T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

REEL KUADRATİK CİSİMLERDE BİRİMLER

YÜKSEK LİSANS TEZİ

Aygen KOÇ

Enstitü Anabilim Dalı	**:**	**MATEMATİK**
Bilim Dalı	**:**	**Cebir ve Sayılar Teorisi**
Tez Danışmanı	**:**	**Prof. Dr. Refik KESKİN**

Mayıs 2012

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

REEL KUADRATİK CİSİMLERDE BİRİMLER

YÜKSEK LİSANS TEZİ

Aygen KOÇ

Enstitü Anabilim Dalı	**:**	**MATEMATİK**
Bilim Dalı	**:**	**Cebir ve Sayılar Teorisi**

Bu tez 12/05/2012 tarihinde aşağıdaki jüri tarafından Oybirliği ile kabul edilmiştir.

Prof. Dr.	**Yrd. Doç. Dr.**	**Doç. Dr.**
Refik KESKİN	**Bahar D. BİTİM**	**Yusuf ATALAY**
Jüri Başkanı	**Üye**	**Üye**

ÖNSÖZ

Bu çalışma konusunu bana veren, çalışmalarım boyunca ilgi ve yardımlarını esirgemeyen değerli danışman hocam Sayın Prof. Dr. Refik KESKİN' e ve yaşamım boyunca her konuda destekçim olan aileme teşekkür ederim.

İÇİNDEKİLER

SİMGELER VE KISALTMALAR LİSTESİ

$\mathbb{N}$	: Doğal sayılar kümesi
$\mathbb{R}$	: Reel sayılar kümesi
$\mathbb{Z}$	: Tam sayılar kümesi
$\Leftrightarrow$	: Ancak ve ancak
$[\ \ ]$	: Sürekli kesir
$\equiv$	: Denktir
$\not\equiv$	: Denk değildir
$[\![\ \ ]\!]$	: Tam değer
a | b	: a , b’yi böler
$\|\ \ \|$	: Mutlak değer
$\Rightarrow$	: İse
$\in$	: Elemanıdır
$\left(\frac{p}{q}\right)$	: Legendre sembolü

TABLOLAR LİSTESİ

ÖZET

Anahtar kelimeler: Temel Birim, Sürekli Kesirler, Sonsuz Sürekli Kesirler, Periyodik Sonsuz Sürekli Kesirler, Tamamıyla Periyodik Sürekli Kesirler, Fibonacci Sayıları, Lucas Sayıları, Pell ve Pell-Lucas Sayıları, Diophantine Denklemleri

Bu çalışma 5 bölümden ibaret olup,

Birinci bölümde ileriki bölümlerde kullanılacak bazı temel tanım ve teoremler verildi.

İkinci bölümde real kuadratik cisimlerde birimler incelendi.

Üçüncü bölümde sonlu sürekli kesirler, sonsuz sürekli kesirler, periyodik sonsuz sürekli kesirler, tamamıyla periyodik sürekli kesirler ve $\sqrt{d}$' nin sürekli kesirlere açılımı incelenmiştir.

Dördüncü bölümde temel birim hesaplandı.

Beşinci bölümde bazı Diophantine denklemlerinin çözümleri verildi.

FUNDAMENTAL UNITS IN REAL QUADRATIC FIELDS

SUMMARY

Key Words: Fundamental Unit, Continued Fractions, Infinite Continued Fractions, Periodic Infinite Continued Fractions , Pure Periodic Infinite Continued Fractions, Fibonacci Numbers, Lucas Numbers, Pell and Pell-Lucas Numbers, Diophantine Equations

This study consists of five chapters.

In the first chapter, some basic definations and theorems are given.

In the second chapter, units in the real quadratic fields are examined.

In the third chapter, finite continued fractions, infinite continued fractions, periodic continued fractions, pure periodic infinite continued fractions, and infinite continuous fraction expansion of $\sqrt{d}$ are investigated.

In the fourth chapter, the fundamental units of the real quadratic fields are calculated.

In the fifth chapter, solutions of some diophantine equations are given.

BÖLÜM 1. GİRİŞ

1.1. Kongrüanslar

Tanım 1.1.1. Sıfırdan farklı bir m tamsayısı $a - b$ farkını bölüyorsa a' ya m modülüne göre b' ye denktir denir ve bu $a \equiv b \ (mod\ m)$ şeklinde gösterilir. m, $a - b$ farkını bölmüyorsa a' ya m modülüne göre b' ye denk değildir denir ve bu $a \not\equiv b \ (mod\ m)$ şeklinde gösterilir.

Böylece $a - b$' nin m ile bölünebilmesi, $-m$ ile de bölünebilmesini gerektireceğinden genellikle modülü pozitif olarak sınırlayacağız.

Kongrüansların aşağıdaki özellikleri vardır.

Teorem 1.1.1. a, b, c, d, x ve y tamsayılar olmak üzere;

a) $a \equiv b \ (mod\ m)$ ise $b \equiv a \ (mod\ m)$ ve $a - b \equiv 0 \ (mod\ m)$,

b) $a \equiv b \ (mod\ m)$ ve $b \equiv c \ (mod\ m)$ ise $a \equiv c \ (mod\ m)$,

c) $a \equiv b \ (mod\ m)$ ve $c \equiv d \ (mod\ m)$ ise $ax + cy \equiv bx + dy \ (mod\ m)$,

d) $a \equiv b \ (mod\ m)$, $c \equiv d \ (mod\ m)$ ise $ac \equiv bd \ (mod\ m)$,

e) $a \equiv b \ (mod\ m)$ ve $d|m$, $d > 0$ ise $a \equiv b \ (mod\ d)$

özellikleri geçerlidir.

Teorem 1.1.2.

a) $(a,m)=d$ ise $ax\equiv ay\ (mod\ m)$ olması için gerek ve yeter şart $x\equiv y\ \left(mod\ \frac{m}{d}\right)$ olmasıdır.

b) $(a,m)=1$ ve $ax\equiv ay\ (mod\ m)$ ise $x\equiv y\ (mod\ m)$' dir.

Teorem 1.1.3. $(a,m)=d$ olmak üzere $ax\equiv b\ (mod\ m)$ kongrüansının çözümünün olması için gerek ve yeter şart $d|b$ olmasıdır.

Teorem 1.1.4. p asal, $p|a^2+b^2$ ve $p\equiv 3\ (mod\ 4)$ ise $p|a$ ve $p|b$' dir.

Tanım 1.1.2. p tek asal ve $(a,p)=1$ olsun. Bu taktirde $\left(\frac{a}{p}\right)$ şeklinde gösterilen Legendre sembolü,

$$\left(\frac{a}{p}\right)=\begin{cases} 1\ , & a^{(p-1)/2}\equiv 1\ (mod\ p)\ ise \\ -1\ , & a^{(p-1)/2}\equiv -1\ (mod\ p)\ ise \\ 0\ , & a\equiv 0\ (mod\ p)\ ise \end{cases}$$

şeklinde tanımlanır.

Örnek 1.1.1. $a=6$ ve $p=11$ için Legendre sembolünü bulalım.

$$\left(\frac{6}{11}\right)=6^{(11-1)/2}=6^5\ \equiv -1(mod\ 11)$$

olduğundan $\left(\frac{6}{11}\right)=-1$ dir.

Örnek 1.1.2. $p=7$ ise

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

dir.

Önerme 1.1.1. $q>2$ bir asal sayı olsun.

$$\left(-\frac{1}{q}\right)=1 \quad \Leftrightarrow \quad q\equiv 1\ (mod\ 4)$$

$$\left(-\frac{1}{q}\right)=-1 \quad \Leftrightarrow \quad q\equiv 3\ (mod\ 4)$$

dir. Ayrıca p asal sayı olmak üzere $a\equiv b\ (mod\ p)$ ise

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

dir.

1.2. Kuadratik Cisimler

F bir cisim olmak üzere, katsayıları F' den alınan ve x değişkenli polinomların kümesi $F[x]$ ile gösterilir. Eğer $F=\mathbb{Q}$ alınırsa $\mathbb{Q}[x]$ ile katsayıları rasyonel sayılar olan x değişkenli polinomlar kümesi gösterilir. $a_i\in\mathbb{Q}$, $i=1,2,3,\dots,n$ olmak üzere

$$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n$$

polinomunu göz önüne alalım. Burada $a_0\neq 0$ olmak üzere n' ye polinomun derecesi ve a_0' a polinomun baş katsayısı denir. Eğer $a_0=1$ ise bu polinoma monik polinom ve $(a_0,a_1,\dots,a_n)=1$ ise $f(x)$' e ilkel polinom denir.

İki polinomun çarpımının derecesi, polinomların dereceleri toplamına eşittir. Sıfırdan farklı bir $g(x)$ polinomu için $f(x)=g(x)q(x)$ olacak şekilde bir $q(x)$ polinomu varsa $f(x)$' e $g(x)$ ile bölünebilir denir ve bu $g(x)|f(x)$ şeklinde gösterilir. Burada $g(x)$' in derecesi $f(x)$' in derecesinden küçük veya eşittir.

Teorem 1.2.1. $g(x) \neq 0$ olmak üzere $f(x)$ ve $g(x)$, $\mathbb{Q}[x]$ de iki polinom olsun. $f(x) = g(x)q(x) + r(x)$ olacak şekilde bir tek $q(x)$ ve $r(x)$ polinomları vardır ve $r(x) = 0$ veya $r(x)$' in derecesi $g(x)$' in derecesinden küçüktür.

Teorem 1.2.2. Sıfırdan farklı $f(x)$ ve $g(x)$ polinomları için aşağıdaki özellikleri sağlayan tek türlü $d(x)$ monik polinomu vardır.

a) $d(x)|f(x)$ ve $d(x)|g(x)$ dir.

b) $d(x)$, $f(x)$ ve $g(x)$' in lineer kombinasyonu olarak yazılır.

c) $f(x)$ ve $g(x)$' in herhangi bir ortak böleni, $d(x)$' in de bir bölenidir ve $d(x)$' in derecesinden daha büyük olan polinomlar ortak bölen değildir.

Tanım 1.2.1. Teorem 1.2.2' de anlatılan $d(x)$ polinomuna $f(x)$ ve $g(x)$ polinomlarının en büyük ortak böleni denir ve bu,

$$d(x) = \big(f(x), g(x)\big)$$

şeklinde gösterilir.

Tanım 1.2.2. $f(x)$ özdeş olarak sıfır olmayan bir polinom olsun. $f(x) = g(x)h(x)$ olacak şekilde derecesi $f(x)$' den küçük olan pozitif dereceli $g(x)$ ve $h(x)$ polinomları $\mathbb{Q}[x]$' de bulunamıyorsa $f(x)$ polinomuna $\mathbb{Q}[x]$' de indirgenemez veya asaldır denir.

Teorem 1.2.3. $p(x)$ indirgenemez polinomu $f(x)g(x)$ çarpımını bölüyor ise $p(x)$ polinomu $f(x)$ veya $g(x)$' den en az birinini böler.

Tanım 1.2.3. $a_0, a_1, a_2, \dots, a_n$ sıfırdan farklı tamsayılar olmak üzere,

$$a_0\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0 \tag{1.1}$$

denklemini sağlayan α sayısına cebirsel sayı denir.

Teorem 1.2.4. Bir α cebirsel sayısı $\mathbb{Q}$ üzerinde tek türlü indirgenemez $h(x)$ monik polinomu $h(\alpha) = 0$ olacak biçimde vardır. Üstelik $\mathbb{Q}$ üzerinde α' yı sıfır yeri kabul eden her polinom $h(x)$ ile bölünebilir [1].

Tanım 1.2.4. Bir α cebirsel sayısı $a_0 = 1$ olması durumunda (1.1) denklemini sağlıyorsa o zaman α cebirsel sayısına cebirsel tamsayı denir.

Teorem 1.2.5. Rasyonel sayılarda sadece $0, \pm1, \pm2, \dots$ tamsayıları cebirsel tamsayılardır.

İspat.

$$f(x) = x^n + a_1x^{n-1} + \cdots + a_n = 0$$

olmak üzere $f(x)$ polinomu $x - m$ polinomu olarak alındığında $f(m) = 0$ olacağından herhangi bir m tamsayısı cebirsel tamsayıdır. Diğer taraftan, herhangi bir $\frac{m}{q}$ rasyonel sayısı, $(m, q) = 1$ olmak üzere cebirsel tamsayı ise o zaman,

$$\left(\frac{m}{q}\right)^n + a_1\left(\frac{m}{q}\right)^{n-1} + \cdots + a_n = 0$$

$$m^n + a_1qm^{n-1} + \cdots + a_nq^n = 0$$

olur. Böylece $q|m^n$ olduğu görülür. Buradan $q = \pm 1$ elde edilir. O halde $\frac{m}{q}$ bir tamsayıdır.

Tanım 1.2.5. α irrasyonel sayısı katsayıları tamsayılar olan kuadratik bir polinomun kökü ise α sayısına bir kuadratik irrasyonel sayı denir. Yani a, b, c tamsayılar ve $a \neq 0$ olmak üzere,

$$a\alpha^2 + b\alpha + c = 0$$

ise α' ya kuadratik irrasyonel sayı denir [2].

Sonuç 1.2.5.1. α' nın kuadratik irrasyonel sayı olması için gerekli ve yeter şart u, v birer rasyonel sayı $(v \neq 0)$ ve m karesiz pozitif bir tamsayı olmak üzere α' nın $u + v\sqrt{m}$ biçiminde olmasıdır [3].

Önerme 1.2.1. Her α kuadratik sayısı m karesiz pozitif bir tamsayı ve $b|(m - a^2)$ $(b \neq 0\ ,\ a, b \in \mathbb{Z})$ olmak üzere,

$$\alpha = \frac{a + \sqrt{m}}{b}$$

biçiminde yazılabilir [3].

Tanım 1.2.6. m sıfırdan farklı karesiz bir tamsayı olmak üzere $\mathbb{Q}(\sqrt{m})$ kuadratik cismi $\mathbb{Q}(\sqrt{m}) = \{a + b\sqrt{m}\ :\ a, b \in \mathbb{Q}\}$ olarak tanımlanır.

Tanım 1.2.7. $m > 0$ ise $\mathbb{Q}(\sqrt{m})$ kuadratik cismine reel kuadratik cisim adı verilir [4].

Teorem 1.2.6. m karesiz bir tamsayı olmak üzere $\mathbb{Q}(\sqrt{m})$' nin cebirsel tamsayıları,

a) $m \equiv 2,3 \ (mod\ 4)$ ise a, b tamsayılar olmak üzere $a + b\sqrt{m}$ biçimindedir.

b) $m \equiv 1 \ (mod\ 4)$ ise a, b ikisi de tek ya da ikisi de çift tamsayı olmak üzere $\frac{a+b\sqrt{m}}{2}$ biçimindedir [5].

Bu tezde $\mathbb{Q}(\sqrt{m})$ cisminin cebirsel tamsayılarına kısaca tamsayı denilecektir.

Sonuç 1.2.6.1. $m \equiv 1 \ (mod\ 4)$ ise $\mathbb{Q}(\sqrt{m})$' nin bir α elemanı tamsayıdır $\Leftrightarrow$ a ve b tamsayılar olmak üzere $\alpha = a + b\left(\frac{1+\sqrt{m}}{2}\right)$ biçiminde yazılabilir.

İspat. $\Rightarrow$) $m \equiv 1 \ (mod\ 4)$ olmak üzere $\alpha = \frac{a+b\sqrt{m}}{2}$ bir tamsayı olsun. $a, b \in \mathbb{Z}$ için a ve b' nin ikisi de tek ya da ikisi de çift olduğundan $\frac{a-b}{2}$ de tamsayıdır. O halde,

$$\frac{a-b}{2} + b\left(\frac{1+\sqrt{m}}{2}\right) = \frac{a+b\sqrt{m}}{2} = \alpha$$

olduğundan $\alpha = a + b\left(\frac{1+\sqrt{m}}{2}\right)$ biçiminde yazılabilir.

$\Leftarrow$) $a, b \in \mathbb{Z}$ ise $a + b\left(\frac{1+\sqrt{m}}{2}\right) = \frac{2a+b+b\sqrt{m}}{2}$ olup b tek ise $2a + b$ de tek, b çift ise $2a + b$ de çifttir. O halde önceki teoreme göre $a + b\left(\frac{1+\sqrt{m}}{2}\right)$ bir tamsayıdır.

Teorem 1.2.6' da bahsedilen $\mathbb{Q}(\sqrt{m})$ cisminin tamsayıları kümesi $O_{\mathbb{Q}(\sqrt{m})}$ ile gösterilir ve aşağıdaki sonuç verilebilir.

Sonuç 1.2.6.2.

$$\alpha = \begin{cases} \sqrt{m}\ , & m \equiv 2,3\ (mod\ 4)\ ise \\ \dfrac{1+\sqrt{m}}{2}, & m \equiv 1\ (mod\ 4)\ \ ise \end{cases}$$

olmak üzere,

$$O_{\mathbb{Q}(\sqrt{m})} = \mathbb{Z}[\alpha] = \{a\alpha + b : a, b \in \mathbb{Z}\}$$

dir.

Tanım 1.2.8. $a, b \in \mathbb{Q}$ olmak üzere $\alpha = a + b\sqrt{m}$ olsun. $\overline{\alpha} = a - b\sqrt{m}$ ye α' nın eşleniği denir.

Tanım 1.2.9. $\mathbb{Q}(\sqrt{m})$ cisminde bir α tamsayısının normu $N(\alpha)$ ile gösterilir ve

$$N(\alpha) = \alpha\overline{\alpha}$$

olarak tanımlanır.

Tanım 1.2.10. $\varepsilon \in O_{\mathbb{Q}(\sqrt{m})}$ için $\frac{1}{\varepsilon} \in O_{\mathbb{Q}(\sqrt{m})}$ ise ε değerine birim denir. Ayrıca $O_{\mathbb{Q}(\sqrt{m})}$' nin birimlerinin kümesi $U\left(O_{\mathbb{Q}(\sqrt{m})}\right)$ ile gösterilir.

Önerme 1.2.2. θ, $O_{\mathbb{Q}(\sqrt{m})}$' de bir tamsayı olmak üzere $N(\theta) = \pm 1$ olması için gerek ve yeter şart θ' nın birim olmasıdır [6].

Tanım 1.2.11. $\alpha, \beta \in O_{\mathbb{Q}(\sqrt{m})}$ ve $\alpha \neq 0$ olmak üzere $\beta = \alpha\gamma$ olacak şekilde bir $\gamma \in O_{\mathbb{Q}(\sqrt{m})}$ tamsayısı varsa α' ya β' nın bir böleni denir ve bu $\alpha | \beta$ şeklinde gösterilir. Sıfırdan farklı α ve β tamsayıları için α/β birim ise α ve β birbirleriyle ilgilidir denir.

Teorem 1.2.7. Çarpımın normu çarpanların normlarının çarpımına eşittir. $N(\alpha) = 0$ olması için gerek ve yeter şart $\alpha = 0$ olmasıdır [6].

Teorem 1.2.8. Herhangi bir reel kuadratik cismin sonsuz sayıda birimleri vardır [7].

Tanım 1.2.12. $\mathbb{Q}(\sqrt{m})$ kuadratik cisminde birimden farklı olan α cebirsel tamsayısının bölenleri birim veya kendisiyle ilgili olan böleni ise α' ya asaldır denir.

Teorem 1.2.9. Eğer $\mathbb{Q}(\sqrt{m})$ kuadratik cismindeki α tamsayısının normu p asal olmak üzere,

$$N(\alpha) = \pm p$$

ise α asaldır [7].

Teorem 1.2.10. $\mathbb{Q}(\sqrt{m})$' nin sıfırdan ve birimden farklı her tamsayısı ya asaldır ya da asalların çarpımı olarak yazılabilir [7].

Teorem 1.2.6' da m karesiz bir tamsayı olmak üzere $\mathbb{Q}(\sqrt{m})$' nin tamsayıları m' nin durumuna göre incelenmişti. Şimdi de m karesiz bir tamsayı olmak üzere $O_{\mathbb{Q}(\sqrt{m})}$' de m' nin durumuna göre birimleri inceleyelim.

$m \equiv 1\ (mod\ 4)$ ise $\mathbb{Q}(\sqrt{m})$' nin tamsayıları a ve b ler her ikisi de tek ya da çift tamsayılar olmak üzere $(a + b\sqrt{m})/2$ biçimindeydi. Herhangi bir $\theta \in O_{\mathbb{Q}(\sqrt{m})}$ cebirsel tamsayısının birim olabilmesi için Önerme 1.2.2' ye göre $N(\theta) = \pm 1$ olmalıdır. Dolayısıyla,

$$N(\theta) = \frac{a + b\sqrt{m}}{2} . \frac{a - b\sqrt{m}}{2} = \frac{a^2 - mb^2}{4} = \pm 1$$

elde edilir.

Eğer $m \equiv 1\ (mod\ 4)$ ise $O_{\mathbb{Q}(\sqrt{m})}$' nin birimleri, $\frac{a+b\sqrt{m}}{2}$ biçiminde olacağından $a^2 - mb^2 \equiv \pm 4\ (mod\ 4)$ bulunur. Buradan $a^2 - b^2 \equiv 0\ (mod\ 4)$ kongrüansı elde edilir ki, bu kongrüansın çözülebilir olması için a ve b nin her ikisinin tek ya da çift olması gerekir.

Eğer m, $m \equiv 1\ (mod\ 8)$ olacak şekilde bir tamsayı ise o zaman $\frac{a^2-mb^2}{4} = \pm 1$' den $a^2 - mb^2 = \pm 4$ olup,

$$a^2 - b^2 \equiv \pm 4\ (mod\ 8)$$

elde edilir. Bu kongrüansın çözülebilir olması için ya $a = 4k + 2$, $b = 4k$ şeklinde ya da $a = 4k$, $b = 4k + 2$ olmalıdır. Bu nedenle $m \equiv 1\ (mod\ 8)$ olması durumunda $O_{\mathbb{Q}(\sqrt{m})}$' nin birimi $a = 4k + 2$, $b = 4k$ şeklinde ya da $a = 4k$, $b = 4k + 2$ olmak üzere,

$$\theta = \frac{a + b\sqrt{m}}{2}$$

biçimindedir.

Eğer $m \equiv 2\ (mod\ 4)$ ise $\mathbb{Q}(\sqrt{m})$ kuadratik cisminin elemanları $a + b\sqrt{m}$ biçiminde olduğundan $\theta \in O_{\mathbb{Q}(\sqrt{m})}$ elemanları için $\theta = a + b\sqrt{m}$ olmak üzere,

$$N(\theta) = (a + b\sqrt{m})(a - b\sqrt{m})$$

$$= a^2 - mb^2 \equiv \pm 1\ (mod\ 4)$$

$$\Rightarrow a^2 - 2b^2 \equiv \pm 1 \ (mod\ 4)$$

olup bu kongrüans a ve b tek tamsayılar veya a tek , b çift olduğunda bir çözüme sahiptir. Bu nedenle a ve b' nin diğer durumları için kongrüans çözülemezdir.

Eğer $m \equiv 3 \ (mod\ 4)$ ise $a, b \in \mathbb{Z}$ olmak üzere $\mathbb{Q}(\sqrt{m})$ kuadratik cisminin tamsayıları $a + b\sqrt{m}$ biçiminde olduğundan $\theta \in O_{\mathbb{Q}(\sqrt{m})}$ elemanları için $\theta = a + b\sqrt{m}$ olmak üzere,

$$N(\theta) = \left(a + b\sqrt{m}\right)(a - b\sqrt{m})$$

$$= a^2 - mb^2 \equiv \pm 1 \ (mod\ 4)$$

$$\Rightarrow a^2 + b^2 \equiv \pm 1 \ (mod\ 4)$$

olup bu kongrüans a ve b çift veya tek tamsayılar olduğunda bir çözüme sahip değildir. Bu nedenle a ve b' nin diğer durumları için kongrüans çözülebilirdir.

Şimdi aşağıdaki sonuç verilebilir.

Sonuç 1.2.1. m karesiz bir tamsayı olmak üzere $O_{\mathbb{Q}(\sqrt{m})}$' nin birimleri,

a) $m \equiv 1 \ (mod\ 4)$ ise o zaman a ve b nin her ikisi de çift ya da tek olmak üzere $\theta = \frac{a+b\sqrt{m}}{2}$ biçiminde,

b) $m \equiv 1 \ (mod\ 8)$ ise o zaman $a = 4k + 2$, $b = 4k$ ya da $a = 4k$, $b = 4k + 2$ olmak üzere $\theta = \frac{a+b\sqrt{m}}{2}$ biçiminde,

c) $m \equiv 2 \ (mod\ 4)$ ise o zaman a ve b tek tamsayılar veya a tek ve b çift olmak üzere $\theta = a + b\sqrt{m}$ biçiminde,

d) $m \equiv 3 \ (mod\ 4)$ ise a ve b' lerden biri tek diğeri çift tamsayı olmak üzere $\theta = a + b\sqrt{m}$ biçiminde olmalıdır [8].

BÖLÜM 2. REEL KUADRATİK CİSİMLERDE BİRİMLER

2.1. $\mathbb{Z}[\sqrt{2}]$' nin Birimleri

Teorem 2.1.1. $\mathbb{Z}[\sqrt{2}]$' nin tüm birimleri $n \in \mathbb{Z}$ olmak üzere $\pm(1+\sqrt{2})^n$ biçimindedir.

İspat. Öncelikle,

$$1 < \lambda < 1 + \sqrt{2} \tag{2.1}$$

aralığında $\mathbb{Z}[\sqrt{2}]$' nin hiçbir λ biriminin olmadığını gösterelim.

$1 < \lambda < 1 + \sqrt{2}$ olacak şekilde $\mathbb{Z}[\sqrt{2}]$' nin bir λ biriminin olduğunu kabul edelim. λ birim olduğundan $\lambda | 1$ dir. O halde $1 = \lambda\mu$ olacak biçimde $\mu \in \mathbb{Z}[\sqrt{2}]$ vardır. Burada,

$$1 = \lambda\mu$$

olduğundan,

$$\overline{\lambda\mu} = 1$$

dir. Ayrıca $\alpha, \beta \in \mathbb{Z}[\sqrt{2}]$ olmak üzere $\overline{\alpha\beta} = \overline{\alpha}\overline{\beta}$ dir. O halde,

$$1 = \lambda\mu = \overline{\lambda\mu} = \overline{\lambda}\overline{\mu}$$

dir. Böylece,

$$1 = (\lambda\overline{\lambda})(\mu\overline{\mu})$$

olur. $\lambda\overline{\lambda} \in \mathbb{Z}$ ve $\mu\overline{\mu} \in \mathbb{Z}$ olduğundan,

$$\lambda\overline{\lambda} = \pm 1$$

elde edilir.

Bunu iki durumda inceleyelim: (a) $\lambda\overline{\lambda} = 1$ ve (b) $\lambda\overline{\lambda} = -1$

(a) $\lambda\overline{\lambda} = 1$ durumu: $\lambda\overline{\lambda} = 1$ olduğundan, $\lambda = 1/\overline{\lambda}$ dir. Şimdi (2.1) eşitsizliğinde λ yerine eşiti olan $1/\overline{\lambda}$ yazalım. Yani,

$$1 < 1/\overline{\lambda} < 1 + \sqrt{2}$$

dir. Buradan,

$$\sqrt{2} - 1 = \frac{1}{\sqrt{2}+1} < \overline{\lambda} < 1 \tag{2.2}$$

olup, (2.1) ve (2.2) eşitsizlikleri taraf tarafa toplanırsa,

$$\sqrt{2} < \lambda + \overline{\lambda} < 2 + \sqrt{2}$$

elde edilir. Buradan da,

$$0{,}7 < \frac{1}{\sqrt{2}} < \frac{\lambda + \overline{\lambda}}{2} < 1 + \frac{1}{\sqrt{2}} < 1{,}8$$

elde edilir. $\frac{\lambda+\overline{\lambda}}{2} \in \mathbb{Z}$ olduğundan $\frac{\lambda+\overline{\lambda}}{2} = 1$ olmak zorundadır.

$\lambda\overline{\lambda} = 1$ ve $\lambda + \overline{\lambda} = 2$ eşitliklerinden $\lambda = \overline{\lambda} = 1$ elde edilir. Bu da (2.1)' de $\lambda > 1$ olmasıyla çelişir.

(b) $\lambda\overline{\lambda} = -1$ durumu: $\lambda\overline{\lambda} = -1$ olduğundan $\lambda = -1/\overline{\lambda}$ dir. Şimdi (2.1) eşitsizliğinde λ yerine eşiti olan $-1/\overline{\lambda}$ yazalım. Yani,

$$1 < -1/\overline{\lambda} < 1 + \sqrt{2}$$

dir. Buradan,

$$-1 < \overline{\lambda} < 1 - \sqrt{2} \tag{2.3}$$

olduğu görülür. Böylece (2.1) ve (2.3) eşitsizlikleri taraf tarafa toplanırsa,

$$0 < \lambda + \bar{\lambda} < 2$$

elde edilir. Buradan da,

$$0 < \frac{\lambda + \bar{\lambda}}{2} < 1$$

elde edilir. Bu da $\frac{\lambda+\bar{\lambda}}{2} \in \mathbb{Z}$ olmasıyla çelişir. O halde $\mathbb{Z}[\sqrt{2}]$' nin 1 ile $1+\sqrt{2}$ aralığında birimi yoktur.

Şimdi de $\eta > 1$ olacak biçimde herhangi bir η birimini ele alalım. 1 ile $1+\sqrt{2}$ aralığında birim olmadığından $\eta \geq 1+\sqrt{2}$ olur. O zaman,

$$\left(1+\sqrt{2}\right)^{n} \leq \eta < \left(1+\sqrt{2}\right)^{n+1}$$

olacak biçimde tek türlü pozitif n tamsayısı vardır. Böylece,

$$1 \leq \eta\left(1+\sqrt{2}\right)^{-n} < 1+\sqrt{2}$$

olur. $n \in \mathbb{N}$ olmak üzere $\eta\left(1+\sqrt{2}\right)^{-n}$, $\mathbb{Z}[\sqrt{2}]$' nin bir birimi olduğundan $\eta\left(1+\sqrt{2}\right)^{-n} = 1$ olmalıdır. O zaman,

$$\eta = \left(1+\sqrt{2}\right)^{n} \tag{2.4}$$

elde edilir.

Eğer $0 < \eta < 1$ ise bu durumda $\frac{1}{\eta}$ bir birimdir ve $\frac{1}{\eta} > 1$ dir. Böylece (2.4)' e göre bazı $n \in \mathbb{N}$ için $\frac{1}{\eta} = (1+\sqrt{2})^{n}$ olup,

$$\eta = \left(1+\sqrt{2}\right)^{-n}$$

elde edilir.

Eğer η, $-1 < \eta < 0$ aralığında bir birim ise bu durumda $-\frac{1}{\eta}$ bir birimdir ve $-\frac{1}{\eta} > 1$ dir. Böylece $n \in \mathbb{N}$ olmak üzere (2.4)' e göre,

$$-\frac{1}{\eta} = (1+\sqrt{2})^n$$

olup,

$$\eta = -\left(1+\sqrt{2}\right)^{-n}$$

elde edilir.

Eğer $\eta < -1$ olan bir birim ise bu durumda $-\eta > 1$ olup, $n \in \mathbb{N}$ olmak üzere (2.4)' e göre,

$$-\eta = (1+\sqrt{2})^n$$

yazılabilir. Buradan,

$$\eta = -\left(1+\sqrt{2}\right)^{n}$$

elde edilir. Açıkça,

$$\pm 1 = \pm(1+\sqrt{2})^0$$

dir.

O halde , $k \in \mathbb{Z}$ olmak üzere $\mathbb{Z}[\sqrt{2}]$' nin tüm birimleri,

$$\eta = \pm\left(1+\sqrt{2}\right)^{k}$$

biçimindedir.

2.2. $x^2 - my^2 = 1$ Denklemi

Bu kısımda m tamkare olmayan pozitif bir tamsayı olmak üzere $x^2 - my^2 = 1$ denkleminin $(x, y) \neq (\pm 1,0)$ olan x ve y tamsayı çözümlerinin olduğunu belirten teorem ispatı gösterilmeden verilecektir.

Teorem 2.2.1. m tamkare olmayan pozitif bir tamsayı olsun. $x^2 - my^2 = 1$ denkleminin $(x, y) \neq (\pm 1, 0)$ olan x ve y tamsayı çözümleri vardır [9].

2.3. Normu 1 Olan Birimler

m karesiz pozitif bir tamsayı olsun. Teorem 2.2.1' e göre $x^2 - my^2 = 1$ denkleminin x ve y pozitif tamsayı çözümleri vardır. Böylece $\lambda = x + y\sqrt{m}$ $O_{\mathbb{Q}(\sqrt{m})}$' nin $\lambda > 1$ ve $N(\lambda) = 1$ olan bir birimidir. Ayrıca λ birimse her $n \in \mathbb{Z}$ için λ^n de bir birimdir. $n \neq m$ ise $\lambda^n \neq \lambda^m$ olduğundan $O_{\mathbb{Q}(\sqrt{m})}$' nin sonsuz sayıda birimi vardır. Tüm bu birimler u ve v, $u^2 - mv^2 = 1$ denklemini sağlayan tamsayılar olmak üzere $u + v\sqrt{m}$ biçimindedir. Fakat $m \equiv 1\ (mod\ 4)$ durumunda u ve v ikisi de tek tamsayılar olmak üzere $O_{\mathbb{Q}(\sqrt{m})}$' nin $\frac{u+v\sqrt{m}}{2}$ biçiminde birimleri olabilir de olmayabilir de. Örneğin $O_{\mathbb{Q}(\sqrt{5})}$' in normu 1 olan bir birimi $\frac{3+\sqrt{5}}{2}$ dir. Aksine, u ve v ikisi de tek tamsayılar olmak üzere $O_{\mathbb{Q}(\sqrt{17})}$, $\frac{u+v\sqrt{m}}{2}$ biçiminde birimler içermez. Çünkü u ve v ikisi de tek tamsayılar olmak üzere $u^2 - 17v^2 \equiv \pm 4\ (mod\ 8)$ kongrüansının çözümü yoktur.

x ve y' nin her ikisi de tamsayı ya da $m \equiv 1\ (mod\ 4)$ durumunda ikisi de tek tamsayıların yarısı olsun. $O_{\mathbb{Q}(\sqrt{m})}$' nin normu 1 olan bir $\lambda = x + y\sqrt{m}$ birimini alalım. Şimdi $\lambda = x + y\sqrt{m}$' nin $(-\infty, -1)$, $(-1, 0)$, $(0, 1)$ ve $(1, \infty)$ aralıklarında olması durumlarında x ve y' nin işaretlerini belirleyelim.

Teorem 2.3.1. m karesiz pozitif bir tamsayı olmak üzere x ve y tamsayılar veya x ve y tek tamsayıların yarısı biçiminde ve $x^2 - my^2 = 1$ olsun. Bu durumda,

$$x + y\sqrt{m} > 1 \Leftrightarrow x > 0\,, y > 0 \tag{2.5}$$

$$0 < x + y\sqrt{m} < 1 \Leftrightarrow x > 0\,, y < 0 \tag{2.6}$$

$$-1 < x + y\sqrt{m} < 0 \Leftrightarrow x < 0\,, y > 0 \tag{2.7}$$

$$x + y\sqrt{m} < -1 \Leftrightarrow x < 0\,, y < 0 \tag{2.8}$$

dir.

İspat. Önce (2.5)' i ispatlayalım:

Öncelikle,

$$x > 0\,,\; y > 0 \Rightarrow x \geq \tfrac{1}{2}\,, y \geq \tfrac{1}{2} \Rightarrow x + y\sqrt{m} \geq \tfrac{1+\sqrt{m}}{2} \geq \tfrac{1+\sqrt{2}}{2} > 1$$

olur. Tersine $x + y\sqrt{m} > 1$ olsun. O zaman,

$$\left(x + y\sqrt{m}\right)\left(x - y\sqrt{m}\,\right) = x^2 - my^2 = 1$$

olduğundan,

$$x + y\sqrt{m} > 1 \Rightarrow 0 < x - y\sqrt{m} < 1$$

dir. O halde,

$$x = \frac{1}{2}\left[\left(x + y\sqrt{m}\right) + \left(x - y\sqrt{m}\right)\right] > \frac{1}{2} > 0$$

ve

$$y = \frac{1}{2\sqrt{m}}\left[\left(x + y\sqrt{m}\right) - \left(x - y\sqrt{m}\right)\right] > \frac{1-1}{2\sqrt{m}} = 0$$

olur. Bu da (2.5)' i ispatlar.

Şimdi (2.6)' yı ispatlayalım:

$$\left(x + y\sqrt{m}\right)\left(x - y\sqrt{m}\,\right) = x^2 - my^2 = 1$$

olduğundan,

$$x > 0\,,\; y < 0 \;\Rightarrow\; x > 0\,, -y > 0 \Rightarrow\; x \geq \tfrac{1}{2}\,, -y \geq \tfrac{1}{2}$$

$$\Rightarrow x - y\sqrt{m} \geq \tfrac{1+\sqrt{m}}{2} \geq \tfrac{1+\sqrt{2}}{2} > 1$$

$$\Rightarrow 0 < \ x + y\sqrt{m} < 1$$

olur. Tersine $0 < \ x + y\sqrt{m} < 1$ olsun. Bu durumda,

$$0 < \ x + y\sqrt{m} < 1 \ \Rightarrow \ x - y\sqrt{m} > 1$$

dir. O halde,

$$x = \frac{1}{2}\left[\left(x + y\sqrt{m}\right) + \left(x - y\sqrt{m}\right)\right] > \frac{1}{2} > 0$$

ve

$$y = \frac{1}{2\sqrt{m}}\left[\left(x + y\sqrt{m}\right) - \left(x - y\sqrt{m}\right)\right] < \frac{1-1}{2\sqrt{m}} = 0$$

dır. Bu da (2.6)' yı ispatlar.

(2.8) durumu (2.5)' te, (2.7) durumu ise (2.6)' da x yerine $-x$ ve y yerine $-y$ alınarak ispatlanabilir.

Tanım 2.3.1. m karesiz pozitif bir tamsayı olsun.

a) $m \equiv 2{,}3 \ (mod\ 4)$ ise $S_m = \{(x, y) \colon \ x \in \mathbb{N}, \ y \in \mathbb{N}\}$

olsun. $(a, b) \in S_m$, $x^2 - my^2 = 1$ denklemini sağlasın. Yani, $a^2 - mb^2 = 1$ olsun ve a bu şartı sağlayanların en küçüğü olsun. Bu durumda $O_{\mathbb{Q}(\sqrt{m})}$' nin normu 1 olan $\epsilon = a + b\sqrt{m}$ birimine $O_{\mathbb{Q}(\sqrt{m})}$' nin normu 1 olan temel birimi denir.

b) $m \equiv 1 \ (mod\ 4)$ ise $S_m = \{\left(\frac{x}{2}, \frac{y}{2}\right) \colon x \in \mathbb{N} \ , \ y \in \mathbb{N} \ , \ x \equiv y \ (mod\ 2)\}$

olsun. $(a, b) \in S_m$ olsun. Yani, $a^2 - mb^2 = 1$ olsun ve a bu şartı sağlayanların en küçüğü olsun. Bu durumda $O_{\mathbb{Q}(\sqrt{m})}$' nin normu 1 olan $\epsilon = a + b\sqrt{m}$ birimine $O_{\mathbb{Q}(\sqrt{m})}$' nin normu 1 olan temel birimi denir. Burada $(a, b) \in S_m$ ise $(a, b) = \left(\frac{x}{2}, \frac{y}{2}\right)$ ve $x \equiv y \ (mod\ 2)$ olduğuna dikkat ediniz.

NOT. $m \equiv 2,3 \ (mod\ 4)$ ise $\epsilon \geq 1 + \sqrt{m} \geq 1 + \sqrt{2}$ ve

$m \equiv 1 \ (mod\ 4)$ ise $\epsilon \geq \frac{1+\sqrt{m}}{2} \geq \frac{1+\sqrt{5}}{2}$

olduğundan $\epsilon > 1$ dir.

Şimdiki teorem $O_{\mathbb{Q}(\sqrt{m})}$' nin normu 1 olan birimleri ile normu 1 olan temel birim arasındaki ilişkiyi göstermektedir.

Teorem 2.3.2. m karesiz pozitif bir tamsayı olsun. ϵ' da $O_{\mathbb{Q}(\sqrt{m})}$' nin normu 1 olan temel birimi olsun. Bu durumda,

(a) ϵ, $O_{\mathbb{Q}(\sqrt{m})}$' nin normu 1 olan 1'den büyük en küçük birimidir.

(b) Bazı n tamsayıları için $O_{\mathbb{Q}(\sqrt{m})}$' nin normu 1 olan her birimi $n \in \mathbb{Z}$ olmak üzere $\pm\epsilon^n$ biçimindedir.

(c) $\tau > 1$ olmak üzere $O_{\mathbb{Q}(\sqrt{m})}$' nin normu 1 olan bir birimi τ olsun. Ayrıca $n \in \mathbb{Z}$ olmak üzere $O_{\mathbb{Q}(\sqrt{m})}$' nin normu 1 olan her birimi $\pm\tau^n$ biçiminde olsun. Bu taktirde $\tau = \epsilon$ dir.

İspat. (a) ϵ, $O_{\mathbb{Q}(\sqrt{m})}$' nin normu 1 olan temel birimi olduğundan Tanım 2.3.1' e göre a en küçük tamsayı olmak üzere,

$$\epsilon = a + b\sqrt{m}\ ,\ (a,b) \in S_m\ ,\ a^2 - mb^2 = 1$$

dir.

ϵ_1, $O_{\mathbb{Q}(\sqrt{m})}$' nin normu 1 olan ve $1 < \epsilon_1 < \epsilon$ şartını sağlayan bir birimi olsun. Teorem 1.2.6 ve Teorem 2.3.1' e göre,

$$\epsilon_1 = a_1 + b_1\sqrt{m}, \quad (a_1, b_1) \in S_m, \quad a_1^2 - mb_1^2 = 1$$

yazılabilir. a' nın minimal olması nedeniyle,

$$a < a_1$$

dir ve

$$b^2 = \frac{a^2 - 1}{m} < \frac{{a_1}^2 - 1}{m} = b_1^2$$

dir. Böylece,

$$b^2 < b_1^2$$

olup,

$$b < b_1$$

elde edilir. Buradan,

$$\epsilon = a + b\sqrt{m} < a_1 + b_1\sqrt{m} = \epsilon_1$$

bulunur. Bu da $\epsilon_1 < \epsilon$ olmasıyla çelişir. O halde $O_{\mathbb{Q}(\sqrt{m})}$' nin 1'den büyük ve normu 1 olan ϵ' dan küçük bir ϵ_1 birimi yoktur.

(b) η, $O_{\mathbb{Q}(\sqrt{m})}$' nin normu 1 olan bir birimi olsun. $O_{\mathbb{Q}(\sqrt{m})}$' nin normu 1 olan η^* birimi aşağıdaki gibi tanımlansın:

$$\eta^* = \begin{cases} \eta\,, & \eta \geq 1 \ \ ise \\ \frac{1}{\eta}, & 0 < \eta < 1 \ ise \\ -\frac{1}{\eta}, & -1 < \eta < 0 \ ise \\ -\eta\,, & \eta \leq -1 \ \ ise. \end{cases} \tag{2.9}$$

Böylece $\eta^* \geq 1$ dir. O zaman $\epsilon > 1$ olduğundan,

$$\epsilon^k \leq \eta^* < \epsilon^{k+1}$$

olacak biçimde negatif olmayan bir k tamsayısı vardır. Eşitsizliğin her tarafını ϵ^{-k} ile çarpılırsa,

$$1 \leq \eta^* \epsilon^{-k} < \epsilon$$

elde edilir. Burada $\eta^*\epsilon^{-1}$, $O_{\mathbb{Q}(\sqrt{m})}$' nin normu 1 olan bir birimidir. Fakat (a)' da $O_{\mathbb{Q}(\sqrt{m})}$' nin normu 1 olan ve 1 ile ϵ arasında bulunan hiçbir biriminin olmadığı görüldü. O halde,

$$\eta^*\epsilon^{-k} = 1$$

dir ve böylece,

$$\eta^* = \epsilon^k$$

dir. O halde (2.9)' a göre,

$$\eta = \pm\epsilon^n$$

olacak biçimde n tamsayısının mevcut olduğu görülür.

(c) ϵ biriminin normu 1 olduğundan, kabulümüzden,

$$\epsilon = \pm\tau^l$$

olan bir l tamsayısı vardır. (b)' ye göre,

$$\tau = \pm\epsilon^n$$

olacak biçimde bir n tamsayısının olduğu bilinmektedir. Böylece,

$$\epsilon = \pm\tau^l = \pm(\pm\epsilon^n)^l = \pm\epsilon^{ln}$$

ve buradan,

$$\epsilon^{ln-1} = \pm 1$$

elde edilir. Eşitliğin her iki tarafının karesi alınırsa,

$$\epsilon^{2(ln-1)} = 1$$

olur. $ln - 1 \neq 0$ olduğunu kabul edelim. Bu durumda ϵ reel sayı olduğundan $\epsilon = \pm 1$ dir. Bu da $\epsilon > 1$ olmasıyla çelişir. O halde $ln - 1 = 0$ yani,

$$ln = 1$$

dir. Buradan,

$$l = n = \pm 1$$

elde edilir. Bu da,

$$\tau = \pm\epsilon \quad \text{ya da} \quad \tau = \pm\epsilon^{-1}$$

olduğunu gösterir.

$$\tau > 1 \quad \text{ve} \quad \epsilon > 1$$

olduğundan,

$$\tau = \epsilon$$

olduğu görülür.

2.4. Normu -1 Olan Birimler

m karesiz pozitif bir tamsayı olsun. $\mathbb{Q}(\sqrt{m})$ reel kuadratik cisminin $O_{\mathbb{Q}(\sqrt{m})}$ kümesini oluşturan tamsayılarının normu -1 olan birimleri olabilir de, olmayabilir de. Örneğin $O_{\mathbb{Q}(\sqrt{2})}$' de,

$$N(1+\sqrt{2}) = (1+\sqrt{2})(1-\sqrt{2}) = 1^2 - (\sqrt{2})^2 = -1$$

olduğundan $O_{\mathbb{Q}(\sqrt{2})}$' nin normu -1 olan bir birimi $1+\sqrt{2}$ dir. Fakat $O_{\mathbb{Q}(\sqrt{3})}$' de bir $\theta \in U(O_{\mathbb{Q}(\sqrt{3})})$ birimini ele alırsak a ve b' ler tamsayı olmak üzere $\theta = a + b\sqrt{3}$' ün normu,

$$N(\theta) = (a+b\sqrt{3})(a-b\sqrt{3})$$

dir. Eğer $a^2 - 3b^2 = -1$ ise $a^2 \equiv -1 \ (mod\ 3)$ dir. O halde $3 | a^2 + 1$ dir. Teorem 1.1.4' e göre bu olamaz. O halde $O_{\mathbb{Q}(\sqrt{3})}$' ün normu -1 olan birimi yoktur.

Bu bölümde $O_{\mathbb{Q}(\sqrt{m})}$' nin normu -1 olan birimlerinin olduğu kabul edilerek, $O_{\mathbb{Q}(\sqrt{m})}$' nin normu -1 olan bir tek $\sigma > 1$ biriminin olduğu ve $O_{\mathbb{Q}(\sqrt{m})}$' nin normu -1 olan tüm birimlerinin $n \in \mathbb{Z}$ olmak üzere $\pm\sigma^{2n+1}$ biçiminde olduğu ve $O_{\mathbb{Q}(\sqrt{m})}$' nin normu 1 olan tüm birimlerinin de $n \in \mathbb{Z}$ olmak üzere $\pm\sigma^{2n}$ biçiminde olduğu gösterilecektir.

Teorem 2.4.1. m karesiz pozitif bir tamsayı olsun ve $O_{\mathbb{Q}(\sqrt{m})}$' nin normu -1 olan birimleri var olsun. Bu taktirde $O_{\mathbb{Q}(\sqrt{m})}$' nin normu -1 olan bir tek $\sigma > 1$ birimi vardır ve $O_{\mathbb{Q}(\sqrt{m})}$' deki normu -1 olan her birim n bir tek tamsayı olmak üzere $\pm\sigma^{n}$ biçimindedir.

İspat. ρ , $O_{\mathbb{Q}(\sqrt{m})}$' de normu -1 olan bir birim olsun. $\overline{\rho}$ de bunun eşleniği olsun. O halde,

$$\rho\overline{\rho} = N(\rho) = -1$$

dir. Eşitliğin her iki tarafının karesi alınırsa,

$$\rho^2(\overline{\rho})^2 = 1$$

olur. Böylece ρ^2, $O_{\mathbb{Q}(\sqrt{m})}$' nin normu 1 olan bir birimidir. Teorem 2.3.2(b)' ye göre,

$$\rho^2 = \pm\epsilon^n$$

olacak biçimde bir $n \in \mathbb{Z}$ olduğu bilinmektedir. (Buradaki ϵ, Tanım 2.3.1' deki $O_{\mathbb{Q}(\sqrt{m})}$' nin normu 1 olan temel birimidir.) Açıkça $\rho^2 > 0$ dir ve $\epsilon^n > 0$ dır. O halde,

$$\rho^2 = \epsilon^n$$

dir. Eğer n çiftse,

$n = 2k$ için

$$\rho^2 = \epsilon^{2k}$$

olduğundan,

$$\rho = \pm\epsilon^k$$

olur. Böylece,

$$N(\rho) = N(\pm\epsilon^k) = N(\epsilon)^k = 1$$

elde edilir. Bu da $N(\rho) = -1$ olmasıyla çelişir. O halde n tek olmak zorundadır.

$n = 2l + 1$ olsun. O zaman,

$$\rho^2 = \epsilon^{2l+1}$$

olur. Bu eşitlikten,

$$\epsilon = (\rho\epsilon^{-l})^2 \tag{2.10}$$

elde edilir. Şimdi $\sigma^* = \rho\epsilon^{-l}$ olsun. Bu durumda σ^* normu -1 olan bir birimdir ve

$$\epsilon = (\sigma^*)^2$$

dir. Eğer μ, $O_{\mathbb{Q}(\sqrt{m})}$' nin normu -1 olan birimiyse $\mu\rho^{-1}$ de $O_{\mathbb{Q}(\sqrt{m})}$' nin normu 1 olan bir birimdir ve Teorem 2.3.2(b)' ye göre,

$$\mu\rho^{-1} = \pm\epsilon^k$$

olacak biçimde bir k tamsayısı vardır. Böylece,

$$\rho = \epsilon^l\sigma^* \quad \text{ve} \quad \epsilon = (\sigma^*)^2$$

olduğundan,

$$\mu = \pm\epsilon^k\rho = \pm\epsilon^{k+l}\sigma^* = \pm(\sigma^*)^{2(k+l)+1}$$

elde edilir. Eğer μ, $O_{\mathbb{Q}(\sqrt{m})}$' nin normu 1 olan birimiyse o zaman Teorem 2.3.2(b)' ye göre,

$$\mu = \pm\epsilon^k$$

olan k tamsayısı vardır. Böylece,

$$\epsilon = (\sigma^*)^2$$

olduğundan,

$$\mu = \pm\epsilon^k = \pm(\sigma^*)^{2k}$$

elde edilir. O halde $O_{\mathbb{Q}(\sqrt{m})}$' nin tüm birimleri $n \in \mathbb{Z}$ olmak üzere $\pm(\sigma^*)^n$ biçimindedir.

n' nin çift olmasının normu 1 olan birimleri, n' nin tek olmasının da normu -1 olan birimleri verdiğini not edelim. Şu halde,

1- $\sigma^* > 1$ ise $\sigma = \sigma^*$,
2- $0 < \sigma^* < 1$ ise $\sigma = \frac{1}{\sigma^*}$,
3- $-1 < \sigma^* < 0$ ise $\sigma = -\frac{1}{\sigma^*}$,
4- $\sigma^* < -1$ ise $\sigma =-\sigma^*$

olarak alınırsa normu -1 olan her birimin $\pm(\sigma)^n$ biçiminde olduğu görülür ve $\sigma > 1$ dir. Şimdi σ' nın tekliğini görelim.

σ ve τ, $O_{\mathbb{Q}(\sqrt{m})}$' de normu -1 olan, 1 den büyük iki birim olsun. Teorem 2.4.1' e göre her birim $n \in \mathbb{Z}$ olmak üzere $\pm\sigma^n$ ve $q \in \mathbb{Z}$ olmak üzere $\pm\tau^q$ biçimindedir. Buna göre,

$$\sigma = \pm\tau^k, \quad \tau = \pm\sigma^l$$

olan k ve l tamsayıları vardır. Böylece,

$$\sigma = \pm\tau^k = \pm(\pm\sigma^l)^k = \pm\sigma^{kl}$$

dir ve buradan,

$$\sigma^2 = \sigma^{2kl}$$

olduğu görülür. Böylece,

$$\sigma^{2(kl-1)} = 1$$

elde edilir. Eğer $kl - 1 \neq 0$ ise σ reel sayı olduğundan $\sigma = \pm 1$ olur. Bu da $\sigma > 1$ olmasıyla çelişir. O halde,

$$kl - 1 = 0$$

yani

$$kl = 1$$

dir. Buradan,

$$k = l = \pm 1$$

elde edilir. Böylece,

$$\sigma = \pm\tau \quad \text{veya} \quad \sigma = \pm\tau^{-1}$$

dir. Fakat $\sigma > 1$ ve $\tau > 1$ idi. O halde,

$$\sigma = \tau$$

olur. Bu da σ' nın tekliğini gösterir.

Tanım 2.4.1. σ , $O_{\mathbb{Q}(\sqrt{m})}$' nin normu -1 olan 1 den büyük bir birimi olsun. Eğer σ, Teorem 2.4.1 deki şartları sağlıyorsa o zaman $O_{\mathbb{Q}(\sqrt{m})}$' nin bu σ birimine $O_{\mathbb{Q}(\sqrt{m})}$' nin normu -1 olan temel birimi denir.

Şimdiki teoremde $O_{\mathbb{Q}(\sqrt{m})}$' nin normu 1 olan temel birimi ϵ ile $O_{\mathbb{Q}(\sqrt{m})}$ normu -1 olan birimler içerdiğinde normu -1 olan temel birimi σ arasındaki bağıntı kurulacaktır.

Teorem 2.4.2. m karesiz pozitif bir tamsayı olsun ve $O_{\mathbb{Q}(\sqrt{m})}$ normu -1 olan birimler içersin. $O_{\mathbb{Q}(\sqrt{m})}$' nin normu 1 olan temel birimi ϵ ile normu -1 olan temel birimi σ arasında,

$$\epsilon = \sigma^2$$

eşitliği vardır.

İspat. Teorem 2.4.1' e göre,

$$\epsilon = \pm\sigma^k$$

olan bir k tamsayısı vardır.

$$\epsilon > 1 \quad \text{ve} \quad \sigma > 1$$

olduğundan $k \in \mathbb{Z}$ olmak üzere,

$$\epsilon = \sigma^k$$

dir. Böylece,

$$1 = N(\epsilon) = N(\sigma^k) = N(\sigma)^k = (-1)^k$$

elde edilir. O halde k çifttir. $g \in \mathbb{Z}$ için $k = 2g$ olsun. O halde,

$$\epsilon = \sigma^{2g} \tag{2.11}$$

olur. Böylece,

$$N(\sigma^2) = N(\sigma)^2 = (-1)^2 = 1$$

olduğundan σ^2 normu 1 olan bir birimdir ve Teorem 2.3.2(b)' ye göre,

$$\sigma^2 = \pm\epsilon^l$$

olan bir l tamsayısı vardır.

$$\epsilon > 1 \quad \text{ve} \quad \sigma > 1$$

olduğundan,

$$\sigma^2 = \epsilon^l \tag{2.12}$$

dir. (2.11) ve (2.12)' ye göre,

$$\epsilon = \epsilon^{gl}$$

elde edilir. Buradan,

$$\epsilon^{gl-1} = 1$$

dir. Eğer $gl - 1 \neq 0$ ise ϵ bir reel sayı olduğundan,

$$\epsilon = \pm 1$$

olur. Bu da $\epsilon > 1$ olmasıyla çelişir. O halde,

$$gl - 1 = 0$$

yani,

$$gl = 1$$

dir. Buradan,

$$g = l = \pm 1$$

elde edilir. O halde,

$$\epsilon = \sigma^2 \quad \text{ya da} \quad \epsilon = \sigma^{-2}$$

dir. $\epsilon > 1$ ve $\sigma > 1$ olduğundan,

$$\epsilon = \sigma^2$$

elde edilir.

2.5. Temel Birim

Tanım 2.5.1. m karesiz pozitif bir tamsayı olsun. $O_{\mathbb{Q}(\sqrt{m})}$' nin temel birimi η, eğer $O_{\mathbb{Q}(\sqrt{m})}$ normu -1 olan birimler içeriyorsa Tanım 2.4.1' de bahsedilen σ, içermiyorsa Tanım 2.3.1' de bahsedilen ϵ olarak tanımlanır.

Teorem 2.3.2 ve Teorem 2.4.1' den aşağıdaki teorem verilebilir.

Teorem 2.5.1. m karesiz pozitif bir tamsayı ve η, $O_{\mathbb{Q}(\sqrt{m})}$' nin temel birimi olsun. Bu taktirde $O_{\mathbb{Q}(\sqrt{m})}$' nin her birimi $n \in \mathbb{Z}$ olmak üzere $\pm\eta^n$ biçimindedir. Eğer

$O_{\mathbb{Q}(\sqrt{m})}$ normu -1 olan birimler içerirse, normu -1 olan birimler n tek olmak üzere $\pm\eta^n$ biçiminde ve normu 1 olan birimlerde, n çift olmak üzere $\pm\eta^n$ biçimindedir [9].

Teorem 2.3.2(a)' nın benzeri olan aşağıdaki teorem, Teorem 2.5.1' in bir sonucudur.

Teorem 2.5.2. $\mathbb{Q}(\sqrt{m})$ bir reel kuadratik cisim olsun. $O_{\mathbb{Q}(\sqrt{m})}$' nin temel birimi 1 den büyük olan $O_{\mathbb{Q}(\sqrt{m})}$' nin en küçük birimidir.

İspat. $O_{\mathbb{Q}(\sqrt{m})}$' nin temel birimi η olsun ve

$$1 < \theta < \eta$$

olan bir θ biriminin olduğunu kabul edelim.

Teorem 2.5.1' e göre,

$$\theta = \pm\eta^n$$

olan bir n tamsayısı vardır. θ ve η' nin ikisi de pozitif olduklarından,

$$\theta = \eta^n$$

olur. $n \geq 1$ ise

$$\theta = \eta^n \geq \eta$$

olur ve bu durum $\theta < \eta$ olmasıyla çelişir.

$n \leq 0$ ise

$$\theta = \eta^n \leq 1$$

olup $\theta > 1$ olmasıyla çelişir.

O halde böyle bir θ yoktur. Yani η, 1' den büyük olan en küçük birimdir.

Tablo 2.1. $m,\ 2 \leq m < 40$ aralığındaki karesiz bir tamsayı olmak üzere $O_{\mathbb{Q}(\sqrt{m})}$' nin temel birimleri.

m	Normu 1 olan temel birim (ϵ)	Normu -1 olan temel birim (σ)	Temel birim (η)	Norm $N(\eta)$
2	$3+2\sqrt{2}$	$1+\sqrt{2}$	$1+\sqrt{2}$	-1
3	$2+\sqrt{3}$		$2+\sqrt{3}$	1
5	$\left(3+\sqrt{5}\right)/2$	$\left(1+\sqrt{5}\right)/2$	$\left(1+\sqrt{5}\right)/2$	-1
6	$5+2\sqrt{6}$		$5+2\sqrt{6}$	1
7	$8+3\sqrt{7}$		$8+3\sqrt{7}$	1
10	$19+6\sqrt{10}$	$3+\sqrt{10}$	$3+\sqrt{10}$	-1
11	$10+3\sqrt{11}$		$10+3\sqrt{11}$	1
13	$\left(11+3\sqrt{13}\right)/2$	$\left(3+\sqrt{13}\right)/2$	$\left(3+\sqrt{13}\right)/2$	-1
14	$15+4\sqrt{14}$		$15+4\sqrt{14}$	1
15	$4+\sqrt{15}$		$4+\sqrt{15}$	1
17	$33+8\sqrt{17}$	$4+\sqrt{17}$	$4+\sqrt{17}$	-1
19	$170+39\sqrt{19}$		$170+39\sqrt{19}$	1
21	$\left(5+\sqrt{21}\right)/2$		$\left(5+\sqrt{21}\right)/2$	1
22	$197+42\sqrt{22}$		$197+42\sqrt{22}$	1
23	$24+5\sqrt{23}$		$24+5\sqrt{23}$	1
26	$51+10\sqrt{26}$	$5+\sqrt{26}$	$5+\sqrt{26}$	-1
29	$\left(27+5\sqrt{29}\right)/2$	$\left(5+\sqrt{29}\right)/2$	$\left(5+\sqrt{29}\right)/2$	-1
30	$11+2\sqrt{30}$		$11+2\sqrt{30}$	1
31	$1520+273\sqrt{31}$		$1520+273\sqrt{31}$	1
33	$23+4\sqrt{33}$		$23+4\sqrt{33}$	1
34	$35+6\sqrt{34}$		$35+6\sqrt{34}$	1
35	$6+\sqrt{35}$		$6+\sqrt{35}$	1
37	$73+12\sqrt{37}$	$6+\sqrt{37}$	$6+\sqrt{37}$	-1

38	$37+6\sqrt{38}$		$37+6\sqrt{38}$	1
39	$25+4\sqrt{39}$		$25+4\sqrt{39}$	1

Teorem 2.5.3. $p,\ p\equiv 1\ (mod\ 4)$ olan bir asal sayı olsun. Bu durumda $O_{\mathbb{Q}(\sqrt{p})}$' nin temel biriminin normu -1 dir [9].

Teorem 2.5.4. m karesiz pozitif bir tamsayı olsun. Eğer $q\equiv 3\ (mod\ 4)$ olacak biçimde m' yi bölen bir q asal sayısı varsa $O_{\mathbb{Q}(\sqrt{m})}$ ' nin temel biriminin normu 1 dir.

İspat. $O_{\mathbb{Q}(\sqrt{m})}$' nin temel birimi η' nin normunun -1 olduğunu kabul edelim. x ve y,

$$\begin{cases} x\equiv y\equiv 0\ (mod\ 2), & m\equiv 2,3\ (mod\ 4)\ \ ise \\ x\equiv y\ (mod\ 2), & m\equiv 1\ (mod\ 4)\ \ ise \end{cases}$$

olan tamsayılar olmak üzere,

$$\eta=\frac{x+y\sqrt{m}}{2}$$

olsun. Buna göre,

$$\frac{x^2-my^2}{4}=N(\eta)=-1$$

dir. Böylece,

$$x^2-my^2=-4$$

olur. $q|m$ olduğundan,

$$x^2\equiv -4\ (mod\ q)$$

dir. Böylece,

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

olduğundan Önerme 1.1.1’ e göre $q \equiv 1 \ (mod\ 4)$’ tür. Bu da $q \equiv 3 \ (mod\ 4)$ olmasıyla çelişir. O halde η’ nin normu 1 dir.

Teorem 2.5.5. $p,\ p \equiv 5 \ (mod\ 8)$ olan bir asal sayı olsun. Bu durumda $O_{\mathbb{Q}(\sqrt{2p})}$’ nin temel biriminin normu -1 dir [9].

Teorem 2.5.6. p ve q,

$$p \equiv q \equiv 1 \ (mod\ 4) \quad \text{ve} \quad \left(\frac{p}{q}\right) = -1$$

olan birbirinden farklı asal sayılar olsun. Bu durumda $O_{\mathbb{Q}(\sqrt{pq})}$’ nun temel biriminin normu -1 dir [9].

BÖLÜM 3. SÜREKLİ KESİRLER

Bu kısımda Bölüm 4' te temel birimin hesaplanması için gereken sürekli kesirlerle ilgili temel tanım ve teoremler verilecektir.

3.1. Sonlu Sürekli Kesirler

Tanım 3.1.1. a_0 hariç hepsi pozitif olan $a_0, a_1, a_2, \dots, a_n$ reel sayıları için,

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots \, \cfrac{1}{a_{n-1+\frac{1}{a_n}}}}}}}$$

ifadesine sonlu sürekli kesir denir. Burada $a_1, a_2, \dots, a_n$ reel sayılarına sürekli kesrin kısmi bölenleri denir. Eğer $a_0, a_1, a_2, \dots, a_n$ tamsayılar ise o zaman bu sürekli kesre basittir denir. Sürekli kesirlerin bu gösterimi,

$$a_0 + \frac{1}{a_1+} \frac{1}{a_2+} \dots \frac{1}{+a_n} \quad \text{veya} \quad [a_0, a_1, a_2, \dots, a_n]$$

olarak da gösterilebilir.

Sonlu sürekli kesirler için,

$$[a_0] = \frac{a_0}{1} = a_0$$

$$[a_0, a_1] = a_0 + \frac{1}{a_1}$$

ve $1 \leq k < n$ için

$$[a_0, a_1, \dots, a_{k-1}, a_k] = \left[a_0, a_1, \dots, a_{k-1} + \frac{1}{a_k}\right] = a_0 + \frac{1}{[a_1, a_2, \dots, a_k]}$$

eşitlikleri vardır.

Teorem 3.1.1. Her rasyonel sayı sonlu sürekli kesirlerle ifade edilebilir. Tersine her sonlu sürekli basit kesir bir rasyonel sayı ifade eder [10].

Tanım 3.1.2. $0 < k < n$ olmak üzere $[a_0, a_1, \dots, a_{k-1}, a_k]$ sürekli kesrine, $[a_0, a_1, a_2, \dots, a_n]$ sürekli kesrinin k' yıncı yaklaşımı denir ve bu C_k ile gösterilir.

Teorem 3.1.2. a_0 hariç hepsi pozitif olan $a_0, a_1, a_2, \dots.$ tamsayılarını ele alalım.

p_n ve q_n,

$$p_{-2} = 0 \ , \ q_{-2} = 1$$

$$p_{-1} = 1 \ , \ q_{-1} = 0$$

başlangıç şartlarıyla ve $n \geq 1$ için,

$$
\begin{array}{ll}
p_0 = a_0 & q_0 = 1 \\
p_1 = a_1 p_0 + 1 & q_1 = a_1 \\
p_2 = a_2 p_1 + p_0 & q_2 = a_2 q_1 + 1 \\
\dots\dots & \dots\dots \\
p_n = a_n p_{n-1} + p_{n-2} & q_n = a_n q_{n-1} + q_{n-2}
\end{array}
$$

biçiminde tanımlansın. O zaman $[a_0, a_1, a_2, \dots, a_k]$ sürekli kesrinin n. yaklaşımı $C_n = [a_0, a_1, a_2, \dots, a_n]$ veya $C_n = \frac{p_n}{q_n}$ ile verilir [11].

İspat. Tümevarım ile ispatlayalım.

$k = 0$ için $C_0 = [a_0] = \frac{a_0}{1} = \frac{p_0}{q_0}$ olduğundan doğrudur.

$k = 1$ için $C_1 = [a_0, a_1] = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1} = \frac{p_1}{q_1}$

olur. Şimdi de $2 \leq k < N$ olan pozitif k tamsayısı için teorem doğru olsun. Yani,

$$C_k = [a_0, a_1, a_2, \dots, a_k] = \frac{p_k}{q_k} = \frac{a_k p_{k-1} + p_{k-2}}{a_k q_{k-1} + q_{k-2}}$$

olsun. $k + 1$ için,

$$\begin{aligned}
C_{k+1} &= [a_0, a_1, a_2, \dots, a_k, a_{k+1}] \\
&= [a_0, a_1, a_2, \dots, a_{k-1}, [a_k, a_{k+1}]] \\
&= [a_0, a_1, a_2, \dots, a_{k-1}, a_k + \tfrac{1}{a_{k+1}}] \\
&= \frac{\left(a_k + \frac{1}{a_{k+1}}\right) p_{k-1} + p_{k-2}}{\left(a_k + \frac{1}{a_{k+1}}\right) q_{k-1} + q_{k-2}} \\
&= \frac{a_{k+1}(a_k p_{k-1} + p_{k-2}) + p_{k-1}}{a_{k+1}(a_k q_{k-1} + q_{k-2}) + q_{k-1}} \\
&= \frac{a_{k+1} p_k + p_{k-1}}{a_{k+1} q_k + q_{k-1}} = \frac{p_{k+1}}{q_{k+1}}
\end{aligned}$$

elde edilir. Bu da $k + 1$ için ifadenin doğru olduğunu gösterir. O halde ifade $k + 1$ için de doğru olduğundan istenilen elde edilir.

Teorem 3.1.3. $k \geq 1$ için $a_k > 0$ olmak üzere $a_0, a_1, a_2, \dots$ dizisi verilsin.

$$p_k = a_k p_{k-1} + p_{k-2}, \quad q_k = a_k q_{k-1} + q_{k-2} \tag{3.1}$$

Teorem 3.1.2' de tanımlandığı gibi olsun. Bu taktirde,

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1} \tag{3.2}$$

dir.

İspat. Tümevarım ile ispatlayalım.

$k = 1$ için $p_1 q_0 - q_1 p_0 = (a_0 a_1 + 1)1 - a_0 a_1 = 1 = (-1)^{1-1}$ dir.

İddia k için doğru olsun. $k + 1$ için doğru olduğunu gösterelim.

$$\begin{aligned} p_{k+1} q_k - q_{k+1} p_k &= (a_{k+1} p_k + p_{k-1})q_k - p_k(a_{k+1} q_k + q_{k-1}) \\ &= a_{k+1} p_k q_k + q_k p_{k-1} - a_{k+1} q_k p_k - q_{k-1} p_k \\ &= q_k p_{k-1} - q_{k-1} p_k \\ &= (-1)(p_k q_{k-1} - q_k p_{k-1}) \\ &= (-1)^{k-1+1} = (-1)^k \end{aligned}$$

olduğundan istenilen elde edilir.

Sonuç 3.1.3.1. (3.1)' deki gibi tanımlanan p_k ve q_k değerleri aralarında asaldır.

İspat. $(p_k, q_k) = d$ olsun. (3.2) eşitliğinden,

$$p_k q_{k-1} - q_k p_{k-1} = (-1)^{k-1}$$

dir. $(p_k, q_k) = d$ olduğundan $d|p_k$ ve $d|q_k$ dir. O halde,

$$d|(p_k q_{k-1} - p_{k-1} q_k)$$

yani

$$d|(-1)^{k-1}$$

dir. Bu ise $d = 1$ olduğunu gösterir.

Teorem 3.1.4. $k \geq 1$ için $a_k > 0$ olmak üzere $a_0, a_1, a_2, \ldots$ dizisi verilsin.

$$p_k = a_k p_{k-1} + p_{k-2} \quad , \quad q_k = a_k q_{k-1} + q_{k-2}$$

Teorem 3.1.2' deki tanımlandığı gibi olsun. Bu taktirde,

$$p_k q_{k-2} - p_{k-2} q_k = a_k (-1)^k \tag{3.3}$$

dir [12].

İspat. (3.1)' deki p_k ve q_k değerlerini (3.3)' te yerine yazalım. Bu durumda,

$$\begin{aligned} p_k q_{k-2} - q_k p_{k-2} &= (a_k p_{k-1} + p_{k-2}) q_{k-2} - (a_k q_{k-1} + q_{k-2}) p_{k-2} \\ &= a_k (p_{k-1} q_{k-2} - q_{k-1} p_{k-2}) \\ &= a_k (-1)^{(k-1)-1} \\ &= a_k (-1)^k \end{aligned}$$

olduğu görülür.

Sonuç 3.1.4.1. (p_k) ve (q_k), (3.1)' de verilen tamsayı dizileri ve $C_k = \frac{p_k}{q_k}$ olsun. $k \geq 1$ için,

$$C_k - C_{k-1} = \frac{(-1)^{k-1}}{q_k q_{k-1}}$$

dir. Ayrıca her $k \geq 2$ tamsayısı için,

$$C_k - C_{k-2} = \frac{a_k (-1)^k}{q_k q_{k-2}}$$

dir [12].

Teorem 3.1.5. (3.1)' de tanımlı (p_k) ve (q_k) dizileri ile elde edilen $C_k = \frac{p_k}{q_k}$ değerleri,

$$C_o < C_2 < \cdots < C_3 < C_1$$

sonsuz eşitlik zincirini sağlar. Diğer bir deyişle,

a) Çift indisli C_k değerleri artan bir dizi,

b) Tek indisli C_k değerleri azalan bir dizi teşkil eder.

c) Her $n, m \in \mathbb{N}$ için $C_{2n} < C_{2m-1}$ dir [12].

Önerme 3.1.1. Eğer $C_k = \frac{p_k}{q_k}$, $[a_0, a_1, a_2, \dots, a_n]$ sürekli kesrinin k' yıncı yaklaşımı ve $a_0 > 0$ ise,

$$\frac{p_k}{p_{k-1}} = [a_k, a_{k-1}, \dots, a_1, a_0]$$

ve

$$\frac{q_k}{q_{k-1}} = [a_k, a_{k-1}, \dots, a_2, a_1]$$

dir [12].

3.2. Sonsuz Sürekli Kesirler

Tanım 3.2.1. a_0 hariç hepsi pozitif olan $a_0, a_1, a_2, \dots$ tamsayıları için,

$$[a_0, a_1, a_2, \dots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}}}$$

şeklindeki bir ifadeye sonsuz sürekli kesir denir.

Teorem 3.2.1. (3.1) ile tanımlı (p_k) ve (q_k) dizileri verilsin. Bu taktirde her pozitif x reel sayısı için,

$$[a_0, a_1, a_2, \dots, a_{k-1}, x] = \frac{xp_{k-1} + p_{k-2}}{xq_{k-1} + q_{k-2}}$$

dir [3].

İspat. İspat için tümevarım kullanılırsa $k = 1$ için,

$$[a_0, x] = \frac{xp_0 + p_{-1}}{xq_0 + q_{-1}}$$

olduğu açıktır.

$$[a_0, a_1, a_2, \dots, a_{k-1}, x] = \frac{xp_{k-1} + p_{k-2}}{xq_{k-1} + q_{k-2}}$$

eşitliğinin ilk k terim için doğru olduğunu kabul edelim.

$$[a_0, a_1, a_2, \dots, a_k, x] = [a_0, a_1, a_2, \dots, a_{k-1}, a_k + \frac{1}{x}] = \frac{\left(a_k + \frac{1}{x}\right) p_{k-1} + p_{k-2}}{\left(a_k + \frac{1}{x}\right) q_{k-1} + q_{k-2}}$$

$$= \frac{x(a_k p_{k-1} + p_{k-2}) + p_{k-1}}{x(a_k q_{k-1} + q_{k-2}) + q_{k-1}}$$

$$= \frac{xp_k + p_{k-1}}{xq_k + q_{k-1}}$$

elde edilir ve böylece $k + 1$ terim için de eşitliğin doğru olduğu görülür. Böylece istenilen elde edilmiş olur.

Teorem 3.2.2. $\forall k \geq 0$ tamsayısı için,

$$C_k = [a_0, a_1, a_2, \dots, a_k] \text{ ise } C_k = \frac{p_k}{q_k}$$

dir.

Teorem 3.2.3. $\forall k \geq 1$ için $a_k > 0$ olmak üzere $a_0, a_1, a_2, ...$ tamsayı dizisi verildiğinde $C_k = [a_0, a_1, a_2, ..., a_k]$ ise $\lim_{k\to\infty} C_k$ mevcuttur ve $\forall r, s \geq 0$ tamsayıları için,

$$C_{2r} < \lim_{k\to\infty} C_k < C_{2s+1}$$

dir.

Tanım 3.2.2. a_0 hariç hepsi pozitif tamsayı olan $a_0, a_1, a_2, ...$ tamsayı dizisi ile oluşturulan $[a_0, a_1, a_2, ...]$ sürekli kesrine sonsuz basit sürekli kesir denir. $[a_0, a_1, a_2, ...]$' in değeri $\lim_{k\to\infty}[a_0, a_1, a_2, ..., a_k]$ olarak tanımlanır. Bu limit $\lim_{k\to\infty} C_k$ şeklinde de ifade edilebilir [2].

Teorem 3.2.4. $k \geq 1$ için $a_k > 0$ olmak üzere $a_0, a_1, a_2, ...$ tamsayı dizisi verilsin. Bu durumda $[a_0, a_1, a_2, ..., a_n, ...]$ sonsuz sürekli kesri irrasyoneldir. Aksine her irrasyonel sayının bir sonsuz sürekli kesir açılımı vardır [7].

Teorem 3.2.5. (a_n) ve (b_n),

$$[a_0, a_1, a_2, ...] = [b_0, b_1, b_2, ...]$$

olan iki sonsuz sürekli kesir olsun. Bu durumda $n \in \mathbb{Z}$ olmak üzere,

$$a_n = b_n$$

dir [13].

Teorem 3.2.6. $\beta = [a_0, a_1, a_2, ...]$ olsun. Bu taktirde $\beta_1 = [a_1, a_2, ...]$ olmak üzere $[\![\beta]\!] = a_0$ ve $\beta = a_0 + \frac{1}{\beta_1}$ dir [7].

Teorem 3.2.7. $k \geq 1$ için $a_k > 0$ olmak üzere $a_0, a_1, a_2, \dots$ tamsayı dizisi verilsin. $\alpha = \alpha_0$ irrasyonel sayısı için,

$$a_k = [\![\alpha_k]\!] \quad \text{ve} \quad \alpha_{k+1} = \frac{1}{\alpha_k - a_k} \quad (k = 0,1,2,3, \dots)$$

şeklinde tanımlanırsa $\alpha = [a_0, a_1, a_2, \dots]$' dir.

Teorem 3.2.8. $k \geq 1$ için $a_k > 0$ olmak üzere $a_0, a_1, a_2, \dots$ tamsayı dizisi için $[a_0, a_1, a_2, a_3 \dots]$ sonsuz sürekli kesrini ele alalım. k, pozitif bir tamsayı ve $\alpha_k = [a_k, a_{k+1}, a_{k+2} \dots]$ olsun. O zaman,

$$[a_0, a_1, a_2, a_3 \dots] = [a_0, a_1, a_2, a_3, \dots, a_{k-1}, \alpha_k]$$

dir [12].

Örnek 3.2.1. $\sqrt{3}$ irrasyonel sayısının sürekli kesir açılımını bulunuz.

Çözüm.

$$a_0 = [\![\sqrt{3}]\!] = 1\,, \qquad \alpha_1 = \frac{1}{\sqrt{3}-1} = \frac{\sqrt{3}+1}{2}$$

$$a_1 = \left[\!\!\left[\frac{\sqrt{3}+1}{2}\right]\!\!\right] = 1\,, \qquad \alpha_2 = \frac{1}{\alpha_1 - a_1} = \frac{2}{\sqrt{3}-1} = \sqrt{3}+1$$

$$a_2 = [\![\sqrt{3}+1]\!] = 2\,, \qquad \alpha_3 = \frac{1}{\alpha_2 - a_2} = \frac{1}{\sqrt{3}-1} = \frac{\sqrt{3}+1}{2}$$

$\alpha_3 = \alpha_1$ olduğundan, $\alpha_4 = \alpha_2$ dir ve böylece $\alpha_5 = \alpha_3 = \alpha_1$ elde edilir. Bu durumda $k > 0$ için,

$$a_k = \begin{cases} 1\,, & k \;\; tek\, ise \\ 2, & k \;\; çift\, ise \end{cases}$$

olur. Yani $\sqrt{3} = [1,1,2,1,2, \dots]$ dır. (3.1)' de verilen p_k ve q_k eşitliklerini kullanarak bu sonsuz sürekli kesrin C_k yaklaşımlarını yazabiliriz. $\sqrt{3}$ sonsuz sürekli kesrinin birkaç yaklaşımı,

$$1,2,\frac{5}{3},\frac{7}{4},\frac{19}{11},\frac{26}{25}$$

şeklindedir.

Örnek 3.2.2. $\sqrt{21}$ irrasyonel sayısının sürekli kesir açılımını bulunuz.

Çözüm.

$$a_0 = [\![\sqrt{21}]\!] = 4\,, \quad \alpha_1 = \frac{1}{\sqrt{21}-4} = \frac{\sqrt{21}+4}{5}$$

$$a_1 = \left[\!\!\left[\frac{\sqrt{21}+4}{5}\right]\!\!\right] = 1 \;,\; \alpha_2 = \frac{1}{\frac{\sqrt{21}+4}{5}-1} = \frac{5}{\sqrt{21}-1} = \frac{5(\sqrt{21}+1)}{20} = \frac{\sqrt{21}+1}{4}$$

$$a_2 = \left[\!\!\left[\frac{\sqrt{21}+1}{4}\right]\!\!\right] = 1 \;,\; \alpha_3 = \frac{1}{\frac{\sqrt{21}+1}{4}-1} = \frac{4}{\sqrt{21}-3} = \frac{4(\sqrt{21}+3)}{12} = \frac{\sqrt{21}+3}{3}$$

$$a_3 = \left[\!\!\left[\frac{\sqrt{21}+3}{3}\right]\!\!\right] = 2 \,,\; \alpha_4 = \frac{1}{\frac{\sqrt{21}+3}{3}-2} = \frac{3}{\sqrt{21}-3} = \frac{3(\sqrt{21}+3)}{12} = \frac{\sqrt{21}+3}{4}$$

$$a_4 = \left[\!\!\left[\frac{\sqrt{21}+3}{4}\right]\!\!\right] = 1 \,,\; \alpha_5 = \frac{1}{\frac{\sqrt{21}+3}{4}-1} = \frac{4}{\sqrt{21}-1} = \frac{4(\sqrt{21}+1)}{20} = \frac{\sqrt{21}+1}{5}$$

$$a_5 = \left[\!\!\left[\frac{\sqrt{21}+1}{5}\right]\!\!\right] = 1 \,,\; \alpha_6 = \frac{1}{\frac{\sqrt{21}+1}{5}-1} = \frac{5}{\sqrt{21}-4} = \frac{5(\sqrt{21}+4)}{5} = \sqrt{21}+4$$

$$a_6 = [\![\sqrt{21}+4]\!] = 8 \,,\; \alpha_7 = \frac{1}{\sqrt{21}+4-8} = \frac{1}{\sqrt{21}-4} = \frac{\sqrt{21}+4}{5}$$

$\alpha_7 = \alpha_1$ olduğundan, $\alpha_8 = \alpha_2$, $\alpha_9 = \alpha_3, \ldots$ dir. Devam edilirse $\alpha_{13} = \alpha_7 = \alpha_1$ olduğu görülür. O halde,

$$\alpha = [4,1,1,2,1,1,8,1,1,2,1,1,8,\ldots]$$

dir.

3.3. Periyodik Sürekli Kesirler

Tanım 3.3.1. $n \geq 1$ için $a_n > 0$ olmak üzere $a_0, a_1, a_2, \ldots$ tamsayı dizisi verilsin. Her $m \geq M$ için $a_m = a_{m+k}$ eşitliğini sağlayan bir $M > 0$ varsa bu sonsuz sürekli kesre periyodik sürekli kesir denir. En küçük k değerine de bu sonsuz sürekli kesrin periyodu denir ve bu,

$$[a_0, a_1, a_2, a_3, \ldots, \overline{a_M, a_{M+1}, \ldots, a_{M+k-1}}]$$

şeklinde gösterilir.

Örnek 3.3.1. $\sqrt{21}$ için Örnek 3.2.2' den,

$\sqrt{21} = [4,1,1,2,1,1,8,1,1,2,1,1,8, \ldots] = [4, \overline{1,1,2,1,1,8}]$ olup periyodu 6' dır.

Teorem 3.3.1. Her periyodik basit sürekli kesir bir kuadratik irrasyonel sayıya eşittir [3].

Örnek 3.3.2. $\alpha = [5, \overline{1,10}]$ sayısını irrasyonel olarak ifade ediniz.

Çözüm. $\alpha = [5, \overline{1,10}]$ alınırsa α' nın değerini bulmak için $\beta = [\overline{1,10}]$ alınsın. Buradan $\alpha = [5, \beta]$ olur.

$$\beta = [1,10,1,10, \ldots] = [1,10, \beta]$$

dir. Böylece,

$$\beta = 1 + \cfrac{1}{10 + \cfrac{1}{\beta}} \Rightarrow \beta = \frac{11\beta + 1}{10\beta + 1}$$

$$\Rightarrow 10\beta^2 - 10\beta - 1 = 0$$

kuadratik denklemi bulunur. $\beta > 0$ olduğundan bu denklemin kökü,

$$\beta = 5 + \sqrt{35}$$

bulunur. O halde,

$$\alpha = [5, \beta] = 5 + \frac{1}{5 + \sqrt{35}} = \frac{45 + \sqrt{35}}{85}$$

elde edilir.

Örnek 3.3.3. $\alpha = [1,1,1,1, \ldots]$ sonsuz sürekli kesrini irrasyonel sayı olarak ifade ediniz.

Çözüm. $\alpha = [1,1,1,1, \ldots] = \big[1, [1,1, \ldots]\big] = [1, \alpha]$ şeklinde yazılabilir. Buradan,

$$\alpha = 1 + \frac{1}{\alpha} \Rightarrow \alpha^2 - \alpha - 1 = 0$$

kuadratik denklemi elde edilir. α pozitif olacağından,

$$\alpha = \frac{1 + \sqrt{5}}{2}$$

bulunur.

Önerme 3.3.1. Her α kuadratik irrasyonel sayısı D tamkare olmayan pozitif bir tamsayı ve $Q | D - P^2$ $(Q \neq 0,\ Q, P \in \mathbb{Z})$ olmak üzere,

$$\alpha = \frac{P + \sqrt{D}}{Q}$$

biçiminde yazılabilir [3].

Teorem 3.3.2. Her kuadratik irrasyonel sayının sürekli kesre açılımı periyodiktir [14].

İspat. $\alpha = \alpha_0 = [a_0, a_1, a_2, a_3 \dots]$ kuadratik irrasyonel sayı olsun. Önerme 3.3.1' e göre,

$$\alpha_0 = \frac{P_0 + \sqrt{D}}{Q_0} \quad , \quad Q_0 \big| D - {P_0}^2$$

biçiminde yazılabilir. $\alpha = \alpha_0$ için aşağıdaki eşitlikler $\forall k \geq 0$ olmak üzere,

$$P_{k+1} = a_k Q_k - P_k \tag{3.4}$$
$$Q_{k+1} = \frac{D - P_{k+1}^2}{Q_k}$$

biçiminde tanımlansın. Tanımlanan bu eşitlikler için aşağıdaki ifadeler doğrudur. Her $k \geq 0$ tamsayısı için,

a) P_k , $Q_k \in \mathbb{Z}$ ve $Q_k \neq 0$

b) $\alpha_k = \frac{P_k + \sqrt{D}}{Q_k}$, $[\![\alpha_k]\!] = a_k$ (3.5)

c) $Q_k \big| D - {P_k}^2$

dir. Bunların ispatları tümevarımla kolayca yapılabilir. $\overline{\alpha_k}$ ile α_k' nın eşleniğini gösterilirse,

$$\overline{\alpha_k} = \frac{P_k - \sqrt{D}}{Q_k} \quad \text{ve} \quad \bar{\alpha} = \overline{\alpha_k} = [a_0, a_1, \dots, a_{k-1}, \overline{\alpha_k}]$$

olur ve buradan,

$$\overline{\alpha_0} = \frac{\overline{\alpha_k} p_{k-1} + p_{k-2}}{\overline{\alpha_k} q_{k-1} + q_{k-2}}$$

elde edilir. Son eşitlikten $\overline{\alpha_k}$ çekilirse,

$$\overline{\alpha_k} = -\frac{q_{k-2}}{q_{k-1}}\left(\frac{\bar{\alpha} - p_{k-2}/q_{k-2}}{\bar{\alpha} - p_{k-1}/q_{k-1}}\right)$$

bulunur. k' nın sonsuza gitmesi durumunda limit alınırsa $\frac{p_{k-2}}{q_{k-2}}$ ve $\frac{p_{k-1}}{q_{k-1}}$ değerlerinin ikisi de α_0' a yaklaşır ve böylece yukarıdaki parantezin içi 1 olur. Bu yüzden N keyfi sabit bir tamsayı olmak üzere $k > N$ olacak şekilde yeterince büyük k pozitif tamsayısı için yukarıdaki parantez içi pozitiftir ve $-1 < \overline{\alpha_k} < 0$ dır. Her $k \geq 1$ için α_k pozitif olduğundan $k > N$ için $\alpha_k - \overline{\alpha_k} > 0$ dır.

(3.5)' e göre $\alpha_k - \overline{\alpha_k} = 2\sqrt{D}/Q_k > 0$ dır ve buradan $Q_k > 0$ olduğu görülür. Yine (3.4) ve (3.5) eşitliklerinden $k > N$ için,

$$Q_k Q_{k+1} = D - P_{k+1}^2 \leq D \quad , \qquad Q_k \leq Q_k Q_{k+1} \leq D$$

ve

$$P_{k+1}^2 \leq P_{k+1}^2 + Q_k Q_{k+1} = D \quad , \quad |P_{k+1}| < \sqrt{D}$$

bulunur. Böylece D sabit pozitif bir tamsayı olduğundan, Q_k ve P_{k+1} sayılarının $k > N$ için alabilecekleri değerlerin sonlu sayıda olduğu sonucuna varılır. Ayrıca bu eşitliklerin ikisini birden sağlayan (P_k, Q_k) çifterinin sayısı sonlu olacaktır.

Böylece öyle m ve n tamsayıları vardır ki $P_m = P_n$ ve $Q_m = Q_n$ dir. O halde $\alpha_m = \alpha_n$ yazılabilir. Bu ise açılımın periyodik olduğunu gösterir [2].

Sonuç 3.3.2.1. Teorem 3.3.2' de verilen (3.4) ve (3.5) eşitlikleri yardımı ile $\alpha = \frac{P+\sqrt{D}}{Q}$ şeklinde verilen bir kuadratik irrasyonel sayının sonsuz sürekli kesirlere açılımı bulunabilir.

Örnek 3.3.4. $\alpha = \frac{1+\sqrt{2}}{3}$ irrasyonel sayısının sonsuz sürekli kesir açılımını bulunuz.

Çözüm. $D = 2,\ P_0 = 1,\ Q_0 = 3$ değerleri alınarak açılım yapılamaz, çünkü $Q_0 \big| D - {P_0}^2$ şartı sağlanamaz. Bunun için α' yı Teorem 3.3.2' e göre,

$$\alpha = \frac{3 + \sqrt{18}}{9}$$

şekline getirmek gerekir. Bu durumda $D = 18$, $P_0 = 3$, $Q_0 = 9$ dir. Buradan $a_0 = [\![\alpha]\!] = 0$ ve

$$P_1 = 0.9 - 3 = -3 \qquad \alpha_1 = \left(-3 + \sqrt{18}\right)/1$$

$$Q_1 = (18 - (-3)^2)/9 = 1 \qquad a_1 = [\![\left(-3 + \sqrt{18}\right)/1]\!] = 1$$

$$P_2 = 1.1 - (-3) = 4 \qquad \alpha_2 = \left(4 + \sqrt{18}\right)/2$$

$$Q_2 = (18 - (4)^2)/1 = 2 \qquad a_2 = [\![\left(4 + \sqrt{18}\right)/2]\!] = 4$$

$$P_3 = 4.2 - 4 = 4 \qquad \alpha_3 = \left(4 + \sqrt{18}\right)/1$$

$$Q_3 = (18 - (4)^2)/2 = 1 \qquad a_3 = [\![\left(4 + \sqrt{18}\right)/1]\!] = 8$$

$$P_4 = 8.1 - 4 = 4 \qquad \alpha_4 = \left(4 + \sqrt{18}\right)/2$$

$$Q_4 = (18 - (4)^2)/1 = 2 \qquad a_4 = [\![\left(4 + \sqrt{18}\right)/2]\!] = 4$$

ve böyle devam edilirse $P_2 = P_4$ ve $Q_2 = Q_4$ yinelemesi elde edilir. Buradan,

$$\left(1 + \sqrt{2}\right)/3 = [0,1,4,8,4,8,\dots] = [0,1,\overline{4,8}]$$

bulunur. Burada a_k' lar kısmi bölümler, α_k'lar da kuadratik irrasyonellerdir.

Teorem 3.3.3. x,

$$\left|\frac{p}{q} - x\right| < \frac{1}{2q^2}$$

olan bir irrasyonel sayı ise $\frac{p}{q}$, x' in yaklaşımlarından biridir [13].

Önerme 3.3.1. d tamkare olmayan pozitif bir tamsayı olsun. p_n ve q_n, (3.1)' de ve P_n ve Q_n değerleri de (3.4)' te tanımlandığı gibi olsun. Bu taktirde $n \geq 1$ olmak üzere,

$$p_n^2 - dq_n^2 = (-1)^{n-1}Q_{n+1}$$

dir.

3.4. Tamamıyla Periyodik Sürekli Kesirler

Tanım 3.4.1. $k = 0,1,2,3,\dots$ için $a_k = a_{n+k}$ olacak şekilde bir n tamsayısı varsa

$[a_0, a_1, a_2, a_3, \dots]$ sürekli kesrine tamamıyla periyodik sürekli kesir denir ve bu,

$$[a_0, a_1, a_2, a_3, \dots] = [\overline{a_0, a_1, a_2, a_3, \dots, a_{n-1}}]$$

şeklinde gösterilir. Bu sürekli kesrin periyodu ise n' dir.

Tanım 3.4.2. α bir kuadratik irrasyonel olsun. Eğer $\alpha > 1$ ve $-1 < \bar{\alpha} < 0$ ise α' ya indirgenmiş kuadratik irrasyonel sayı denir. Burada $\bar{\alpha}$ ile α' nın eşleniği ifade edilmektedir [12].

Örneğin $\sqrt{3} + 1 = [\overline{2,1}]$ bir indirgenmiş kuadratik irrasyonel sayıdır. Çünkü $\bar{\alpha} = 1 - \sqrt{3}$ olup $-1 < \bar{\alpha} < 0$ dir.

Teorem 3.4.1. α kuadratik irrasyonel sayısının sürekli kesirlere açılımının tamamıyla periyodik olması için gerek ve yeter şart α' nın indirgenmiş kuadratik irrasyonel sayı olmasıdır [15].

3.5. $\sqrt{d}$' nin Sürekli Kesre Açılımı

Bu kısımda d tamkare olmayan pozitif bir tamsayı olmak üzere $\sqrt{d}$ biçimindeki kuadratik irrasyonel sayısının sürekli kesre açılımı incelenecektir.

Teorem 3.5.1. d tamkare olmayan pozitif bir tamsayı olsun. $\sqrt{d}$ kuadratik irrasyonel sayısının sürekli kesre açılımı $a_0 = [\![\sqrt{d}]\!]$ olmak üzere,

$$\sqrt{d} = [a_0, \overline{a_1, a_2, \ldots, a_{n-1}, 2a_0}\,]$$

biçimindedir. Burada periyod n' dir [3].

Örnek 3.5.1. $\sqrt{2}$ irrasyonel sayısının sonsuz sürekli kesir açılımını bulunuz.

Çözüm.

$$a_0 = [\![\sqrt{2}]\!] = 1 \quad , \quad \alpha_1 = \frac{1}{\sqrt{2}-1} = \sqrt{2}+1$$

$$a_1 = [\![\sqrt{2}+1]\!] = 2 = 2a_0$$

dır. Böylece $\sqrt{2} = [1, \overline{2}]$ bulunur. Aksine $[1, \overline{2}]$' nin $\sqrt{2}$ olduğunu gösterelim.

$$\alpha = [1,2,2, \ldots] \Rightarrow \alpha = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{\ddots}}} \Rightarrow \alpha - 1 = \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{\ddots}}}$$

olup,

$$\alpha - 1 = \frac{1}{2 + (\alpha - 1)} \Rightarrow \alpha - 1 = \frac{1}{\alpha + 1} \Rightarrow \alpha^2 - 1 = 1$$

$$\Rightarrow \alpha^2 = 2 \Rightarrow \alpha = \sqrt{2}$$

dir.

Örnek 3.5.2. $\sqrt{6}$ irrasyonel sayısının sonsuz sürekli kesir açılımını bulunuz.

Çözüm.

$$a_0 = [\![\sqrt{6}]\!] = 2 \quad , \qquad \alpha_1 = \frac{1}{\sqrt{6}-2} = \frac{\sqrt{6}+2}{2}$$

$$a_1 = \left[\!\!\left[\frac{\sqrt{6}+2}{2}\right]\!\!\right] = 2 \quad , \qquad \alpha_2 = \frac{1}{\frac{\sqrt{6}+2}{2}-2} = \frac{2}{\sqrt{6}-2} = \frac{2(\sqrt{6}+2)}{2} = \sqrt{6} + 2$$

$$a_2 = [\![\sqrt{6} + 2]\!] = 4 = 2a_0$$

olduğundan $\alpha = [2, \overline{2,4}]$ elde edilir.

Teorem 3.5.2. d tamkare olmayan pozitif bir tamsayı olsun. $a_0 = [\![\sqrt{d}]\!]$ olmak üzere,

$$\begin{aligned} \alpha_k &= \frac{P_k+\sqrt{d}}{Q_k} \\ a_k &= [\![\alpha_k]\!] \\ Q_{k+1} &= \frac{n-P^2{}_{k+1}}{Q_k} \end{aligned} \tag{3.6}$$

$k = 0,1,2,\ldots$ için ardışık olarak tanımlanırsa,

$$\alpha = [a_0, a_1, a_2, \ldots]$$

dir.

Açıkça $\alpha_n > 1$ dir ve $P_0 = 0$, $Q_0 = 1$ ve $n \geq 1$ için P_n, Q_n tamsayılar olmak üzere,

$$\alpha_n = \frac{P_n + \sqrt{m}}{Q_n}, \qquad n = 0,1,2,\ldots$$

dir.

Örnek 3.5.3. $m = \sqrt{23}$' ün sürekli kesir açılımını bulalım.

Çözüm.

$$\alpha_0 = \sqrt{23}$$

$$\alpha_1 = \frac{1}{\alpha_0 - [\![\alpha_0]\!]} = \frac{1}{\sqrt{23} - 4} = \frac{\sqrt{23} + 4}{7},$$

$$\alpha_2 = \frac{1}{\alpha_1 - [\![\alpha_1]\!]} = \frac{1}{\frac{\sqrt{23} + 4}{7} - 1} = \frac{\sqrt{23} + 3}{2},$$

$$\alpha_3 = \frac{1}{\alpha_2 - [\![\alpha_2]\!]} = \frac{1}{\frac{\sqrt{23} + 3}{2} - 3} = \frac{\sqrt{23} + 3}{7},$$

$$\alpha_4 = \frac{1}{\alpha_3 - [\![\alpha_3]\!]} = \frac{1}{\frac{\sqrt{23} + 3}{7} - 1} = \sqrt{23} + 4,$$

$$\alpha_5 = \frac{1}{\alpha_4 - [\![\alpha_4]\!]} = \frac{1}{\sqrt{23} + 4 - 8} = \frac{\sqrt{23} + 4}{7} = \alpha_1,$$

$$\alpha_6 = \alpha_2 \ , \qquad \alpha_7 = \alpha_3, \ldots$$

O halde $m = \sqrt{23}$' ün sürekli kesir açılımı,

$$\sqrt{23} = \left[4, \overline{1,3,1,8}\right]$$

dir.

Teorem 3.5.3. d tamkare olmayan pozitif bir tamsayı olsun. P_k ve Q_k (3.6)' daki gibi tanımlansın. $\frac{p_k}{q_k}$, $\sqrt{d}$' nin k' yıncı yaklaşımı ve n periyodu göstersin. O zaman,

$$Q_k = 1 \Leftrightarrow n|k$$

dir [12].

Teorem 3.5.4. d tamkare olmayan pozitif bir tamsayı olsun. P_k ve Q_k, (3.6)' daki gibi tanımlansın. Bu taktirde $\frac{p_k}{q_k}$, $\sqrt{d}$' nin k' yıncı yaklaşımı olmak üzere,

$$p^2{}_k - dq^2{}_k = (-1)^{k-1}Q_{k+1}$$

dir.

İspat. $\sqrt{d} = [a_0, a_1, a_2, a_3, \dots, a_k, \alpha_{k+1}]$ olduğundan,

$$\sqrt{d} = \frac{\alpha_{k+1}p_k + p_{k-1}}{\alpha_{k+1}q_k + q_{k-1}}$$

yazılabilir. Ayrıca $\alpha_{k+1} = \frac{P_{k+1}+\sqrt{d}}{Q_{k+1}}$ olduğu kullanılırsa,

$$\sqrt{d} = \frac{\left(\frac{P_{k+1}+\sqrt{d}}{Q_{k+1}}\right)p_k + p_{k-1}}{\left(\frac{P_{k+1}+\sqrt{d}}{Q_{k+1}}\right)q_k + q_{k-1}}$$

$$= \frac{(P_{k+1}+\sqrt{d})p_k + p_{k+1}Q_{k+1}}{(P_{k+1}+\sqrt{d})q_k + q_{k+1}Q_{k+1}}$$

elde edilir. İçler dışlar çarpımı yapılırsa,

$$dq_k + (P_{k+1}q_k + Q_{k+1}q_{k-1})\sqrt{d} = (P_{k+1}p_k + Q_{k+1}p_{k-1}) + p_k\sqrt{d}$$

olup buradan,

$$dq_k = P_{k+1}p_k + Q_{k+1}p_{k-1}$$

ve

$$p_k = P_{k+1}q_k + Q_{k+1}q_{k-1}$$

bulunur.

Birinci denklem $-q_k$ ve ikinci denklem p_k ile çarpılıp toplanırsa,

$$\begin{aligned} p^2{}_k - dq^2{}_k &= -Q_{k+1}p_{k-1}q_k + Q_{k+1}q_{k-1}p_k \\ &= Q_{k+1}(-p_{k-1}q_k + q_{k-1}p_k) \end{aligned}$$

$$= Q_{k+1}(-1)^{k-1}$$

elde edilir.

Önerme 3.5.1. d tamkare olmayan pozitif bir tamsayı olsun. $\sqrt{d}$' nin sürekli kesir açılımının periyodu k olsun.

$p_n^2 - dq_n^2 = \pm 1$ dir $\Leftrightarrow h$ pozitif tamsayı olmak üzere $n = hk - 1$ dir.

Böylece,

$$p_{hk-1}^2 - dq_{hk-1}^2 = (-1)^{kh}$$

dir [13].

Teorem 3.5.5. d tamkare olmayan pozitif bir tamsayı olsun. $\sqrt{d}$' nin sürekli kesir açılımının periyodu k olsun. $x^2 - dy^2 = \pm 1$ denkleminin tüm tamsayı çözümleri, $n \in \mathbb{Z}$ ve p_{k-1}/q_{k-1}, $\sqrt{d}$' nin sürekli kesir açılımının $k-1$' inci yaklaşımı olmak üzere,

$$x + y\sqrt{d} = \pm(p_{k-1} + q_{k-1})^n$$

biçimindedir [13].

Sürekli kesirler için verdiğimiz bu tanım ve teoremler 4. Bölümde, bir reel kuadratik cismin temel biriminin nasıl belirleneceğini belirlememizi sağlar.

BÖLÜM 4. TEMEL BİRİMİN HESAPLANMASI

m karesiz pozitif bir tamsayı olsun. $O_{\mathbb{Q}(\sqrt{m})}$' nin temel birimi η' nın hesaplanmasının standart metodu; $\sqrt{m}$' nin sürekli kesir açılımıdır.

Tanım 4.1. $x^2 - my^2 = N$ Pell denkleminin çözümü mevcut olsun ve eğer $x_1 + y_1\sqrt{m}$, $x^2 - my^2 = N$' nin pozitif bir çözümü ve $x_2 + y_2\sqrt{m}$, $x^2 - my^2 = N$ Pell denkleminin $x_1 + y_1\sqrt{m}$' den farklı bir pozitif çözümü iken $x_1 + y_1\sqrt{m} < x_2 + y_2\sqrt{m}$ ise $x_1 + y_1\sqrt{m}$' ye $x^2 - my^2 = N$ Pell denkleminin temel çözümü denir.

$a + b\sqrt{m}$ ve $r + s\sqrt{m}$, $x^2 - my^2 = N$ denkleminin iki çözümü olsun. Bu durumda,

$$a = r \text{ dir } \Leftrightarrow b = s \text{ dir.}$$

Ayrıca,

$$a + b\sqrt{m} < r + s\sqrt{m} \text{ dir } \Leftrightarrow a < r \text{ ve } b < s \text{ dir.}$$

Teorem 4.1. m karesiz pozitif bir tamsayı olsun. $\sqrt{m}$' nin sonsuz sürekli kesir açılımının yaklaşımları $\frac{p_n}{q_n}$ $(n = 0,1,2,\ldots)$ olsun. l' de bu açılımın periyod uzunluğu olsun. Bu durumda,

a) Eğer l çiftse $x^2 - my^2 = -1$ denkleminin hiçbir x, y tamsayı çözümü yoktur ve $x^2 - my^2 = 1$ denkleminin çözümleri içerisinde x' i en küçük yapan (x, y) çözümü $(x, y) = (p_{l-1}, q_{l-1})$ dir.

b) Eğer l tekse $x^2 - my^2 = -1$ denkleminin x ve y tamsayı çözümleri vardır ve $x^2 - my^2 = -1$ denkleminin çözümleri içerisinde x' i en küçük yapan (x, y) çözümü $(x, y) = (p_{l-1}, q_{l-1})$

özellikleri geçerlidir [9].

Teorem 4.2. Eğer $m \equiv 5\ (mod\ 8)$ ve $O_{\mathbb{Q}(\sqrt{m})}$' nin x ve y tek olmak üzere $\frac{1}{2}(x + y\sqrt{m})$ biçiminde birimleri mevcut ise $O_{\mathbb{Q}(\sqrt{m})}$' nin temel birimi; A ve B her ikisi de tek pozitif tamsayılar olmak üzere $\eta = \frac{A+B\sqrt{m}}{2}$ biçimindedir ve $\eta^3 \in \mathbb{Z}[\sqrt{m}]$' dir. Ayrıca η^3, $x^2 - my^2 = \pm 1$ Pell denkleminin temel çözümüdür [9],[16].

Teorem 4.1 $\sqrt{m}$' nin sürekli kesir açılımındaki periyot uzunluğunun tek veya çift olmasına bağlı olarak $x^2 - my^2 = \pm 1$ denkleminin en küçük çözümlerini vermektedir. Bu teorem kullanarak temel birim η, m' nin durumuna göre aşağıdaki gibi hesaplanır.

Eğer $m \equiv 2{,}3\ (mod\ 4)$ veya $m \equiv 1\ (mod\ 8)$ ise x ve y tamsayılar olmak üzere, $O_{\mathbb{Q}(\sqrt{m})}$' nin tüm birimleri Sonuç 1.2.1' den $x + y\sqrt{m}$ biçiminde olmak durumundadır. Bu durumda $O_{\mathbb{Q}(\sqrt{m})}$' nin temel birimi η Teorem 2.5.2 ve Teorem 4.1' e göre,

$$\eta = p_{l-1} + q_{l-1}\sqrt{m}\,, \qquad N(\eta) = (-1)^l$$

dir.

Eğer $m \equiv 5\ (mod\ 8)$ ise x ve y tek tamsayılar olmak üzere $O_{\mathbb{Q}(\sqrt{m})}$' nin $\frac{1}{2}(x + y\sqrt{m})$ biçiminde birimleri olabilir de olmayabilir de. Eğer böyle birimler yoksa $\eta \in \mathbb{Z}[\sqrt{m}]$ dir ve $O_{\mathbb{Q}(\sqrt{m})}$' nin tüm birimleri $x + y\sqrt{m}$ biçiminde olmak durumundadır. Bu durumda $O_{\mathbb{Q}(\sqrt{m})}$' nin temel birimi η,

$$\eta = p_{l-1} + q_{l-1}\sqrt{m}\,, \qquad N(\eta) = (-1)^l$$

olur. Eğer $m \equiv 5\ (mod\ 8)$ iken $O_{\mathbb{Q}(\sqrt{m})}$' nin x ve y tek olmak üzere $\frac{1}{2}(x + y\sqrt{m})$ biçiminde birimleri varsa $O_{\mathbb{Q}(\sqrt{m})}$' nin temel birimi η, Teorem 4.2' ye göre A ve B her ikisi de tek pozitif tamsayılar olmak üzere $\eta = \frac{A+B\sqrt{m}}{2}$ biçimindedir ve η^3, $x^2 - my^2 = \pm 1$ denkleminin temel çözümüdür. Dolayısıyla Teorem 2.5.2 ve Teorem 4.1' e göre,

$$\eta^3 = p_{l-1} + q_{l-1}\sqrt{m}\,, \qquad N(\eta) = (-1)^l$$

dir. O halde,

$$\left(\frac{A + B\sqrt{m}}{2}\right)^3 = p_{l-1} + q_{l-1}\sqrt{m}$$

olduğu kullanılırsa,

$$A^3 + 3AB^2m = 8p_{l-1}$$

ve

$$3A^2B + B^3m = 8q_{l-1}$$

elde edilir. Böylece yukarıdaki denklemlerden,

$$A|p_{l-1}\,, \qquad 1 \leq A < 2p_{l-1}^{1/3}$$

ve

$$B|q_{l-1}\,, \qquad 1 \leq B < 2\left(\frac{q_{l-1}}{m}\right)^{1/3}$$

bulunur.

O halde, pozitif karesiz bir tamsayı olan m için $O_{\mathbb{Q}(\sqrt{m})}$' nin temel birimi η' nın belirlenmesi için gereken adımlar aşağıda sıralandığı gibidir.

1. adım. $p_{-1} = 1$, $q_{-1} = 0$,

$$P_0 = 0\ ,\ \ Q_0 = 1\ ,\ \ a_0 = [\![\sqrt{m}]\!]\ ,\ \ p_0 = [\![\sqrt{m}]\!]\ ,\ \ q_0=1$$

dir.

2. adım. $n = 1,2,\ldots$ için $P_n,\ Q_n,\ a_n,\ p_n,\ q_n$ değerleri belirlenir. Bunlar aşağıda ifade edildiği gibidir.

$$P_n = -P_{n-1} + a_{n-1}Q_{n-1}\ , \qquad n = 1,2,\ldots$$

$$Q_n = \frac{m - P_n^2}{Q_{n-1}}\ , \qquad n = 1,2,\ldots$$

$$a_n = \left[\!\!\left[\frac{P_n + \sqrt{m}}{Q_n}\right]\!\!\right]\ , \qquad n = 1,2,\ldots$$

$$p_n = a_n . p_{n-1} + p_{n-2}\ \ , \qquad n = 1,2,\ldots$$

$$q_n = a_n . q_{n-1} + q_{n-2}\ , \qquad n = 1,2,\ldots$$

Ardından $P_N = P_1$ ve $Q_N = Q_1$ olan ilk $N > 1$ tamsayısında durulur.

3. adım. $l = N - 1$' dir.

4. adım. Eğer $m \equiv 2,3\ (mod\ 4)$ veya $m \equiv 1\ (mod\ 8)$ ise

$$\eta = p_{l-1} + q_{l-1}\sqrt{m}\ , \qquad N(\eta) = (-1)^l$$

dir.

5. adım. Eğer $m \equiv 5\ (mod\ 8)$ ise p_{l-1}' in $2p_{l-1}^{1/3}$' den küçük tüm tek A pozitif bölenleri belirlenir ve q_{l-1}' in de $2\left(\frac{q_{l-1}}{m}\right)^{1/3}$' den küçük tüm tek B pozitif bölenleri belirlenir. Eğer bazı (A, B) çiftleri için,

$$A^3 + 3AB^2m = 8p_{l-1}$$

$$3A^2B + B^3m = 8q_{l-1}$$

elde ediliyorsa,

$$\eta = \frac{A + B\sqrt{m}}{2}\ , \qquad N(\eta) = (-1)^l$$

dir. Diğer bir deyişle,

$$\eta = p_{l-1} + q_{l-1}\sqrt{m}\,, \qquad N(\eta) = (-1)^{l}$$

dir.

Örnek 4.1. $m = \sqrt{23}$, $23 \equiv 3\ (mod\ 4)$ için temel birimi bulalım.

Çözüm. O halde, $p_{-1} = 1$, $q_{-1} = 0$, $P_0 = 0$, $Q_0 = 1$, $a_0 = [\![\sqrt{23}]\!] = 4$, $p_0 = [\![\sqrt{23}]\!] = 4$, q_0=1 olmak üzere, 2. adımdaki P_n, Q_n, a_n, p_n, q_n $(n = 1,2,\dots)$ değerlerini belirleyelim.

Tablo 4.1. $\sqrt{23}$ sayısı için bulunan P_n, Q_n, a_n, p_n, q_n $(n = 1,2,\dots)$ değerleri.

n	P_n	Q_n	a_n	p_n	q_n
-1				1	0
0	0	1	4	4	1
1	4	7	1	5	1
2	3	2	3	19	4
3	3	7	1	24	5
4	4	1	8	211	44
5	4	7	1	235	49

$$P_5 = P_1 = 4 \ \text{ ve } \ Q_5 = Q_1 = 7$$

olduğundan,

$$N = 5, \qquad l = N - 1 = 5 - 1 = 4$$

ve

$$p_{l-1} = p_3 = 24 \quad , \qquad q_{l-1} = q_3 = 5$$

olup,

$$\eta = p_{l-1} + q_{l-1}\sqrt{m} = 24 + 5\sqrt{23}\ , \qquad N(\eta) = (-1)^l = (-1)^4 = 1$$

bulunur.

O halde, $O_{\mathbb{Q}(\sqrt{23})}$' ün normu 1 olan temel birimi $24 + 5\sqrt{23}$ olur.

Örnek 4.2. $m = 17 \equiv 1\ (mod\ 8)$ için temel birimi bulalım.

Çözüm. $\sqrt{17} = [4, \overline{8}]$ dir. $P_n,\ Q_n,\ a_n,\ p_n,\ q_n \quad (n = 1,2,\dots)$ değerlerini belirleyelim.

Tablo 4.2. $\sqrt{17}$ sayısı için bulunan $P_n,\ Q_n,\ a_n,\ p_n,\ q_n \quad (n = 1,2,\dots)$ değerleri.

n	P_n	Q_n	a_n	p_n	q_n
-1				1	0
0	0	1	4	4	1
1	4	1	8	33	8
2	4	1	4	268	65

$$P_2 = P_1 = 4 \ \text{ ve } \ Q_2 = Q_1 = 1$$

olduğundan,

$$N = 2, \qquad l = N - 1 = 2 - 1 = 1$$

ve

$$p_{l-1} = p_0 = 4 \quad , \qquad q_{l-1} = q_0 = 1$$

olup,

$$\eta = p_{l-1} + q_{l-1}\sqrt{m} = 4 + \sqrt{17}\ , \qquad N(\eta) = (-1)^l = (-1)^1 = -1$$

bulunur.

O halde, $O_{\mathbb{Q}(\sqrt{17})}$' nin normu -1 olan temel birimi $4+\sqrt{17}$ olur.

Örnek 4.3. $m = 42 \equiv 2\ (mod\ 4)$ için temel birimi bulalım.

Çözüm. $\sqrt{42} = [6, \overline{2,12}]$ dir. $P_n,\ Q_n,\ a_n,\ p_n,\ q_n\quad (n = 1,2,\dots)$ değerlerini belirleyelim.

Tablo 4.3. $\sqrt{42}$ sayısı için bulunan $P_n,\ Q_n,\ a_n,\ p_n,\ q_n\quad (n = 1,2,\dots)$ değerleri.

n	P_n	Q_n	a_n	p_n	q_n
-1				1	0
0	0	1	6	6	1
1	6	6	2	13	2
2	6	1	12	162	25
3	6	6	2	337	52

$$P_3 = P_1 = 6 \text{ ve } Q_3 = Q_1 = 6$$

olduğundan,

$$N = 3, \quad l = N - 1 = 3 - 1 = 2$$

ve

$$p_{l-1} = p_1 = 13 \quad , \quad q_{l-1} = q_1 = 2$$

olup,

$$\eta = p_{l-1} + q_{l-1}\sqrt{m} = 13 + 2\sqrt{42} \ , \qquad N(\eta) = (-1)^l = (-1)^2 = 1$$

bulunur.

O halde, $O_{\mathbb{Q}(\sqrt{42})}$' nin normu 1 olan temel birimi $13 + 2\sqrt{42}$ olur.

Örnek 4.4. $m = 13 \equiv 5\ (mod\ 8)$ için temel birimi bulalım.

Çözüm. $\sqrt{13} = \left[3, \overline{1,1,1,1,6}\right]$ dir. $P_n,\ Q_n,\ a_n,\ p_n,\ q_n \quad (n = 1,2, ...)$ değerlerini belirleyelim.

Tablo 4.4. $\sqrt{13}$ sayısı için bulunan $P_n,\ Q_n,\ a_n,\ p_n,\ q_n \quad (n = 1,2, ...)$ değerleri.

n	P_n	Q_n	a_n	p_n	q_n
-1				1	0
0	0	1	3	3	1
1	3	4	1	4	1
2	1	3	1	7	2
3	2	3	1	11	3
4	1	4	1	18	5
5	3	1	6	119	33
6	3	4	1	137	38

$$P_6 = P_1 = 3 \quad \text{ve} \quad Q_6 = Q_1 = 4$$

olduğundan,

$$N = 6, \qquad l = N - 1 = 6 - 1 = 5$$

ve

$$p_{l-1} = p_4 = 18 \quad , \qquad q_{l-1} = q_4 = 5$$

dir.

A tek olduğundan; $A|p_{l-1}$, $1 \leq A < 2p_{l-1}^{1/3} \Rightarrow A|9$, $1 \leq A < 5{,}3 \Rightarrow A = 1$ veya $A = 3$

B tek olduğundan; $B|q_{l-1}$, $1 \leq B < 2\left(\frac{q_{l-1}}{m}\right)^{1/3} \Rightarrow B|5$, $1 \leq B < 1{,}5 \Rightarrow B = 1$

$(A,B) = (1{,}1)$ ve $(3{,}1)$ çözümlerinden sadece $(3{,}1)$ için,

$$A^3 + 39AB^2 = 144$$

$$3A^2B + 13B^3 = 40$$

denklemlerinin çözümü vardır.

O halde, $O_{\mathbb{Q}(\sqrt{13})}$' ün normu -1 olan temel birimi $\eta = \frac{3+\sqrt{13}}{2}$ olur.

Örnek 4.5. $m = 37 \equiv 5\ (mod\ 8)$ için temel birimi bulalım.

Çözüm. $\sqrt{37} = [6, \overline{12}]$ dir. $P_n,\ Q_n,\ a_n,\ p_n,\ q_n$ $(n = 1,2,\ldots)$ değerlerini belirleyelim.

Tablo 4.5. $\sqrt{37}$ sayısı için bulunan $P_n,\ Q_n,\ a_n,\ p_n,\ q_n$ $(n = 1,2,\ldots)$ değerleri.

n	P_n	Q_n	a_n	p_n	q_n
-1				1	0
0	0	1	6	6	1
1	6	1	12	73	12
2	6	1	12	882	145

$$P_2 = P_1 = 6 \quad \text{ve} \quad Q_2 = Q_1 = 1$$

olduğundan,

$$N = 2, \quad l = N - 1 = 2 - 1 = 1$$

ve

$$p_{l-1} = p_0 = 6 \quad , \quad q_{l-1} = q_0 = 1$$

dir. Açıkça,

$$A^3 + 111AB^2 = 48$$

ve

$$3A^2B + 37B^3 = 8$$

denklemlerinin pozitif tamsayı çözümleri yoktur. O halde $O_{\mathbb{Q}(\sqrt{37})}$' nin $\frac{1}{2}(x + y\sqrt{m})$ biçiminde birimleri yoktur. Dolayısıyla $O_{\mathbb{Q}(\sqrt{37})}$' nin birimleri $x + y\sqrt{m}$ biçimindedir. O halde,

$$\eta = p_{l-1} + q_{l-1}\sqrt{m}\,, \qquad N(\eta) = (-1)^l$$

olup $O_{\mathbb{Q}(\sqrt{37})}$' nin normu -1 olan temel birimi $\eta = 6 + \sqrt{37}$ olur.

BÖLÜM 5. BAZI DIOPHANTINE DENKLEMLERİNİN ÇÖZÜMÜ

Bu bölümde $x^2 - 2y^2 = \pm 1$ Pell denklemi ile $x^2 - 3xy + y^2 = \pm 5$, $x^2 - 5y^2 = \pm 4$, $x^2 - xy - y^2 = \pm 5$, $x^2 - 3xy + y^2 = \pm 1$ ve $x^2 - xy - y^2 = \pm 1$ Diophantine denklemlerinin pozitif tamsayı çözümleri verildi.

Önerme 5.1. $\alpha = \frac{1+\sqrt{5}}{2}$ olmak üzere $a\alpha + b \in \mathbb{Z}[\alpha]$ bir birimdir $\Leftrightarrow$ $b^2 - ab - a^2 = \pm 1$ dir.

İspat. $a\alpha + b$ birimse $N(a\alpha + b) = \pm 1$ dir. $\alpha = \frac{1+\sqrt{5}}{2}$ olduğundan,

$$\left[b + a\left(\frac{1+\sqrt{5}}{2}\right)\right]\left[b - a\left(\frac{1+\sqrt{5}}{2}\right)\right] = \frac{1}{4}[(2b+a)^2 - 5a^2]$$

$$= \frac{4b^2 - 4ab - 4a^2}{4} = b^2 - ab - a^2 = \pm 1$$

dir.

Tersine $b^2 - ab - a^2 = \pm 1$ ise $N(a\alpha + b) = \pm 1$ olduğunu görmek kolaydır.

Teorem 5.1. $\mathbb{Z}[\alpha] = \{a\alpha + b : a, b \in \mathbb{Z}\}$ kümesinin birimlerinin kümesi $\{\pm\alpha^n : n \in \mathbb{Z}\}$ dir [4].

Bu bölümde, Diophantine denklemlerini Teorem 5.1 yardımıyla çözeceğiz. Şimdi Fibonacci ve Lucas sayılarını tanımlayarak ilgili teoremleri verelim.

Tanım 5.1. Başlangıç şartları $F_0 = 0$, $F_1 = 1$ ve $n \geq 2$ olmak üzere,

$$F_n = F_{n-1} + F_{n-2}$$

şeklinde tanımlanan tekrarlı bağıntılarından elde edilen sayılara Fibonacci sayıları denir. Bu tekrarlı bağıntısının ürettiği tamsayılar dizisine Fibonacci dizisi denir ve bu dizi (F_n) ile gösterilir. Burada F_n, n' yinci Fibonacci sayısını gösterir.

Karakteristik denklem $\lambda^2 - \lambda - 1 = 0$ olmak üzere karakteristik denklemin kökleri,

$$\alpha = \frac{1+\sqrt{5}}{2} \quad , \quad \beta = \frac{1-\sqrt{5}}{2}$$

dir. Açıkça $\alpha + \beta = 1$, $\alpha - \beta = \sqrt{5}$ ve $\alpha\beta = -1$ dir.

Önerme 5.2. $n > 0$ için $\alpha^n = \alpha F_n + F_{n-1}$ dir.

İspat. Tümevarım uygulanırsa $n = 1$ için $\alpha = \alpha F_1 + F_0 = \alpha.1 + 0 = \alpha$ olur. O halde iddia doğrudur. n için $\alpha^n = \alpha F_n + F_{n-1}$ doğru olsun.

$$\begin{aligned} \alpha^{n+1} = \alpha^n \alpha = \alpha(\alpha F_n + F_{n-1}) &= \alpha^2 F_n + \alpha F_{n-1} \\ &= (\alpha + 1)F_n + \alpha F_{n-1} \\ &= \alpha F_n + \alpha F_{n-1} + F_n \\ &= \alpha(F_n + F_{n-1}) + F_n \\ &= \alpha F_{n+1} + F_n \end{aligned}$$

bulunur. Böylece $n + 1$ için de iddia doğrudur.

Aşağıdaki önermenin ispatı benzer biçimde yapılır.

Önerme 5.3. $n > 0$ için $\beta^n = \beta F_n + F_{n-1}$ dir.

Teorem 5.2. Her $n \geq 1$ için $F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$ dir.

İspat. Önerme 5.2 ve Önerme 5.3' e göre $n \geq 1$ için , $\alpha^n = \alpha F_n + F_{n-1}$ ve $\beta^n = \beta F_n + F_{n-1}$ dir. Bu denklemleri taraf tarafa çıkarırsak,

$$\alpha^n - \beta^n = \alpha F_n + F_{n-1} - \beta F_n - F_{n-1}$$

$$= F_n(\alpha - \beta)$$

bulunur. Buradan $F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$ elde edilir.

Aşağıdaki önermeler tümevarımla veya $F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$ olduğu kullanılarak ispatlanabilir.

Önerme 5.4. $n > 0$ için $F_n^2 - F_n F_{n-1} - F_{n-1}^2 = (-1)^{n+1}$ dir.

Önerme 5.5. $n > 0$ için $F_{2n+2}^2 - 3F_{2n+2}F_{2n} + F_{2n}^2 = 1$ dir.

Tanım 5.2. Başlangıç şartları $L_0 = 2$, $L_1 = 1$ ve $n \geq 2$ olmak üzere,

$$L_n = L_{n-1} + L_{n-2}$$

şeklinde tanımlanan rekürans bağıntılarından elde edilen sayılara Lucas sayıları denir. Bu rekürans bağıntısının ürettiği tamsayılar dizisine Lucas dizisi denir ve bu dizi (L_n) ile gösterilir. Burada L_n , n' yinci Lucas sayısını gösterir.

Uyarı 5.1. Tanım 5.1 ve Tanım 5.2 göz önüne alınırsa Fibonacci ve Lucas sayıları arasında,

$$F_n = \frac{1}{5}(L_{n-1} + L_{n+1})$$

bağıntısının olduğu görülür.

Teorem 5.3. $n \geq 1$ için $L_n = \alpha^n + \beta^n$ dir.

İspat. Tümevarımla ispat yapılacaktır.

$n = 1$ için $L_1 = \alpha + \beta$ dır.

$n = 2$ için $L_2 = 3 = (\alpha + \beta)^2 - 2\alpha\beta = \alpha^2 + \beta^2$ bulunur.

$n \geq 3$ için $L_{n-1} = \alpha^{n-1} + \beta^{n-1}$ ve $L_{n-2} = \alpha^{n-2} + \beta^{n-2}$ olsun. O zaman,

$$\begin{aligned} L_n &= L_{n-1} + L_{n-2} \\ &= \alpha^{n-1} + \beta^{n-1} + \alpha^{n-2} + \beta^{n-2} \\ &= \alpha^{n-2}(\alpha + 1) + \beta^{n-2}(\beta + 1) \\ &= \alpha^{n-2}\alpha^2 + \beta^{n-2}\beta^2 \\ &= \alpha^n + \beta^n \end{aligned}$$

olarak bulunur.

Teorem 5.4. $n > 1$ için $L_n = F_{n-1} + F_{n+1}$ dir.

İspat. $\alpha\beta = -1$ olduğu kullanılırsa,

$$F_{n-1} + F_{n+1} = \frac{\alpha^{n-1} - \beta^{n-1}}{\alpha - \beta} + \frac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta}$$

$$= \frac{-(\alpha\beta)\alpha^{n-1} + (\alpha\beta)\beta^{n-1} + \alpha^{n+1} - \beta^{n+1}}{\alpha - \beta}$$

$$= \frac{\alpha^n(-\beta + \alpha) + \beta^n(\alpha - \beta)}{\alpha - \beta}$$

$$= \frac{(\alpha^n + \beta^n)(\alpha - \beta)}{\alpha - \beta}$$

$$= \alpha^n + \beta^n = L_n$$

olarak bulunur.

Teorem 5.5. $n \geq 1$ için $5F_n^2 = L_n^2 - 4(-1)^n$ dir.

İspat. $\alpha\beta = -1$ olduğundan,

$$L_n^2 - 4(-1)^n = (\alpha^n + \beta^n)^2 - 4(-1)^n$$

$$= \alpha^{2n} + \beta^{2n} + 2(\alpha\beta)^n - 4(-1)^n$$

$$= \alpha^{2n} + \beta^{2n} - 2(-1)^n$$

$$= (\alpha^n - \beta^n)^2 = 5F_n^2$$

dir.

Aşağıdaki önermeler tümevarımla ispatlanabilir.

Önerme 5.6. $n > 0$ için $L_n^2 - L_nL_{n-1} - L_{n-1}^2 = 5(-1)^n$ dir.

Önerme 5.7. $n > 0$ için $L_{2n+1}^2 - 3L_{2n+1}L_{2n-1} - L_{2n-1}^2 = 5$ dir.

Şimdi Pell ve Pell-Lucas dizilerini tanımlayalım.

Tanım 5.3. p ve q sıfırdan farklı, aralarında asal ve $p^2+4q \neq 0$ olacak şekilde tamsayılar olsun. U_n ve V_n dizileri $n \geq 2$ için,

$$U_n = pU_{n-1} + qU_{n-2}\ , \qquad U_0 = 0\ , \qquad U_1 = 1$$

$$V_n = pV_{n-1} + qV_{n-2}\ , \qquad V_0 = 2\ , \qquad V_1 = p$$

şeklinde tanımlansın. Eğer $p = 2$ ve $q = 1$ alınırsa,

$$P_n = 2P_{n-1} + P_{n-2} \qquad , \qquad P_0 = 0\ , \qquad P_1 = 1$$

$$Q_n = 2Q_{n-1} + Q_{n-2} \qquad , \qquad Q_0 = 0\ , \qquad Q_1 = 2$$

elde edilir. Burada P_n ve Q_n dizilerine sırasıyla Pell ve Pell-Lucas dizisi denir [17].

Önerme 5.8. P_n ve Q_n dizileri için,

$$Q_n^2 - 8P_n^2 = 4(-1)^n \tag{5.1}$$

ve

$$P_{n+1} + P_{n-1} = Q_n \tag{5.2}$$

eşitlikleri vardır [17].

Teorem 5.6. $x^2 - xy - y^2 = \pm 1$ olan $x > 0\,,\ y > 0$ vardır $\Leftrightarrow$ $n > 1$ olmak üzere $x = F_n\,,\ y = F_{n-1}$ dir.

İspat. $\Leftarrow$) $n \in \mathbb{N}$ olmak üzere $x = F_n$, $y = F_{n-1}$ ise Önerme 5.4' e göre,

$$x^2 - xy - y^2 = F_n^2 - F_n F_{n-1} - F_{n-1}^2 = (-1)^{n+1} = \pm 1$$

dir.

$\Rightarrow$) $x^2 - xy - y^2 = \pm 1$ olan $x > 0$, $y > 0$ mevcut olsun. Önerme 5.1' e göre $\alpha x + y$ bir birimdir. $x > 0$, $y > 0$ olduğundan $\alpha x + y > 1$ dir.

Ayrıca Teorem 5.1' e göre $\alpha x + y = \alpha^n$ olan $n > 1$ vardır. O halde Önerme 5.2' e göre,

$$\alpha x + y = F_n \alpha + F_{n-1} \Rightarrow x = F_n \quad , y = F_{n-1}$$

olur.

Sonuç 5.6.1. $x^2 - xy - y^2 = 1$' in tüm pozitif x, y tamsayı çözümleri $n \geq 1$ olmak üzere $(x, y) = (F_{2n+1}, F_{2n})$ biçimindedir.

Sonuç 5.6.2. $x^2 - xy - y^2 = -1$' in tüm pozitif x, y tamsayı çözümleri $n \geq 1$ olmak üzere $(x, y) = (F_{2n}, F_{2n-1})$ biçimindedir.

Teorem 5.7. $x^2 - 5y^2 = 4$' ün tüm pozitif tamsayı çözümleri $n \geq 1$ olmak üzere $(x, y) = (L_{2n}, F_{2n})$ biçimindedir.

İspat. $x^2 - 5y^2 = 4$ olsun. Buradan x ve y' nin aynı türden olduğu elde edilir. $u = \frac{x+y}{2}$, $v = y$ alalım. O zaman,

$$u^2 - uv - v^2 = \left(\frac{x+y}{2}\right)^2 - \left(\frac{x+y}{2}\right) y - y^2$$

$$= \frac{x^2 + y^2 + 2xy}{4} - \frac{xy + y^2}{2} - y^2$$

$$= \frac{x^2 - 5y^2}{4} = \frac{4}{4} = 1$$

yazılabilir. Sonuç 5.6.1' e göre,

$$u = F_{2n+1}\,, \qquad v = F_{2n}$$

olan $n > 0$ vardır.

$$u = F_{2n+1} = \frac{x+y}{2} \Rightarrow x = 2F_{2n+1} - y\,, \qquad v = y = F_{2n}$$

$$\Rightarrow x = 2F_{2n+1} - F_{2n}$$

$$\Rightarrow x = F_{2n+1} + F_{2n+1} - F_{2n}$$

$$\Rightarrow x = F_{2n+1} + F_{2n-1}$$

olur. Teorem 5.4' e göre,

$$x = L_{2n}$$

elde edilir.

$y = v$ ve $v = F_{2n}$ olduğundan $y = F_{2n}$ dir. O halde $(x, y) = (L_{2n}, F_{2n})$ elde edilir.

Benzer biçimde aşağıdaki sonuç verilebilir.

Sonuç 5.7.1. $x^2 - 5y^2 = -4$' ün tüm pozitif tamsayı çözümleri $n \geq 0$ olmak üzere,

$$(x, y) = (L_{2n+1}, F_{2n+1})$$

biçimindedir.

Teorem 5.8. $x^2 - xy - y^2 = \pm 5$' in tüm pozitif tamsayı çözümleri $n \geq 0$ olmak üzere $(x, y) = (L_{n+1}, L_n)$ biçimindedir.

İspat. $x^2 - xy - y^2 = \pm 5$ olsun. $2x - y \geq 0$ kabul edelim. Eşitliğin her iki tarafını 4 ile çarpalım.

$$4x^2 - 4xy - 4y^2 = \pm 20$$

$$(2x - y)^2 - 5y^2 = \pm 20$$

$$25\left(\frac{2x - y}{5}\right)^2 - 5y^2 = \pm 20$$

$$y^2 - 5\left(\frac{2x - y}{5}\right)^2 = \pm 4$$

Teorem 5.7' ye göre $y = L_n$, $F_n = \frac{2x-y}{5}$ olan $n \geq 0$ vardır. O zaman,

$$y = L_n \ , \ x = \frac{5F_n + y}{2}$$

$$\Rightarrow x = \frac{5F_n + L_n}{2}$$

$$\Rightarrow x = \frac{L_{n+1} + L_{n-1} + L_n}{2}$$

$$\Rightarrow x = \frac{2L_{n+1}}{2} = L_{n+1}$$

olur. Dolayısıyla $(x, y) = (L_{n+1}, L_n)$ bulunur.

Tersine eğer $(x, y) = (L_{n+1}, L_n)$ ise Önerme 5.6' dan $x^2 - xy - y^2 = \pm 5$ elde edilir.

Sonuç 5.8.1. $x^2 - xy - y^2 = 5$' in tüm pozitif tamsayı çözümleri $n \geq 0$ olmak üzere,

$$(x, y) = (L_{2n}, L_{2n-1})$$

biçimindedir.

Sonuç 5.8.2. $x^2 - xy - y^2 = -5$’ in tüm pozitif tamsayı çözümleri $n \geq 0$ olmak üzere,

$$(x, y) = (L_{2n+1}, L_{2n})$$

biçimindedir.

Teorem 5.9. $x^2 - 3xy + y^2 = 1$’ in tüm pozitif tamsayı çözümleri $n \geq 1$ olmak üzere,

$$(x, y) = (F_{2n+2}, F_{2n})$$

biçimindedir.

İspat. $x^2 - 3xy + y^2 = 1$ olsun. $x > y$ alalım. Bu taktirde,

$$(x - y)^2 - (x - y)y - y^2 = x^2 - 3xy + y^2 = 1$$

olur. Sonuç 5.6.1’ e göre $(x - y, y) = (F_{2n+1}, F_{2n})$ olan $n \geq 1$ vardır. Böylece $x - y = F_{2n+1}$, $y = F_{2n}$ dir.

Burada $x = F_{2n+1} + y$, $y = F_{2n}$ yani $x = F_{2n+1} + F_{2n} = F_{2n+2}$ dir. O halde $n \geq 1$ olmak üzere $(x, y) = (F_{2n+2}, F_{2n})$ dir.

Tersine, eğer $(x, y) = (F_{2n+2}, F_{2n})$ ise $x^2 - 3xy + y^2 = 1$ olduğu Önerme 5.5’ ten görülür.

Benzer biçimde aşağıdaki sonuç verilebilir.

Sonuç 5.9.1. $x^2 - 3xy + y^2 = -1$' in tüm pozitif tamsayı çözümleri $n \geq 0$ olmak üzere,

$$(x, y) = (F_{2n+1}, F_{2n-1})$$

dir.

Teorem 5.10. $x^2 - 3xy + y^2 = 5$' in tüm pozitif tamsayı çözümleri $n > 0$ olmak üzere,

$$(x, y) = (L_{2n+1}, L_{2n-1})$$

biçimindedir.

İspat. $x^2 - 3xy + y^2 = 5$ olsun. $x > y$ alalım. $x = y$ olamayacağını görmek kolaydır. O zaman,

$$(x - y)^2 - y(x - y) - y^2 = x^2 - 3xy + y^2 = 5$$

dir. Sonuç 5.8.1' e göre $(x - y, y) = (L_{2n}, L_{2n-1})$ olan $n > 0$ vardır.

Buradan $x - y = L_{2n}$, $y = L_{2n-1}$ bulunur. Böylece $x = L_{2n} + y = L_{2n} + L_{2n-1} = L_{2n+1}$ elde edilir. O halde $(x, y) = (L_{2n+1}, L_{2n-1})$ bulunur.

Tersine $(x, y) = (L_{2n+1}, L_{2n-1})$ ise $x^2 - 3xy + y^2 = 5$ olduğu Önerme 5.7' den görülür.

Benzer biçimde aşağıdaki sonuç verilebilir.

Sonuç 5.10.1. $x^2 - 3xy + y^2 = -5$' in tüm pozitif tamsayı çözümleri $n \geq 0$ olmak üzere,

$$(x, y) = (L_{2n+2}, L_{2n})$$

biçimindedir.

Teorem 5.11. $x^2 - 2y^2 = \pm 1$ Pell denkleminin tüm pozitif tamsayı çözümleri $n \geq 1$ olmak üzere $(x, y) = \left(\frac{Q_n}{2}, P_n\right)$ dir.

İspat. $x^2 - 2y^2 = \pm 1$ olduğunu kabul edelim. O zaman $(x - \sqrt{2}y)(x + \sqrt{2}y) = \pm 1$ dir. O halde $x - \sqrt{2}y$, $\mathbb{Z}[\sqrt{2}]$' de bir birimdir. Ayrıca $x > 0$ ve $y > 0$ olduğundan $x + \sqrt{2}y > 1$ olur. Böylece Teorem 2.1.1' e göre,

$$x + \sqrt{2}y = (1 + \sqrt{2})^n = (1 + \sqrt{2})P_n + P_{n-1}$$

olan n pozitif tamsayısı vardır.

$$(1 + \sqrt{2})P_n + P_{n-1} = P_n + P_{n-1} + \sqrt{2}P_n$$

olduğundan,

$$(x, y) = (P_n + P_{n-1}, P_n)$$

elde edilir. Böylece (5.2)' e göre,

$$\begin{aligned} x = P_n + P_{n-1} &= \frac{1}{2}(2P_n + 2P_{n-1}) \\ &= \frac{1}{2}(2P_n + P_{n-1} + P_{n-1}) \\ &= \frac{1}{2}(P_{n+1} + P_{n-1}) \\ &= \frac{1}{2}Q_n \end{aligned}$$

bulunur.

O halde $x = \frac{1}{2}Q_n$ ve $y = P_n$ dir.

Aksine $(x, y) = \left(\frac{Q_n}{2}, P_n\right)$ ise (5.1)' den $x^2 - 2y^2 = \pm 1$ elde edilir.

(5.1) ve Teorem 5.11 kullanılarak aşağıdaki sonuçlar verilebilir.

Sonuç 5.11.1. $x^2 - 2y^2 = 1$ Pell denkleminin tüm pozitif tamsayı çözümleri $n \geq 1$ olmak üzere $(x, y) = \left(\frac{Q_{2n}}{2}, P_{2n}\right)$ biçimindedir.

Sonuç 5.11.2. $x^2 - 2y^2 = -1$ Pell denkleminin tüm pozitif tamsayı çözümleri $n \geq 0$ olmak üzere $(x, y) = \left(\frac{Q_{2n+1}}{2}, P_{2n+1}\right)$ biçimindedir.

BÖLÜM 6. SONUÇLAR VE ÖNERİLER

Bu çalışmada m karesiz pozitif bir tamsayı olmak üzere, $\mathbb{Q}(\sqrt{m})$ reel kuadratik cisminin temel birimi hesaplanıp, bununla ilgili temel özellikler incelendi. Benzer özellikler $\mathbb{Q}(\sqrt[3]{m})$ için incelenebilir. Bu çalışmada bu konuya girilmemiştir. Bu konuyla ilgili olarak [9] nolu kaynağa bakılabilir.

KAYNAKLAR

[1] STARK, H.M., An Introduction to Number Theory, Markham Publishing Company, Chicago, 1970.

[2] ROSEN, H.K., Elementary Number Theory And Its Application 3th Edition, Addison-Wesley, 1993.

[3] ÇALLIALP, F., Sayılar Teorisi, İstanbul, 1999.

[4] HARDY, G. H., An Introduction to the Theory of Numbers, 4th Edition, Oxford at the Clarenden Press, 1960.

[5] FROHLICH, A., TAYLOR, J., Algebraic Number Theory, Cambridge University Press, 1993.

[6] DO, A., Quadratic Integer Rings, Master Thesis, University of California, 2008.

[7] NIVEN, I., ZUCKERMAN, S.H., An Introduction to the Theory of Numbers, John Wiley Sons Inc., New York, 1972.

[8] ATASOY, M., $\mathbb{Q}(\sqrt{m})$ Cisminde Bazı Diophantine Denklemlerinin Çözüm Metodları, Doktora Tezi, Erciyes Üniversitesi, Temmuz-1995.

[9] ALACA, Ş., WILLIAMS, K.S., Introductory Algebraic Number Theory, Cambridge University Press, 2004.

[10] ADLER, A., CLOURY, J.E., The Theory of Numbers, A text and Source Book of Problems, Jones and Bartlett Publishers, Baston, MA., 1995.

[11] MOLLIN, R. A., Continued Fraction Gems, Nieuw Archief voor Wiskunde 17, 383-405, 1999.

[12] OLDS, C.D., Continued Fractions, Random House, New Mathematical Library, 1963.

[13] MABILLARD, I., Continued Fractions and Fundamental Units in Quadratic Fields, Semester Project, 2011.

[14] HERMSTEIN, I.N., Topic in Algebra, Blasdell Pub. Co., New York, 1964.

[15] REDMOND, D., Number Theory: An Introduction, Markel Dekker, Inc, 1996.

[16] STOLT, B., On the Diophantine Equation $u^2 - dv^2 = -4N$, Arkiv för Math., 2 , 1-23, 1951.

[17] KARAATLI, O., KESKİN, R., Journal of Algebra, Number Theory: Advances and Applications, Scientific Advances Publishers, 71-89, 2010.

[18] VAJDA, S., Fibonacci and Lucas Numbers and the Golden Section: Theory and Applications, Ellies Horwood Limited Publ., England, 1989.

[19] LEVEQUE, W.J., Topics in Numbers Theory, Printed in the United States of America, 1956.

[20] MELHAM, R., Sums Involving Fibonacci and Pell Numbers, Portugaliae Mathematica 56(3), 309-317, 1999.

[21] KESKİN, R., Solutions of Some Quadratic Diophantine Equations, Computers and Mathematics with Applications, 60, 2225-2230, 2010.

[22] DEMİRTÜRK, B., KESKİN, R., Integer Solutions of Some Diophantine Equations via Fibonacci and Lucas Numbers, Journal of Integer Sequences, 12 2009.

ÖZGEÇMİŞ

Aygen KOÇ, 27.03.1985 tarihinde Malatya’ da doğdu. İlkokul eğitimini Malatya’ da tamamladı. 2002 yılında Kolukısa Anadolu Lisesi’ nden mezun oldu. 2003 yılında başladığı İnönü Üniversitesi Eğitim Fakültesi İlköğretim Matematik Öğretmenliği bölümünü 2007 yılında bitirdi. Aynı yıl öğretmen olarak atandı. 2010 yılında Sakarya Üniversitesi’ nde yüksek lisansa başladı.