15462

Erciyes Üniversitesi

Fen Bilimleri Enstitüsü Müdürlüğüne

Bu çalışma jürimiz tarafından Matematik Anabilim Dalında Yüksek Lisans Tezi Olarak kabul edilmiştir.

10./.9../1991

Başkan: Proj. Dr. Okan Öztürk

Üye : Yrd. Doç. Dr. Hüseyin Çakallı

Üye : Yrd. Doç. Dr. İlhan Öztürk

ONAY

Yukarıdaki imzaların adı geçen öğretim üyelerine ait olduğunu onaylarım.

10./.9../1991

Doç. Dr. İbrahim Uzmay

Enstitü Müdürü V.

Bu çalışma konusunu bana veren ve çalışma boyunca yardımlarını esirgemeyen hocam , Sayın Yrd. Doç. Dr. Hüseyin ALTINDİŞ'e teşekkür eder , saygılar sunarım.

Muzaffer ATASOY

ÖZGEÇMİŞ

Adı soyadı : Muzaffer ATASOY

Baba adı : Şakir

Ana adı :Hatice

İlk ve orta öğrenimini Şefaatli'de , Lise öğrenimini Kayseri'de tamamladı . Erciyes Üniversitesi Fen Edebiyat Fakültesi Matematik Bölümünden lisans diploması alarak 1988 yılında mezun oldu. 9.11.1989 tarihinde Erciyes Üniversitesi Matematik Bölümü 'Cebir ve Sayılar Teorisi' Ana Bilim dalına Araştırma Görevlisi olarak atandı . Halen bu görevi yürütmektedir.

ÖZET

Bu çalışma iki bölümden ibaret olup , birinci bölüm, ileride kullanacağımız temel tanım ve teoremleri ihtiva etmektedir. İkinci bölümde çalışmanın temelini teşkil eden değişik Diophantine denklemlerinin çözümleri incelenmiştir.

ABSTRACT

This study consists of two chapters. First chapter contains basic definitions and results that will be needed later. In the second chapter , we examine the various kind of Diophantine equations which are the main goal of this work.

İÇİNDEKİLER

BÖLÜM I

1.1 TAMSAYILARIN BAZI ÖZELLİKLERİ 1
Bölünebilme 1
1.2 SONLU SÜREKLİ KESİRLER 3
1.3 SONSUZ SÜREKLİ KESİRLER 7
1.4 İRRASYONEL SAYILARIN SONSUZ SÜREKLİ KESİRLE TEMSİLİ 8
1.5 KONGRÜANSLAR 10
1.6 CEBİRSEL SAYILAR 12

BÖLÜM II

2.1 LİNEER DİOPHANTİNE DENKLEMLERİ 19
2.2 İKİNCİ DERECEDEN DİOPHANTİNE DENKLEMLERİ 23
Kuadratik formlar 23
Pell Denklemleri 27
$U^2-DV^2=N$ Diophantine Denklemleri 33
Pell Denklemleri için indirgeme Bağıntıları 37
$U^2-DV^2=N$ Denklemleri için indirgeme Bağıntıları 38
$x^2+y^2=z^2$ Diophantine Denklemi 43
2.3 ÜÇÜNCÜ ve DÖRDÜNCÜ DERECEDEN BAZI DİOPHANTİNE DENKLEMLERİ 45
$X^3+Y^3=Z^3$ Diophantine Denklemi 45
$x^4-y^4=z^2$ Diophantine Denklemi 48
2.4 $Q(\sqrt{m})$ de BAZI DİOPHANTİNE DENKLEMLERİ 53
$Q(\sqrt{m})$ de ax+by=c Diophantine Denklemleri 53
$x^3+y^3=z^3$ Diophantine Denklemi 55
KAYNAKLAR 59

BÖLÜM I

Bu bölümde ilerdeki bölümlerde kullanılacak temel tanım ve teoremler ifade edildi.

1.1 TAMSAYILARIN BAZI ÖZELLİKLERİ

BÖLÜNEBİLME

TANIM 1.1.1. a sıfırdan farklı bir tamsayı olmak üzere, b=ac olacak şekilde bir c tamsayısı varsa, bu taktirde b, a ile bölünebilirdir denir ve $a|b$ şeklinde gösterilir. Eğer b,a ile bölünemiyorsa $a\nmid b$ şeklinde gösterilir.

$a|b$ gösterimi a böler b, a, b nin bir böleni veya b, a nın bir katı şeklinde söylenir. Bölünebilmenin bazı özelliklerini aşağıdaki teoremle ifade edelim.

TEOREM 1.1.1.

i) $a|b$ ise her $c\in\mathbb{Z}$ için $a|bc$

ii) $a|b$ ve $b|c$ ise $a|c$

iii) $a|b$ ve $a|c$ ise her $x,y\in\mathbb{Z}$ için $a|bx+cy$

iv) $a|b$ ve $b|a$ ise $a=\mp b$

v) $a|b$, $a>0$, $b>0$ ise $a\leq b$ [1].

TANIM 1.1.2. $d|b$ ve $d|c$ ise d ye b ile c nin bir ortak böleni denir. Sıfırdan farklı herhangi bir tamsayının sonlu sayıda böleni vardır ve bu nedenle b ve c nin sonlu sayıda ortak böleni mevcuttur. Sıfırdan farklı b ve c tamsayılarının ortak bölenlerinden en büyüğüne b ve c nin en büyük ortak böleni denir ve

$(b,c)=d$ şeklinde gösterilir. Benzer olarak $b_1, b_2, \ldots, b_n$ ler sıfırdan farklı tamsayılar olmak üzere, bunların en büyük ortak böleni $(b_1, b_2, \ldots, b_n)$ şeklinde gösterilir.

TEOREM 1.1.2. b ve c tamsayılarının en büyük ortak böleni d ise bu durumda d ;

i) x ve y tamsayılar olmak üzere $bx+cy$ nin en küçük pozitif değeridir.

ii) b ve c nin bütün pozitif ortak bölenleriyle bölünebilen pozitif tamsayıdır [1].

TEOREM 1.1.3. Pozitif tamsayıların boş olmayan her S alt cümlesinin bir en küçük elemanı vardır.

İspat. Kabul edelim ki S nin bir en küçük elemanı olmasın. Bu takdirde $1 \notin S$ dir. Şimdi

$$K=\{x:\ x<y,\ y\in S\}$$

cümlesini gözönüne alalım. 1 hiç bir pozitif tamsayının ardışığı olmadığı için $1\in K$ dır. $x\in K$ ve $y\in S$ ise $x+1=x_1\leq y$ yazabiliriz. $x_1=y$ ise x_1, S nin en küçük elemanı olur. Kabulümüzden dolayı bu olamayacağından $x_1\in K$ dır. Yani $x_1<y$ olur. Benzer düşünceler tekrar edilince, sonlu adımdan sonra yine $a\in K$ olmak üzere,

$$x_1<x_2<\ldots<a$$

elde edilir. Bu ise K nın bütün pozitif tamsayıları kapsadığını gösterir ki, bu da S cümlesinin boş olmasını gerektirir. Halbuki $S\neq\Phi$ alındığından $S=\Phi$ olması bir çelişkidir. O halde S cümlesinin bir en küçük elemanı vardır.

Bu teoreme pozitif tamsayılarda iyi sıralama prensibi adı verilir.

TEOREM 1.1.4.(Bölme algoritması). a,b iki tamsayı ve $b>0$ olmak üzere

$$a=bq+r\quad,\quad 0\leq r<b$$

olacak şekilde bir tek q ve r tamsayı çifti vardır.

İspat. $C=\{a-sb\ :\ s\in Z, a-sb\geq 0\}$

cümlesini gözönüne alalım. $a\geq 0$ ise $a-0b$ sayısı C cümlesinin elemanıdır. $a<0$ ise $b\geq 1$ için $a-ab=a(1-b)\geq 0$ olur ki, C nin elemanıdır. Böylece a nın her iki durumu için C boş değildir. Bu yüzden Teorem 1.1.3 e göre C nin bir en küçük elemanı vardır. C deki en küçük eleman r olacak şekilde s ye verilecek değer q olsun. O zaman $r=a-bq$ olur ki bu $0\leq r$ olmasıdır ve

$$r-b=a-bq-b=a-(q+1)b<0$$

olur. Buradan $0\leq r<b$ elde edilir.

Şimdi q ve r tamsayılarının tekliğini gösterelim. Kabul edelim ki

$$a=bq+r \quad , \quad 0\leq r<b$$

$$a=bq_1+r_1 \quad , \quad 0\leq r_1<b$$

şartını sağlayan q, q_1, r, r_1 tamsayıları mevcut olsun. $q=q_1$ ve $r=r_1$ olduğunu göstermemiz yeterlidir. $q_1<q$ olsun. Bu takdirde $q_1+1\leq q$ dir ve

$$r=a-bq\leq a-b(q_1+1)=a-bq_1-b=r_1-b<0$$

elde edilir ki bu $0\leq r$ olmasıyla çelişir. Benzer olarak $q_1>q$ içinde çelişki elde edilir. Bu ikisinden $q=q_1$ olmak zorundadır. $q=q_1$ olduğundan,

$$bq+r=a=bq+r_1$$

yazılır. Bu ise $r=r_1$ olmasıdır [2].

1.2 SONLU SÜREKLİ KESİRLER

TANIM 1.2.1. N+1 tane $a_0, a_1, a_2, \ldots, a_n, \ldots, a_N$ değişkenlerinin

$$a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\ddots+\cfrac{1}{a_N}}} \qquad (1.2.1)$$

ifadesine sonlu sürekli kesir veya başka bir anlama gelme riski olmadığı zaman sadece sürekli kesir adı verilir. (1.2.1) gösterimi karışık bir yapıya sahip olduğundan bir sürekli kesir

$$a_0+\frac{1}{a_1+}\;\frac{1}{a_2+}\;\cdots\;+\frac{1}{a_N}$$

veya

$$[a_0,a_1,\dots,a_N]$$

şeklinde gösterilir. Buradaki $a_0,a_1,\dots,a_N$ lere sürekli kesrin kısmi bölenleri ya da sadece paydaları denir.

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

$$[a_0,a_1]=a_0+\frac{1}{a_1} \qquad (1.2.2)$$

$1\leq n\leq N$ için

$$[a_0,a_1,\dots,a_{n-1},a_n]=[a_0,a_1,\dots,a_{n-2},a_{n-1}+\frac{1}{a_n}] \qquad (1.2.3)$$

$$[a_0,a_1,\dots,a_n]=a_0+\frac{1}{[a_1,a_2,\dots,a_n]}$$

$$=[a_0,[a_1,a_2,\dots,a_n]] \qquad (1.2.4)$$

eşitlikleri vardır. Bu üç eşitlik daha genel olarak $1\leq m\leq n\leq N$ olmak üzere

$$[a_0,a_1,\dots,a_n]=[[a_0,a_1,\dots,a_{m-1}],[a_m,\dots,a_n]]$$

şeklinde tanımlanır.

TANIM 1.2.2. $[a_0,a_1,\dots,a_n]$, $0\leq n\leq N$ ifadesine $[a_0,a_1,\dots,a_N]$ sürekli kesrinin n. yakınsayanı denir ve bu yakınsayan sürekli kesrin değeridir.

TEOREM 1.2.1. p_n ve q_n ler

$$p_0=a_0 \ , \ p_1=a_0a_1+1 \ , \ p_n=a_np_{n-1}+p_{n-2} \qquad (2\leq n\leq N)$$

$$q_0=1 \ , \ q_1=a_1 \ , \ q_n=a_nq_{n-1}+q_{n-2} \qquad (2\leq n\leq N)$$

eşitlikleriyle tanımlanmak üzere

$$[a_0,a_1,\dots,a_n]=\frac{p_n}{q_n}=\delta_n$$

dir [3]. Bu da $[a_0,a_1,\dots,a_n]$ sonlu sürekli kesrinin n. yakınsayanıdır.

Ispat. Ispatı n üzerinden tümevarımla yapalım.

n=0 için

$$[a_0]=\frac{p_0}{q_0}=a_0$$

n=1 için

$$[a_0,a_1]= \frac{p_1}{q_1} = \frac{a_0a_1+1}{a_1} = a_0+ \frac{1}{a_1} =[a_0,a_1]$$

dir.

$m\in N$ ve $n\leq m$ için doğruluğunu kabul edelim. Bu takdirde p_{m-1}, p_{m-2} , q_{m-1} , q_{m-2} ler sadece $[a_0,a_1,...,a_{m-1}]$ sürekli kesrine bağlıdır ve kabulümüz

$$[a_0,a_1,...,a_{m-1},a_m]= \frac{p_m}{q_m} = \frac{a_mp_{m-1}+p_{m-2}}{a_mq_{m-1}+q_{m-2}}$$

olur. Şimdi n= m+1 için bunun doğruluğunu gösterelim.

$$[a_0,a_1,...,a_{m-1},a_m,a_{m+1}]=[a_0,a_1,...,a_{m-1},a_m+ \frac{1}{a_{m+1}}]$$

$$= \frac{(a_m+ \frac{1}{a_{m+1}})p_{m-1}+p_{m-2}}{(a_m+ \frac{1}{a_{m+1}})q_{m-1}+q_{m-2}}$$

$$= \frac{(a_ma_{m+1}+1)p_{m-1}+a_{m+1}p_{m-2}}{(a_ma_{m+1}+1)q_{m-1}+a_{m+1}q_{m-2}}$$

$$= \frac{a_{m+1}(a_mp_{m-1}+p_{m-2})+p_{m-1}}{a_{m+1}(a_mq_{m-1}+q_{m-2})+q_{m-1}}$$

$$= \frac{a_{m+1}p_m+p_{m-1}}{a_{m+1}q_m+q_{m-1}}$$

$$= \frac{p_{m+1}}{q_{m+1}}$$

elde edilir ki bu m+1 için doğruluğunu gösterir. Bu ise toremin ispatını tamamlar.

Bu teoremden faydalanarak verilen sürekli kesrin yakınsayanlarının değerleri bulunur. Buna göre;

$$S_0=a_0$$

$$S_1 = \frac{p_1}{q_1}= a_0 + \frac{1}{a_1}$$

$$S_2 = \frac{p_2}{q_2}= \frac{a_2p_1+p_0}{a_2q_1+q_0}$$

$$= \frac{a_2(a_1a_0+1)+a_0}{a_2a_1+1}$$

$$= \frac{a_0(a_1a_2+1)+a_2}{a_1a_2+1}$$

$$= a_0 + \frac{a_2}{a_1a_2+1}$$

$$= a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2}}$$

$$\vdots$$

$$S_n = \frac{p_n}{q_n} = \frac{a_np_{n-1}+p_{n-2}}{a_nq_{n-1}+q_{n-2}} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}}$$

şeklindedir.

Verilen sürekli kesrin yakınsayanları ile ilgili aşağıdaki teoremleri ifade edelim.

TEOREM 1.2.2. p_n ve q_n değerleri

$$p_nq_{n-1} - p_{n-1}q_n = (-1)^{n-1}$$

veya

$$\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n-1}}{q_nq_{n-1}}$$

eşitliklerini sağlar [3].

TEOREM 1.2.3. p_n ve q_n değerleri

$$p_nq_{n-1} - p_{n-2}q_n = (-1)^n a_n$$

veya

$$\frac{p_n}{q_n} - \frac{p_{n-2}}{q_{n-2}} = \frac{(-1)^n a_n}{q_nq_{n-2}}$$

eşitliklerini sağlar [3].

TEOREM 1.2.4. Çift indisli S_{2n} yakınsayanı n ile monoton artar ken, tek indisli S_{2n+1} yakınsayanı n ile monoton azalandır.

TEOREM 1.2.5. Her tek yakınsayan herhangi bir çift yakınsayandan büyüktür.

TEOREM 1.2.6.Bir sürekli kesrin değeri,herhangi bir çift yakın sayandan büyük, herhangi bir tek yakınsayandan küçüktür.

TEOREM 1.2.7. Her rasyonel sayı sonlu sürekli kesirle temsil edilebilir.

TEOREM 1.2.8. $q_n \geq n$ dir. Eşitlik n=3 için vardır [3].

1.3. SONSUZ SÜREKLİ KESİRLER

Verilen bir rasyonel sayının sonlu sürekli kesir ile temsil edildiği incelendi. Bu kesimde bir irrasyonel sayının sürekli kesirle nasıl temsil edilebileceğini ele alacağız.

TANIM 1.3.1. $a_0, a_1, a_2, \ldots$ ler a_0 hariç, hepsi pozitif olan tamsayıların bir dizisi olsun. Bu taktirde $[a_0, a_1, \ldots]$ kesrine sonsuz sürekli kesir adı verilir ve $\lim_{n\to\infty} [a_0, a_1, \ldots, a_n]$ değerine $[a_0, a_1, \ldots]$ kesrinin değeri denir. Bu limit, $\lim_{n\to\infty} \delta_n$ limitiyle aynıdır. Diğer bir söyleyişle bu limit, $\lim_{n\to\infty} \frac{p_n}{q_n}$ şeklindedir.

TEOREM 1.3.1. Sürekli kesrin δ_n yakınsayanlarının değerleri

$$\delta_0 < \delta_2 < \delta_4 < \ldots < \ldots < \delta_5 < \delta_3 < \delta_1$$

şeklindeki diziyi oluştururlar. δ_n yakınsayanı, çift indislilerle monoton artarken, tek indislilerle monoton azalandır ve her δ_{2n} yakınsayanı her δ_{2n-1} yakınsayandan daha küçüktür. Ayrıca $\lim_{n\to\infty} \delta_n$ mevcut olup

$$\delta_{2j} < \lim_{n\to\infty} \delta_n < \delta_{2j+1} \quad , \quad \forall\, j \geq 0$$

dır [1].

TEOREM 1.3.2. Bütün sonsuz sürekli kesirler yakınsaktır.

Ispat. $\delta_n = \frac{p_n}{q_n} = [a_0, a_1, \ldots, a_n]$ yazalım ve bu sürekli kesre $[a_0, a_1, \ldots]$ kesrinin yakınsayanı diyelim. Bu yakınsayanların, yani $\delta_0, \delta_1, \ldots$ dizisinin bir limite gittiğini göstermeliyiz. $N \geq n$ ise δ_n yakınsayanı aynı zamanda $[a_0, a_1, \ldots, a_N]$ sürekli kesrinin yakınsayanıdır. Çift yakınsayan artan ve tek yakınsayan azalan olup ve her bir çift yakınsayan δ_1 den küçük olduğundan çift yakınsayanın artan bir dizisi üstten sınırlıdır. Yine her tek yakınsayan ε_0 dan büyük olduğundan, tek yakınsayanın azalan dizisi alttan sınırlıdır. O halde çift yakınsayanlar dizisi bir ε_1 limitine ve tek yakınsayanlar dizisi ε_2 limitine gider. $\varepsilon_1 \leq \varepsilon_2$ olduğu açıktır. Sonuç olarak Teorem 1.2.2 ve Teorem 1.2.8 den

$$\left| \frac{p_{2n}}{q_{2n}} - \frac{p_{2n-1}}{q_{2n-1}} \right| = \frac{1}{q_{2n}\, q_{2n-1}} \leq \frac{1}{2n(2n-1)}$$

yazılır. $n \to \infty$ için limit alınınca

$$\left| \frac{p_{2n}}{q_{2n}} - \frac{p_{2n-1}}{q_{2n-1}} \right| = 0$$

olur ki, bu $\varepsilon_1 = \varepsilon_2$ olmasıdır. Bu ise tek ve çift yakınsayanlar dizisinin aynı bir x e yakınsadığını gösterir.

Sonuç olarak $[a_0, a_1, \ldots]$ sonsuz sürekli kesri x e yakınsar [3]. Sonlu sürekli kesirlerde vermiş olduğumuz teoremler, sonsuz sürekli kesirler için de geçerlidir.

TEOREM 1.3.3. Herhangi bir $[a_0, a_1, \ldots]$ sonsuz sürekli kesrin değeri bir irrasyonel sayıdır [1].

1.4. IRRASYONEL SAYILARIN SONSUZ SÜREKLİ KESİRLE TEMSİLİ

Bu kesimde herhangi bir sonsuz sürekli kesrin bir irrasyonel sayı temsil ettiği, tersine olarak ε veya ε_0 bir irrasyonel sayı ise sonsuz sürekli kesre nasıl açılabildiği gösterilecek. a_i ler tam sayılar ve ε_i ler irrasyonel sayılar olmak üzere

$$a_0 = [\varepsilon_0] \ , \qquad \varepsilon_1 = \frac{1}{(\varepsilon_0 - a_0)} \ , \quad a_1 = [\varepsilon_1] \ , \qquad \varepsilon_2 = \frac{1}{(\varepsilon_1 - a_1)}$$

ve

$$a_i = [\varepsilon_i] \ , \quad \varepsilon_{i+1} = \frac{1}{\varepsilon_i - a_i} \qquad (1.4.1)$$

olarak tanımlayalım. Ayrıca $i \geq 1$ için $a_i \geq 1$ dir. Çünkü $a_{i-1} = [\varepsilon_{i-1}]$ ve ε_{i-1} irrasyonel sayı olduğundan

$$a_{i-1} < \varepsilon_{i-1} < 1 + a_{i-1} \quad , \quad 0 < \varepsilon_{i-1} - a_{i-1} < 1$$

$$\varepsilon_i = \frac{1}{\varepsilon_{i-1} - a_{i-1}} > 1$$

olur. Buradan $a_i = [\varepsilon_i] \geq 1$ elde edilir.

(1.4.1) eşitliklerini ard arda uyguladığımızda

$$\varepsilon_i = a_i + \frac{1}{\varepsilon_{i+1}}$$

$$\varepsilon = \varepsilon_0 = a_0 + \frac{1}{\varepsilon_1} = [a_0, \varepsilon_1]$$

$$= [a_0, a_1 + \frac{1}{\varepsilon_2}] = [a_0, a_1, \varepsilon_2]$$

$$\cdots\cdots$$

$$= [a_0, a_1, \ldots, a_{m-2}, a_{m-1} + \frac{1}{\varepsilon_m}]$$

$$= [a_0, a_1, \ldots, a_{m-1}, \varepsilon_m]$$

elde edilir. Bu bize a_i lerle belirtilen $[a_0, a_1, \ldots]$ sonsuz sürekli kesrin değerinin ε olduğunu önerir, fakat bunu ispatlamaz. Bunun ispatı için Teorem 1.2.1 den

$$\varepsilon - \delta_{n-1} = \varepsilon - \frac{p_{n-1}}{q_{n-1}}$$

$$= \frac{\varepsilon_n p_{n-1} + p_{n-2}}{\varepsilon_n q_{n-1} + q_{n-2}} - \frac{p_{n-1}}{q_{n-1}}$$

$$= \frac{-(p_{n-1} q_{n-2} - p_{n-2} q_{n-1})}{q_{n-1}(\varepsilon_n q_{n-1} + q_{n-2})}$$

$$= \frac{(-1)^{n-1}}{q_{n-1}(\varepsilon_n q_{n-1} + q_{n-2})}$$

yazılır. Bu kesrin değeri $n \to \infty$ için sıfırdır. Çünkü q_n tamsayısı n ile monoton artan ve $\varepsilon_n > 0$ dır. Böylece $\varepsilon - \delta_{n-1}$, $n \to \infty$ için sıfırdır. Bu durumda Tanım 1.3.1 den

$$\varepsilon = \lim_{n \to \infty} \delta_n = \lim_{n \to \infty} [a_0, a_1, \ldots, a_n] = [a_0, a_1, \ldots]$$

dir.

TANIM 1.4.1. (Peryodik sürekli kesir) Yeterince büyük r tamsayıları için $a_r = a_{n+r}$ olacak şekilde bir $n > 0$ tamsayısı varsa $[a_0, a_1, \ldots]$ sonsuz sürekli kesrine peryodiktir denir, buradaki $n > 0$ tamsayısına sürekli kesrin peryodu adı verilir. Böyle bir peryodik sürekli kesir

$$[b_0, \ldots, b_j, a_0, \ldots, a_{n-1}, a_0, \ldots, a_{n-1}, \ldots] = [b_0, \ldots, b_j, \overline{a_0, \ldots, a_{n-1}}]$$

şeklinde gösterilir.

$a_0, a_1, \ldots, a_{n-1}$ tamsayıları üzerindeki çizgi, bu blok sınırsız olarak tekrarlandığını göstermektedir. Mesela, $[\overline{2,3}]$ peryodik kesri $[2,3,2,3,\ldots]$ yı temsil eder ve bunun değeri kolaylıkla hesaplanır. $[\overline{2,3}]=\theta$ yazıldığında

$$\theta = 2 + \cfrac{1}{3 + \cfrac{1}{\theta}}$$

olup , θ ya göre kuadratik bir denklemdir ve

$$\theta = \frac{3+\sqrt{15}}{3}$$

elde edilir.

Bu örnek bize aşağıdaki sonucu verir.

TEOREM 1.4.1. Herhagi bir peryodik sürekli kesir bir kuadratik irrasyonel sayıdır ve bunun tersi de doğrudur [1].

1.5 KONGRÜANSLAR

TANIM 1.5.1. Sıfırdan farklı bir m tamsayısı a−b farkını bölüyor ise a ya m modülüne göre b ye denktir denir ve $a \equiv b \pmod m$ şeklinde gösterilir. m, a−b farkını bölmüyorsa a, m modülüne göre b ye denk değildir denir ve $a \not\equiv b \pmod m$ şeklinde gösterilir. Böylece a−b nin m ile bölünebilmesi , −m ile de bölünebilmesini gerektireceğinden genellikle modülü pozitif olarak sınırlayacağız.

Kongrüansların aşağıdaki özellikleri vardır.

TEOREM 1.5.1. a,b,c,d,x ve y tamsayılar olmak üzere;

i) $a \equiv b \pmod m$ ise $b \equiv a \pmod m$ ve $a-b \equiv 0 \pmod m$,

ii) $a \equiv b \pmod m$ ve $b \equiv c \pmod m$ ise $a \equiv c \pmod m$,

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

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

v) $a \equiv b \pmod m$ ve $d|m$, $d>0$ ise $a \equiv b \pmod m$.

TEOREM 1.5.2.

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

ii) $(a,m)=1$ ise $ax \equiv b \pmod m$ kongrüansının bir çözümü vardır.

TEOREM 1.5.3. $(a,m)=d$ olmak üzere $ax \equiv b \pmod m$ kongrüansının çöçümünün olması için gerek ve yeter şart $d|b$ olmasıdır.

TANIM 1.5.2. $(a,m)=1$ olmak üzere $x^2 \equiv a \pmod m$ kongrüansının çözümü varsa a ya m nin kuadratik rezidüsü, aksi takdirde kuadratik non rezidüsü denir ve sırası ile KR veya KN olarak gösterilir.

TANIM 1.5.3. p tek asal ve $(a,p)=1$ olsun. Bu takdirde $\left(\frac{a}{p}\right)$ şeklinde gösterilen Legendre sembolü;

$$\left(\frac{a}{p}\right)= \begin{cases} 1, & \text{KR ise} \\ -1, & \text{KN ise} \end{cases}$$

şeklinde tanımlanır.

TEOREM 1.5.4. P tek asal ve a,b ler $(a,p)=(b,p)=1$ olacak şekilde tamsayılar ise bu takdirde;

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

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

iii) $\left(\frac{a}{p}\right)= \left(\frac{b}{p}\right)$ dir. $\Leftrightarrow$ $a\equiv b \pmod p$ ise ,

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

özellikleri sağlanır [1].

TANIM 1.5.4. $(P,Q)=1$, $Q\geq 0$, Q tek ve $Q=q_1q_2\ldots q_s$ farklı olması gerekmeyen tek asalların çarpımı olsun. $\left(\frac{P}{Q}\right)$ şeklinde gösterilen Jakobi sembolü

$$\left(\frac{P}{Q}\right) = \prod_{j=1}^{s} \left(\frac{P}{q_j}\right)$$

şeklinde tanımlanır. Burada $\left(\frac{P}{q_j}\right)$ Legendre sembolüdür. Q tek asal ise Legendre ve Jakobi sembolleri aynıdır ve $\left(\frac{P}{Q}\right) = \mp 1$ olduğu açıktır. Fakat $\left(\frac{P}{Q}\right)=1$ olması ,P nin Q nun bir kuadratik rezidüsü olmasını gerektirmez. Mesela, $\left(\frac{2}{9}\right)=1$ olmasına rağmen $x^2\equiv 2 \pmod 9$ kongrüansının çözümü yoktur. p nin Q nun bir kuadratik rezidüsü olması için $(P,Q)=1$ ve P, Q nun her q_j asal böleni için kuadratik rezidü olması gerekir.

TEOREM 1.5.5. Q ve Q_1 pozitif tek sayılar ve $(PP_1,QQ_1)=1$ olsun.

Bu takdirde ;

i) $\left(\frac{P}{Q}\right)\left(\frac{P}{Q_1}\right)=\left(\frac{P}{QQ_1}\right)$

ii) $\left(\frac{P}{Q}\right)\left(\frac{P^1}{Q}\right)=\left(\frac{PP^1}{Q}\right)$

iii) $\left(\frac{P^2}{Q}\right)=\left(\frac{P}{Q^2}\right)=1$

iv) $Q=8k\mp1$ şeklinde ise $\left(\frac{2}{Q}\right)=1$, $Q=8k\mp3$ ise $\left(\frac{2}{Q}\right)=-1$ dir.

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

vi) P , Q pozitif tamsayılar ve $(P,Q)=1$ ise

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right)=(-1)^{\frac{1}{2}(P-1)\,\frac{1}{2}(Q-1)}$$

özellikleri sağlanır.

1.6 CEBİRSEL SAYILAR

Bu kesimde katsayıları rasyonel olan polinomları gözönünde bulunduracağız. Bu polinomlara Q, rasyonel sayıların cismi olmak üzere Q üzerindeki polnomlardır denir. Rasyonel katsayılı ,x de ğişkenli polinomların cümlesi Q[x] ile, katsayıları tamsayılar ve x değişkenli polinomlar cümlesi Z[x] ile ve F herhangi bir sayı cismi olmak üzere, katsayıları F den alınan x değişkenli polinomlar cümlesi de F[x] ile tanımlanır.

$$f(x)=a_0x^n+a_1x^{n-1}+\dots+a_n \quad , \; a_n \neq 0 \; , \; n\in N$$

polinomunu gözönüne alalım. Burada n ye polinomun derecesi ve a_0 a başlangıç katsayısı adı verilir. Eğer $a_0=1$ ise bu polinoma monik polinom denir.
iki 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 $g(x)|f(x)$ şeklinde gösterilir. Burada g(x) in derecesi f(x) in derecesinden küçük veya eşittir

TEOREM 1.6.1. $g(x)\not\equiv0$ olmak üzere f(x) ve g(x), Q üzerinde iki polinom olsun. f(x)=g(x)q(x)+r(x) olacak şekilde bir tek q(x) ve r(x) polinomları vardır ve $r(x)\equiv0$ veya r(x) in derecesi g(x) in derecesinden daha küçüktür.

TEOREM 1.6.2. Sıfırdan farklı $f(x)$ ve $g(x)$ polinomlarının bir tek $d(x)$ monik polinomu vardır ve $d(x)$ polinomu ;

i) $d(x)|f(x)$, $d(x)|g(x)$.

ii) $d(x)$, $f(x)$ ve $g(x)$ in lineer kombinasyonu olarak yazılır,

iii) $f(x)$ ve $g(x)$ in herhangi bir ortak böleni, $d(x)$ in bir bölenidir ve $d(x)$ in derecesinden daha yüksek olan polinomlar , ortak bölen değildir.

TANIM 1.6.1. Teorem 1.6.2 de anlatılan $d(x)$ polinomuna $f(x)$ ve $g(x)$ polinomlarının en büyük ortak böleni denir ve

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

şeklinde gösterilir.

TANIM 1.6.2 $f(x)$ özdeş olarak sıfır olmayan bir polinom olsun. $f(x)=g(x)h(x)$ olacak şekilde ,Q üzerinde pozitif dereceli $g(x)$ ve $h(x)$ polinomları yoksa, $f(x)$ polinomuna Q üzerinde indirgenemezdir veya asaldır denir.

TEOREM 1.6.3. $p(x)$ indirgenemez polinomu $f(x)g(x)$ çarpımını bölüyor ise, $p(x)$ polinomu $f(x)$ veya $g(x)$ den en az birinin bölenidir [1].

TEOREM 1.6.4. $Q[x]$ üzerinde pozitif dereceli bir $f(x)$ polinomu $p_j(x)$ ler asal polinomlar olmak üzere ;

$$f(x) = cp_1(x)p_2(x)\ldots p_k(x)$$

şeklinde çarpanların sıra değişikliği hariç tek türlü çarpanlarına ayrılabilirdir.

TANIM 1.6.3. Tam katsayılı $f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_n$ polinomuna $(a_0,a_1,\ldots,a_n) = 1$ ise ilkel polinom adı verilir.

TANIM 1.6.4. $Q[x]$ üzerindeki bir $f(x)$ polinomu için $f(x)=0$ denklemini sağlayan α kompleks sayısına cebirsel sayı denir.

TEOREM 1.6.5. α cebirsel sayısı , $Q[x]$ üzerindeki $g(x)=0$ olan bir tek indirgenemez monik polinom denklemini sağlar. Bununla beraber α nın $Q[x]$ üzerinde sağladığı her polinom denklemi $g(x)$ ile bölünebilir.

TANIM 1.6.5. Teorem 1.6.5 de sözü edilen $g(x)=0$ denklemine α ce birsel sayısının sağladığı **minimal denklem denir** ve $g(x)$, α nın sağladığı minimal polinomdur. Bu polinomun derecesi cebirsel sayının derecesidir.

TANIM 1.6.6. α cebirsel sayısı , katsayıları tamsayılar olan

$$f(x)=x^{n}+b_{1}x^{n-1}+..+b_{n}=0$$

şeklindeki monik polinom denklemini sağlıyor ise bu takdirde α cebirsel sayısına cebirsel tamsayı adı verilir.

TEOREM 1.6.6. Rasyonel sayılar arasında sadece $0,\mp1,\mp2,...$ tam sayıları cebirsel tamsayılardır.

Ispat. $f(x)$ de x-m alındığında, 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

$$\left(\frac{m}{q}\right)^{n}+b_{1}\left(\frac{m}{q}\right)^{n-1}+...+b_{n}=0$$

$$m^{n}+b_{1}qm^{n-1}+...+b_{n}q^{n}=0$$

olur. Böylece $q|m^{n}$ olduğu görülür. Buradan $q=\mp1$ olduğundan $\frac{m}{q}$ bir tamsayıdır. Tanım 1.6.6 daki tamsayı kelimesi, önceki kullandıklarımızın basit bir genelleştirmesidir.

Cebirsel sayılar teorisinde $0,\mp1,\mp2,...$ ler ,rasyonel olmayan diğer cebirsel tamsayılardan ayırmak için çoğu kez rasyonel tamsayılar olarak belirtilir.Örneğin $\sqrt{2}$ cebirsel tamsayı fakat rasyonel tamsayı değildir.

TEOREM 1.6.7. Bir cebirsel tamsayının sağladığı minimal denklem katsayıları tamsayılar olan bir monik denklemdir.

TEOREM 1.6.8. α ve β cebirsel sayılar ise $\alpha+\beta$, $\alpha\beta$ da cebirsel sayı , α ve β cebirsel tamsayılar ise $\alpha+\beta$ ve $\alpha\beta$ da cebirsel tamsayılardır.

TEOREM 1.6.9. Bütün cebirsel sayıların cümlesi bir cisim ve bütün cebirsel tamsayıların sınıfı bir halkadır.

Teorem 1.6.9 da anlatılan cisim,cebirsel sayıların bütününü ihtiva eder. Genel olarak bütün bu kolleksiyonların cisim, olan herhangi bir alt cümlesi cebirsel sayı cismidir. Mesela, $f(x)$ $h(x)$, $Q[x]$ üzerindeki polinomlar ve α cebirsel sayı ise bu takdirde $h(\alpha)\neq 0$ olmak üzere $f(\alpha)/h(\alpha)$ formundaki bütün sayıların kolleksiyonu bir cisimdir. Bu cisme Q nun α ile genişletilmesi denir ve $Q(\alpha)$ şeklinde gösterilir.

TEOREM 1.6.11. α , n. dereceden cebirsel bir sayı ise $Q(\alpha)$ nun her elemanı , a_i ler rasyonel tamsayılar olmak üzere

$$a_0+a_1\alpha+\ldots+a_{n-1}\alpha^{n-1}$$

şeklinde tek türlü yazılır.

Herhangi bir sayı cismi 0,1 ve diğer cisim aksiyomları dikkate alındığında bütün rasyonel sayıları da ihtiva eder. Dolayısıyle herhangi bir cebirsel sayı cismi en azından bazı cebirsel tamsayıları,rasyonel tamsayıları ihtiva eder. Aşağıdaki teorem genelde bir cebirsel sayı cisminin diğer cibirsel tamsayıları da ihtiva ettiğini göstermektedir.

TEOREM 1.6.12.α herhangi bir cebirsel sayı ise $b\alpha$ cebirsel tam sayı olacak şekilde bir b rasyonel tamsayısı vardır.

Ispat. $f(x)$,$f(\alpha)=0$ olacak şekilde $Q[x]$ üzerinde bir polinom olsun. $f(x)$ polinomunun katsayılarını rasyonel tamsayılar olarak düşünebiliriz. (Zira katsayılarının en küçük ortak katı ile çarpmak suretiyle bu durumu gerçekleştirebiliriz)

$$f(x) = bx^n+a_1x^{n-1}+\ldots+a_n= bx^n+\sum_{j=1}^{n}a_j$$

şeklinde alınabilir. Burada b ve a_j ler rasyonel tamsayılardır.Ozaman $b\alpha$

$$b^{n-1}f(\tfrac{x}{b}) = x^n+\sum_{j=1}^{n}a_jb^{j-1}x^{n-1}$$

polinomunun sıfırı olur ki,bu da $b\alpha$ nın cebirsel tamsayı olmasıdır.

TANIM 1.6.7 Herhangi bir F cebirsel sayı cisminde $\alpha\neq 0$ olmak üzere $\beta=\alpha\gamma$ olacak şekilde γ tamsayısı varsa, α ya β nın bir böleni denir ve $\alpha|\beta$ şeklinde gösterilir. 1 in herhangi bir bölenine F nin birimi denir. Sıfırdan farklı α ve β tamsayıları için $\frac{\alpha}{\beta}$ birim ise birbiriyle ilgildir denir.

α , Q üzerindeki indirgenemez kuadratik bir polinomun kökü olmak üzere , kuadratik cisim $Q(\alpha)$ formundadır. Bu gibi cismin elemanları a_0, a_1 rasyonel sayılar olmak üzere $a_0+a_1\alpha$ şeklindeki sayıların tamamıdır. a,b,c ve m tamsayılar olmak üzere

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

formunda olduğundan,

$$Q(\alpha)=Q(\frac{a+b\sqrt{m}}{c})=Q(a+b\sqrt{m})=Q(b\sqrt{m})=Q(\sqrt{m})$$

dir. Burada $c\neq 0$ ve m, içerisinde karesel çarpan ihtiva etmeyen 1 den farklı bir tamsayıdır. Diğer taraftan m ve n içerisinde karesel çarpan ihtiva etmeyen $m\neq 1$, $n\neq 1$ olacak şekilde iki tamsayı ise bu takdirde $\sqrt{m}$,$Q(\sqrt{n})$ nin elemanı olmadığından $Q(\sqrt{m})\neq Q(\sqrt{n})$ dir. Yani,$\sqrt{m}=a+b\sqrt{n}$ olacak şekilde a ve b rasyonel sayıları bulmak imkansızdır.

TEOREM 1.6.13.m içerisinde karesel çarpan ihtiva etmeyen,1 den farklı, pozitif veya negatif rasyonel tamsayı olmak üzere her kuadratik cisim $Q(\sqrt{m})$ formundadır. Eğer $m \equiv 2 (\mathrm{mod}\ 4)$ veya $m \equiv 3 (\mathrm{mod}\ 4)$ ise a ve b rasyonel tamsayılar olmak üzere $a+b\sqrt{m}$ formundaki sayılar $Q(\sqrt{m})$ cisminin tamlarıdır. Eğer $m\equiv 1 (\mathrm{mod}\ 4)$ ise a,b ler tek rasyonel tamsayılar olmak üzere $\frac{a+b\sqrt{m}}{2}$ formundaki sayılar $Q(\sqrt{m})$ cisminin tamlarıdır ve bundan başka cismin tamları yoktur.

TANIM 1.6.8. $Q(\sqrt{m})$ cisminde bir $\alpha = \frac{a+b\sqrt{m}}{c}$ tamının normu, α ile eşleniğinin çarpımıdır. Yani,

$$N(\alpha)=\alpha\,\bar{\alpha} = \frac{a^2-mb^2}{c^2}$$

dir.

TEOREM 1.6.14. Çarpımın normu,çarpanlarının normlarının çarpımına eşittir. $N(\alpha) = 0$ olması için gerek ve yeter şart $\alpha = 0$ olmasıdır. $Q(\sqrt{m})$ cismindeki tamsayıların normu rasyonel tamsayılardır. Eğer γ, $Q(\sqrt{m})$ cisminin tamsayısı ise $N(\gamma) = \mp 1$ olması için gerek ve yeter şart γ nın birim olmasıdır.

Bir $Q(\sqrt{m})$ kuadratik cismine $m<0$ ise imajener kuadratik cisim $m>0$ ise reel kuadratik cisim adı verilir.

TEOREM 1.6.15. m , içerisinde karesel çarpan ihtiva etmeyen negatif rasyonel tamsayı olsun. Bu takdirde $Q(\sqrt{m})$ cismi ∓ 1 birimlerine sahiptir ve bunlar m=-1 ve m=-3 durumları hariç tek birimlerdir. Q(i) cisminin birimleri ∓1 ve ∓i dir. Q($\sqrt{-3}$) cisminin birimleri ∓1 ,(1∓$\sqrt{-3}$)/2 ve (-1∓$\sqrt{-3}$)/2 dir [1].

TEOREM 1.6.16. Herhangi bir reel kuadratik cismin sonsuz sayıda birimleri vardır [1].

TANIM 1.6.9. Q($\sqrt{m}$) kuadratik cisminde birimden farklı olan, α cebirsel tamsayısının böleni sadece cismin birimi ve kendisiyle ilgili olanı ise α ya asaldır denir.

TEOREM 1.6.17. Eğer Q($\sqrt{m}$) kuadratik cismindeki α tamsayısının normu, p rasyonel asal olmak üzere,

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

ise α asaldır [1].

TEOREM 1.6.18. Q($\sqrt{m}$) nin sıfırdan ve birimden farkı her tamsayısı asalların çarpımı olarak yazılabilir.

TANIM 1.6.10. Q($\sqrt{m}$) kuadratik cismindeki sıfırdan ve birimden farklı her α sayısı ,asalların ve ilgili asalların sıra değişikliği hariç asalların çarpımı olarak tek türlü yazılabiliyorsa, Q($\sqrt{m}$) kuadratik cismine tek çarpan özelliğine sahiptir denir [1].

TANIM 1.6.11. Q($\sqrt{m}$) cismindeki tamsayılar Euclid algoritmasını sağlıyorsa ,Yani $\alpha,\beta \in$ Q($\sqrt{m}$) , $\beta \neq 0$ olduğunda $\alpha = \beta\gamma+\delta$, $|N(\delta)|<|N(\beta)|$ olacak şekilde γ,δ tamsayıları varsa, Q($\sqrt{m}$) kuadratik cisme Euclid kuadratik cismi adı verilir.

TEOREM 1.6.19. Her Euclid kuadratik cismi tek çarpan özelliğine sahiptir [1].

TEOREM 1.6.20. m=-1,-2,-3,-7,2,3 için Q($\sqrt{m}$) Euclidyen ve tek çarpan özelliğine sahiptir.

Ispat. Q($\sqrt{m}$) de $\beta\neq0$ olmak üzere herhangi α,β tamsayılarını gözönüne alalım. Bu durumda $\alpha/\beta = u+v\sqrt{m}$ dir. Burada u ve v rasyonel sayılar olup, x ve y rasyonel tamsayılarını, u ve v ye yakın olacak şekilde seçelim. Yani,

$$0\leq|u-x|\leq \tfrac{1}{2} \quad , \quad 0\leq|v-y|\leq \tfrac{1}{2} \qquad (1.6.1)$$

dir .Eğer x+y$\sqrt{m}$ yi γ ile ve $\alpha-\beta\gamma$ yı δ ile gösterirsek bu durumda γ ve δ lar $Q(\sqrt{m})$ de tamsayılar olur ve

$$N(\delta)=N(\alpha-\beta\gamma)=N(\beta)N(\tfrac{\alpha}{\beta}-\gamma)$$
$$=N(\beta)N((u-x)+(v-y)\sqrt{m})$$
$$=N(\beta)\{(u-x)^2-m(v-y)^2\}$$
$$|N(\delta)|=|N(\beta)||(u-x)^2-m(v-y)^2|$$

dir. (1.6.1) den $m>0$ ise, $-\frac{m}{4} \leq (u-x)^2-m(v-y)^2 \leq \frac{1}{4}$,

$m<0$ ise $0 \leq (u-x)^2-m(v-y)^2 \leq \frac{1}{4} + \frac{1}{4}(-m)$

dir. Buna bağlı olarak $m=2,3,-1,-2$ ise $|N(\delta)| < |N(\beta)|$ dir. Bu nedenle $Q(\sqrt{m})$,m nin bu değeri için Eucledyendir.

TEOREM 1.6.21. $Q(\sqrt{m})$ tek çarpan özelliğine sahip olsun. $Q(\sqrt{m})$ deki herhangi bir π asalına $\pi|p$ olacak şekilde bir ve yalnız bir p rasyonel asalı karşılık gelir [1].

TEOREM 1.6.22. $Q(\sqrt{m})$ tek çarpan özelliğine sahip olsun. Bu tak dirde ,

i) Herhangi bir rasyonel p asalı ya cismin π gibi bir asalı ya da $Q(\sqrt{m})$ cismin farklı olması gerekmeyen $\pi_1\pi_2$ asallarının çarpımıdır.

ii) π,π_1,π_2 asallarının ve (i) deki rasyonel asalların hepsi ilgilileriyle birlikte $Q(\sqrt{m})$ cisminin bütün asallarının cümlesini oluşturur.

iii) $(p,m)=1$ olacak şekilde p rasyonel asalının, $Q(\sqrt{m})$ cisminin $\pi_1\pi_2$ gibi iki asalının çarpımı olması için gerek ve yeter şart,

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

olmasıdır. Bununla beraber eğer $p=\pi_1\pi_2$ şeklinde iki asalın çarpımı ise π_1 ve π_2 birbirinin ilgilisi değildir. Fakat $\pi_1,\overline{\pi}_2$ ile π_2 , $\overline{\pi}_1$ ile ilgilidir.

iv) Eğer $m\equiv3 (\mathrm{mod}\ 4)$ için $(2,m)=1$ ise 2 ye bir asalın karesiyle ilgilidir, $m\equiv5(\mathrm{mod}\ 8)$ ise 2 ye asaldır ve $m\equiv1(\mathrm{mod}\ 8)$ ise 2 ye farklı iki asalın çarpımıdır denir.

v) m yi bölen herhangi bir p rasyonel asalına , $Q(\sqrt{m})$ de bir asalın karesiyle ilgilidir denir [1].

BÖLÜM II

Bu bölümde Diophantine denklemlerinin çözümleri incelendi. Katsayıları tamsayılar olan 1 ve daha yüksek mertebeden n bilinmeyen ihtiva eden denklemler genel olarak Diophantine denklemleri olarak bilinirler. Bu tür denklemlerin tamsayılı çözüm leri bulunması problemi eski çağlardan beri bir çok matematikcinin uğraştığı konular arasındadır. İskenderiyeli matematikci DIOPHANTUS'a (M.S II-III yy.) kadar uzandığı için bu tür denklemlere Diophantine denklemleri adı verilir.

2.1 LİNEER DİOPHANTİNE DENKLEMLERİ

TANIM 2.1.1. $a_0, a_1, \ldots, a_{n-1}$ lerden en az biri sıfırdan farklı herhangi tamsayılar olmak üzere

$$a_0x_0+a_1x_1+\ldots+a_{n-1}x_{n-1}=b \quad , \quad n=1,2,\ldots \qquad (2.1.1)$$

şeklindeki denklemlere,birinci dereceden n bilinmeyenli lineer diophantine denklemi adı verilir.

TEOREM 2.1.1. (2.1.1) şeklindeki lineer diophantine denklemi nin $x_0, x_2, \ldots, x_{n-1}$ tamsayılarına göre çözümünün olması için gerek ve yeter şart $(a_0, a_1, \ldots, a_{n-1})=d$ olmak üzere $d|b$ olmasıdır [4].

TANIM 2.1.2. n=1 halinde (2.1.1) lineer diophantine denklemi

$$a_0x_0=b \qquad (2.1.2)$$

şekline dönüşür ve bu denkleme birinci dereceden bir bilinmeyenli lineer diophantine denklemi denir. Bu denklemin bir tam sayı çözümünün olabilmesi için $a_0|b$ olması gerekir. Bu takdirde (2.1.2) denkleminin bir tamsayı çözümü $x_0 = \frac{b}{a}$ şeklindedir.

TANIM 2.1.3. $n=2$ olması halinde (2.1.1) denklemi

$$a_0x_0+a_1x_1=b \qquad (2.1.3)$$

şekline dönüşür. Bu denkleme birinci dereceden iki bilinmeyenli lineer diophantine denklemi denir.

(2.1.3) şeklindeki denklemlerin tamsayı çözümlerini bulmak için $(a_0,a_1)=1$ kabul edeceğiz. Çünkü $(a_0,a_1) = d > 1$ ise $d|a_0$ ve $d|a_1$ olur. Buradan $a_0=a_0' d$, $a_1=a_1' d$ ve $(a_0',a_1')=1$ elde edilir.

(2.1.3) denkleminde $b=0$ ise bu takdirde lineer diophantine denklemi

$$a_0x_0+a_1x_1= 0$$

şekline dönüşür. Bu denklemin x_0'a göre çözümü $x_0=-\frac{a_1}{a_0}x_1$ dir $(a_0,a_1)=1$ ve x_0 tamsayı olması gerektiğinden $a_0|x_1$ olmalıdır ki, bu durumda $x_1=a_0t$, $t\in\mathbb{Z}$ olur. Ozaman $a_0x_0+a_1x_1= 0$ denkleminin bütün tamsayılı çözümleri

$$x_0=-a_1t \quad , \quad x_1=a_0t \quad , \quad t \in \mathbb{Z}$$

şeklindedir.

$a_0x_0+a_1x_1=b$ şeklindeki herhangi bir lineer diophantine denkleminin tamsayı çözümü sürekli kesirler yardımıyla bulunur.

TEOREM 2.1.2. p_n ve q_n ler, Teorem 1.2.1 deki şartları sağlayan tamsayılar olmak üzere $a_0x_0+a_1x_1=b$ diophantine denkleminin bir çözümü

$$x_0=(-1)^{n-1}\, bq_{n-1} \quad , \quad x_1=(-1)^n\, bp_{n-1}$$

formülleriyle verilir.

Ispat. Tanım 1.2.2 ve Teorem 1.2.2 den

$$\frac{a_0}{a_1} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n-1}}{q_1q_{n-1}}$$

yazılır. Buradan $a_0q_{n-1} - a_1p_{n-1} = (-1)^{n-1}$ olur. Bu ifadenin her iki tarafını $(-1)^{n-1}b$ ile çarpınca

$$a_0(-1)^{n-1}b\, q_{n-1} - a_1(-1)^{n-1}bp_{n-1} = b$$

elde edilir. Bu eşitlik

$$a_0((-1)^{n-1}bq_{n-1}) + a_1((-1)^{n}bp_{n-1}) = b$$

şeklinde olduğundan

$$x_0 = (-1)^{n-1}bq_{n-1} \quad , \quad x_1 = (-1)^{n}bp_{n-1}$$

olmalıdır. Bu ise teoremin ispatını tamamlar.

TEOREM 1.2.3. $a_0x_0 + a_1x_1 = b$ Lineer diophantine denkleminin $[x_0', x_1']$ bilinen bir çözümü ise bütün çözümleri

$$x_0 = x_0' + a_1t \quad , \quad x_1 = x_1' - a_0t \quad , \quad t \in \mathbb{Z}$$

şeklinde verilir.

Ispat. $[x_0', x_1']$, $a_0x_0 + a_1x_1 = b$ dekleminin bir çözümü ise, bu takdirde x_0' ve x_1' tamsayıları denklemi sağlar. Yani,

$$a_0x_0' + a_1x_1' = b$$

dir. Bunlardan

$$a_0(x_0 - x_0') + a_1(x_1 - x_1') = 0$$

veya

$$a_0(x_0 - x_0') = -a_1(x_1 - x_1')$$

elde edilir. Bu ise $a_1 | a_0(x_0 - x_0')$ veya $a_0 | -a_1(x_1 - x_0')$ demektir. $(a_0, a_1) = 1$ olduğundan ya $a_1 | (x_0 - x_0')$ ya da $a_0 | -(x_1 - x_1')$ dir. Eğer $a\ | x_0 - x_0'$ ise $x_0 - x_0' = a_1t$, $t \in \mathbb{Z}$ olur. Buradan $x_0 = x_0' + a_1t$, $t \in \mathbb{Z}$ dir. Benzer olarak $a_0 | -(x_1 - x_1')$ ise $-x_1 + x_1' = a_0t$, $t \in \mathbb{Z}$ olur ki, bu $x_1 = x_1' - a_0t$, $t \in \mathbb{Z}$ olmasıdır. Böylece $a_0x_0 + a_1x_1 = b$ lineer diophantine denkleminin bütün çözümlerinin, t bir tamsayı olmak üzere

$$x_0=x_0'+a_1t \quad , \quad x_1=x_1'-a_0t$$

şeklinde olduğu görülür.

Şimdi $n\geq 2$ bilinmeyenli lineer diophantine denklemlerinin çözümünün olduğunu kabul edelim. Bu takdirde (2.1.1) denkleminin çözümlerini bulmak için o denklemi iki bilinmeyenli lineer diophantine denklemine indirgeyeceğiz. Bunun için α,β,γ ve δ lar $\alpha\delta-\beta\gamma=1$ olacak şekildeki tamsayılar olmak üzere,

$$x_{n-2}=\alpha u+\beta v \quad , \quad x_{n-1}=\gamma u+\delta v \qquad (2.1.4)$$

yazalım. Buradan $u=\delta x_{n-2}-\beta x_{n-1}$, $v=-\gamma x_{n-2}+\alpha x_{n-1}$ olur ve x_{n-2} , x_{n-1} ler tamsayılar ise u ve v birer tamsayıdır.

Eğer

$$\beta=\frac{a_{n-1}}{(a_{n-2},a_{n-1})} \quad , \quad \delta=-\frac{a_{n-2}}{(a_{n-2},a_{n-1})}$$

alırsak $(\beta,\delta)=1$ olur ve Teorem 2.1.2 yardımıyla $\alpha\delta-\beta\gamma=1$ olacak şekildeki α ve γ tamsayıları bulunur. Bununla birlikte α ve γ nın sadece bir değerine ihtiyacımız vardır. Böylece (2.1.1) denklemi

$$a_0x_0+a_1x_1+\ldots+a_{n-3}x_{n-3}+(a_{n-2}\alpha+a_{n-1}\gamma)u=b \qquad (2.1.5)$$

şeklinde bir eksik bilinmeyene indirgenir.

$$a_{n-2}\alpha+a_{n-1}\gamma = -(a_{n-2},a_{n-1})\alpha\delta+(a_{n-2},a_{n-1})\gamma\beta$$

$$=-(a_{n-2},a_{n-1})$$

$$(a_0,a_1,\ldots,a_{n-3},(a_{n-2},a_{n-1})) = (a_0,a_1,\ldots,a_{n-1})$$

olduğunu da dikkate alırsak (2.1.5) denklemi (2.1.1) denklemiyle aynı özelliğe sahip olur. Katsayıları sıfırdan farklı ve katsayıların en büyük ortak böleni b yi böler. Eğer $n>3$ ise bu indirgeme metodu (2.1.5) denklemine tekrar uygulanarak n-3 değişkenli denklem elde edene kadar tekrarlanır.

Yine biliyoruz ki, iki bilinmeyenli bir lineer diophantine denklemi bir çözüme sahipse bu denklemin bütün çözümleri bir tek t parametrisine bağlıdır. Benzer olarak n bilinmeyenli (2.1.1) denkleminin çözümleri n-1 parametriye bağlıdır. Bu, n üzerinden tümevarımla gösterilebilir. Eğer (2.1.5) deki gibi n-1 bilinmeyenli herhangi bir denklem, n-2 parametrili $v_0,\ldots,v_{n-3}$ ün terimlerine göre $x_0,x_1,\ldots,x_{n-3},u$ çözümlerine sahip ise bu durumda (2.1.4) den (2.1.5) denkleminin çözümleri

$$x_0,x_1,\ldots,x_{n-3},\alpha u+\beta v,\gamma u+\delta v$$

ile verilir. Bunlar n-1 parametri olan $v_0,v_1,\ldots,v_{n-3},v$ yi içine alır. Bu çözümlerin

$$x=b_i+d_{i,0}v_0+d_{i,1}v_1+\ldots+d_{i,n-2}v_{n-2}$$

formunda olduğunu görmek kolaydır. Burada v yerine v_{n-2} yazılmıştır [1].

Bu indirgeme metotu yardımıyle n bilinmeyenli lineer diophantine denklemlerinin çözümünü elde etmiş oluruz.

2.2 İKİNCİ DERECEDEN DİOPHANTİNE DENKLEMLERİ

KUADRATIK FORMLAR

Form, bir homogen polinomdur. Yani,bütün terimleri aynı dereceden olan çok değişkenli bir polinomdur.Bir f kuadratik formu ikinci dereceden terimlere sahip olan

$$f(x_1,x_2,\ldots,x_n)=\sum_{i,j=1}^{n}a_{ij}x_ix_j \qquad (2.2.1)$$

şeklinde bir ifadedir. Biz kuadratik formları sadece katsayıları tamsayılar olan kuadratik forma kısıtlayacağız.

Eğer hepsi sıfırdan farklı $x_1,x_2,\ldots,x_n$ tamsayıları için $f(x_1,x_2,\ldots,x_n)$formu pozitif ise bu durumda f ye bir pozitif form, eğer $f(x_1,x_2,\ldots,x_n)$ formu negatif oluyorsa f ye negatif form denir. Pozitif veya negatif olan formlara belirli form denir. Mesela, $x_1^2+y_1^2$ bir pozitif kuadratik form, $-x_1^2-3x_2^2$ bir negatif kuadratik form x^2-y^2 formuna ise belirsiz form denir. f, bir pozitif form ise $-f$ nin bir negatif form olduğu açıktır ve bunun tersi de doğrudur.

Eğer $f(b_1,b_2,\ldots,b_n) = m$ olacak şekilde $b_1,b_2,\ldots,b_n$ tamsayıları varsa (2.2.1) kuadratik formuna m sayısını temsil ediyor denir. Mesela, $x_1^2+x_2^2$ 5 i temsil eder fakat 6 yı temsil etmez. Bu durumda her kuadratik form sıfırı temsil eder. Hepsi birden sıfır olmayan $b_1,b_2,\ldots,b_n$ tamsayıları için

$$f(b_1,b_2,\ldots,b_n) = 0$$

ise, f formuna sıfır form denir. $f(x,y)=ax^2+bxy+cy^2$ şeklinde iki değişken içeren forma, binary kuadratik form,

$$x^2+y^2+z^2 \quad , \quad xy+xz+yz \quad , \quad x^2-yz$$

şeklindekilere üç değişkenli kuadratik form,

$$x^2+y^2+z^2+t^2 \quad , \quad xy+zt$$

şeklindekilere dört değişkenli kuadratik form adı verilir [5].

TEOREM 2.2.1. $a>0$, $c>0$ olmak üzere $f(x,y)=ax^2+bxy+cy^2$ kuadratik formunun pozitif form olması için gerek ve yeter şart,

$$b^2-4ac<0$$

olmasıdır [1].

THUE TEOREMİ. m nin bir doğal sayı ve a, m ile aralarında asal olan bir tamsayı olmak üzere, $ay\mp x$ m ile bölünebilecek şekilde her ikisi de $\sqrt{m}$ den küçük olan x,y doğal sayıları vardır. Sıfırdan farklı tamsayılar için (2.1.1) kuadratik formunun bir m sayısını temsil ettiğini biliyoruz. m nin asal olması durumu için aşağıdaki teoremleri ifade edelim.

TEOREM 2.2.2.

i) $p\equiv1 \pmod 4$ şeklindeki her p asalı, x ve y doğal sayılar olmak üzere $p=x^2+y^2$ formunda yazılabilir. Bu özelliği sağlayan başka tek asal sayı yoktur.

ii) $p\equiv1 \pmod 6$ şeklindeki her p asalı, x ve y doğal sayılar olmak üzere $p=x^2+3y^2$ formunda yazılabilir. Bu özelliği sağlayan başka asal yoktur.

iii) $p\equiv1 \pmod 8$ veya $p\equiv3 \pmod 8$ şeklindeki her p asalı, x ve y doğal sayılar olmak üzere $p=x^2+2y^2$ formunda yazılabilir. Bu özelliği sağlayan başka asallar yoktur.

iv) $p\equiv1 \pmod{14}$, $p\equiv9 \pmod{14}$ veya $p\equiv11 \pmod{14}$ şeklindeki asallar, x ve y doğal sayılar olmak üzere $p=x^2+7y^2$ formunda yazılabilir. Bu özelliği sağlayan başka asallar yoktur.

v) $p\equiv5 \pmod{24}$ veya $p\equiv11 \pmod{24}$ şeklindeki asallar, x ve y doğal sayılar olmak üzere $p=2x^2+3y^2$ formunda yazılabilir. Bu özelliği sağlayan başka asallar yoktur [6].

İspat. $d=1,2,3,7$ ve p asal olmak üzere,

$$z^2+d \equiv 0 \pmod p \qquad (2.2.2)$$

kongrüansını gözönüne alalım.

$d=1$ için, $z^2+1\equiv0 \pmod p$ veya $z^2\equiv-1 \pmod p$ olur. Tanım 1.4.2 ve Teorem 1.4.4 den $p\equiv1 \pmod 4$ olmalıdır. Yani, -1 sayısı $p=4k+1$ asalları için KR dir.

$d=2$ için, $z^2\equiv-2 \pmod p$ kongrüansının çözümü olabilmesi için gerek ve yeter şart, $p\equiv1$, $3 \pmod 8$ olmalıdır.

$d=3$ için, $z^2\equiv-3 \pmod p$ kongrüansının çözümü olabilmesi için gerk ve yeter şart, $p\equiv1 \pmod 6$ olmasıdır. ($p=3$ hariç)

$d=7$ için, $z^2\equiv-7 \pmod p$ kongrüansının çözümü olabilmesi için gerek ve yeter şart, $p\equiv1 \pmod{14}$, $p\equiv9 \pmod{14}$ veya $p\equiv11 \pmod{14}$ olmalıdır. ($p=7$ hariç)

z sayısı (2.2.2) nin bir çözümü ve modül de herhangi bir p asal sayısı olsun. Thue teoremine göre $\sqrt{p}$ den küçük x,y doğal sayıları bulabiliriz ki, bunlar $z=\mp\frac{x}{y} \pmod p$ şartını sağlarlar. $(x,y)=1$ kabul edersek $z^2\equiv\frac{x^2}{y^2} \pmod p$ yazabiliriz.

Buradan (2.2.2) kongrüansı $x^2+dy^2\equiv0 \pmod p$ şekline dönüşür Böylece $m\leq d$, $m\in\mathbb{N}$ olmak üzere,

$$x^2+dy^2=mp \qquad (2.2.3)$$

elde ederiz.

$d=1$ için (2.2.3) eşitliğinde $m=1$ olacağından $x^2+y^2=p$ elde ederiz ki, bu (i) nin ispatıdır.
$d=2$ için $m=1$ veya $m=2$ dir. Ozaman (2.2.2) eşitliği

$$x^2+2y^2=p \quad \text{veya} \quad x^2+2y^2=2p$$

elde edelir. $x^2+2y^2=2p$ daima çift olduğundan, x^2 nin çift olması gerekir. Yani,

$$4x_1^2+2y^2=2p \quad \text{den} \quad 2x_1^2+y^2=p$$

bulunur.

$d=3$ için $m=1,2,3$ olacaktır. (2.2.2) denkleminden

$$x^2+3y^2=p \quad , \quad x^2+3y^2=2p \text{ veya } x^2+3y^2=3p$$

elde edilir. Üçüncü eşitlikte $x=3x_1$ yazarsak $3x_1^2+y^2=p$ dir ve ikinci eşitlik, $p\neq 2$ olması durumunda çözümü yoktur.
$d=7$ için $m=1,2,3,4,5,6,7$ olacaktır. Eğer m çift ise x ve y nin her ikiside tek olmak zorundadır. m çift ise x^2+7y^2 ifadesi 8 ile bölünebilir. Fakat bp , 8 ile bölünemez. Ohalde m çift olamaz.
$m=1$ ise $x^2+7y^2=p$ dir.
$m=3$ veya $m=5$ ise çözümü yoktur. Çünkü -7 sayısı 3 ve 5 için bir KN dir.
$m=7$ ise $x^2+7y^2=7p$ den $7x_1^2+y^2=p$
elde edilir. Böylece (ii),(iii) ve(iv) ü ispatlamış oluruz.

TEOREM 2.2.3 c ve d verilen doğal sayılar ve x,y herhangi iki doğal sayı olmak üzere p asal sayısının $p=cx^2+dy^2$ şeklindeki ifadesi en fazla bir tanedir.

$$p=cx^2+dy^2 \tag{2.2.4}$$

ve

$$p=cu^2+dv^2 \tag{2.2.5}$$

şeklinde iki türlü ifade edilebildiğini kabul edelim. Bu iki eşitlikten

$$p(y^2-v^2)=c(u^2y^2-x^2v^2)$$

elde edilir ve $c<p$ dir.

$$uy \equiv \mp xv \pmod p \qquad (2.2.6)$$

dir. (2.24) ve (2.2.5) den

$$p^2=(cux \pm dyv)^2+cd(uy \mp vx)^2 \qquad (2.2.7)$$

elde edilir. Eğer $uy=vx$ ise $(x,y)=(u,v)=1$ olur. Bu durumda $u=x$, $v=y$ olur ki bu p nin tek olarak yazılmasıdır. $uy \neq vx$ ise (2.2.6) ve (2.2.7) den

$$|uy \mp vx|=p \quad , \quad c=d=1 \quad , \quad cxu+dvy=0$$

olur. Bu eşitlik ancak $u=x$ ve $v=y$ olmasıyla mümkündür. Bu da p nin tek olarak ifade edildiğini gösterir.

TEOREM 2.2.4. Her N doğal sayısı, x_1,x_2,x_3,x_4 tamsayılar olmak üzere

$$x_1^2+x_2^2+x_3^2+x_4^2=N$$

şeklinde dört tamsayının kareleri toplamı olarak yazılabilir.

PELL DENKLEMLERİ

D tamkare olmayan bir doğal sayı olmak üzere genel olarak

$$X^2-DY^2=N \quad , \quad N \in \mathbb{Z}$$

denklemi Pell denklemi olarak bilinir. Fakat Pell genelde

$$X^2-DY^2=1$$

denklemiyle uğraşmıştır. Biz bundan sonra Pell denklemi olarak

$$X^2-DY^2=1$$

denklemini ifade edeceğiz.

$X^2-DY^2=\mp 1$ DENKLEMLERİ

TEOREM2.2.5. A irrasyonel bir sayı ise

$$|x-Ay|<\frac{1}{y}$$

eşitsizliğini sağlayan sonsuz tane x,y tamsayıları vardır.

LEMMA 2.2.1. D tamkare olmayan bir doğal sayı olmak üzere

$$|x^2-Dy^2|<1+2\sqrt{D} \tag{2.2.8}$$

eşitsizliğini sağlayan sonsuz tane x,y doğal sayı çifti vardır.

İspat. x,y Teorem 2.2.5 i sağlayan tamsayı çifti ise bu takdirde

$$|x+y\sqrt{D}|=|x-y\sqrt{D}+2y\sqrt{D}|$$
$$\leq|x-y\sqrt{D}|+|2y\sqrt{D}|$$
$$<\frac{1}{y}+2y\sqrt{D}$$
$$\leq(1+2\sqrt{D})y$$

dir. Böylece

$$|x+y\sqrt{D}|<(1+2\sqrt{D})y$$
$$|x-y\sqrt{D}|<\frac{1}{y}$$
$$|x^2-Dy^2|<1+2\sqrt{D}$$

elde edilir. Bu ise bizim göstermek istediğimizdir.

TEOREM 2.2.6. D tamkare olmayan bir doğal sayı ise

$$X^2-DY^2=1 \tag{2.2.9}$$

denklemini sağlayan en az bir x,y doğal sayı çifti vardır.

İspat. Lemma 2.2.1 den sonsuz sayıda x,y doğal sayı çifti için

$$X^2-DY^2=k$$

denklemini sağlayan sıfırdan farklı en az bir $k\in\mathbb{Z}$ vardır. Bu x,y doğal sayı çifti arasından

$$x_1\equiv x_2(\mathrm{mod}|k|) \text{ ve } y_1\equiv y_2(\mathrm{mod}|k|) \tag{2.2.10}$$

şartını sağlayan en az iki (x_1,y_1) ve (x_2,y_2) tamsayı çiftleri vardır. Buradan

$$x_1^2-Dy_1^2=x_2^2-Dy_2^2=k \tag{2.2.11}$$

olduğunu kabul edelim. Böylece x_1,y_1,x_2 ve y_2 (2.2.10) kongrüanslarını sağlarlar.

$$(x_1-y_1\sqrt{D})(x_2+y_2\sqrt{D})=x_1x_2-Dy_1y_2+(x_1y_2-x_2y_1)\sqrt{D}$$

çözümü, (2.2.10) ve (2.2.11) den

$$x_1x_2-y_1y_2D\equiv x_1^2-Dy_1^2\equiv 0(\mathrm{mod}|k|)$$

ve

$$x_1y_2-x_2y_1\equiv x_1y_1-x_1y_1\equiv 0(\mathrm{mod}|k|)$$

dir. Bu yüzden

$$x_1x_2-Dy_1y_2=ku$$

$$x_1y_2-x_2y_1=kv$$

olacak şekilde u,v tamsayı çifti vardır. Böylece

$$(x_1-y_1\sqrt{D})(x_2+y_2\sqrt{D})=k(u+v\sqrt{D})$$

$$(x_1+y_1\sqrt{D})(x_2-y_2\sqrt{D})=k(u-v\sqrt{D})$$

dir. Buradan her iki eşitliği taraf tarafa çarpınca,

$$(x_1^2-Dy_1^2)(x_2^2-Dy_2^2)=k^2(u^2-Dv^2)$$

olup $u^2-Dv^2=1$ elde edilir. Burada $v\neq 0$ dır. Eğer $v=0$ olsaydı

$$x_1y_2=x_2y_1 \quad , \quad u=\mp 1 \text{ ve}$$

$$(x_1-y_1\sqrt{D})(x_2+y_2\sqrt{D})(x_2-y_2\sqrt{D})=\mp k(x\ -y\ \sqrt{D})$$

$$(x_1-y_1\sqrt{D})k=\mp(x_2-y_2\sqrt{D})$$

ve buradan

$$(x_1-y_1\sqrt{D})=\mp(x_2-y_2\sqrt{D})$$

elde edilir bu ise

$$x_1=\mp x_2 \quad , \quad y_1=\mp y_2$$

anlamına gelir. Fakat $|x_1|\neq|x_2|$ olduğundan $v\neq 0$ olmalıdır. Bu ise teoremin ispatını tamamlar [6].

TANIM 2.2.1. D tamkare olmayan bir doğal sayı ve k bir tamsayı olsun. Eğer $x=u$ ve $y=v$ tamsayıları

$$X^2-DY^2=k \qquad (2.2.12)$$

diophantine denklemini sağlıyor ise u ve v sayılarına (2.2.12) denkleminin bir çözümü denir ve $u+v\sqrt{D}$ şeklinde gösterilir.

TANIM 2.2.2. $X^2-DY^2=1$ denkleminin bütün çözümlerini gözönüne alalım. Bunlar arasında en az bir $x_1+y_1\sqrt{D}$ çözümü vardır ki x_1 ve y_1 tamsayıları en küçük pozitif değerlerini alırlar. Bu şekildeki $x_1+y_1\sqrt{D}$ sayısına (2.2.12) denkleminin minimal (temel) çözümü adı verilir.

Verilen Pell denkleminin minimal çözümünün bulunması için aşağıdaki teoremlerden faydalanılır.

TEOREM 2.2.7. D tamkare olmayan bir pozitif tamsayı ve $\sqrt{D}$ nin sürekli kesre açılımında n. yakınsayanı $\frac{p_n}{q_n}$ olsun. N tamsayısı $|N|<\sqrt{D}$ şartını sağlasın. Bu durumda

$$X^2-DY^2=N$$

denkleminin $(s,t)=1$, $s,t \in \mathbb{Z}$ olmak üzere herhangi bir pozitif $x=s$ ve $y=t$ çözümü, bazı n doğal sayısı için $s=p_n$, $t=q_n$ eşitliklerini sağlarlar [1].

TEOREM 2.2.8. $X^2-DY^2=\mp1$ denkleminin bütün pozitif çözümleri $x=p_n$, $y=q_n$ arasında bulunur. Burada $\frac{p_n}{q_n}$, $\sqrt{D}$ nin sürekli kesre açılımındaki n. yakınsayanıdır. r , bu kesrin peryodu olmak üzere ,

i) r çift ise , $X^2-DY^2=-1$ denkleminin hiç bir tamsayı çözümü yoktur ve $X^2-DY^2=1$ denkleminin bütün pozitif çözümleri $n=1,2,3,\ldots$ için,

$$x=p_{nr-1} \qquad y=q_{nr-1}$$

eşitlikleriyle verilir.

ii) r tek ise, $X^2-DY^2=-1$ denkleminin bütün pozitif tamsayı çözümleri $n=1,3,5,\ldots$ olmak üzere ,

$$x=p_{nr-1} \quad , \quad y=q_{nr-1}$$

ile, $X^2-DY^2=1$ deklemininin bütün pozitif çözümleri $n=2,4,\ldots$ olmak üzere ,

$$x=p_{nr-1} \quad , \quad y=q_{nr-1}$$

eşitlikleriyle verilir [1].

TEOREM 2.2.9. D tamkare olmayan bir doğal sayı olmak üzere

$$X^2-DY^2=1$$

denklemin sonsuz sayıda $x+y\sqrt{D}$ çözümü vardır. Bu çözümler $x_1+y_1\sqrt{D}$ verilen Pell denkleminin temel çözümü olmak üzere

$$x_n+y_n\sqrt{D}=(x_1+y_1\sqrt{D})^n \qquad (2.2.13)$$

eşitliğiyle elde edilir. Burada $x_1+y_1\sqrt{D}$ çözümünün n. kuvveti ni almak sûretiyle $x_n$ve y_n ,

$$x_n=x_1^n+\sum_{k=1}\binom{n}{2k}x_1^{n-2k}y_1^{2k}D^k$$
$$\qquad (2.2.14)$$
$$y_n=\sum_{k=1}\binom{n}{2k-1}x_1^{n-2k+1}y_1^{2k-1}D^{k-1}$$

formülüyle elde edilir [6].

İspat. (2.2.13) eşitliğinden $x_n-y_n\sqrt{D} = (x_1-y_1\sqrt{D})^n$ olduğu açıktır. Bu durumda bu denklem ile (2.2.13) denklemi taraf tafafa çarpılınca

$$x_n^2-Dy_n^2=(x_1-y_1\sqrt{D})^n(x_1+y_1\sqrt{D})^n$$
$$=(x_1^2-y_1^2D)$$
$$=1$$

elde edilir. Bu ise $x_n+y_n\sqrt{D}$ nin (2.2.9) denkleminin bir çözümü olduğunu verir. Kabul edelim ki u,v pozitif tamsayıları için $u+v\sqrt{D}$ çözümü (2.2.12) formülüyle elde edilemesin. Bu takdirde ,

$$(x_1+y_1\sqrt{D})^n < u+v\sqrt{D} < (x_1+y_1\sqrt{D})^{n+1}$$

şartını sağlayan bir n doğal sayısı mevcuttur. Buradan,

$$x_n+y_n\sqrt{D} < u+v\sqrt{D} < (x_1+y_1\sqrt{D})(x_n+y_n\sqrt{D})$$

elde edilir. Bu eşitsizlik $x_n-y_n\sqrt{D}$ pozitif tamsayısı ile çarpıldığında

$$(x_n+y_n\sqrt{D})(x_n-y_n\sqrt{D})<(u+v\sqrt{D})(x_n-y_n\sqrt{D})<(x_1+y_1\sqrt{D})(x_n+y_n\sqrt{D})(x_n-y_n\sqrt{D})$$
$$= x_n^2-Dy_n^2 < (u+v\sqrt{D})(x_n-y_n\sqrt{D}) < (x_1+y_1\sqrt{D})(x_n^2-y_n^2D)$$
$$= 1 < (u+v\sqrt{D})(x_n-y_n\sqrt{D}) < (x_1+y_1\sqrt{D}) \qquad (2.2.15)$$

elde edilir. Eğer

$$(u+v\sqrt{D})(x_n-y_n\sqrt{D})=x+y\sqrt{D}$$

dersek

$$ux_n-Dvy_n+(vx_n-uy_n)\sqrt{D}$$

olur. Buradan ,

$$x=ux_n-Dvy_n \quad , \quad y=vx_n-uy_n$$

ve

$$(u-v\sqrt{D})(x_n+y_n\sqrt{D}) = x-y\sqrt{D}$$

olur. Bu iki eşitlikten

$$(u^2-Dv^2)(x_n^2-Dy_n^2)=x^2-Dy^2=1$$

elde edilir. Bu ise $x+y\sqrt{D}$ sayısının (2.2.9) denkleminin bir çözümü olduğunu gösterir. (2.2.15) den

$$x+y\sqrt{D} > 1 \quad , \quad 0 < x-y\sqrt{D} = \frac{1}{x+y\sqrt{D}} < 1$$

dir. Bu üç eşitlikten x ve y nin pozitif tamsayılar olmaları gerektiği söylenebilir ve (2.2.15) den dolayı

$$x+y\sqrt{D} < x_1+y_1\sqrt{D}$$

elde edilir ki bu ise $x_1+y_1\sqrt{D}$ sayısının (2.2.9) denkleminin temel çözümü olmasıyla çelişir. Ohalde (2.2.9) denkleminin bütün çözümleri (2.2.13) formülüyle elde edilir.

TEOREM 2.2.10. D tamkare olmayan bir doğal sayı olsun. Kabul-edelim ki

$$\xi^2-D\eta^2=-1 \qquad (2.2.16)$$

denklemi çözülebilir ve $\xi_1+\eta_1\sqrt{D}$ sayısı bu denklemin temel çözümü olsun. Bu takdirde

$$x_1+y_1\sqrt{D} = (\xi_1+\eta_1\sqrt{D})^2= \xi_1^2+D\eta_1^2+2\xi_1\eta_1\sqrt{D}$$

sayısı (2.2.9) denkleminin bir temel çözümüdür. Üstelik

$$\xi_n= \xi_1^n+\sum_{k=1}\binom{n}{2n}\xi_1^{n-2k}\eta_1^{2k}D^k$$

$$\eta_n = \sum_{k=1} \binom{n}{2k-1} \xi_1^{n-2k+1} \eta_1^{2k-1} D^{k-1}$$

olmak üzere $\xi_n + \eta_n\sqrt{D} = (\xi_1 + \eta_1\sqrt{D})^n$ yazarak bu formül bize

i) n, bütün pozitif tek tamsayıları alırken (2.2.16) denkleminin bütün ξ ve η çözümlerini,

ii) n bütün çift tamsayı değerlerini alırken (2.2.9) denkleminin bütün $x=\xi_n$, $y=\eta_n$ pozitif çözümlerini ,

verir [6].

TEOREM 2.2.11. $p=4k+1$, $k\in\mathbb{Z}$ şartını sağlayan bir asal ise

$$\xi^2 - p\eta^2 = -1$$

denkleminin ξ ve η tamsayı çözümleri vardır.

İspat. $x_1 + y_1\sqrt{p}$, $x^2 - Dy^2 = 1$ denkleminin temel çözümü olsun. Bu durumda

$$x_1^2 - 1 = py_1^2 \qquad (2.2.17)$$

elde edlir. Buradan x_1 çift olamaz. Eğer çift olsaydı

$$-1 \equiv p \pmod 4$$

olurdu ki bu $p\equiv 1 \pmod 4$ olmasıyla çelişirdi. x_1 tek ise bu takdirde $(x_1-1, x_1+1)=2$ dir. Bu yüzden (2.2.17) den ξ ve η doğal sayılar ve $y_1 = 2\xi\eta$ olmak üzere ,

$$x_1 \pm 1 = 2\xi^2 \quad , \quad x_1 \mp 1 = 2p\eta^2$$

elde edilir. Bu son eşitlikten

$$\pm 1 = \xi^2 - p\eta^2$$

elde edilir. $\eta < y_1$ olduğundan $+1 = \xi^2 - p\eta^2$ denklemini almayacağız. Böylece $-1 = \xi^2 - p\eta^2$ olur ki bu ise ispatı tamamlar.

$U^2 - DV^2 = N$ DIOPHANTINE DENKLEMLERI

D tamkare olmayan bir doğal sayı ve $C\neq 0$ bir tamsayı olmak üzere

$$U^2 - DV^2 = C \qquad (2.2.18)$$

diophantine denklemini gözönüne alalım. Kabul edelim ki bu denklem çözülebilir ve $u+v\sqrt{D}$ bunun bir çözümü olsun.

$X^2-DY^2=1$ denkleminin herhangi bir çözümü $x+y\sqrt{D}$ ise

$$(u+v\sqrt{D})(x+y\sqrt{D})=ux+Dvy+(uy+vx)\sqrt{D}$$

de (2.2.18) in bir çözümüdür. Bu çözüme $u+v\sqrt{D}$ ile bileşik çözüm adı verilir. Birbirine bileşik olan bu çözümler cümlesi (2.2.18) denkleminin çözümler sınıfını oluştururlar ve her sınıf sonsuz sayıda çözüm ihtiva eder.

Verilen iki $u+v\sqrt{D}$ ve $u'+v'\sqrt{D}$ çözümlerinin aynı sınıfa ait olup olmadığını tesbit etmek mümkündür. Gerçekten bu iki çözümün bileşik çözüm olması için gerek ve yeter şart,

$$\frac{uu'-Dvv'}{C} \quad \text{ve} \quad \frac{vu'-uv'}{C}$$

sayılarının tamsayı olmasıdır.

K , $u_i+v_i\sqrt{D}$, $i=1,2,...$ çözümlerini kapsayan bir sınıf ise $u_i-v_i\sqrt{D}$, $i=1,2,...$ çözümlerinin de $\bar{K}$ ile gösterilen bir sınıf oluşturduklarını söylemek mümkündür. K ve $\bar{K}$ sınıfları biri diğerinin konjüge sınıfıdır. Konjüge sınıflar genellikle biri diğerinden farklı sınıflardır. Fakat bazı zaman çakışırlar. Bu durumda bulunan sınıflara belirsiz sınıf adı verilir.

Verilen bir K sınıfının $u+v\sqrt{D}$ çözümleri arasından bir $u'+v'\sqrt{D}$ çözümünü şöyle seçmek mümkündür. v', v nin K sınıfındaki en küçük pozitif değeri olsun. Eğer K sınıfı belirsiz sınıf değilse $-u'+v'\sqrt{D}$ çözümleri K nın konjüge sınıfına ait olacak şekilde yalnız bir tane u' sayısı vardır.

K belirsiz sınıf ise $u'\geq 0$ kabul ederek yalnız bir tane u' bulunur. $u'+v'\sqrt{D}$ şeklinde tanımlanan çözüme K sınıfının temel çözümü denir.

Temel çözümde $|u'|$ sayısı , $|u|$ için mümkün olan en küçük değeri alırken $u+v\sqrt{D}$, K sınıfına ait olur. $u'=0$ durumuna sadece belirsiz sınıflarda raslanır.

Şimdi $U^2-DV^2=C$ denkleminde C sayısını pozitif ,yani C=N olduğunu kabul edelim. Bu durumda aşağıdaki teoremi ifade edelim.

TEOREM 2.2.12. $u+v\sqrt{D}$, $U^2-DV^2=N$ denkleminin bir K sınıfının temel çözümü ve $x_1+y_1\sqrt{D}$ de $X^2-DY^2=1$ denkleminin temel çözümü ise bu takdirde ,

$$0 \le v \le \frac{y_1}{\sqrt{2(x_1+1)}}\sqrt{N} \qquad (2.2.19)$$

$$0 < |u| \le \frac{\sqrt{(x_1+1)N}}{\sqrt{2}} \qquad (2.2.20)$$

eşitsizlikleri vardır.

İspat. (2.2.19) ve (2.2.20) eşitsizlikleri bir K sınıfı için doğru ise onun konjigesi olan bir $\bar{K}$ için de doğrudur. Böylece u nun pozitif olduğunu kabul edebiliriz. Ohalde açıkca görülür ki :

$$ux_1-Dvy_1=ux_1-\sqrt{(u^2-N)(x_1^2-1)} > 0 \qquad (2.2.21)$$

dir. Şimdi

$$(u+v\sqrt{D})(x_1-y_1\sqrt{D})=ux_1-Dvy_1+(vx_1-uy_1)\sqrt{D}$$

çözümlerini gözönüne alalım. Bu çözüm $u+v\sqrt{D}$ çözümüyle aynı sınıftandır. $u+v\sqrt{D}$, K sınıfının temel çözümü ve

$$ux_1-Dvy_1>0$$

olduğundan ,

$$ux_1-Dvy_1 \ge u \quad ,$$

$$u(x_1-1) \ge Dvy_1$$

$$u^2(x_1-1)^2 \ge D^2v^2y_1^2=(u^2-N)(x_1^2-1)$$

veya

$$\frac{x_1-1}{x_1+1} \ge 1-\frac{N}{u^2}$$

$$\frac{N}{u^2} \ge 1-\frac{x_1-1}{x_1+1} = \frac{2}{x_1+1}$$

$$u \le \frac{\sqrt{(x_1+1)N}}{\sqrt{2}}$$

elde edilir ki bu (2.2.20) eşitsizliğinin ispatını tamamlar. Bu eşitsizliğin doğru olması (2.2.19) eşitsizliğinin doğru olmasıdır. Bu da teoremin ispatını tamalar.

$U^2-DV^2=C$ denkleminde C yi negatif yani $C=-N$ alalım. Bu takdirde aşağıdaki teoremi ifade ve ispat edelim.

TEOREM 2.2.13. $u+v\sqrt{D}$, $U^2-DV^2=-N$ denkleminin bir K sınıfının temel çözümü ve $X^2-DY^2=1$ denkleminin temel çözümü de $x_1+y_1\sqrt{D}$ ise, bu takdirde,

$$0<v \le \frac{y_1\sqrt{N}}{\sqrt{2(x_1-1)}} \tag{2.2.22}$$

$$0\le |u| \le \frac{\sqrt{(x_1-1)N}}{\sqrt{2}} \tag{2.2.23}$$

eşitsizlikleri vardır.

İspat. (2.2.22) ve (2.2.23) eşitsizlikleri bir K sınıfı için doğru ise onun konjige sınıfı olan $\bar{K}$ için de doğru olacağından $u\ge 0$ alınabilir. $x_1+y_1\sqrt{D}$ verilen Pell denkleminin bir çözümü olduğundan denklemi sağlar. Yani, $x_1^2-Dy_1^2=1$ dir. Benzer olarak $u+v\sqrt{D}$ de $U^2-DV^2=-N$ denklemini sağlar. Ohalde bu iki denklemden

$$x_1^2=Dy_1^2+1 \qquad \text{ve} \qquad v^2=\frac{u^2+N}{D}$$

elde edilir. Bunlardan ,

$$(x_1v)^2=(y_1^2+\frac{1}{D})(u^2+N) > y_1^2u^2$$

veya

$$x_1v-y_1u > 0$$

olduğu görülür. Şimdi $u+v\sqrt{D}$ çözümüyle aynı sınıftan olan

$$(u+v\sqrt{D})(x_1-y_1\sqrt{D}) = ux_1-Dvy_1+(vx_1-uy_1)\sqrt{D}$$

çözümlerini gözönüne alalım. $u+v\sqrt{D}$ K sınıfının temel çözümü ve

$$x_1v-y_1u > 0$$

olduğundan

$$x_1v-y_1u \ge v$$

olmalıdır. Buradan

$$v(x_1-1) \ge y_1u$$

$$Dv^2(x_1-1)^2 \ge Dy_1^2u^2$$

$$u^2+N(x_1^2-1)^2 \ge (x_1^2-1)u^2$$

$$1+\frac{N}{u^2} \geq \frac{x_1+1}{x_1-1}$$

$$u^2 \leq \frac{N(x_1-1)}{2}$$

elde edilir ki bu (2.2.23) eşitsizliğinin varlığını gösterir. Burada u^2 yerine v cinsinden değeri yazılınca (2.2.22) eşitsizliğinin varlığı gösterilmiş olur. Bu da teoremin ispatını tamamlar.

TEOREM 2.2.14. D tamkare olmayan bir doğal sayı ve N bir doğal sayı olsun. Bu takdirde ,

$$U^2-DV^2=N \quad , \quad U^2-DV^2=-N$$

diophantine denklemlerinin sonlu sayıda çözüm sınıfı vardır. Bütün sınıfların temel çözümleri Teorem 2.2.12 ve Teorem 2.2.13 deki eşitsizlikler kullanılarak sonlu sayıda denemelerle elde edilir. $u'+v'\sqrt{D}$, K sınıfının bir temel çözümü ise K sınıfının bütün $u+v\sqrt{D}$ çözümleri

$$u+v\sqrt{D} = (u'+v'\sqrt{D})(x+y\sqrt{D})$$

formülüyle elde edilir. Burada $x+y\sqrt{D}$, $X^2-DY^2= 1$ denkleminin ∓ 1 dahil bütün çözüm değerlerini alır.
Eğer $U^2-DV^2=N$ denkleminin (2.2.19) ve (2.2.20) eşitsizliklerini sağlayan çözümü yoksa hiç bir çözümü yoktur. Benzer olarak $U -DV =-N$ denkleminin , (2.2.22) ve (2.2.23) eşitsizlik lerini sağlayan çözümü yoksa hiç bir çözümü yoktur [6].
Buraya kadar $X^2-DY^2=1$ ve $U^2-DV^2=N$ denklemlerini inceledik. Şimdi verilen bu denklemlerin herhangi bir çözümünü bulmak için veya bu çalışmada değinmediğimiz Pell denklem sistemlerinin ortak çözümünün incelenmesinde kolaylık sağlayan indirgeme bağıntıları üzerinde duralım.

PELL DENKLEMLERI İÇİN İNDİRGEME BAĞINTILARI

$x_r+y_r\sqrt{D}$ verilen Pell denkleminin çözümü olmak üzere aşağıdaki indirgeme bağıntıları mevcuttur.

i) $x_{r+s}= x_r x_s+Dy_r y_s$

ii) $y_{r+s}= x_r y_s + y_r x_s$

iii) $x_{2r}= 2x_r^2 -1$

iv) $y_{2r}= 2x_r y_r$

v) $x_{3r}=x_r(4x_r^2 -3)$

vi) $y_{3r}= y_r(4x_r^2 -1)$ [11].

İspat. i),ii). $x_1+y_1\sqrt{D}$ (2.2.9)denkleminin temel çözümü olmak üzere,Teorem 2.2.8. den

$$x_1+y_1\sqrt{D} = (x_1+y_1\sqrt{D})^r \quad , \quad r \in \mathbb{N}$$

yazılabilir. Bu yüzden

$$(x_{r+s}+\sqrt{D}y_{r+s})=(x_1+y_1\sqrt{D})^{r+s}$$
$$=(x_1+y_1\sqrt{D})^r(x_1+y_1\sqrt{D})^s$$
$$=(x_r+y_r\sqrt{D})(x_s+y_s\sqrt{D})$$
$$=x_r x_s+Dy_r y_s+(x_r y_s+y_r x_s)\sqrt{D}$$

elde edilir. Buradan

$$x_{r+s}=x_r x_s+Dy_r y_s$$
$$y_{r+s}=x_r y_s+y_r x_s$$

elde edilir,ki bu da göstermek istediğimizdir.

iii), iv). $x_{2r}+\sqrt{D}y_{2r}= (x_1+y_1\sqrt{D})^{2r}= (x_r+y_r\sqrt{D})^2$

$$= x_r^2+Dy_r^2+2x_r y_r\sqrt{D}$$
$$= 2x_r^2-1+2x_r y_r\sqrt{D}$$

elde edilir. Buradan

$$x_{2r}= 2x_r^2-1 \quad \text{ve} \quad y_{2r}= 2x_r y_r$$

bulunur. Diğer eşitsizlikler de benzer olarak gösterilir.

$U^2-DV^2=N$ DENKLEMLERİ İÇİN İNDİRGEME BAĞINTILARI

$U^2-DV^2=N$ denkleminin bir K sınıfının temel çözümü $u+v\sqrt{D}$ olsun. K sınıfının bütün çözümleri, $x_1+y_1\sqrt{D}$, $X^2-DY^2=1$ denkleminin çözümü olmak üzere Teorem 2.2.14 den

$$u_r+v_r\sqrt{D}= (u+v\sqrt{D})(x_1+y_1\sqrt{D})^r \quad , \quad r=0,1,2,...$$

yazılır. Bu takdirde $U^2-DV^2=N$ denklemi için aşağıdaki indirgeme bağıntıları mevcuttur.

i) $u_r= ux_r+Dvy_r$

ii) $v_r= vx_r+uy_r$

iii) $u_{-r}= ux_r-Dvy_r$

iv) $v_{-r}= vx_r-uy_r$

v) $u_{r+s}= x_s u_r+Dy_s v_r$

vi) $v_{r+s}= y_s u_r+x_s v_r$

vii) $u_{r+2s}= -u_r+2x_s^2 u_r+2Dx_s y_s v_r$

viii) $u_{r+2s}= u_r+2Dy_s^2 u_r+2 Dx_s y_s v_r$

ix) $v_{r+2s}=2x_s y_s u_r+2x_s^2 v_r-v_r$

x) $v_{r+2s}=2x_s y_s u_r+2Dy_s v_r+v_r$ [11].

İspat. i),ii). $(u_r+v_r\sqrt{D}) = (u+v\sqrt{D})(x_1+y_1\sqrt{D})^r$

$$= (u+v\sqrt{D})(x_r+y_r\sqrt{D})$$

$$= ux_r+Dvy_r+(uy_r+vx_r)\sqrt{D}$$

elde edilir ki,bu

$$u = ux_r+Dvy_r \quad \text{ve} \quad v = uy_r+vx_r$$

olmasını gerektirir.

iii),iv). $u_{-r}+v_{-r}\sqrt{D}= (u+v\sqrt{D})(x_1+y_1\sqrt{D})^{-r}$

$$= (u+v\sqrt{D})(x_r+y_r\sqrt{D})^{-1}$$

$$= (u+v\sqrt{D})(x_r-y_r\sqrt{D})$$

$$= ux_r-Dvy_r+(vx_r-uy_r)\sqrt{D}$$

olur. Bunun anlamı,

$$u_{-r}=ux_r-Dvy_r \quad \text{ve} \quad v_{-r}=vx_r-uy_r$$

olmasıdır.

Diğer ifadeler de benzer olarak gösterilebilir.

Şimdi verilen bir sabit katsayılı genel konik denklemlerini inceleyelim. Bunun için önce aşağıdaki tanımı verelim.

TANIM 2.2.3 (Latis noktası). Düzlemde bileşenleri tamsayılar olan noktalara Latis noktası adı verilir.

Tamkatsayılı

$$f(x,y)= Ax^2+Bxy+Cy^2+Dx+Ey+F =0 \qquad (2.2.24)$$

konik denklemini ele alalım. Eğer (2.2.24) denklemi bir parabolü temsil ediyorsa , a,b,c,d,e sayıları birer tamsayı ve Δ = ad−bc $\neq$ 0 olmak üzere (2.2.24) denklemi

$$(ax+by)^2+cx+dy+e = 0 \qquad (2.2.25)$$

şeklinde yazılabilir. Buradan ,

$$x = \frac{1}{\Delta}(bu^2+du+be) \qquad (2.2.26)$$

$$y = -\frac{1}{\Delta}(au^2+cu+ae) \qquad (2.2.27)$$

eşitliklerini elde ederiz. Böylece şu sonuç ortaya çıkar. (2.2.25) parabolü üzerinde latis noktası olabilmesi için gerek ve yeter şart,

$$au^2+cu+ae\equiv 0(\mathrm{mod}\ |\Delta|) \qquad (2.2.28)$$

$$bu^2+du+be\equiv 0(\mathrm{mod}\ |\Delta|) \qquad (2.2.29)$$

kongrüanslarının her ikisi de u nun aynı değeri için sağlanmasıdır. Bu kongrüanslar bir u_1 tamsayısı için sağlanıyorsa bu takdirde (2.2.26) ve (2.2.27) eşitliklerinde , t herhangi bir tamsayı olmak üzere $u = u_1+\Delta t$ değeri yerine yazılarak x ve y değerleri bulunur. Böylece (2.2.25) parabolü üzerindeki tüm latis noktalarını bulmak için $t= 0,\mp1,\mp2,\ldots,\mp r$ şeklinde sonlu değerler vererek

$$x = g_i(t) \quad y = h_i(t) \quad i=1,2,\ldots,r$$

formüllerini kullanmak yeterlidir. Burada $g_i(t)$ ve $h_i(t)$ polinomları birinci veya ikinci derecedendir. ve bunlardan en az biri ikinci derecedendir. r sayısı da (2.2.28) ve(2.2.29) kongrüanslarının oluşturduğu sistemin (mod $|\Delta|$) ya göre birbirine kongrüent olmayan çözümlerinin sayısıdır. Böylece bir parabol üzerinde ya hiç latis noktası yoktur. Ya da sonsuz sayıda latis noktası vardır.

ÖRNEK 1. $2x^2-3y-1=0$ parabolü üzerinde ,

$$2x^2-1\equiv 0 \pmod 3$$

kongrüansının çözümü olmadığından hiç bir latis noktası yoktur.

ÖRNEK 2. $x^2-2xy+y^2-x-2y=0$ parabolü üzerindeki latis noktalarını inceleyelim. Bu parabol

$$(x-y)^2-x-2y=0$$

şeklinde yazılabilir ve

$$u^2-u \equiv 0 \pmod 3$$

kongrüansının çözümleri $u_1=3t$ veya $u_2=3t+1$ $t \in \mathbb{Z}$ olur.Yine

$$-u^2-2u \equiv 0 \pmod 3$$

kongrüansının çözümleri $u_1=3t$ veya $u_2=3t+1$ $t\in\mathbb{Z}$ olur ki u_1 ve u_2,her iki kongrüansı sağlar. Buradan

$$x = 3t^2+2t \quad , \quad y = 3t^2-t \qquad t\in\mathbb{Z}$$

ve

$$x = 3t^2+4t+1 \quad , \quad y = 3t^2+t \quad t\in\mathbb{Z}$$

bulunur.

Eğer verilen konik denklemi elips veya daire ise bu durumda her iki konik üzerinde sonlu sayıda latis noktaları vardır öyle ki bunlar deneme yoluyla bulunur.

Şimdi hiperbolü ele alalım. Problem verilen bir hiperbolün her hangi bir latis noktasından geçip geçmediğidir. Diğer problemde latis noktalarından geçtiğini bildiğimiz bir hiperbolün bütün latis noktalarını bulmak için bir metot vermektir.

D ve N doğal sayılar olmak üzere tamkatsayılı lineer dönüşümler yardımıyle bir hiperbol denklemi

$$U^2-DV^2=N \qquad (2.2.30)$$

şeklinde bir denkleme dönüştürülebilir. Böylece problemimiz (2.2.30) denkleminin

$$u \equiv \mu \pmod{\delta} \quad , \quad v \equiv \nu \pmod{\delta} \qquad (2.2.31)$$

kongrüanslarını sağlayan u ve v tamsayılı çözümleri bulma problemine indirgenmiş olur. Burada μ , ν ve δ tamsayıları (2.2.24) denkleminin katsayıları cinsinden ifade edilen katsayılardır. Eğer D sayısı karesel bir sayı ise (2.2.30) denkleminin sonlu sayıda çözümü vardır. D karesel bir sayı değilse bu durumda (2.2.30) denkleminin ya hiç çözümü yoktur ya da sonsuz sayıda çözümü vardır. Eğer (2.2.30) çözülebilir ise çözümlerinin hepsi Teorem 2.2.14 de verilen temel çözümler yardımıyle bulunur. Sonuçta bulunan bu çözümlerden hangilerinin (2.2.31) kongrüanslarını sağladığını bulmak kolaydır.

Örneğin, $5x^2-14xy+7y^2=-1$ hiperbol denklemini alalım.

$$u=5x-7y \quad \text{ve} \quad v=y$$

yazarsak,

$$u^2-14v^2=-5 \tag{2.2.32}$$

şekline dönüşür. Buradaki u ve v çözümleri

$$u\equiv 5x-7y\equiv -2v \pmod 5 \tag{2.2.33}$$

kongrüansını sağlamalıdır. (2.2.32) denkleminin temel çözümü $\pm 3+\sqrt{14}$ dür ve onun bütün çözümleri

$$u+v\sqrt{14}=\pm(3+\sqrt{14})(15+4\sqrt{14})^n,\ n\in\mathbb{N} \tag{2.2.34}$$

ve

$$u+v\sqrt{14}=\pm(-3+\sqrt{14})(15+4\sqrt{14})^n,\ n\in\mathbb{N} \tag{2.2.35}$$

dir. Eğer $n=2m$ ise (2.2.34) den ,

$$u\equiv(-1)^m 3 \pmod 5 \quad , \quad v\equiv(-1)^m \pmod 5$$

ve (2.2.35) den ,

$$u\equiv(-1)^m 2 \pmod 5 \quad , \quad v\equiv(-1)^m \pmod 5$$

elde edilir. Eğer $n=2m+1$ ise (2.2.34) den ,

$$u\equiv(-1)^m \pmod 5 \quad , \quad v\equiv(-1)^m 2 \pmod 5$$

ve (2.2.35) den

$$u\equiv(-1)^m \pmod 5 \quad , \quad v\equiv(-1)^m 3 \pmod 5$$

elde edilir.

Böylece (2.2.33) kongrüansı , (2.2.34) formülünün alınmasıyla sağlandığı ,fakat (2.2.35) in alınmasıyle sağlanmadığı görülür.

Sonuç olarak $5x^2-14xy+7y^2=-1$ denkleminin çözümlerinin bütün cümlesi

$$x=\frac{1}{5}(u+7v) \quad , \quad y=v$$

bağıntısıyla elde edilir. Buradaki u ve v , (2.2.34) den belirlenir. (2,1) , (-2,-1) , (58,27) , (-58,-27) noktaları verilen denklem için birer latis noktalarıdır.

$X^2+Y^2=Z^2$ DIOPHANTINE DENKLEMI

$X^2+Y^2=Z^2$ diophantine denkleminin pozitif tamsayılardaki çözümlerini araştıracağız. Eğer $(x,y)=d$ ise bu takdirde

$$x=dx_1 \quad , \quad y=dy_1 \quad , \quad x_1,y_1\in\mathbb{Z}$$

olur ve

$$d^2x_1^2+d^2y_1^2=z^2$$

ifadesinden $d^2|z^2$ olup buradan $d|z$ elde edilir. Böylece $(x,y,z)=((x,y),z)=d$ olur. Bu ise

$$(x,y,z)=(x,y)=(x,z)=(y,z)=d$$

olup

$$\left[\frac{x}{d}\right]^2+\left[\frac{y}{d}\right]^2=\left[\frac{z}{d}\right]^2 \text{ve } \left[\frac{x}{d},\frac{y}{d}\right]=\left[\frac{y}{d},\frac{z}{d}\right]=\left[\frac{x}{d},\frac{z}{d}\right]=1$$

elde edilir. Eğer x_1,y_1 ve z_1 tamsayıları aralarında ikişer ikişer asal olan üç çözüm ise bu çözüme ilkel çözüm adı verilir. Böylece verilen denklemin her x,y ve z tamsayı çözümü x_1,y_1ve z_1 ler ilkel çözüm olmak üzere dx_1 dy_1 ve dz_1 formundadır. Bu yüzden verilen bir $x^2+y^2=z^2$ diophantine denkleminin ilkel çözümünün bulunmasına ihtiyaç vardır. Bu çözümü bulmaya çalışalım.

x ve y her ikisi birden çift olmayan tamsayılar olsun. Bu durumda x ve y tek tamsayılar ise

$$x^2\equiv1(\mathrm{mod}4) \quad \text{ve} \quad y^2\equiv1(\mathrm{mod}4)$$

olur ki, bunu sağlayan bir z tamsayısı bulmak mümkün değildir. Benzer şekilde her ikisi birden çift olursa bu takdirde (x,y,z) =1 olmasıyle çelişir. O halde y çift , x ve z tek tamsayılar olsun. Ozaman

$$\left[\frac{z+x}{2} \right] \left[\frac{z-x}{2} \right] = \left[\frac{y}{2} \right]^2 \qquad (2.2.36)$$

olur.

$$\left[\frac{z+x}{2} , \frac{z-x}{2} \right] \mid \left[\frac{z+x}{2} + \frac{z-x}{2} \right] = z$$

ve

$$\left[\frac{z+x}{2} , \frac{z-x}{2} \right] \mid \left[\frac{z+x}{2} - \frac{z-x}{2} \right] = x$$

olup

$$\left[\frac{z+x}{2} , \frac{z-x}{2} \right] = 1$$

dir.

Burada (2.2.36) denklemi ile $(z+x)/2 = r^2$ ve $(z-x)/2 = s^2$ olacak şekilde r ve s pozitif tamsayıları olsun. Bu durumda

$$(r,s)=1 \ , \quad r>s \quad , \ x=r^2-s^2, \ y=2rs \ , z=r^2+s^2$$

olduğu görülür. Üstelik z tek ise r ve s den biri tek, diğeri çifttir..

Diğer taraftan $r>s>0$, $(r,s)=1$ ve biri tek diğeri çift olacak şekilde herhangi iki tamsayı olsun. O zaman

$$x=r^2-s^2 \quad , \quad y=2rs \quad , \quad z=r^2+s^2$$

olup x , y ve z ler pozitif ve

$$x +y =(r^2-s^2) +(2rs) =r^4-2r^2s^2+s^4+4r^2s^2$$
$$=(r^2+s^2)^2 = z^2$$

olur. y çift ve x tek olduğundan $(x,y)=1$ dir. Bununla beraber y çift olduğundan x,y ve z ilkel çözümdür. Bu ifadelerin tamamından aşağıdaki sonuç elde edilir.

TEOREM 2.2.15. $x^2+y^2=z^2$ diophantine denkleminin pozitif ilkel çözümü y çift , olmak üzere

$$x = r^2-s^2 \quad , \quad y = 2rs \quad , \quad z = r^2+s^2$$

şeklindedir. Burada r ve s , biri tek diğeri çift, $r>s>0$ ve $(r,s) = 1$ olacak şekildeki keyfi tamsayılardır [1].

Bu denklemin genel hali olan, $ax^2+by^2+cz^2=0$ diophantine denklemlerinin çözümüyle ilgili olan aşağıdaki teoremleri ifade edelim.

TEOREM 2.2.16. a, b ve c sayıları abc square-free olacak şekilde üç tamsayı olsun. Bu durumda $ax^2+by^2+cz^2$ diophantine denkleminin hepsi sıfır olmayan x, y ve z tamsayılarına göre çözülebilir olması için gerek ve yeter şart, aşağıdaki şartların sağlanmasıdır.

i) $-bc$, a nın kuadratik rezidüsü,

ii) $-ac$, b nin kuadratik rezidüsü,

iii) $-ab$, c nin kuadratik rezidüsü,

iv) $ax^2+by^2+cz^2 \equiv 0 \pmod 8$ kongrüansının hepsi çift olmayan x, y ve z tamsayılarına göre çözülebilir olmasıdır [6].

TEOREM 2.2.17. a, b ve c sayıları abc square-free olacak şekilde üç tamsayı olsun. Bu durumda $ax^2+by^2+cz^2=0$ diophantine denkleminin çözülebilir olması için gerek ve yeter şart ,

$$ax^2+by^2+cz^2 \equiv 0 \pmod N$$

kongrüansının $(x,y,z,N) = 1$ olmak üzere x, y ve z tamsayılarına göre her N tam modülü için çözülebilir olmasıdır [6].

2.3 ÜÇÜNCÜ VE DÖRDÜNCÜ DERECEDEN BAZI DİOPHANTİNE DENKLEMLERİ

$X^3+Y^3 = Z^3$ DİOPHANTİNE DENKLEMLERİ

LEMMA 2.3.1. $x\ +3y\ = z$ denkleminin bütün çözümleri

$$x+y\sqrt{-3}=\pm(p+q\sqrt{-3})^n \quad , \quad z=p^2+3q^2$$

formülüyle verilir. Burada $(x,y) = 1$, z pozitif tek tamsayı ve p, q lar $(p,3q)=1$ olacak şekildeki biri tek diğeri çift tamsayılardır [5].

örneğin , $n=2$ için $p=1$ ve $q=2$ alındığında $x+y\sqrt{-3}=\pm(1+2\sqrt{-3})^2$
$x=-11$, $y=4$ ve $z=13$ bulunur.
$n=3$ için $p=2$ $q=3$ alındığında $x=-154$, $y=-45$, $z=31$ bulunur.
x_1, y_1 ve z_1 tamsayıları , z_1 en küçük pozitif tamsayı olacak şekilde

$$x^3+y^3=z^3 \qquad (2.3.1)$$

denkleminin sıfırdan farklı çözümleri olsun. $(x_1,y_1)=1$ kabul edersek $(x_1,y_1)=(x_1,z_1)=(y_1,z_1)=1$ olur. Bu sayıların ikisi tek olmalıdır. x_1 ve y_1 in tek olduğunu kabul edelim. x_1 ve z_1 tek olsaydı (2.3.1) denklemi

$$x^3+(-z)^3=(-y)^3$$

formunda yazılabilirdi ki bu (2.3.1) denklemi ile aynıdır. Şimdi p ve q lar aralarında asal ve biri tek diğeri çift sayılar olmak üzere,

$$x_1=p+q \quad , \quad y_1=p-q$$

alalım. Böylece x ve y tek olur. Bunlar (2.3.1) de yerine yazılınca ,

$$2p(p^2+3q^2)=z^3 \qquad (2.3.2)$$

elde edilir. p nin sıfırdan farklı olduğu açıktır. Şimdi z nin 3 ile bölünebildiğini veya bölünemediğini inceleyelim. İlk olarak z , 3 ile bölünemesin. Böylece $(2p,p^2+3q^2)=1$ olduğundan

$$p=4\alpha^3 \quad , \quad p^2+3q^2=\beta^3 \quad , \quad z=2\alpha\beta$$

olmalıdır. $(p,q)=1$ olduğundan Lemma 2.3.1 den $p^2+3q^2=\beta^3$ denkleminin

$$p+q\sqrt{-3} = (r+s\sqrt{-3})^3$$

şeklinde çözümü vardır. Buradan

$$p=r(r^2-9s^2) \quad , \quad q=3s(r^2-s^2)$$

olur. Fakat $p=4\alpha^3$ olduğundan

$$r(r^2-9s^2)=r(r+3s)(r-3s)=4\alpha^3$$

olmalıdır. r ve s $(r,3s)=1$ ve biri tek diğeri çift ve $r,r+3s$, $r-3s$ aralarında asal olmaları nedeniyle

$$r+3s=k^3 \quad , \quad r-3s=t^3 \quad , \quad r=\frac{m^3}{2}$$

olmalıdır. Bu ifadelerden

$$k^3+t^3=m^3$$

elde edilir. k,t ve m nin sıfırdan farklı oldukları açıktır. Şimdi

$$|m|<|z|$$

olduğunu gösterelim.

$$z=ktm\beta \quad , \quad \beta=r^2+3s^2>16$$

olduğundan ,

$$|m|<|\frac{z}{16}|<|z|$$

olduğu görülür.

Kabul edlim ki z , 3 ile bölünsün.O zaman (2.3.2) den dolayı p , 3 ile bölünebilir ve her iki taraf 9 ile kısaltılınca

$$\frac{2p}{3}(q^2+3(\frac{p}{3})^2) = 3(\frac{z}{3})^3$$

olur. Burada soldaki çarpanlar aralarında asal olduğundan

$$p=36\alpha^3 \quad , \quad q^2+3(\frac{p}{3})^2=\beta^3 \quad , \quad z=6\alpha\beta$$

dir. Tekrar Lemma 2.3.1 den

$$q+\frac{p}{3}\sqrt{-3} = (r+s\sqrt{-3})^3$$

çözümünden

$$p=9s(r^2-s^2)=36\alpha^3 \quad \text{veya} \quad p=s(r^2-s^2)=4\alpha^3$$

yazılır. Fakat s,r+s ve r+s ifadeleri , (r,s)=1 olduğundan aralarında asaldır. Böylece

$$r+s=k^3 \; , \; r-s=-t^3 \; , \; s=\frac{m^3}{2}$$

ve

$$k^3+t^3=m^3$$

elde edilir. Burada k,t ve m sıfırdan farklı sayılardır. Bununla beraber

$$z=-3ktm\beta \quad , \quad \beta=r^2+3s^2>48$$

ve

$$|m|<|\frac{z}{144}|<|z|$$

dir.

Böylece z çift olmak üzere sıfırdan farklı x,y ve z tamsayılarının (2.3.1) çözümü olarak başlayıp, m<z olan yeni bir k,t,m çözümleri elde edildi. Fakat bu ise z nin bir en küçük çözüm olmasıyla çelişir. Böylece

$$x^3+y^3=z^3$$

denkleminin sıfırdan farklı tamsayı çözümünün olmadığını ifade eder [5].

$X^4-Y^4=Z^2$ DENKLEMİ

TEOREM 2.3.1. $$x^4-y^4=z^2 \qquad (2.3.3)$$
diophantine denkleminin x,y ve z doğal sayılarına göre hiç bir çözümü yoktur.

İspat. x,y ve z nin pozitif olduklarını kabul edelim. Eğer

$$(x,y)=d \text{ ise }, \frac{x}{d}=x_1 , \frac{y}{d}=y_1 , \frac{z}{d^2}=z_1$$

alınırsa, (2.3.3) denklemi z_1 bir t tamsayı olmak üzere

$$x_1^4-y_1^4=z_1^2$$

denklemine dönüşür. $(x_1,y_1)=1$ olduğundan $(x_1,z_1)=(y_1,z_1)=1$ dir. Böylece x,y ve z ler aralarında ikişer ikişer asal kabulederek teoremi ispatlamaya çalışalım.

y^4+z^2, 4 ile bölünemediğinden x tektir. Şimdi (2.3.3) denkleminin [x,y,z] çözümüne sahip olduğunu kabul edelim. Burada x (2.3.3)denklemini sağlayan en küçük pozitif tamsayıdır.

İlk olarak y nin çift olma durumunu gözönüne alalım. Bu takdirde x^2+z ile x^2-z nin en büyük ortak böleni 2 dir. Bu sayıların çarpımı 16 ile bölünebilirdir. Bu çarpanlardan biri 2 ve diğeri 8 ile bölünür. Bu nedenle

$$\frac{1}{2}(x^2 \pm z) \quad \text{ve} \quad \frac{1}{8}(x^2 \mp z)$$

sayıları aralarında asaldır ve bunların çarpımı dördüncü kuvvetten olduğundan kendileri de dördüncü kuvvetten olmalıdır.Bu nedenle ,

$$x^2 \pm z=2a^4 , \quad x^2 \mp z=8b^4$$

olup, burada a tek, y=2ab ,(a,b)=1 dir.
Bu son iki eşitlikten

$$x^2=a^4+4b^2$$

denklemi elde edilir. Bu denklem $(x+a^2)(x-a^2)=4b^4$ olarak yazılabilir. Soldaki iki çarpanın en büyük ortak böleni 2 olduğundan

$$x+a^2=2c^4 , \quad x-a^2=2d^4$$

olarak yazılabilir. Burada c ve d , b=cd olacak şekilde aralarında asal doğal sayılardır. Yukarıdaki eşitlikler taraf tarafa çıkartılırsa

$$a^2=c^4-d^4$$

denklemi elde edilir. y bir çift sayı olmak üzere (2.3.3) ün bir [x,y,z] çözümünden başlandığında , yeni bir [c,d,a] çözümünün olduğu sonucuna varılır. Bu çözüm

$$c<2acd=y<x$$

eşitsizliğini sağlar. Bu ise x in tanımıyla bir tezattır. O halde y çift olması durumunda (2.3.3) denkleminin bir tamsayı çözümü yoktur.

Şimdi y nin tek olduğunu kabul edelim. $(x^2-y^2,x^2+y^2)=2$ olduğundan z çifttir. Ozaman (2.3.3) den

$$x^2+y^2=2a^2 \quad , \quad x^2-y^2=2b^2$$

sonucuna varılır. Burada a ve b ler 2z=ab ve aralarında asal olacak şekildeki doğal sayılardır. Ozaman

$$x^2=a^2+b^2 \quad , \quad y^2=a^2-b^2$$

ifadeleri taraf tarafa çarpıldığında ,

$$(xy)^2=a^4-b^4$$

elde edilir. y bir tek sayı olmak üzere (2.3.3) denkleminin [x,y,z] çözümünden başlandığında , yeni bir [a,b,xy] çözümü elde edilir. Fakat

$$a<\sqrt{a^2+b^2}=x$$

olduğundan bu x ile ilgili hipotezimize tezattır. Bu da $z\neq0$ olduğunda (2.3.3) denkleminin çözülemediğini gösterir.

TEOREM 2.3.2. $$x^4+y^4=z^2 \qquad (2.3.4)$$
diophantine denklemi x,y ve z doğal sayılarına göre hiç bir çözüme sahip değildir.

İspat. x,y ve z sayılarını ikişer ikişer aralarında asal kabul edelim. Bu durumda (2.2.4) denkleminde z tek,x ve y sayılarından biri çift olmalıdır. y çift olsun. (2.3.4) denkleminin $[x,y,z]$ çözümüne sahip olduğunu ve z nin bu çözümün en küçük değeri olduğunu kabul edelim. $(z+x^2,z-x^2)=2$ olduğundan

$$(z+x^2)(z-x^2)=z^2-x^4=y^4$$

elde edilir. a tek ve b ile aralarında asal pozitif tamsayılar olmak üzere

$$z-x^2=2a^4 \quad , \quad z+x^2=8b^4 \quad , \quad y=2ab \qquad (2.3.5)$$

elde edilir. (2.3.5) ifadesinde z yi yok etmekle

$$\pm x^2=a^4-4b^4$$

elde ederiz. Burada (+) işareti seçilmelidir. Çünkü (−) işaretlisi (mod 4) ü sağlamaz. $(x+a^2,a^2-x)=2$ olduğundan yukarıdaki ifadeden

$$a^2+x=2c^4 \quad , \quad a^2-x=2d^4 \quad , \quad b=cd$$

elde edilir. Burada c ve d aralarında asal pozitif tamsayılardır. x yok edilerek

$$a^2=c^4+d^4$$

elde edilir. Böylece $[x,y,z]$ nin (2.3.4) denkleminin bir çözümü olması, yeni bir $[c,d,a]$ çözümünün varlığını gösterir. Fakat

$$z=a^4+4b^4 > a^4 \geq a^2$$

olduğundan bu z nin en küçük çözümü olmasıyla çelişir. Bu ise (2.3.4) denkleminin x,y ve z sayılarına göre çözümünün olmadığını verir.

TEOREM 2.3.3. $$x^4 - y^4 = 2z^2 \qquad (2.3.6)$$

diophantine denkleminin x,y ve z doğal sayılarına göre çözümü yoktur.

İspat. x,y ve z aralarında asal olduğunu kabul edelim. (2.3.6) denkleminde x ve y her ikisi tek ve z çift olmalıdır. $(x^2+y^2,x+y,x-y)=2$ olduğundan (2.3.6) denkleminden

$$x^2+y^2=2a^2 \quad , \quad x+y=2b^2 \quad , \quad x-y=2c^2 \qquad (2.3.7)$$

olduğu görülür. Burada a,b ve c ler aralarında asal doğal sayılar ve $z=2abc$ dir. (2.3.7) deki en son iki eşitlikten

$$x=b^2+c^2 \quad , \quad y=b^2-c^2$$

elde edilir. x ve y nin bu değerleri (2.3.7) deki ilk denklemde yerine yazıldığında ,

$$a^2=b^4+c^4$$

eşitliği bulunur.

Fakat Teorem 2.3.2 ye göre bu denklem a,b ve c doğal sayılarına göre çözülemez. Bundan (2.3.6) denkleminin $z\neq 0$ için tamsayı çözümüne sahip olmadığı sonucuna varılır.

TEOREM 2.3.4. $$x^4 - y^4 = pz^2 \qquad (2.3.8)$$

diophantine denkleminin, $p\equiv 3 \pmod 8$ şeklinde asallar olmak üzere x,y ve z doğal sayılarına göre çözümü yoktur.

İspat. ilk olarak z nin tek olduğunu kabul edelim. Bu durumda ya x ya da y çifttir. ilk durumda yani x çift y tek olduğunda

$$-1\equiv p \pmod 8$$

ikinci durumda yani, x tek y çift olduğunda

$$1\equiv p \pmod 8$$

elde edilir. Fakat $p\equiv 3 \pmod 8$ olduğundan bu imkansızdır. Bu nedenle z çifttir.

Şimdi (2.3.8) denkleminin [x,y,z] çözümüne sahip olduğunu kabül edelim. Burada x en küçük pozitif değere sahip olsun. z zorunlu olarak 4 ile bölünür. $(x-y,x+y,x^2+y^2)=2$ dir. Bu durumda

$$x\pm y=2u^2 \quad , \quad x\mp y=4pv^2 \quad , \quad x^2+y^2=2w^2 \qquad (2.3.9)$$

sistemini veya

$$x\pm y=2pu^2 \quad , \quad x\mp y=4v^2 \quad , \quad x^2+y^2=2w^2 \qquad (2.3.10)$$

sistemini elde ederiz. Burada, u,v ve w aralarında asal pozitif tamsayılar, u ve w tekdir. x ve y nin yok edilmesiyle (2.3.9) dan

$$u^4+4p^2v^4=w^2 \qquad (2.3.11)$$

ve benzer olarak (2.3.10) dan

$$p^2u^4+4v^4=w^2$$

elde edilir, bu denklemden

$$w+pu^2=2a^4 \quad , \quad w-pu^2=2b^4$$

olduğu görülür. Burada a ve b ler aralarında asal doğal sayılardır. Bu nedenle

$$pu^2=a^4-b^4$$

dir. Bu diophantine denklemi (2.3.10) ile aynı türdendir. Fakat burada u tekdir ve (2.3.10) da z nin çift olması gerektiği gösterilmişti. Öte yandan, $(w+2pv^2,w-2pv^2)=1$ olduğundan (2.3.11) denkleminden a ve b aralarında asal pozitif tamsayılar olmak üzere

$$w+2pv^2=a^4 \quad , \quad w-2pv^2=b^4$$

olduğu görülür. Bu ifadelerin taraf tarafa çıkartılmasıyla

$$a^4-b^4=p(2v)^2$$

bulunur. Böylece $[x,y,z]$ nin (2.3.10) denkleminin bir çözümü olması kabülü yeni bir $[a,b,2v]$ çözümünün varlığına götürür. Fakat

$$a \leq a^2b^2 < a^2b^2+2pv^2 = u^2+2pv^2 = x$$

olduğundan bulunan çözüm x e ilişkin hipotezle çelişkidir. Ohalde (2.3.8) denklemini sağlayan x,y ve z doğal sayıları yoktur. Bu teoremde p ye ilişkin kısıtlama gerekliydi. Halbuki $p\equiv1(\text{mod}8)$, $p\equiv5(\text{mod}8)$ ve $p\equiv7(\text{mod}8)$ asallarının her biri için (2.3.8) denkleminin çözümü mevcuttur. Mesela, (2.3.8) denklemi p=41 için [5,4,3] çözümüne, p=5 için [3,1,4] çözümüne ve p=7 için [4,3,5] çözümüne sahiptir.

TEOREM 2.3.5.(Fermat'ın son teoremi).

$$x^n + y^n = z^n \qquad (2.3.12)$$

diophantine denkleminin $n>2$ halinde pozitif tamsayılarda hiç bir çözümü yoktur [7].

Fermat'ın bu teoremi büyük bir üne sahiptir. Fermat, diophantine aritmatiğinin bashet baskısının kopyasında ispatlamadan

iddia etti ki (2.3.12) denkleminin, sıfırdan farklı tamsayılara göre çözümü yoktur.
Böylece gerçekten teoremin ilginç bir ispatını yaptığına inanıyordu. Fakat onun bu ispatı hiçbir yerde ifade edilmemiştir. Şimdiye kadar Fermat'ın son teoremi sadece n nin özel değerleri için ispatlanmıştır.
n=4 olması durumunda Fermat, gerçekten iddia ettiğini ispatladı. Teorem 2.3.11. de sadece z^2 yerine z^4 alarak yaptı. n=4 halinden başka n nin p gibi tek asal olması durumunda da bazı incelemeler yapılmıştır. Fermat'ın iddiasının p=3 için doğru olduğu sayfa 26 da gösterildi. 1928 de Legendre ve dirichlet p=5 için ispatladılar. Onların ispatları sonsuz descent metodu üzerine kuruludur.
Kummer, Fermat'ın son teoremini p=11,13 ve bazı büyük asallar için ilk olarak ispatlamayı başarmıştır [6].

2.4 $Q(\sqrt{m})$ DE BAZI DİOPHANTİNE DENKLEMLERİ

$Q(\sqrt{5})$ de $ax + by = c$ DİOPHANTİNE DENKLEMLERİ

ax+by=c dekleminin a,b,c ler tamsayı olmak üzere, tamsayılarda çözümleri kesim 2.1 de incelendi. Buna paralel olarak $Q(\sqrt{5})$ de ax+by=c denklemlerin çözümlerini inceliyeceğiz.

$s,t\in\mathbb{Z}$ ve $\lambda=\dfrac{1+\sqrt{5}}{2}$ olmak üzere Kesim 1.6 da $Q(\sqrt{5})$ cisminin tamsayılarnın $s+t\lambda$ formunda olduğunu gördük. Kesim 2.1 deki çözüm metoduna benzer olarak reel sayılardaki sürekli kesir açılımına benzer sürekli kesir açılımına ihtiyacımız vardır. $Q(\sqrt{5})$ cisminin elemanları tek türlü bir sonlu sürekli kesirle temsil edilir. Böyle bir sürekli kesir mevcut ise bu sürekli kesir λ_5-kesri olarak bilinir.
Rosen [10] her sonlu λ_q kesrinin $Q(\lambda_q)$ sayı cisminin bir elemanı olduğunu ve Leutbecha [9] de q=5 için $Q(\sqrt{5})$ cismindeki her elemanı sonlu bir λ_5 kesrine sahip olduğunu göstermiştir. Dolayısıyla bir reel sayının $Q(\sqrt{5})$ cisminin elemanı olması için gerek ve yeter şart, bu sayının bir λ_5 sürekli kesir açılımına ve her reel sayının tek türlü $\lambda_5$kesir açılımına sahip olmasıdır.

$Q(\sqrt{5})$ cismindeki λ_q kesirleri,

$$r_0\lambda+\cfrac{\varepsilon_1}{r_1\lambda+\cfrac{\varepsilon_2}{r_2\lambda}+\ldots}$$

sürekli kesir formundadır. Burada q sabit , $\lambda=2\cos(\frac{\pi}{q})$, $q\in Z^+$, $q\geq 3$, $r_0\in Z$ ve $i\geq 1$ için $r_i\in Z^+$ dır. Bundan sonra λ_5 yerine λ kesri alınacaktır.

TEOREM 2.4.1. $p,q,r\in Z(\sqrt{5})$ olsun. Birimler hariç p,q,r lerin aralarında asal olduklarını kabul edelim. Bu durumda

$$px+qy=r$$

diophantine denklemi, $Q(\sqrt{5})$ de tamsayı çözümlerine sahiptir. Eğer x_0,y_0 bunun bir özel çözümü ise diğer herhangi bir çözümü

$$x=x_0+qt \quad , \quad y=y_0-pt$$

formunda verilir. $(p,q)=d$ ve $d|r$ ise denklemi $Q(\sqrt{5})$ de çözülebilirdir [8].

İspat. Rasyonel tam sayılarda olduğu gibi önce $px+qy=1$ denklemini çözelim. Bu p/q nun tek olarak λ kesrine açılımı ile yapılır. Sondan bir önceki yakınsayan x ve y değerlerini verir. $px+qy=r$ yi çözmek için x ve y değerleri r ile çarpılır. Eğer özel bir çözüm x_0 ,y_0 ise, bütün $t\in Z(\lambda)$ için

$$x=x_0+qt \quad , \quad y=y_0-pt$$

yazarak sonsuz tane x,y çözümleri elde edilir. Ek olarak $a,b\in Z(\sqrt{5})$ de herhangi bir çözüm ise yani $pa+qb=r$ ise $a=x_0+qt$, $b=y_0-pt$ dir bazı t ler için bu açıktır. Zira $pa+qb=r$ ve $px_0+qy_0=r$ olmasından $p(x_0-a)+q(y_0-b)=0$ dir. Böylece $p(x_0-a)=-q(y_0-b)$ olur. $(p,q)=1$ olduğundan $p|y_0-b$ olur. Böylece $pk=y_0-b$. Fakat $p(x_0-a)=-qpk$ olduğundan $x_0-a=-qk$ olur ki bu da teoremin ispatını tamamlar. Son olarak teoremin son çözümleri kolayca ilk çözümlerinden elde edilir. Çünkü p/d,q/d r/d aralarında asaldır. Şimdi bu teoremin bir uygulamasını verelim.

ÖRNEK. $(3+7\lambda)x + (5-2\lambda)y = 6+5\lambda$ (2.4.1)

denklemini çözelim. $\frac{3+7\lambda}{5-2\lambda}$, λ kesrine açıldığında ,

$$\frac{3+7\lambda}{5-2\lambda} = 5\lambda + \cfrac{1}{20\lambda - \cfrac{1}{\lambda - \cfrac{1}{3\lambda}}}$$

formunda olur. Sağ taraf hesaplandığında

$$\frac{487+788\lambda}{97\lambda+60}$$

şeklini alır. Pay $(34+55\lambda)(3+7\lambda)$ ve payda ise $(34+55\lambda)(5-2\lambda)$, $(55\lambda+34=\lambda^{10})$ dir. Sondan bir önceki yakınsayan

$$5\lambda + \cfrac{1}{20\lambda - \cfrac{1}{\lambda}} = \frac{196\lambda+100}{20\lambda+19}$$

dir. Böylece $x=(20\lambda+19)$ ve $y=-(196\lambda+100)$ olur. Bu

$$(487+788\lambda)x + (97\lambda+60)y = 1$$

denkleminin bir çözümüdür. $x'=(20\lambda+19)(5\lambda+6) = 214+315\lambda$ ve $y'= -(196\lambda+100)(5\lambda+6) = -(2656\lambda+1580)$ da $(487+788\lambda)x' + (97\lambda+60)y' = 6+5\lambda$ denkleminin bir çözümü olduğu görülür. Böylece (2.4.1) denklemini çözmek için $(34+55\lambda)$ birim çarpanı ile x ve y çarpılmalıdır. Bu durumda

$$(3+7\lambda)x'' + (5-2\lambda)y'' = 6+5\lambda$$

denkleminin çözümü

$$x'' = (214+315\lambda)\ (34+55\lambda) = 2460+39805\lambda$$

$$y'' = -(1580+2656\lambda)\ (34+55\lambda) = -(199800+3223284\lambda)$$

dir. Bir çözümü bilindiğine göre bütün çözümleri $(p,q)=1$ olmak üzere

$$x = x'' + qt \quad , \quad y = y'' - pt \ , \ t \in Z(\sqrt{5})$$

şeklinde verilir.

$X^3 + Y^3 = Z^3$ DIOPHANTINE DENKLEMI

$x^3 + y^3 = z^3$ diophantine denkleminin x, y ve z pozitif rasyonel tamsayılarına göre çözümünün olmadığını gösterdik. Şimdi $\alpha^3 + \beta^3 + \gamma^3 = 0$ denkleminin $Q(\sqrt{-3})$ kuadratik cisminde sıfırdan farklı tamsayılara göre çözülemez olduğu gösterilecek ve bu $\alpha^3 + \beta^3 = \gamma^3$ denkleminin sıfırdan farklı tamsayılara göre $Q(\sqrt{-3})$ de çözülemeyeceğinin ispatıyla aynıdır. Çünkü bu denklem

$$\alpha^3 + \beta^3 + (-\gamma^3) = 0$$

şeklinde ifade edilebilir.

Bu inceleme boyunca, w ile $\frac{(-1+\sqrt{-3})}{2}$ yi göstereceğiz ve bu w, $w^3 = 1$, $w^2+w+1 = 0$ denklemini sağlar. Böylece Teorem 1.6.12 den $Q(\sqrt{-3})$ kuadratik cisminin birimleri ∓ 1, $\mp w$, $\mp w^2$ dir ve bu cismin herhangi bir asalı $\sqrt{-3}$ dür. Bundan böyle asalı θ ile göstereceğiz.

θ , birimlerin altısı ile de çarpılınca, elde edilen

$$\pm (1-w) \ , \ \pm (1-w \ ) \ , \ \pm (w-w^2) = \pm \theta = \pm\sqrt{-3} \qquad (2.3.1)$$

sayıların hepsi θ nın ilgilileridir. $\alpha^3+\beta^3+\gamma^3=o$ denkleminin çözülemeyeceğini göstermeden önce aşağıdaki lemmaları ifade edelim.

LEMMA 2.4.1. $Q(\sqrt{-3})$ kuadratik cisminin her bir tamsayısı θ modülüne göre 0,1 veya -1 den sadece birine kongrüenttir.

İspat. a ve b ler ikisi birden çift veya tek olan rasyonel tamsayılar olmak üzere $Q(\sqrt{-3})$ cisminin, $\frac{a+b\theta}{2}$ tamsayısını gözönüne alalım. O zaman $\frac{a+b\theta}{2}$ de bir tamsayıdır ve böylece

$$\frac{1}{2}\ (a+b\theta) = \frac{1}{2}\ (b+a\theta) + 2a \equiv 2a(\text{mod } p)$$

dır. Buradan 2a rasyonel tamsayısı 3 modülüne göre 0,1 veya -1 den birine denktir ve $\theta | 3$ olup bu da lemmayı ispatlar.

LEMMA 2.4.2. ξ ve η , $Q(\sqrt{-3})$ cisminin θ ile bölünemeyen tamsayıları olsun. Eğer

$$\xi\equiv 1(\text{mod } \theta) \quad \text{ise} \quad \xi^3\equiv 1(\text{mod } \theta^4)$$

$$\xi\equiv -1(\text{mod } \theta) \quad \text{ise} \quad \xi^3\equiv -1(\text{mod } \theta^4)$$

$$\xi^3+\eta^3\equiv 0(\text{mod } \theta) \quad \text{ise} \quad \xi^3+\eta^3\equiv 0(\text{mod } \theta^4)$$

ve son olarak

$$\xi^3-\eta^3\equiv 0(\text{mod } \theta) \quad \text{ise} \quad \xi^3-\eta^3\equiv 0(\text{mod } \theta^4)$$

dir.

İspat. Lemma 2.4.1 den $\xi\equiv \pm 1(\text{mod}\theta)$ olduğundan birinci durum olarak $\xi\equiv 1(\text{mod } \theta)$ ise $\xi=1+\beta\theta$ olacak şekilde β tamsayısı vardır. Buradan $\theta^4=9$ olduğundan

$$\xi^3=(1+\beta\theta)^3=1+3\beta\theta-9\beta^2+\beta^3\theta^3\equiv1+3\beta\theta+\beta^3\theta^3 \pmod{\theta^4}$$

yazılır.

$$3\beta\theta+\beta^3\theta^3=\theta^3(\beta^3-\beta)=\theta^3(\beta(\beta-1)(\beta+1)$$

şeklinde ifade edilir. Fakat Lemma2.4.1 den θ , $\beta(\beta-1)(\beta+1)$ in böleni olduğundan $\xi^3\equiv1 \pmod{\theta^4}$ elde edilir.

İkinci durum olarak $\xi\equiv(-1) \pmod{\theta}$ ise $(-\xi)\equiv1 \pmod{\theta}$ olup $(-\xi^3)\equiv1 \pmod{\theta^4}$ ve buradan

$$\xi^3\equiv(-1) \pmod{\theta^4}$$

elde edilir.

Şimdi $\xi^3\equiv\xi \pmod{\theta}$ olduğundan θ, $\xi(\xi-1)(\xi+1)$ in bir bölenidir. ve $\xi^3+\eta^3\equiv0 \pmod{\theta}$ olması $\xi+\eta\equiv0 \pmod{\theta}$ olmasını gerektirir. Eğer $\xi\equiv1 \pmod{\theta}$ ise $\eta\equiv-1 \pmod{\theta}$ olup

$$\xi^3+\eta^3\equiv0 \pmod{\theta^4}$$

bulunur. Son olarak $\xi^3-\eta^3\equiv0 \pmod{\theta}$ ise $\xi^3+(-\eta)^3\equiv0 \pmod{\theta}$ olur. Bu da

$$\xi^3+(-\eta)^3\equiv0 \pmod{\theta^4}$$

olmasıdır.

LEMMA 2.4.3. $\alpha^3+\beta^3+\gamma^3=0$ denkleminin $Q(\sqrt{-3})$ cisminde α, β ve γ tamsayılarına göre çözülebildiğini kabul edelim. Bu takdirde $(\alpha,\beta,\gamma)=1$ ise o zaman θ, α, β ve γ dan sadece birinin bölenidir.

İspat. θ nın α , β ve γ tamsayılarının hiç birini bölmediğini kabul edelim. Bu takdirde Lemma 2.4.2 den

$$0=\alpha^3+\beta^3+\gamma^3\equiv \pm1 \pm1 \pm1 \pmod{\theta^4}$$

dir. İşaretlerin bütün konbinasyonları gözönünde bulundurulduğunda θ^4 ün 3,1,−1 veya −3 ün bir böleni olduğu sonucuna varırız. Halbuki $\theta^4=q$ olduğundan bu mümkün değildir.O halde θ nın α,β ve γ dan en az birini böldüğü sonucuna varırız. Bununla beraber θ, onların her hangi ikisini bölerse, üçüncüsünü de bölmek zorundadır. Bu ise hipotezimizle çelişir.

LEMMA 2.4.4. ε_1 ve ε_2 birimler ,r bir pozitif rasyonel tamsayı ve $\theta \nmid \alpha\beta\gamma$ olmak üzere $\alpha^3+\varepsilon_1\beta^3+\varepsilon_2(\theta^r\gamma)^3=0$ denklemi $Q(\sqrt{-3})$ cis minde sıfırdan farklı α, β ve γ tamsayıları için çözülebildiğini kabul edelim. Bu takdirde $\varepsilon_1 = \pm 1$ ve $r \geq 0$ dır.

İspat. $r > 0$ için $\alpha^3+\varepsilon_1\beta^3 \equiv 0 (\mathrm{mod}\ \theta^3)$ olduğu görülebilir.

Lemma 2.4.2 yi uyguladığımızda $\alpha^3+\varepsilon_1\beta^3 \equiv \pm 1+\varepsilon_1(\pm 1) \equiv 0 (\mathrm{mod}\ \theta^3)$ elde edilir. ε birimi, ± 1, $\pm w$, $\pm w^2$ den biri olup işaretlerin bütün kombinasyon ihtimallerine göre $\pm 1+\varepsilon_1(\pm 1)$, $2, 0, -2, \pm(1\pm w)$ $\pm(1\pm w^2)$ den biridir. Fakat θ^3, 0 haricinde diğerlerini bölmez Çünkü. $(1-w)$ ve $(1-w^2)$, θ nın ilgilileri, $1+w=-w^2$, $1+w^2=-w$ birimlerdir ve $N(\pm 2)=4$ dür. Halbuki $N(\theta^3)=27$ olduğundan bütün bunların sonucundan $\pm 1+\varepsilon_1(\pm 1)=0$ olduğu görülür ki bu da $\varepsilon_1=\pm 1$ olmasıdır.

Lemma 2.4.2 den $\alpha^3+\varepsilon_1\beta^3 \equiv 0 (\mathrm{mod}\ \theta^3)$ olması $\alpha^3+\varepsilon_1\beta^3 \equiv 0 (\mathrm{mod}\ \theta^4)$ olmasını gerektirir. Bu ise θ^4 ün, $\varepsilon_2(\theta^r\gamma)^3$ ün bir böleni olduğunu gösterir ki bu da $r \geq 2$ olmasıdır.

LEMMA 2.4.5. ε birim ve $r \geq 2$ bir rasyonel tamsayı olmak üzere

$$\alpha^3 + \beta^3 + \varepsilon(\theta^r\gamma)^3 = 0 \qquad (2.4.2)$$

eşitliğinin, $Q(\sqrt{-3})$ cisminde sıfırdan farklı hiç bir α, β ve γ tamsayıları yoktur.

TEOREM 2.4.1. $\alpha^3 + \beta^3 + \gamma^3 = 0$ denkleminin $Q(\sqrt{-3})$ de sıfırdan farklı hiç bir α, β ve γ tamsayı çözümü yoktur.

İspat. $\alpha^3 + \beta^3 + \gamma^3 = 0$ denklemini sağlayan sıfırdan farklı α, β ve γ tamsayılarının olduğunu kabul edelim. $(\alpha, \beta, \gamma)=1$ alabiliriz. Ozaman Lemma 2.4.3 den θ nın α, β ve γ dan birini bölmek zorundadır. $\theta | \gamma$ olsun ve γ, θ nın en yüksek mertebesi olan θ^r ile bölünsün. Bu durumda

$$\gamma = \theta^r\gamma_1$$

yazılır ve $\theta \nmid \gamma_1$ dir. Yine Lemma2.4.4 den $r \geq 2$ olduğu sonucuna varırız ve $\alpha^3 + \beta^3 + (\theta^r\gamma_1)^3 = 0$ olur ki bu Lemma 2.4.5 ile çelişkidir. Yani bu denklemin çözümü yoktur.

KAYNAKLAR

[1] NIVEN I. , An Introduction to the Theory of Numbers John Wiley Sons inc, New York 1972 .

[2] CALVIN T. LONG , Elementary Indroduction to Number Theory .D.C.Heath and Company Boston 1967 .

[3] HARDY G. H. , An Indroduction to the Theory of Number Oxsfortd at the Clarendon Press 1959 .

[4] SIERPINSKI W. ,Elementary Theory of Numbers.Printed In Poland . Warszava 1964 .

[5] USPENSKY J.V , HEASLET M.A. , Elementary Numbers Theory Mcgraw Hill Book Company Inc New York and London 1939.

[6] NAGELL T. , Indroduction to Number Theory .Wiley , New York 1951 .

[7] SHANKS D. , Solved and Unsolved Problems in Number Theory , Spartan Books , Washington, D.C. 1962 .

[8] ROSEN D. , The Diophantine Equation ax+by=c in Q($\sqrt{5}$) and other Number Fields. Pacfic Journal of Math. Vol.119. No 2,1985 ,465-472 .

[9] LENTBECHER A. , Uber die Heckeschen Gruppen G(λ). Abh. Math. Scm. Hamburg. 31 (1971) , 199-205 .

[10] ROSEN D. , A Class of Continued Fractions Associated With Certain Properly Discontinuous Groups,Duke Math 21 (1954) , 549-563 .

[11] MOHANTY S.P. and RAMASAMY A.M.S. , The Characteristic Number of two Simultaneous Pell's Equations and its Application, Simon stevın ,A Quarterly Journal of Pure and Applied Math.Vol. 59(1985),No 2 (June 1985),203-214.