, $\lambda\alpha\beta+\mu\beta\pi=\beta$ bulunur. Kabulümüz gereği $\pi\mid\alpha\beta$ ve açık olarak $\pi\mid\mu\beta\pi$ olduğundan bölünebilmenin lineerlik özeliğine göre $\pi\mid\beta$ olur.

Sonuç 2.3.2. *Her Öklid bölgesi bir tek çarpanlama bölgesi olduğundan* $\mathbb{Z}[i]$ *bir tek çarpanlama bölgesidir.*

Önerme 2.3.3. $\pi\in\mathbb{Z}[i]$ *ve* $N(\pi)$ *bir rasyonel asal ise* π *asal Gauss tamsayısıdır* (Çallıalp 1990).

Önerme 2.3.4. π *bir Gauss asalı olsun. O halde* $\pi\mid p$ *olacak şekilde bir tek* p rasyonel *asalı vardır. Üstelik ya* $N(\pi)=p$ yada $N(\pi)=p^2$ *dır* (Flanders 1985).

Önerme 2.3.5. π *gibi bir Gauss asalı farklı iki rasyonel asalı bölmez* (Şenay 2007).

Teorem 2.3.7. *p asal tamsayısının* $\mathbb{Z}[i]$*de çarpanlara ayrılışı şu şekildedir.*

1) $p=2\Rightarrow\pi=1+i\in\mathbb{Z}[i]$ *için* $p=-i\pi^2$ *ve* $N(\pi)=2$ *dir.*

2) $p\equiv 3\pmod 4$ *ise,* $p=\pi$ *asal Gauss tamsayıdır ve* $N(\pi)=p^2$ *dir.*

3) $p\equiv 1\pmod 4$ *ise,* π *ve* $\overline{\pi}$ *asal Gauss tamsayıları olmak üzere* $p=\pi\cdot\overline{\pi}$ *ve* $N(\pi)=N(\overline{\pi})=p$ *dir.* (Çallıalp 1990)

İspat:

1) $p=2=(1+i)\cdot(1-i)=i\cdot(1-i)^2$ ve $N(1-i)=2$ olduğundan $1-i$ bir asal Gauss tamsayısıdır. 2 asal tamsayısı $\mathbb{Z}[i]$ de (ilgililik düşünülmeden) bir asal Gauss tamsayısının karesidir. Buna 2, $\mathbb{Z}[i]$ *de dallanır* da denir.

2) $p\equiv 3\pmod 4$ olsun. $\pi\mid p\Rightarrow p=\pi\cdot\alpha,\exists\alpha\in\mathbb{Z}[i]$ ve $N(p)=p^2=N(\alpha)N(\pi)$ ve $N(\pi)=p$ veya $N(\pi)=p^2$ olur.

$\pi=x+yi\ \ (x,y\in\mathbb{Z})\Rightarrow N(\pi)=x^2+y^2\equiv 0$, 1 veya 2 $(\mathrm{mod}\ 4)$ olabilir. Şu halde $N(\pi)=p$ olamaz. $N(\pi)=x^2+y^2=p^2$ dir.

$p^2=N(p)=N(\pi)N(\alpha)=p^2N(\alpha)\Rightarrow N(\alpha)=1$ ise, α tersinir olacağından $p\approx\pi$ olduğu anlaşılır. Yani $p\equiv 3\pmod 4$ rasyonel asalı, $\mathbb{Z}[i]$ de de asal kalır.

3) $p\equiv 1\pmod 4$ olsun. p rasyonel asalı için $x^2\equiv -1\pmod p$ nin çözümü vardır. Bir çözüm z ise, $p\mid z^2+1$, $\pi\mid p$ ve π asal Gauss tamsayısı ise $\pi\mid z^2+1=(z+i)(z-i)$ olur. $\mathbb{Z}[i]$ de asal eleman tanımından $\pi\mid z+i$ veya $\pi\mid z-i$ bulunur. Fakat $p\nmid z+i$ ve $p\nmid z-i$ dir. Çünkü $\frac{z}{p}\mp\frac{i}{p}\notin\mathbb{Z}[i]$ dir. Buradan π ile p nin ilgili olmadıkları anlaşılır. Şu halde $N(\pi)\neq N(p)=p^2$ ve $\pi\mid p\Rightarrow N(p)\mid p^2$ olmasından, $N(\pi)=p$ bulunur. Böylece $p\equiv 1\pmod 4$ ise, $p=N(\pi)=\pi\cdot\overline{\pi}$ dir. p nin iki asal böleni π ile $\overline{\pi}$ nin ilgili olmadıklarını görelim.

$\pi = x + yi$, $N(\pi) = x^2 + y^2 = p$ olsun. $u = \mp 1, \mp i$ tersinir elemanlar olmak üzere $\pi = u \cdot \overline{\pi}$ olsa idi;

$$u = 1 \Rightarrow \pi = x + yi = \overline{\pi} = x - yi \Rightarrow y = 0 \Rightarrow p = x^2$$

$$u = -1 \Rightarrow \pi = x + yi = -\overline{\pi} = -x + yi \Rightarrow x = 0 \Rightarrow p = y^2$$

$$u = i \Rightarrow \pi = x + yi = i\overline{\pi} = y + xi \Rightarrow x = y \Rightarrow p = 2x^2$$

$$u = -i \Rightarrow \pi = x + yi = -i\overline{\pi} = -y - xi \Rightarrow x = -y \Rightarrow p = 2x^2$$

Çelişkilerini verirdi. Çünkü p tek, asal tamsayıdır. Buradan p nin iki farklı ilgili olmayan asal Gauss tamsayısının çarpımı olarak ayrıştığı anlaşılır. Yukarıdaki bu tespitlerimiz aşağıdaki teoremin ispatını verir.

Teorem 2.3.8. *Bir π tamsayısının bir Gauss asalı olmasının gerek ve yeter koşul;*

1) *π ya $1-i$ dir ya da bununla ilgilidir.*

2) *π ya $4k+3$ biçiminde rasyonel asaldır veya bu biçimde bir asalla ilgilidir.*

3) *$4k+1$ biçimindeki herhangi bir p rasyonel asalı için $N(\pi) = p$ dir.*

İfadelerinin geçerli olmasıdır (Şenay 2007).

3. TEORİK ESASLAR

3.1. Dördüncü Dereceden Kalanlar

Gauss 1832'de 4. Dereceden kalanlar teoremini ispatsız olarak kurdu. Sonradan 1844 yılında Eisenstein, Jacobi ve Gauss toplamlarını kullanarak pek çok ispatını yaptı. Temel fikir 3. Dereceden kalanlar ile aynı olmasına rağmen daha zordur. Gauss toplamlarını kalanlar teoreminde kullanma fikri Gauss'a aittir ki bunu 2. Dereceden kalanlar teoreminin altıncı ispatını yaparken kullandı. (Ireland ve Rosen 1990)

$\mathbb{Z}[i]$, Gauss tamsayıları halkası olmak üzere, eğer $\alpha \in \mathbb{Z}[i]$ ise (α), α tarafından üretilen bir esas idealdir. $\mathbb{Z}[i]$ de kalanlı bölme teoremi geçerli olduğundan $\mathbb{Z}[i]$ bir öklit halkasıdır. Böylece eğer π bir indirgenemez ve $\pi \mid \alpha\beta$ ise ya $\pi \mid \alpha$ yada $\pi \mid \beta$ dır. Eğer $N(\alpha) = \alpha\bar{\alpha}$, α nın normu ise; $N(\alpha) = 1$ olması için gerek ve yeter şart α nın tersinir olmasıdır.

Lemma 3.1.1. *Eğer π bir indirgenemez ise, $\pi \mid p$ olacak şekilde bir $p \in \mathbb{Z}$ rasyonel asalı vardır* (Ireland ve Rosen 1990).

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

Böylece indirgenemezler, $\mathbb{Z}$ nin tüm asallarının $\mathbb{Z}[i]$ de çarpanlarına ayrılması ile bulunur. Buna göre aşağıdaki lemma kullanışlıdır.

Lemma 3.1.2. *Eğer $\alpha \in \mathbb{Z}[i]$ ve $N(\alpha)$ asalsa, α indirgenemezdir* (Ireland ve Rosen 1990).

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

Lemma 3.1.3. $1+i$ *indirgenemezdir ve 2 nin $\mathbb{Z}[i]$ deki asal çarpanlarına ayrılışı $2 = -i(1+i)^2$ şeklindedir* (Ireland ve Rosen 1990).

İspat: $N(1+i)=2$ ve 2 bir asaldır. O halde $1+i$ indirgenemezdir. (Lemma 3.1.2. gereği)

Lemma 3.1.4. *Eğer* $q \equiv 3 \pmod 4$ $\mathbb{Z}$ *de bir asalsa, o zaman* q, $\mathbb{Z}[i]$*nin bir indirgenemez elemanıdır* (Ireland ve Rosen 1990).

İspat: q, $\mathbb{Z}[i]$de bir indirgenemez olmasın. O halde $N(\alpha)>1$ ve $N(\beta)>1$ olacak şekilde $q=\alpha\beta$ yazabiliriz. Her iki tarafında normlarını alırsak, $q^2=N(\alpha)N(\beta)$ Buradan q bir asal sayı olduğundan $q=N(\alpha)$ olur. Eğer $\alpha=a+bi$ $(a,b\in\mathbb{Z})$ ise, $q=N(\alpha)=a^2+b^2$ olur. Oysa, bu durum $4k+3$ biçimindeki asalların iki kare toplamı şeklinde yazılamayacağından bir çelişkidir. O halde, q indirgenemezdir.

Lemma 3.1.5. *Eğer* p *bir asal ve* $p \equiv 1 \pmod 4$ *ise,* $p=\pi\overline{\pi}$ *olacak şekilde bir* π *indirgenemez elemanı vardır ve üstelik* $(\pi)\neq(\overline{\pi})$ *dir* (Ireland ve Rosen 1990).

İspat: $p \equiv 1 \pmod 4$ olduğundan, $a^2 \equiv -1 \pmod p$ olacak şekilde bir a tamsayısı vardır. Böylece, $p \mid a^2+1=(a+i)(a-i)$ olur. Eğer, p indirgenemez olsaydı, $p \mid a+i$ olurdu. Böylece, $p=\alpha\beta$, $N(\alpha)>1, N(\beta)>1$ dır. Norm alarak, $p=N(\alpha)$ sonucuna varırız. $N(\alpha)$ asal olduğundan Lemma 3.1.2. yardımıyla α indirgenemezdir. Buradan, $(\alpha)\neq(\overline{\alpha})$ olduğu apaçıktır.

Tanım 3.1.1. Tersinir olmayan bir $\alpha\in\mathbb{Z}[i]$ için , eğer $\alpha \equiv 1 \left(\mathrm{mod}(1+i)^3\right)$ ise α ya $\mathbb{Z}[i]$ *nin bir primary elemanı* denir. Eğer $\alpha, \mathbb{Z}[i]$ de primary ise, $\alpha \equiv 1 \pmod{2+2i}$ olduğuna ilgi çekilmelidir.

NOT 3.1.1. Yukardaki tanıma göre $1+i$ ile ilgili olmayan elemanların primary olacağını söyleyebiliriz.

Lemma 3.1.6. $\mathbb{Z}[i]$ *de tersinir olmayan bir* $\alpha = a+bi$ $(a,b \in \mathbb{Z})$ *elemanı primary ise,*

$$a \equiv 1 \pmod 4,\ b \equiv 0 \pmod 4$$

veya,

$$a \equiv 3 \pmod 4,\ b \equiv 2 \pmod 4$$

dır (Ireland ve Rosen 1990).

İspat: $(1+i)^3 = 2i(1+i)$ olduğundan $a+bi$ nin tek olması için gerek ve yeter şart

$$\frac{(a-1)+bi}{2+2i} = \frac{a+b-1}{4} + \frac{b-a+1}{4} i \in \mathbb{Z}[i] \text{ dir.}$$

Bu durum, $a+b \equiv 1 \pmod 4$ ve $a-b \equiv 1 \pmod 4$ kongrüanslarına eşittir. Buradan, Kongüanslık özelliklerinden,

$$\begin{aligned} & a+b \equiv 1 \pmod 4 \\ + \ & a-b \equiv 1 \pmod 4 \\ \hline & 2a \equiv 2 \pmod 4 \Rightarrow a \equiv 1 \pmod 4, b \equiv 0 \pmod 4 \\ & \Rightarrow a \equiv 3 \pmod 4, b \equiv 2 \pmod 4 \end{aligned}$$

NOT 3.1.2. $\mathbb{Z}[i]$ de tersinir olmayan herhangi bir $\alpha \equiv 1 \pmod 4$ şeklindeki elemanı primary dir. Üstelik, eğer α primary ise, NOT 3.1.1. e göre, $(1+i) \nmid \alpha$. Eğer $q, q \equiv 3 \pmod 4$ olacak şekilde bir rasyonel asalsa, $-q$ bir primary indirgenemezdir. $p \equiv 1 \pmod 4$ asallarından ortaya çıkan indirgenemezler için aşağıdaki sonuç geçerlidir.

Lemma 3.1.7. $\alpha \in \mathbb{Z}[i]$ *tersinir olmayan bir eleman ve* $(1+i) \nmid \alpha$ *olsun. O taktirde* $u\alpha$ *primary olacak şekilde bir tek* u *tersinir elemanı vardır* (Ireland ve Rosen 1990).

İspat: a bir tek ve b bir çift sayı olmak üzere, $\varepsilon\alpha = a+bi$ olacak şekilde bir ε elemanı vardır. Gerekirse, -1 ile çarparak, Lemma 3.1.6. α nın bir primary ilgilisi olduğunu gösterir Eğer $u_1\alpha$ ve $u_2\alpha$ olacak şekilde u_1 ve u_2 tersinir elemanlar ise, $(1+i) \nmid \alpha$ olduğundan,

$u_1 \equiv u_2 \left(\mathrm{mod}(1+i)^3\right)$ olur. Buradan, $u_1 - u_2 \left|(1+i)^3\right.$ olup buradan $u_1 = u_2$ olur.

Lemma 3.1.8. $\mathbb{Z}[i]$ *nin bir primary elemanı, primary indirgenemezlerin çarpımı şeklinde yazılabilir* (Ireland ve Rosen 1990).

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

Lemma 3.1.9. *Eğer* $\pi \in \mathbb{Z}[i]$ *bir primary asalsa, ya* $\pi \equiv 1(\mathrm{mod}\,4)$ *yada* $\pi \equiv 3+2i(\mathrm{mod}\,4)$ *tür.*

İspat: Eğer $\pi \in \mathbb{Z}[i]$ bir primary ise, $\pi = a+bi$ olmak üzere, Lemma 3.1.6. dan,

i) $a \equiv 1(\mathrm{mod}\,4)$ için kongrüanslık tanımı gereği $4k = a-1$ olacak şekilde bir $k \in \mathbb{Z}$ vardır.

$b \equiv 0(\mathrm{mod}\,4)$ için kongrüanslık tanımı gereği $4t = b$ olacak şekilde bir $t \in \mathbb{Z}$ vardır.

$$\pi = a+bi = (4k+1)+(4t)i$$
$$= 4(k+ti)+1$$

ise, kongrüanslık tanımından $\pi \equiv 1(\mathrm{mod}\,4)$ tür.

ii) $a \equiv 3(\mathrm{mod}\,4)$ için kongrüanslık tanımı gereği $4m = a-3$ olacak şekilde $m \in \mathbb{Z}$ vardır.

$b \equiv 2(\mathrm{mod}\,4)$ için kongrüanslık tanımı gereği $4n = b-2$ olacak şekilde $n \in \mathbb{Z}$ vardır.

$$\pi = a+bi = (4m+3)+(4n+2)i$$
$$= 4(m+ni)+3+2i$$

ise, kongrüanslık tanımından $\pi \equiv 3+2i(\mathrm{mod}\,4)$ tür.

3.2. 4. Dereceden Kalan Sembolü

Önerme 3.2.1. $\pi \in \mathbb{Z}[i]$ *indirgenemez olmak üzere,* $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ *kalan sınıflar halkası,* $N(\pi)$ *elemanlı sonlu bir cisimdir* (Ireland ve Rosen).

İspat: Öncelikle $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ nin bir cisim olduğunu gösterelim. $\alpha \not\equiv 0 \pmod{\pi}$ olacak şekilde $\alpha \in \mathbb{Z}[i]$ olsun. Buradan, $\beta, \gamma \in \mathbb{Z}[i]$ olmak üzere $(\beta, \gamma) = 1$ ise, $\beta\alpha + \gamma\pi = 1$ olacak şekilde $\alpha, \pi \in \mathbb{Z}[i]$ olacaktır. Böylece $\beta\alpha \equiv 1 \pmod{\pi}$, α nın kalan sınıfının $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ de bir tersinir olduğunu gösterir. Bu da $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ nin bir cisim olduğunu gösterir.

$\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ nin $N(\pi)$ tane elemanı olduğunu göstermek için, varsayalım ki $\pi = q$, 4 modülüne göre 3 e kongrüent olan bir rasyonel asal olsun. İddia ediyoruz ki, $\{a + bi \mid 0 \le a < q$ ve $0 \le b < q\}$ bütün kalan sınıfları temsil eden bir kümedir. Bu da, $\mathbb{Z}[i]/q\mathbb{Z}[i]$ nin $q^2 = N(q)$ tane elemanı olduğunu gösterecektir. $\mu = m + ni \in \mathbb{Z}[i], (m, n \in \mathbb{Z})$ olsun. O halde, $m = qs + a$ ve $n = qt + b$ $(s, t, a, b \in \mathbb{Z})$ ve $(0 \le a\ ,\ b < q)$ olsun.

$$\mu = (qs + a) + (qt + b)i = qs + a + qti + bi = a + bi + q(s + ti)$$

olup,

$$\mu \equiv a + bi \pmod{q}$$

elde edilir. Bundan sonra,

Şimdi $a + bi \equiv a' + b'i \pmod{q}$ $(0 \le a, b, a', b' < q)$ olduğunu düşünelim. O halde, $(a - a')/q + ((b - b')/q)i \in \mathbb{Z}[i]$ demek $(a - a')/q, (b - b')/q \in \mathbb{Z}$ demektir. Bu ise ancak $a = a'$ ve $b = b'$ olduğunda olur.

Artık $p \equiv 1 \pmod{4}$ nin rasyonel asal ve $\pi\overline{\pi} = N(\pi) = p$ olduğunu düşünelim. İddia ediyoruz ki, $\{0, 1, ..., p - 1\}$ tüm kalanlar sınıfını temsil eden bir kümedir. Bu bize, $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ nin $p = N(\pi)$ tane elemanı olduğunu gösterecek.

$\pi = a + bi$ olsun. $p = (a+bi)(a-bi) = a^2 + b^2$ olduğundan $p \nmid b$ dır. $\mu = m + ni$ $(\text{m,n} \in \mathbb{Z})$ olsun. $cb \equiv n \pmod{p}$ olacak şekilde bir c tamsayısı vardır. O halde $\mu - c\pi \equiv m - ca \pmod{p}$ ve buradan, $\mu \equiv m - ca \pmod{\pi}$, $\mathbb{Z}[i]$nin her elemanı π modülüne göre bir tamsayıya kongrüenttir. Eğer $l \in \mathbb{Z}$ ise, $r, s \in \mathbb{Z}$ ve $0 \le r < p$ olmak üzere, $l = sp + r$ dir. Böylece, $l \equiv r \pmod{p}$ dir ve buradan $l \equiv r \pmod{\pi}$ sonucu ortaya çıkar. $\mathbb{Z}[i]$nin her elemanının π modülüne göre $\{0, 1, ..., p-1\}$ kümesinin elemanlarından birine kongrüent olduğunu daha önce gösterdik. Eğer $r \equiv r' \pmod{\pi}$ $(r, r' \in \mathbb{Z}$ ve $0 \le r$, $r' < p)$ ise, $r - r' \equiv \pi\gamma$ ve $(r-r')^2 = pN(\gamma)$ demek $p \mid r - r'$ demektir. Böylece $r = r'$ olur.

$p \equiv 2 \pmod{4}$ ise p asalı sadece 2 olabilir. $p = 2$ için, $N(\pi) = 2$ olan $\pi = a + bi$ $(a, b \in \mathbb{Z})$ vardır. Buradan $a^2 + b^2 = 2$ olduğu görülür. Bu eşitlik ancak ve ancak $a = \mp 1, b = \mp 1$ olması gerekir. Gauss tamsayılarında ilgililik düşünüldüğünde, π nin $1+i$ veya $1-i$ olması ile mümkündür. O halde $\{1+i, 1-i\}$ kümesi $N(\pi) = 2$ eşitliğini sağlayan tüm kalan sınıflarını temsil eden kümedir ve $N(\pi) = 2$ tane elemanı vardır.

Sonuç 3.2.1. *Eğer* $\pi \nmid \alpha$ *ise,* $\alpha^{N(\pi)-1} \equiv 1 \pmod{\pi}$ *dir* (Şenay 2007).

İspat: Bir π Gauss asalının bir tek p rasyonel asalını böldüğünü hatırlatarak $\pi \mid p$ olacak şekildeki p rasyonel asalını göz önüne alalım. Bu durumda, Teorem 2.3.8. e göre üç durum ayırt edebiliriz.

1. durum: $p = 4n + 3$ olsun. O zaman $N(\pi) = x^2 + y^2 = p^2$ olup, ispat için $\alpha^{p^2-1} \equiv 1 \pmod{\pi}$ veya bununla eş anlamda olan $\alpha^{p^2} \equiv \alpha \pmod{p}$ nin geçerli olduğunu göstermek yeterli olacaktır. Gerçekten bu son bağıntıdan $p \mid (\alpha^{p^2} - \alpha)$ ve $\pi \mid p$ olduğundan $\pi \mid \alpha(\alpha^{p^2-1} - 1)$ ve buradan da $\pi \nmid \alpha$ olduğunu göz önüne alarak $\pi \mid (\alpha^{p^2-1} - 1)$ elde edilecektir.

Şimdi $\alpha = x + yi$ olsun. Buradan $\alpha^p \equiv x^p + y^p i^p \pmod{p}$ yazılabilir. Kabulümüze göre p, $4n+3$ biçiminde olduğundan $i^p = -i$ dir. Ayrıca bu p asalı ve bir $a \in \mathbb{Z}$ için, $a^p \equiv a \pmod{p}$ olduğundan $x^p \equiv x \pmod{p}$ ve $y^p \equiv y \pmod{p}$ dir. Tüm bunlardan $\alpha^p \equiv x + yi \equiv \bar{\alpha} \pmod{p}$ elde ederiz. Benzer biçimde $\bar{\alpha} \equiv \alpha \pmod{p}$ dir. O halde iddia edildiği gibi $\alpha^{p^2} \equiv \bar{\alpha} \equiv \alpha \pmod{p}$ buluruz.

2. durum: $p \equiv 2 \pmod{p}$ olsun. Bu kabulle $p = 2$ ve Teorem 2.3.8. e göre π, $1+i$ ile ilgilidir. Böylece $\pi = 1+i$ olduğunu kabul edebiliriz. $N(\pi) = 2$ olduğundan şimdi $\alpha^{N(\pi)-1} \equiv \alpha \equiv 1 \pmod{\pi}$ ve basitçe $1+i$ ile α aralarında asal olduğunda $1+i$ nin $\alpha - 1$ i böldüğünü ispatlamalıyız. Teorem 2.3.8. e göre $1+i$ asal olduğundan $\alpha \in \mathbb{Z}[i]$ olduğunda $\beta = \alpha(\alpha-1)/1+i$ in de bir Gauss tamsayısı olduğunu göstermek yeterlidir. Buna göre $m, n \in \mathbb{Z}$ için, $\alpha = m + ni$ olsun. O zaman,

$$\beta = \frac{1}{2}\left\{\left(m^2 - m - n^2 - n + 2mn\right) + \left(-m^2 + m + n^2 - n + 2mn\right)i\right\}$$

bulunur. Ancak,

$$m^2 - m - n^2 - n + 2mn = m(m-1) - n(n-1) + 2mn,$$

ve

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

Sayılarının ikisi de çift olduğundan β bir Gauss tamsayısıdır.

3. durum: Şimdi $p = 4k+1$ olsun. Bu durumda $N(\pi) = x^2 + y^2 = p$ olup, $\alpha^{p-1} \equiv 1 \pmod{\pi}$ olduğunu göstermeliyiz. Böylece $\pi \mid p$ ve $(\alpha, \pi) = 1$ hipotezini göz önüne alarak $\alpha^p \equiv \alpha \pmod{p}$ olduğunu bilmek yeterlidir. Buna göre $\alpha = u + vi$ olsun. Şimdi 1. durumda olduğu gibi $\alpha^p \equiv u^p + v^p i^p \pmod{p}$ dir. Ancak $p = 4k+1$ biçiminde olduğundan $i^p = i$ ve $\alpha^p \equiv u + vi = \alpha \pmod{p}$ olur ki, bu da ispatı tamamlar.

Not 3.2.1. Eğer π nin normu 2 den farklı ise, o zaman $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ de $1, -1, -i$ ve $+i$ nin kalan sınıfları birbirlerinden farklıdır.

Gerçekten, $i \equiv 1 \pmod{\pi}$ olsun. Buradan $\pi \mid i-1$ olur ve Teorem 2.3.8. e göre $i-1$ bir asal olduğundan π ve $i-1$ ilgili olurlar. Böylece $N(\pi) = N(1-i) = 2$ olur ki bu durum π nin normunun 2 den farklı olması ile çelişir. Diğer durumlarda da aynı düşünce uygulanır. $\{1,-1,i,-i\}$ mertebesi 4 olan devirli bir grup olduğundan; 4, $(\mathbb{Z}[i]/\pi\mathbb{Z}[i])^*$ çarpımsal alt grubunun mertebesini böler. Bu da $4 \mid N(\pi)-1$ olduğunu gösterir.

Önerme 3.2.2. *Eğer* $\pi \nmid \alpha$, $(\pi) \neq (1+i)$ *ise,* $0 \leq j \leq 3$ *olacak şekilde bir tek* j *tamsayısı vardır. Yani,*

$$\alpha^{N(\pi)-1/4} \equiv i^j \pmod{\pi}$$

dır (Ireland ve Rosen 1990).

Not 3.2.2. Bu önermede $(\pi) \neq (1+i)$ hipotezi önemlidir. Gerçekten $(\pi) = (1+i)$ olsaydı, bunların normları aynı olacağından $1+i$ indirgenemez olup $N(1+i) = 2 = -i(1+i)^2$ asal çarpanlarına ayrılacaktı. Ancak π asal olduğundan bu durum çelişki olacaktı.

İspat: $(\pi) \neq (1+i)$, $\pi = a+bi$ $(a,b \in \mathbb{Z})$, $\mathbb{Z}[i]$de asal olsun. $N(\pi) = a^2+b^2 \neq N(1+i) = 2$ olduğundan πnin $4k+1$ biçiminde bir asal olduğunu göz önüne alırsak $N(\pi) = 3$ olması mümkün değildir. Zira 3, $4k+3$ biçiminde olup iki kare toplamı biçiminde olamaz. O halde $N(\pi)$nin değeri en az 4 olmak zorundadır. Öte yandan, $\pi \nmid \alpha$, $\alpha \in \mathbb{Z}[i]$ için, $\alpha^{N(\pi)-1} \equiv 1 \pmod{\pi}$ olup $\mathbb{Z}[i]$de $N(\pi) \neq 2$ koşulunu gerçekleyen bütün $4k+1$ biçimindeki asallar için $N(\pi) = p^2 = (4k+1)^2 = (4k)^2 + 8k + 1$ ise $N(\pi) - 1 = 4(4k^2+2k)$ ve sonuçta $4 \mid N(\pi)-1$ dir. Böylece Sonuç 2.2.1. den,

$$\alpha^{N(\pi)-1/4} \equiv 1 \pmod{\pi}$$

dir.

Gözlem: Şimdi $x^4 \equiv 1(\mathrm{mod}\,\pi)$ olduğunu göz önüne alalım. Buradan,

$$x^4 - 1 \equiv 0(\mathrm{mod}\,\pi),$$

$$(x^2 - 1)(x^2 + 1) \equiv 0(\mathrm{mod}\,\pi),$$

$$(x-1)(x+1)(x-i)(x+i) \equiv 0(\mathrm{mod}\,\pi)$$

dir. Buradan denklemin köklerinin Lagrange Teoremine göre, $+1, -1, +i, -i$ olduğu ortaya çıkar. Öte yandan, $\{+1, -1, +i, -i\}$ mertebesi 4 olan devirli bir grup olduğundan, $(\mathbb{Z}[i]/\pi\mathbb{Z}[i])^*$ çarpımsal alt grubunun mertebesini böler. Bu grubun mertebesi $N(\pi)-1$ olup, $4 \mid N(\pi)-1$ dir. Buradan, $\alpha^{(N(\pi)-1)/4}$ ün aynı zamanda $x^4 \equiv 1(\mathrm{mod}\,\pi)$ kongrüansının bir çözümü olduğu ortaya çıkar. Bu bir çözüm ise, $+1, -1, +i, -i$ birbirlerine kongrüent değildirler. Yani kalan sınıfları farklıdır. O halde,

$$\alpha^{N(\pi)-1/4} \equiv i^j\,(\mathrm{mod}\,\pi)$$

dir.

Tanım 3.2.1. Eğer π bir indirgenemez ise, $N(\pi) \neq 2$ olmak üzere, α nın 4.dereceden kalanı $\pi \nmid \alpha$ için, $\chi_\pi(\alpha) = i^j\ (0 \le j \le 3)$ olarak tanımlanır. Bu ise Legendre sembolünün 4. dereceden kalanlara doğal bir genişlemesidir. Özel olarak, eğer $\pi \mid \alpha$ ise $\chi_\pi(\alpha) = 0$ dır.

Not 3.2.3. Bazı matematikçiler bu durumu,

$$\left(\frac{\alpha}{\pi}\right)_4 = \begin{cases} 1, & \text{Eğer } x^4 \equiv \alpha(\mathrm{mod}\,\pi) \text{ çözülebilirse,} \\ -1, i, -i, & \text{diğer durumda.} \end{cases}$$

şeklinde gösterirler.

Şimdi 4. dereceden kalanlar ile ilgili Legendre Sembolünün özelliklerini verelim.

Önerme 3.2.3. *Eğer $\pi \nmid \alpha$ ise,*

1) $\chi_\pi(\alpha) = 1 \Leftrightarrow x^4 \equiv \alpha(\mathrm{mod}\,\pi)$ $\mathbb{Z}[i]$ *de bir çözümü vardır.*

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

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

4) *Eğer* π *primary bir indirgenemez ise,* $\left(\frac{-1}{\pi}\right)_4 = (-1)^{(a-1)/2}$.

$(\pi = a + bi$ olmak üzere$)$,

5) *Eğer* $\alpha \equiv \beta \pmod{\pi}$ *ise,* $\left(\frac{\alpha}{\pi}\right)_4 = \left(\frac{\beta}{\pi}\right)_4$,

6) *Eğer* $(\pi) = (\lambda)$ *ise,* $\left(\frac{\alpha}{\pi}\right)_4 = \left(\frac{\alpha}{\lambda}\right)_4$

dir.

İspat:

1) Önerme 2.1.2. ve dolayısıyla Sonuç 2.1.3. ten ispat tamamlanır.

2) $\chi_\pi(\alpha\beta) = \left(\frac{\alpha\beta}{\pi}\right)_4 \equiv (\alpha\beta)^{(N(\pi)-1/4)} \pmod{\pi}$

$\equiv \alpha^{(N(\pi)-1)/4} \beta^{(N(\pi)-1)/4} \pmod{\pi}$ Kongrüanslık özelliklerinden,

$\equiv \underbrace{\alpha^{(N(\pi)-1)/4} \pmod{\pi}}_{\left(\frac{\alpha}{\pi}\right)_4} \underbrace{\beta^{(N(\pi)-1)/4} \pmod{\pi}}_{\left(\frac{\beta}{\pi}\right)_4}$ Legendre sembolünden,

$\equiv \left(\frac{\alpha}{\pi}\right)_4 \left(\frac{\beta}{\pi}\right)_4$

dır.

3) $\alpha^{(N(\pi)-1)/4} \equiv \left(\frac{\alpha}{\pi}\right)_4 \pmod{\pi}$ ve π indirgenemez olduğundan, $\pi \mid p \Rightarrow \overline{\pi} \mid p$ dir. Yani π için geçerli olan $\overline{\pi}$ için de geçerlidir. O halde, $\overline{\alpha}^{(N(\overline{\pi})-1)/4} \equiv \left(\frac{\overline{\alpha}}{\overline{\pi}}\right)_4 \pmod{\overline{\pi}}$ yazılır.

Buradan,

$$\overline{\left(\frac{\alpha}{\pi}\right)_4} = \left(\frac{\overline{\alpha}}{\overline{\pi}}\right)_4$$

dır.

4) Lemma 3.1.6 kullanılarak ispat görülür.

5) $\alpha \equiv \beta \pmod{\pi}$ ise, kongrüanslık tanımından $\pi \mid (\alpha - \beta)$ dır. Buradan $\pi k = \alpha - \beta$ olacak şekilde bir $k \in \mathbb{Z}[i]$ vardır. Böylece, $\alpha = \pi k + \beta$ şeklinde yazılabilir.

$$\left(\frac{\alpha}{\pi}\right)_4 \equiv \alpha^{(N(\pi)-1)/4} \pmod{\pi}$$

olup,

$$\equiv \underbrace{(\pi k + \beta)}_{\alpha}^{(N(\pi)-1)/4} \pmod{\pi}$$

$\pi k + \beta \equiv \beta \pmod{\pi}$ olduğundan,

$$\equiv \beta^{(N(\pi)-1)/4} \pmod{\pi}$$

$$\equiv \left(\frac{\beta}{\pi}\right)_4$$

bulunur.

6) Eğer $(\pi) = (\lambda)$ ise, π ve λ ilgilidir. O zaman ilgilik tanımı gereği söz gelişi $\pi = \mp i\lambda$ veya $\pi = \mp 1\lambda$ dır. Bunun için Legendre sembolü tanımından,

$$\left(\frac{\alpha}{\pi}\right)_4 \equiv \alpha^{(N(\pi)-1)} \pmod{\pi}$$

$$\equiv \alpha^{(N(i\lambda)-1)} \pmod{i\lambda}$$

$$\equiv \alpha^{(N(\lambda)-1)} \pmod{\lambda}$$

$$= \left(\frac{\alpha}{\lambda}\right)_4$$

elde edilir.

Not 3.2.4. Legendre Sembolü $(\mathbb{Z}[i]/\pi\mathbb{Z}[i])^*$ den $\mathbb{C}^*$ a bir karakter verir. Böylece $(\mathbb{Z}[i]/\pi\mathbb{Z}[i])^*$ 4 eşit parçaya ayrılır. $p \equiv 1 \pmod{4}$ olduğunda $(\mathbb{Z}[i]/\pi\mathbb{Z}[i])^* \simeq (\mathbb{Z}/p\mathbb{Z})^*$ olur ve bu durum şu şekilde tanımlanır.

Eğer Legendre sembolü 1 e eşitse 4. dereceden kalanlar vardır. İkinci durumda, eğer Legendre sembolü -1 e eşitse 4. dereceden olmayan ikinci dereceden kalanlar vardır. Geri kalan son iki kısımda Legendre sembolünün $\mp i$ olduğu durumlar olup, 2. dereceden kalan olmayanları içerir.

Önerme 3.2.4. $q \equiv 3 \pmod 4$ *olacak şekilde* q *bir asal olsun. O halde* $a \in \mathbb{Z}, q \nmid a$ için $\left(\frac{a}{q}\right)_4 = 1$ *dir* (Ireland ve Rosen 1990).

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

$$\left(\frac{a}{q}\right)_4 = a^{(q^2-1)/4}$$

$$= \left(a^{(q-1)}\right)^{(q+1)/4}$$

Küçük Fermat Teoreminden, q asal ve $q \nmid a$ için, $a^{q-1} \equiv 1 \pmod q$ idi.

$$\left(\frac{a}{q}\right)_4 \equiv 1 \pmod q$$

4.dereceden kalan karakteri aşağıdaki gibi genelleştirilmiştir.

Tanım 3.2.2. $(1+i) \nmid \alpha$ olacak şekilde $\alpha \in \mathbb{Z}[i]$ de tersinir olmasın ve $\beta \in \mathbb{Z}[i]$ olsun. λ_i indirgenemez olmak üzere, $\alpha = \prod_i \lambda_i$ yazalım. Eğer $(\alpha, \beta) = 1$ ise, $\left(\frac{\beta}{\alpha}\right)_4 = \prod_i \left(\frac{\beta}{\lambda_i}\right)_4$ şeklinde tanımlanır. Önerme 3.2.3. (6) dan bunun iyi tanımlı olduğu görülür. (5) ten $\beta \equiv \gamma \pmod \alpha$ ise, $\left(\frac{\beta}{\alpha}\right)_4 = \left(\frac{\gamma}{\alpha}\right)_4$ olduğu görülür.

Önerme 3.2.5. $\alpha \in \mathbb{Z}$, $\alpha \neq 0$ *ve* $a \in \mathbb{Z}$ *tersinir olmayan bir tek sayı olsun. Eğer* $(a, \alpha) = 1$ *ise,* $\left(\frac{\alpha}{a}\right)_4 = 1$ *dir* (Ireland ve Rosen 1990).

İspat: $a > 0$ alalım. p_i ve q_i ler asal olmak üzere, $a \in \mathbb{Z}$, asalların çarpımı şeklinde yazılabileceğinden, $a = \prod p_i \prod q_i$ yazılabilir. Burada $p_i \equiv 1 \pmod 4, q_i \equiv 3 \pmod 4$. Önerme 3.2.4. yardımıyla sadece $\left(\frac{\alpha}{p_i}\right)_4 = 1$ olduğunu göstermek yeterlidir. Çünkü

Önerme 3.2.4. te $q \equiv 3 \pmod 4$ olduğu durumda $\left(\frac{\alpha}{q_i}\right)_4 = 1$ olduğu gösterilmişti. Şimdi, $p_i \equiv 1 \pmod 4$ olduğu için, π indirgenemez olmak üzere $p_i = \pi\overline{\pi}$ şeklinde yazılabilir ise ve Legendre sembolü çarpanlanabilir bir fonksiyon olduğundan dolayı,

$$\left(\frac{\alpha}{p_i}\right)_4 = \left(\frac{\alpha}{\pi}\right)_4 \left(\frac{\alpha}{\overline{\pi}}\right)_4$$

şeklinde yazılır. Buradan,

$$\left(\frac{\alpha}{p_i}\right)_4 = \left(\frac{\alpha}{\pi}\right)_4 \overline{\left(\frac{\alpha}{\pi}\right)_4} \text{ (Önerme 3.2.3. (3))}$$

$$= 1 \qquad (\chi \text{ fonksiyonun özelliği })$$

dır.

Önerme 3.2.6. *Eğer* $n \neq 1$ *bir tamsayı ve* $n \equiv 1 \pmod 4$ *ise,* $\left(\frac{i}{n}\right)_4 = (-1)^{(n-1)/4}$ *dır*

(Ireland ve Rosen 1990).

İspat: Burada n negatif bir tamsayı da olabilir. Eğer n pozitif bir asal ise, $p \equiv 1 \pmod 4$ şeklinde olacağından $p = \pi\overline{\pi}$ şeklinde yazılabilir. Buradan, Legendre sembolünün özellikleri de göz önüne alınarak,

$$\left(\frac{i}{p}\right)_4 = \left(\frac{i}{\pi}\right)_4 \left(\frac{i}{\overline{\pi}}\right)_4 = \left(i^{(p-1)/4}\right)^2 = (-1)^{(p-1)/4}$$

Diğer taraftan $n = -q$, $q \equiv 3 \pmod 4$ şeklinde ve asalsa, o halde,

$\left(\frac{i}{-q}\right)_4 = i^{\left(q^2-1\right)/4} = \left(i^{(q-1)}\right)^{(q+1)/4} = (-1)^{(-q-1)/4}$ olur.

Eğer $n \equiv 1 \pmod 4$ rasgele bir tamsayı ise, her tamsayı asalların çarpımı şeklinde yazılabileceğinden ve $p_i \equiv 1 \pmod 4$, $q_i \equiv 3 \pmod 4$ olmak üzere, $n = p_1 \ldots\ldots p_t (-q_1) \ldots\ldots (-q_s)$ şeklinde yazılabilir.

$$\left(\frac{i}{n}\right)_4 = \left(\frac{i}{p_1 \ldots p_t (-q_1) \ldots (-q_s)}\right)_4 = \left(\frac{i}{p_1}\right)_4 \ldots \left(\frac{i}{p_t}\right)_4 \left(\frac{i}{(-q_1)}\right)_4 \ldots \left(\frac{i}{(-q_s)}\right)_4$$

$$= (-1)^{\frac{p_1-1}{4}} \ldots (-1)^{\frac{p_t-1}{4}} (-1)^{\frac{-q_1-1}{4}} \ldots (-1)^{\frac{-q_s-1}{4}}$$

$$= (-1)^{\sum_i \frac{p_i-1}{4}} (-1)^{\sum_j \frac{-q_j-1}{4}}$$

$$= (-1)^{\sum_i \sum_j \frac{p_i-1}{4} \cdot \frac{-q_j-1}{4}}$$

$$= (-1)^{\frac{p_1 \cdots p_t(-q_1)\cdots(-q_s)-1}{4}}$$

$$= (-1)^{(n-1)/4}$$

bulunur.

Teorem 3.2.1. (4. Dereceden Kalanlar Teoremi) *Eğer* π *ve* θ, $\mathbb{Z}[i]$*de farklı primary asallar ise,*

$$\left(\frac{\pi}{\theta}\right)_4 = \left(\frac{\theta}{\pi}\right)_4 (-1)^{(N(\pi)-1)(N(\theta)-1)/16} \qquad (2)$$

dır (Cox 1989).

Not 3.2.5. Eğer π ve θ primary ise, $\pi = a+bi$ ve $\theta = c+di$ olmak üzere $(N(\pi)-1)(N(\theta)-1)/16$ ile $(a-1)(c-1)/4$ aynı işarete sahiptir. O halde, $\left(\frac{\pi}{\theta}\right)_4 = \left(\frac{\theta}{\pi}\right)_4 (-1)^{(a-1)(c-1)/4}$ yazılabilir.

Lemma 3.2.1. *Eğer* $\pi, \theta \in \mathbb{Z}[i]$ *farklı primary asallar ise,* $\pi = a+bi$ *ve* $\theta = c+di$ *olmak üzere,* π *veya* θ *dan biri 4 modülüne göre 1 e kongrüent ise,* $\left(\frac{\pi}{\theta}\right)_4 = \left(\frac{\theta}{\pi}\right)_4$ *dir. Eğer hem* π *hem de* θ, *4 modülüne göre* $3+2i$ *ye kongrüent ise,* $\left(\frac{\pi}{\theta}\right)_4 = -\left(\frac{\theta}{\pi}\right)_4$ *dir.*

İspat: $\pi \equiv 1 \pmod 4$ ve $\theta \equiv 3+2i \pmod 4$ olsun. O halde $a \equiv 1 \pmod 4$ ise, kongrüanslık tanımı gereği $a = 4k+1$ olacak şekilde bir $k \in \mathbb{Z}$ vardır. $c \equiv 3 \pmod 4$ ise, kongrüanslık tanımı gereği $c = 4t$ olacak şekilde bir $t \in \mathbb{Z}$ vardır. Buradan, 4. dereceden kalanlar teoreminde,

$$\left(\frac{\pi}{\theta}\right)_4 = \left(\frac{\theta}{\pi}\right)_4 (-1)^{((4k+1)-1)((4k+3)-1)/4}$$

$$= \left(\frac{\theta}{\pi}\right)_4 (-1)^{2k(2t+1)}$$

$$= \left(\frac{\theta}{\pi}\right)_4$$

elde edilir.

$\pi \equiv 3+2i \pmod 4$ ve $\theta \equiv 3+2i \pmod 4$ olsun. O halde $a \equiv 3 \pmod 4$ ise, kongrüanslık tanımı gereği $a = 4m+3$ olacak şekilde bir $m \in \mathbb{Z}$ vardır. $c \equiv 3 \pmod 4$ ise, kongrüanslık tanımı gereği $c = 4n+3$ olacak şekilde bir $n \in \mathbb{Z}$ vardır. Buradan, 4. dereceden kalanlar teoreminde,

$$\left(\frac{\pi}{\theta}\right)_4 = \left(\frac{\theta}{\pi}\right)_4 (-1)^{((4m+3)-1)((4n+3)-1)/4}$$

$$= \left(\frac{\theta}{\pi}\right)_4 (-1)^{(2m+1)(2n+1)}$$

$$= -\left(\frac{\theta}{\pi}\right)_4$$

bulunur.

Lemma 3.2.2. *$p \equiv 1 \pmod 4$, $a, b \in \mathbb{Z}$ olmak üzere $b \equiv af \pmod p$ olacak şekilde bir f olsun. $f^2 \equiv -1 \pmod p$ dir.*

İspat: $b \equiv af \pmod p$ ise, kongrüanslık özelliklerinden,

$$b^2 \equiv a^2 f^2 \pmod p \qquad (*)$$

olur.

Öte yandan, $p \equiv 1 \pmod 4$ olduğundan iki kare toplamı şeklinde yazılabilir. $p = a^2 + b^2$ olup kongrüanslık tanımını gereği,

$b^2 \equiv -a^2 \pmod p$ dir. (*) kongrüans denklemini göz önüne alınarak,

$$f^2 \equiv -1 \pmod p$$

elde edilir.

Lemma 3.2.3. $p \equiv 1 \pmod 4$ olmak üzere, $p = a^2 + b^2$ şeklinde yazılır. Ayrıca a tek bir sayı ise,

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

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

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

dir.

İspat:

1) Gauss Lemmasından, $\left(\frac{a}{p}\right) = (-1)^{\mu}$ olduğunu biliyoruz. Buradan $\mu = \frac{p-1}{2} = \frac{(4k+1)-1}{2} = 2k$ olduğundan,

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

elde edilir.

2) $p = a^2 + b^2$ olduğundan,

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

yazılabilir. Kongrüanslık tanımı gereği,

$$p \mid (a+b)^2 - 2ab$$

Buradan,

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

olur.

3) $p \equiv 1 \pmod 4$ olduğuna göre, buradan

$$\left(\frac{p-1}{4}, p\right) = 1$$

dir. O halde, $(a+b)^2 \equiv 2ab \pmod p$ denkleminin her iki tarafının $\frac{p-1}{4}$. dereceden kuvvetini alırsak,

$$\left((a+b)^2\right)^{\frac{p-1}{4}} \equiv (2ab)^{\frac{p-1}{4}} \pmod{p}$$

olup,

$$(a+b)^{\frac{p-1}{2}} \equiv (2ab)^{\frac{p-1}{4}} \pmod{p}$$

elde edilir.

Lemma 3.2.3. *$\pi \in \mathbb{Z}[i]$ bir primary asal olmak üzere,*

1) $\left(\frac{i}{\pi}\right)_4 = i^{-(a-1)/2}$,

2) $\left(\frac{1+i}{\pi}\right)_4 = i^{\left(a-b-1-b^2\right)/4}$

dür (Cox 1989).

Not 3.2.6. Legendre sembolünün tanımı gereği,

$$\left(\frac{i}{\pi}\right)_4 = i^{N(\pi)-1/4}$$

olup, $\pi = a+bi$ $(a,b \in \mathbb{Z}[i])$ olmak üzere,

$$\left(\frac{i}{\pi}\right)_4 = i^{a^2+b^2-1/4}$$

olur.

Şimdi bu özellikler yardımıyla ilk ispatı L. Euler tarafından yapılan aşağıdaki teoremi ifade edelim.

Teorem 3.2.2. *Eğer $\pi = a+bi$, $\mathbb{Z}[i]$ de bir primary asal ise,*

1) $\left(\frac{2}{\pi}\right)_4 = i^{ab/2}$.

2) *p asalının $x, y \in \mathbb{Z}$ için $p = x^2 + 64y^2$ biçiminde temsil edilebilmesi için gerek ve yeter koşul $p \equiv 1 \pmod 4$ ve 2 nin, p modülüne göre bir 4. dereceden kalan olmasıdır* (Cox 1989).

Gözlem: $p \equiv 1 \pmod 4$ asal olsun. Öyleyse $\pi = a + bi$ primary olmak üzere $p = a^2 + b^2 = \pi\overline{\pi}$ şeklinde yazılabilir. Burada a nın tek, b nin de çift olduğunu hatırlayalım. $(\mathbb{Z}/p\mathbb{Z})^* \simeq (\mathbb{Z}[i]/\pi\mathbb{Z}[i])^*$ olduğundan $\left(\frac{2}{\pi}\right)_4 = i^{ab/2}$ bize, 2 nin p modülüne göre 4. dereceden bir kalan olmasının ancak ve ancak b nin 8 ile bölünebilir olması ile mümkün olduğunu gösterir. Buradan teoremin ikinci kısmının ispatı elde edilir.

4. $\mathbb{Z}[i]$ DE P_k KÜMELERİNİN VARLIĞI

Tanım 4.1. k bir tamsayı, A kümesi n elemanlı farklı pozitif tamsayılardan oluşan $\{x_{1,}x_{2,}.....,x_{n,}\}$ küme olsun. Eğer $\forall i,j\in\mathbb{N}$, $i\neq j$, için x_ix_j+k bir tamkare oluyorsa bu kümeye P_k kümesi denir. Mesela $\{1,2,5\}$ 3 elemanlı P_{-1} kümesi, $\{1,79,98\}$ 3 elemanlı P_2 kümesi, $\{51,208,465,19732328\}$ 4 elemanlı P_1 kümesidir. Eğer A kümesi genişletilmek isteniyorsa yeni katılan elemanla oluşan küme yine P_k özelliğini taşımalıdır.

Lemma 4.1. *3 ten büyük rasyonel asal sayılar* $6k\mp1$ *formundadır* (Kaygısız 2007).

Lemma 4.2. P_1 ve P_4 *kümelerinin içinde en fazla bir tane* $6k+1$ *formunda tamsayı bulunabilir* (Kaygısız 2007).

Lemma 4.3. P_1 ve P_4 *kümelerinin içinde en fazla bir tane* $6k-1$ *formunda tamsayı bulunabilir* (Kaygısız 2007).

Lemma 4.4. *Tüm elemanları* 3 *ten büyük* $6k+1$ *veya* $6k-1$ *formunda tamsayı olan* P_1 ve P_4 *kümelerinin iki elemanından biri* $6k+1$ *formumda ise diğeri* $6k-1$ *formundadır* (Kaygısız 2007).

Teorem 4.1. *Tüm elemanları* 3 *ten büyük asal sayı olan* 3 *veya daha fazla elemana sahip* P_1 ve P_4 *kümesi yoktur.*

Teorem 4.2. $x,y\in\mathbb{Z}[i]$, $x\neq y$, $x,y\equiv3\pmod4$ *olsun. Eğer* $\pi=a+bi\in\mathbb{Z}[i]$ $(a,b\in\mathbb{Z})$ *ve* $N(\pi)=A^2,(A\in\mathbb{Z})$ *ise iki elemanlı* $P_4=\{x,y\}$ *kümeleri* $xy\equiv(2i)^2\pmod\pi$ *koşulu ile mevcuttur.*

İspat: $x\neq y$ olduğu için $x=4k+3$ ve $y=4t+3$ $(k\neq t)$ olsun. O halde, iki elemanlı P_4 kümesini oluşturmak için P_4 kümesinin tanımı gereği,

$$\begin{aligned} xy+4 &= (4k+3)(4t+3)+4 \\ &= 16kt+12k+12t+13 \\ &= 4(4kt+3k+3t)+13 \\ &= 1 \pmod 4 \end{aligned} \tag{3}$$

elde edilir. Artık $a,b \in \mathbb{Z}$ için $\pi = a+bi \in \mathbb{Z}[i]$ olmak üzere $xy+4 = a^2+b^2 = N(\pi) = A^2$ eşitliğinden, $xy+4 = (a+bi)(a-bi)$ veya $(a+bi) \mid xy+4$ ve sonuçta $xy+4 \equiv 0 \pmod \pi$ buradan da $xy \equiv (2i)^2 \pmod \pi$ dir.

Lemma 4.5. *$P_4 = \{3,7\}$ kümesi $\mathbb{Z}[i]$ nin asalları ile genişletilemez.*

İspat: $P_4 = \{3,7\}$ kümesinin π, $\mathbb{Z}[i]$ nin asal elemanı olmak üzere $P_4 = \{3,7,\pi\}$ şeklinde genişletildiğini kabul edelim. P_k kümesi tanımından, ve (3) denkleminden,

$$\begin{aligned} 3\pi+4 &= x^2+y^2 \\ 7\pi+4 &= z^2+t^2 \end{aligned} \tag{4}$$

dir. Buradan,

$7(x^2+y^2)-16 = 3(z^2+t^2)$ Eşitliğin sağ tarafı 3 ile bölünebiliyorsa sol tarafı da 3 ile bölünebiliyor demektir. O halde,

$$\begin{aligned} 7(x^2+y^2) &\equiv 16 \pmod 3 \\ x^2+y^2 &\equiv 1 \pmod 3 \end{aligned}$$

Elde edilir. Fakat $4k+3$ biçimindeki iki sayının çarpımının 4 fazlasının $4k+1$ biçiminde bir sayı olduğu bilindiğinden (4) eşitliklerinden x^2+y^2 nin 4 modülüne göre 1 e kongrüent olduğu görülür. Bu durumu sağlayacak bir tamsayının karesi yoktur. Bu bir çelişki olduğundan bu eşitliği sağlayan bir π asalı olmadığı sonucuna varılır.

Not 4.1. P_k cümlesi tanımından kümenin elemanları pozitif tamsayılar olacağından, Gauss asallarının normları alınarak $N(\pi) = p \equiv 1 \pmod 4$ asalları ile P_k kümelerinin oluşup oluşmayacağını inceleyelim.

Lemma 4.6. $P_4 = \{13,17\}$ *kümesi* $\mathbb{Z}[i]$ *nin asalları ile genişletilemez.*

İspat: $P_4 = \{13,17\}$ kümesinin $\theta \in \mathbb{Z}[i]$ ve $N(\theta)$, $4k+1$ biçiminde rasyonel asal olan bir Gauss asalı olmak üzere, $P_4 = \{13,17,N(\theta)\}$ şeklinde genişletildiğini kabul edelim. P_k kümesi tanımından ve iki tane $4k+1$ biçimindeki sayının çarpımına 4 eklediğimizde bu sayının 4 modülüne göre 1 e kongrüent olduğundan,

$$13N(\theta)+4 = x^2 + y^2$$
$$17N(\theta)+4 = z^2 + t^2$$

dir. Buradan, $17\left(x^2+y^2\right)-16 = 13\left(z^2+t^2\right)$ Eşitliğin sağ tarafı 13 e bölünüyorsa sol tarafı da bölünür. O halde,

$$17\left(x^2+y^2\right) \equiv 16 \pmod{13}$$
$$4\left(x^2+y^2\right) \equiv 3 \pmod{13}$$

elde edilir. x^2+y^2 nin $4k+1$ biçiminde bir sayı olduğu bilindiğinden bu kongrüans denklemini sağlayacak hiçbir çözüm yoktur. O halde normu $4k+1$ biçiminde olan Gauss asalları ile yapılan P_4 kümeleri genişletilemez.

Teorem 4.3. $\pi \in \mathbb{Z}[i]$ *için* $N(\pi) = p \equiv 1 \pmod{4}$ *biçiminde bir asal olsun. Eğer bu asal* P_4 *de* $6k+1$ *formunda ise, diğer asal da* $6k-1$ *formundadır.*

İspat: Lemma 4.1. gereği 3 ten büyük tüm asal sayıların $6k \mp 1$ formunda yazılabildiğini biliyoruz. Öte yandan, Lemma 4.2. ve Lemma 4.3. gereği P_4 kümesinde en fazla bir tane $6k+1$ veya $6k-1$ formunda tamsayı vardır. O halde asallardan biri $6k+1$ formunda ise, diğeri $6k-1$ formunda olmalıdır.

Teorem 4.4. $q \equiv 3 \pmod{4}$ *bir Gauss asalı olmak üzere,* $6k+1$ *biçiminde ise,* P_k *deki diğer asal* $6k-1$ *biçimindedir.*

İspat: İspatı Teorem 4.3. ile aynı şekildedir.

Teorem 4.5. *Gauss asalları ile 3 veya daha fazla elemana sahip bir* P_4 *kümesi yazılamaz.*

İspat: Teorem 4.1. gereği, tüm elemanları 3 ten büyük asal sayı olan 3 veya daha fazla elemana sahip P_4 kümesi yazılamaz. Bu da ispatı tamamlar.

5. SONUÇLAR

Biz bu çalışmamızda Gauss tamsayılar halkasında P_k kümelerinin varlığı için bir kriter oluşturarak bazı genişlemeyen P_k kümelerinin var olduğunu gösterdik. Ayrıca Gauss asallarından faydalanılarak nasıl P_4 kümelerinin yazılabileceğini gösterdik.

Primary asalları kullanılarak P_k kümelerinin oluşturulup oluşturulamayacağı da incelenebilir.

6. KAYNAKLAR

[1] COX, D., 1989, Primes of the form $x^2 + ny^2$, A Wiley-Interscience Publication, New York, Chichester, Brisbane.

[2] ÇALLIALP, F., 1999, Sayılar Teorisi, Marmara Üniversitesi, Atatürk Eğitim Fakültesi, İstanbul.

[3] DUJELLA, A., FRANUSIC, Z., 2007, On Differences of Two squares in some quadratic Fields, Rocky Mountain, Journal of Mathematics, Volume 37, Number 2.

[4] FLANDERS, H., 1985, A Tale of Two Squares and Two Rings, Mathematics Magazine, Vol 58, No 1 Jaunary.

[5] IRELAND, K., ROSEN, M., 1990, A Classical Introduction to Modern Number Theory, Springer-Verlag, New York, Berlin, Heidelberg.

[6] KAYGISIZ, K.,ŞENAY, H., 2007, Constructions of Some New Nonextandable P_k Sets, International Mathematical Forum, 2, no. 58.

[7] ŞENAY, Hasan, 2007, Sayılar Teorisi Dersleri, Dizgi Ofset Matbaacılık, Konya.