İSTANBUL ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

İKİNCİ DERECEDEN BAZI DİOFANT DENKLEMLERİ

Duygu ÖZDEN
Matematik Anabilim Dalı

Danışman
Prof. Dr. Bedriye Melek ZEREN

Temmuz, 2010

İSTANBUL

İSTANBUL ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

İKİNCİ DERECEDEN BAZI DİOFANT DENKLEMLERİ

Duygu ÖZDEN
Matematik Anabilim Dalı

Danışman
Prof. Dr. Bedriye Melek ZEREN

Temmuz, 2010

İSTANBUL

Bu çalışma 07/07/2010 tarihinde aşağıdaki jüri tarafından Matematik Anabilim Dalı Yüksek Lisans Tezi olarak kabul edilmiştir.

Tez Jürisi

Prof. Dr. Bedriye Melek ZEREN (Danışman)
İstanbul Üniversitesi

Prof. Dr. Nazım SADIK
İstanbul Üniversitesi

Prof. Dr. Fatma SENYÜCEL
Mimar Sinan Üniversitesi

Yrd. Doç. Dr. Cemal ÇİÇEK
İstanbul Üniversitesi

Yrd. Doç. Dr. Fatma ÇALIŞKAN
İstanbul Üniversitesi

Bu çalışma İstanbul Üniversitesi Bilimsel Araştırma Projeleri Yürütücü Sekreterliğinin 6127 numaralı projesi ile desteklenmiştir.

ÖNSÖZ

Yüksek Lisans öğrenimim ve tez çalışmalarım boyunca desteğini benden esirgemeyen değerli hocam Prof. Dr. Bedriye Melek ZEREN' e en içten dileklerimle teşekkür ederim.

Ayrıca tüm öğrenim hayatım boyunca gösterdikleri her türlü destek için anneme ve babama teşekkürü bir borç bilirim.

Temmuz, 2010 **Duygu ÖZDEN**

İÇİNDEKİLER

SEMBOL LİSTESİ

$\mathbb{N}$: Doğal Sayılar Kümesi

$\mathbb{Z}$: Tam Sayılar Kümesi

$\mathbb{Q}$: Rasyonel Sayılar Kümesi

$\mathbb{R}$: Reel Sayılar Kümesi

$\equiv$: Kogrüans Bağıntısı

$\| \ \|$: Tam Değer Fonksiyonu

$| \ |$: Mutlak Değer Fonksiyonu

$\Rightarrow$: İse Bağlacı

$\Leftrightarrow$: Gerek ve Yeter Koşul Bağlacı

$\{ \ \}$: Küme Parantezi

$\sum$: Toplam Sembolü

$\cup$: Küme Birleşim Sembolü

$\cap$: Küme Kesişim Sembolü

ÖZET

İKİNCİ DERECEDEN BAZI DİOFANT DENKLEMLERİ

Bu çalışmada bazı Pell Denklemleri'nin çözümüne yönelik çeşitli metotlar incelenmiştir. Bu çalışmayı 3 bölüme ayırmak mümkündür.

1.Bölümde kuadratik kongrüanslarla ilgili bilmemiz gereken bazı temel tanım ve özellikler verilmiştir. Bu tanım ve özelliklerin yanı sıra Legendre Sembolü, Jacobi Sembolü gibi kuadratik kongrüansların çözülebilirliği incelenirken sıklıkla kullanılan ifadeler genel hatlarıyla açıklanmıştır.

2. Bölümde ise öncelikle tam sayıların tam karelerin toplamı şeklinde ifade edilmesi konusu incelenmiştir. Bunun için Thue Teoremi detaylı bir şekilde açıklanmıştır. Ardından Bachet Teoremi ile daha genel bir bakış açısı verilmiş ve Pell Denklemleri ile ilgili temel tanım ve teoremler incelenmiştir.

3. Bölümde Sürekli Kesirler konusu açıklanmıştır. Ardından Pell Denklemlerinin çözümüne ilişkin kullanışlı bir metot açıklanmıştır. Böylelikle 2.Bölüm daha da detaylandırılmıştır.

SUMMARY

SOME DIOPHANTINE EQUATIONS OF THE SECOND DEGREE

In this study, some methods for solving some Pell Equations are being examined. This study is separated in three parts.

In the firts part, some fundamental definitions and properties about quadratic congruences are given. Besides this, general phrases, that are often being used when one is searching for the solvability of quadratic congruences, are being explained deeply.

In the second part, the subject of the representation of integers as sums of integral squares is firstly examined. For this reason, Thue Theorem is expressed thoroughly. Then, a wide point of view is given by Bachet Theorem and additionally some essential definitions and theorems are given about some Pell Equations.

In the third part, the subject of Continued Fractions is explained. After that, a useful method is given about solvability of some Pell Equations. In this way, the second part is detailed.

1.GİRİŞ

Bu yüksek lisans tez çalışmasında genel olarak $C \in \mathbb{Z}, C \neq 0; D$ tam kare olmayan bir doğal sayı olmak üzere,

$$x^2 - Dy^2 = C$$

biçimindeki Diofant Denklemlerinin x ve y cinsinden tam sayılı çözümlerinin var olup olmadığı, çözümlerin varlığı halinde bu çözümlerin nasıl bulunacağı ve çözüm sayısı araştırılmaktadır.

Bunun araştırılması demek, aslında bazı özel konikler üzerindeki koordinatları tam sayı olan noktaların dağılımını bulmak demektir. Herhangi bir eğri üzerindeki koordinatları tam sayılar olan noktaların, yani "Lattice" noktalarının dağılımının bilinmesinin matematiğin çeşitli alanlarında çok önemli uygulama alanları vardır.

$$x^2 - Dy^2 = 1$$

Diofant Denklemi ile ilgili ilk teorem ilk defa 1657 de Fermat tarafından ispatsız olarak verilmiştir. Bu Diofant Denkleminin tam sayılı çözümleri hakkındaki ilk ispatı ilk olarak 1768 de Lagrange vermiştir. Yirminci yüzyılın başlarında, M.Ö. 600 yıllarında Hintli Matematikçilerin, bu denklemin tam sayılı çözümlerini bulmakla ilgili bir algoritma bildikleri ortaya çıkmıştır, fakat verdikleri yöntemin bazı özel durumlarda sonuç verdiği anlaşılmaktadır.

Bu tez çalışmasında Dirichlet' nin verdiği çözüm yöntemi derinlemesine ele alınmış ve incelenmiştir.

Yukarıda belirtilen $x^2 - Dy^2 = C$ denklemlerine özel olarak "Pell Denklemleri" denilmektedir. John Pell (1611-1685) bir İngiliz Matematikçi ve Dilbilimcidir. Matematikte özellikle cebirsel çalışmalar yapmış, denklemler teorisi ve matematiksel tablolar gibi konulara yoğunlaşmıştır. İsviçreli bir Matematikçi olan Johann Heinrich Rahn (1622-1676) ın 1659 da yayınlanan "Teutsche Algebra" adlı kitabın düzeltilmiş baskısı 1668 de Pell tarafından yayınlanmıştır. Bu kitapta yukarıda verilen Diofant Denklemleri ele alındığından, bu tür denklemleri daha sonraki yıllarda "haksız yere" Pell Denklemleri diye isimlendirmek adet olmuştur. Pell'in bu denklemlerle hiçbir ilgisi yoktur. Pell' in ayrıca Astronomi ile de ilgilendiği ve bu alanda da çalışmalar yaptığı bilinmektedir.

Bu denklemleri incelemeye geçmeden önce bazı temel Sayılar Teorisi bilgilerini hatırlayalım:

1.1. KUADRATİK KONGRÜANS

Tanım 1.1.1.(Kuadratik Rezidü) n sıfırdan farklı bir tam sayı ve D de n ile aralarında asal olan bir tam sayı olsun.

$$x^2 \equiv D \pmod{n} \tag{1.1}$$

kongrüansının çözümü varsa D sayısına modülo n nin ya da n sayısının bir *kuadratik rezidüsü* denir. Eğer bu kongrüansın çözümü yoksa D sayısına modülo n nin ya da n sayısının bir *kuadratik non rezidüsü* denir.

$n > 1, n \nmid a$ ve $a, b, c \in \mathbb{Z}$ olmak üzere;

$$ax^2 + bx + c \equiv 0 \pmod{n} \tag{1.2}$$

kongrüansı aklımıza gelen en genel kuadratik kongrüans biçimidir. $D = b^2 - 4ac$ ve $(D, n) = 1$ olmak üzere, (1.2) yi

$$x^2 \equiv D \pmod{n}$$

biçiminde bir kongrüansa indirgemek mümkündür:

(1.2) nin her iki yanını $4a$ ile çarpalım:

$$4a^2x^2 + 4abx + 4ac \equiv (2ax + b)^2 - \underbrace{(b^2 - 4ac)}_{=D} \equiv 0 \pmod{4an}$$

olur.

$y = 2ax + b$ alalım $\left[y \equiv b \pmod{2a}\right]$:

$$y^2 - D \equiv 0 \pmod{4an} \tag{1.3}$$

elde edilir. (1.3) kongrüansını elde etmek için uyguladığımız adımların çift yönlü olduğuna dikkat edilirse, şunu söyleyebiliriz: (1.1)'in çözülebilir olması için gerek ve yeter koşul (1.3) ün çözülebilir olmasıdır.

Şimdi D ile n nin aralarında asal olmadığı durumu, yani $(D, n) = d(>1)$ durumunu inceleyelim:

Teorem 1.1.1. $(D,n)=d$, $d=e^2f$, $D=da_1$ ve $n=dn_1$; e,f,a_1 ve $n_1\in\mathbb{Z}$ ve f tam kare olmayan bir sayı olsun. Bu durumda (1.1) in çözülebilir olması için gerek ve yeter koşul $(f,n_1)=1$ ve fa_1 in n_1 in bir kuadratik rezidüsü olmasıdır (*Nagell, 1964, sy 133*).

İspat. $\Rightarrow$) (1.1) çözülebilir olduğundan $x^2-D=nk$ olacak şekilde $k\in\mathbb{Z}$ vardır.

$$\Rightarrow x^2-da_1=dn_1k$$
$$\Rightarrow x^2=d(a_1+n_1k)$$
$$\Rightarrow x^2=e^2f(a_1+n_1k)$$

dir. f tam kare olmadığından $(a_1+n_1k)=fy^2$ biçimindedir. Buradan;

$$\Rightarrow y^2=\frac{a_1}{f}+\frac{n_1k}{f}$$

olur.

$$\Rightarrow f\mid a_1 \tag{1.4}$$

$D=da_1$ ve $n=dn_1$ ve $(D,n)=d$ olduğundan

$$(a_1,n_1)=1 \tag{1.5}$$

olur. Buradan,

$$f\nmid n_1 \tag{1.6}$$

elde edilir. Hipotez gereği $f<n_1$ olduğundan (1.4), (1.5) ve (1.6) dan $(f,n_1)=1$ olur.

$$fy^2=a_1+n_1k\Rightarrow fy^2\equiv a_1 \pmod{n_1}$$

yazılabilir.

$(f,n_1)=1$ olduğundan;

$$f^2y^2\equiv fa_1 \pmod{n_1}$$

olur. Yani fa_1, n_1 in bir kuadratik rezidüsüdür.

$\Leftarrow)$ $(f, n_1) = 1$ ve $\left(\frac{fa_1}{n_1}\right) = 1$ olsun. Bu durumda $y^2 \equiv fa_1 \pmod{n_1}$ kongrüansını sağlayan bir $y \in \mathbb{Z}$ vardır. O halde; $y \equiv fx^*$ kongrüansını sağlayan bir x^* tam sayısı belirlenebilir.

$$\Rightarrow y^2 \equiv fa_1 \equiv f^2(x^*)^2 \pmod{n_1}$$

$(f, n_1) = 1$ olduğundan kongrüansın her iki yanını f ile bölebiliriz:

$$\Rightarrow f(x^*)^2 \equiv a_1 \pmod{n_1}$$

olur. Kongrüansın her iki yanını $d = e^2 f$ ile çarpalım:

$$\Rightarrow e^2 f^2 (x^*)^2 \equiv e^2 f a_1 \pmod{dn_1}$$

olur. $x = efx^*$ alalım.

$$\Rightarrow x^2 \equiv D \pmod{n}$$

elde edilir.

Dolayısıyla; genel bir

$$ax^2 + bx + c \equiv 0 \pmod{n}$$

kuadratik kongrüansının çözümü için, $x^2 \equiv D \pmod{n}$ kongrüansını incelemek yeterlidir.

1.2. EULER KRİTERİ VE LEGENDRE SEMBOLÜ

Teorem 1.2.1. $p = 2h + 1$ bir tek asalsa, D^h nin modülo p +1 ya da -1 e kongrü olmasına göre D tam sayısı p nin kuadratik rezidüsü ya da kuadratik non rezidüsüdür (Bu teorem *Euler Kriteri* olarak bilinir) (*Nagell, 1964, sy 134*).

İspat. p nin bir katı olmayan tüm tam kareler,

$$\underbrace{1^2, 2^2, 3^2, ..., h^2}_{h=\frac{1}{2}(p-1)\tan e}$$

sayılarından bazılarına kongrüdür. Bu sayılar modülo p birbirine kongrü değildir.

Dolayısıyla, p nin herhangi bir kuadratik rezidüsü, bu tam karelerden birine modülo p kongrüdür. $x^2 \equiv D \pmod{p}$ den;

$$D^h \equiv x^{2h} \equiv x^{p-1} \equiv 1 \pmod{p}$$

olur. D, p nin herhangi bir kuadratik non rezidüsü olsun. Bu durum için aşağıdaki kongrüansı göz önünde bulunduralım:

$$xy \equiv D \pmod{p}$$

$0-p$ aralığındaki x in tüm tam değerlerine, aynı aralıkta y nin bir değeri karşılık gelir ve $x \equiv y \pmod{p}$ kongrüansı hiçbir şekilde gerçeklenmez. Dolayısıyla, $xy \equiv D \pmod{p}$ kongrüansını kullanarak, x in $1, 2, ..., p-1$ sayılarının yarısını taraması ve y nin de bu sayıların diğer yarısını taramasıyla $h = \frac{1}{2}(p-1)$ tane kongrüans elde ederiz. Bu kongrüansların tamamı birbiriyle çarpılırsa,

$$1.2.3...(p-1)! \equiv D^h \pmod{p}$$

kongrüansı elde edilir. Bu kongrüansa Wilson Teoremi'ni uygularsak,

$$D^h \equiv -1 \pmod{p}$$

bulunur.

Teorem 1.2.1. den elde edilen bir sonuç olarak aşağıdaki teorem verilebilir:

Teorem 1.2.2. p bir tek asalsa, modülo p ye göre $\frac{p-1}{2}$ adet kuadratik rezidü ve $\frac{p-1}{2}$ adet kuadratik non rezidü vardır (*Nagell, 1964, sy 134*).

İspat. Euler Kriteri'nin ispatından istenen kolaylıkla bulunur.

Tanım 1.2.1. p bir tek asal olmak üzere, aşağıdaki şekilde tanımlanan $\left(\frac{D}{p}\right)$ ifadesine Legendre Sembolü denir.

$\left(\frac{D}{p}\right) = +1$ ise D, p nin bir kuadratik rezidüsüdür.

$\left(\frac{D}{p}\right) = -1$ ise D, p nin bir kuadratik non rezidüsüdür.

Bu sembolün temel bazı özellikleri aşağıdaki gibidir:

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

ii. $D \equiv D' \pmod{p} \Rightarrow \left(\frac{D}{p}\right) = \left(\frac{D'}{p}\right)$

iii. $\left(\frac{DD'}{p}\right) = \left(\frac{D}{p}\right)\left(\frac{D'}{p}\right)$

“ iii ” özelliğinden şu sonuç verilebilir:

Sonuç 1.2.1. İki tane kuadratik rezidü ya da kuadratik non rezidünün çarpımı yine bir kuadratik rezidüdür. Bir tane kuadratik rezidü ve bir tane kuadratik non rezidünün çarpımı ise bir kuadratik non rezidüdür.

Teorem 1.2.3. -1 sayısı $4n+1$ formundaki tüm asalların bir kuadratik rezidüsüdür, $4n+3$ formundaki tüm asalların bir kuadratik non rezidüsüdür. Legendre Sembolü’nü kullanarak da şu bağıntı yazılabilir:

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

(*Nagell, 1964, sy 135*).

İspat. $\left(\frac{-1}{p}\right) = 1 \Leftrightarrow p \equiv 1 \pmod{4}$ olduğu göstermeliyiz.

$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = 1$ olmalı $\Rightarrow (p-1)/2 = 2k$ olacak şekilde bir $k \in \mathbb{Z}$ vardır.

$$p = 4k+1 \Rightarrow p \equiv 1 \pmod{4}$$

$p \equiv 1 \pmod{4}$ olsun $\Rightarrow \left(\frac{-1}{p}\right) = 1$ olduğunu gösterelim:

$p \equiv 1 \pmod{4} \Rightarrow p = 4k+1$ olacak şekilde bir $k \in \mathbb{Z}$ vardır.

$$\Rightarrow \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} \Rightarrow (-1)^{4k/2} = 1$$

Benzer şekilde -1 sayısının $4n+3$ formundaki tüm asalların bir kuadratik non rezidüsü olduğu gösterilebilir.

Sonuç 1.2.2. x^2+1 polinomunun tek asal bölenleri $4n+1$ formundadır.

Teorem 1.2.4. 2 sayısı $8n+1$ ya da $8n+7$ formundaki tüm asalların bir kuadratik rezidüsüdür, $8n+3$ ya da $8n+5$ formundaki tüm asalların bir kuadratik non rezidüsüdür (*Nagell, 1964, sy 136-138*).

Teorem 1.2.3. ve Teorem 1.2.4. deki iddiaları bir bütün olarak düşündüğümüzde bu iki teoremin bir sonucu olarak aşağıdaki teorem verilebilir:

Teorem 1.2.5. -2 sayısı $8n+1$ ya da $8n+3$ formundaki tüm asalların bir kuadratik rezidüsüdür, $8n+5$ ya da $8n+7$ formundaki tüm asalların bir kuadratik non rezidüsüdür (*Nagell, 1964, sy 139*).

1.3. GAUSS LEMMASI

Teorem 1.3.1.(Gauss Lemması) $p>2$ bir asal ve $p \nmid a$ olsun.

$$a, 2a, 3a, \ldots, \left(\frac{p-1}{2}\right)a \tag{1.7}$$

sayılarının p ile bıraktıkları kalanlar içinde $\frac{p}{2}$ den büyük olanların sayısı μ ise,

$$\left(\frac{a}{p}\right) = (-1)^{\mu} \tag{1.8}$$

dir.

Gauss Lemması ve Teorem 1.2.4. den şu sonuç elde edilir:

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

(*Nagell, 1964, sy 139-141*).

İspat. (1.7) sayılarının p ile bıraktıkları kalanlar içinde $\frac{p}{2}$ den büyük olanların sayısı μ, $\frac{p}{2}$ den küçük olanların sayısı λ olsun.

$\frac{p}{2}$ den küçük olanlar : $r_1, r_2, ..., r_\lambda$

$\frac{p}{2}$ den büyük olanlar : $r_{\lambda+1}, r_{\lambda+2}, ..., r_{\lambda+\mu}$

ile gösterilsin.

$$\lambda + \mu = \frac{p-1}{2}$$

olduğuna dikkat edelim:

$$r_{\lambda+1} = p - s_1 \, , r_{\lambda+2} = p - s_2 \, , ..., r_{\lambda+\mu} = p - s_\mu$$

belirleyelim. Burada, $i = 1, 2, ..., \lambda$ ve $j = 1, 2, ..., \mu$ olmak üzere $r_i \neq r_j \, , r_i \neq s_j \, , s_m \neq s_n$ dir. Buradan,

$$0 < r_i < \frac{p}{2} \text{ ve } 0 < s_j < \frac{p}{2}$$

bulunur. Bu eşitsizliklerden $\left(0, \frac{p}{2}\right)$ aralığında $r_1, r_2, ..., r_\lambda, r_{\lambda+1}, r_{\lambda+2}, ..., r_{\lambda+\mu}$ şeklinde $\frac{p-1}{2}$ tane tam sayı olduğu görülür. Yani,

$$\{r_i\} \cup \{s_j\} = \left\{1, 2, ..., \frac{p-1}{2}\right\}$$

dir.

$$\Rightarrow a.(2a)...\left(\frac{p-1}{2}a\right) \equiv r_1.r_2...r_\lambda.r_{\lambda+1}...r_{\lambda+\mu} \pmod{p}$$

$$\Rightarrow \left(1.2...\frac{p-1}{2}\right)a^{\frac{p-1}{2}} \equiv r_1.r_2...r_\lambda\,(p-s_1)...(p-s_\mu) \pmod{p}$$

$$\Rightarrow \left(\frac{p-1}{2}\right)!.a^{\frac{p-1}{2}} \equiv (-1)^\mu .r_1.r_2...r_\lambda.s_1...s_\mu \pmod{p}$$

$$\Rightarrow \left(\frac{p-1}{2}\right)!.a^{\frac{p-1}{2}} \equiv (-1)^\mu \left(\frac{p-1}{2}\right)! \pmod{p}$$

$\left(\left(\frac{p-1}{2}\right)!, p\right) = 1$ olduğundan,

$$a^{\frac{p-1}{2}} \equiv (-1)^{\mu} \pmod{p}$$

elde edilir. Teorem 1.2.1. den,

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

olur. "$\equiv$" bir eşdeğerlik bağıntısı olduğundan;

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

bulunur. Buradan,

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

olur. $\left(\frac{a}{p}\right) - (-1)^{\mu} = 2, 0$ veya -2 olabilir. Oysa p bir tek asal olduğundan, $p \nmid 2$ ve $p \nmid -2$ dir. O halde,

$$p \mid \left(\frac{a}{p}\right) - (-1)^{\mu} \Leftrightarrow \left(\frac{a}{p}\right) - (-1)^{\mu} = 0$$

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

olur.

Şimdi ise (1.7) sayılarından herhangi birini, örneğin ka yı alalım, p ile bölelim ve Bölüm Algoritması uygulayarak devam edelim:

$$ka = Qp + \delta_k \; ; \quad 0 < \delta_k < p$$

$$\Rightarrow \frac{ka}{p} = Q + \frac{\delta_k}{p} \Rightarrow \left\| \frac{ka}{p} \right\| = Q$$

yazılabilir. Buradan,

$$\sum_{k=1}^{\frac{p-1}{2}} ka = a\left(\sum_{k=1}^{\frac{p-1}{2}} k\right) = p\left(\sum_{k=1}^{\frac{p-1}{2}} \left\| \frac{ka}{p} \right\|\right) + \sum_{k=1}^{\frac{p-1}{2}} \delta_k$$

$$\left[\sum_{k=1}^{\frac{p-1}{2}} \delta_k = \sum_{i=1}^{\lambda} r_i + \sum_{j=1}^{\mu} (p - s_j) \;;\; \left(\lambda + \mu = \frac{p-1}{2}\right)\right]$$

$$\Rightarrow a\left(\sum_{k=1}^{\frac{p-1}{2}} k\right) = p\left(\sum_{k=1}^{\frac{p-1}{2}} \left\| \frac{ka}{p} \right\|\right) + \sum_{i=1}^{\lambda} r_i + \sum_{j=1}^{\mu} (p - s_j)$$

$$\Rightarrow a\left(\frac{1}{2}.\frac{p-1}{2}.\frac{p+1}{2}\right) = pM + \sum_{i=1}^{\lambda} r_i + \sum_{j=1}^{\mu} p - \sum_{j=1}^{\mu} s_j$$

$$\Rightarrow a\left(\frac{p^2-1}{8}\right) = pM + \sum_{i=1}^{\lambda} r_i + \mu p - \sum_{j=1}^{\mu} s_j$$

bulunur. Bu eşitliği modülo 2 kongrüans olarak düşünelim:

$$\Rightarrow a(\frac{p^2-1}{8}) \equiv pM + \sum_{i=1}^{\lambda} r_i + \mu p - \sum_{j=1}^{\mu} s_j + 2\sum_{j=1}^{\mu} s_j \pmod 2$$

$$\Rightarrow a(\frac{p^2-1}{8}) \equiv pM + (\sum_{i=1}^{\lambda} r_i + \sum_{j=1}^{\mu} s_j) + \mu p \pmod 2$$

$$\Rightarrow a(\frac{p^2-1}{8}) \equiv pM + \mu p + \frac{p^2-1}{8} \pmod 2$$

$a = 2$ için,

$$(a-1)(\frac{p^2-1}{8}) \equiv pM + \underbrace{\mu p}_{\equiv \mu} \pmod 2 \quad (p \text{ bir tek asal olduğundan } p \equiv 1 \pmod 2)$$

$$M = \sum_{k=1}^{\frac{p-1}{2}} \left\| \frac{2k}{p} \right\| = 0$$

dır. (k nın en büyük değeri için $2(\frac{p-1}{2}).\frac{1}{p} = \frac{p-1}{p} < 1$ olduğundan $\left\| \frac{2k}{p} \right\| = 0$ dır.)

$$\Longrightarrow \frac{p^2-1}{8} \equiv \mu \pmod 2$$

O halde $\frac{p^2-1}{8}$ ile μ nün tekliği ve çiftliği aynıdır.

Dolayısıyla;

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

dir.

1.4. KUADRATİK RESİPROSİTE YASASI

Yardımcı Teorem 1.4.1. a ve b, 3 den büyük eşit tek tam sayılar olsun. $(a,b)=1$ ve $a' = \frac{1}{2}(a-1), b' = \frac{1}{2}(b-1)$ ise aşağıdaki eşitlik vardır.

$$\sum_{u=1}^{a'} \left[\frac{bu}{a}\right] + \sum_{v=1}^{b'} \left[\frac{av}{b}\right] = a'b'$$

(*Nagell, 1964, sy 141-142*).

Teorem 1.4.1. p ve q birbirinden farklı tek asallar ve $h = \frac{1}{2}(p-1)\frac{1}{2}(q-1)$ olmak üzere aşağıdaki eşitlik vardır:

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

(*Nagell, 1964, sy 143*).

1.5. JACOBI SEMBOLÜ

P bir tek doğal sayı olmak üzere Aritmetiğin Temel Teoremi gereğince P birbirinden farklı olmak zorunda olmayan asalların çarpımı şeklinde yazılabilir.

$$P = p_1 p_2 \cdots p_r$$

Tanım 1.5.1. P bir tek doğal sayı ve D de $(D,P)=1$ koşulunu sağlayan bir tam sayı olmak üzere,

$$\left(\frac{D}{P}\right)=\left(\frac{D}{p_1}\right)\left(\frac{D}{p_2}\right)...\left(\frac{D}{p_r}\right) \tag{1.9}$$

eşitliğiyle verilen $\left(\frac{D}{P}\right)$ ifadesine D nin modülo P ye göre Jacobi Sembolü denir.

$i=1,2,...,r$ olmak üzere $\left(\frac{D}{p_i}\right)$ lerin her biri Legendre Sembolüdür.

Açıkça görülüyor ki Jacobi Sembolü Legendre Sembolüne göre daha genel bir semboldür. Çünkü modülo sadece asal bir sayı olmak zorunda değildir.

$(D,P)=1$ ve P bir tek doğal sayı olmak üzere Jacobi Sembolü'nün özellikleri şu şekildedir:

i) $P=1$ için $\left(\frac{D}{1}\right)=+1$ dir.

ii) D, P nin bir kuadratik rezidüsü ise $\left(\frac{D}{P}\right)=+1$ dir.

iii) D, P nin bir kuadratik non rezidüsü ise kesin olarak $\left(\frac{D}{P}\right)=-1$ dir diyemeyiz. Çünkü (1.9) ın sağ tarafındaki Legendre Sembollerinden -1 eşit olanların sayısı çift ise çarpım +1 olacaktır.

iv) D ve D' tam sayıları P ile aralarında asal iseler;

$$\left(\frac{D}{P}\right)\left(\frac{D'}{P}\right)=\left(\frac{DD'}{P}\right)$$

dir.

v) D ve D' tam sayıları P ile aralarında asal ve $D\equiv D' \pmod P$ ise;

$$\left(\frac{D}{P}\right)=\left(\frac{D'}{P}\right)$$

dir.

vi) D, P ve Q sayıları ile aralarında asal ise;

$$\left(\frac{D}{P}\right)\left(\frac{D}{Q}\right)=\left(\frac{D}{PQ}\right)$$

dir.

vii) Herhangi bir tek P doğal sayısı için;

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

dir.

viii) Herhangi bir tek P doğal sayısı için;

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

dir.

Teorem 1.5.1. P ve Q aralarında asal, tek iki tam sayı ve $h=\frac{1}{2}(P-1)\frac{1}{2}(Q-1)$ olmak üzere;

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

dir (*Nagell, 1964, sy 148*).

1.6. KUADRATİK POLİNOMLARIN ASAL BÖLENLERİ

$x^2\equiv D \pmod n$ kongrüansının asal bölenlerini inceleyeceğimiz için modüloyu p ile gösterelim:

$$x^2\equiv D \pmod p \tag{1.10}$$

(1.10) çözülebilir ise $p\mid x^2-D$ dir.

$D=1$ ise $x^2\equiv 1 \pmod p$ olur. Bu kongrüansın her p asalı için en az bir çözümü vardır, örneğin $x=1$ bir çözümdür.

$D=-1$ ise $x^2\equiv -1 \pmod p$ olur. Bu kongrüansın $p\equiv 1 \pmod 4$ için çözümü vardır.

$D = 2$ ise $x^2 \equiv 2 \pmod{p}$ olur. Bu kongrüansın $p \equiv \mp 1 \pmod{8}$ için çözümü vardır.

$D = -2$ ise $x^2 \equiv -2 \pmod{p}$ olur. Bu kongrüansın $p \equiv 1 \pmod{8}$ veya $p \equiv 3 \pmod{8}$ için çözümü vardır.

D bir tam kare ise, $D = C^2$ yazılabilir:

$$x^2 - D \equiv 0 \pmod{p} \Rightarrow x^2 \equiv C^2 \pmod{p} \qquad (1.11)$$

(1.11) in çözümü varsa C^2 modülo p ye göre bir kuadratik rezidüdür. O halde $\left(\frac{C^2}{p}\right) = 1$ olmalıdır. Legendre Sembolünün özelliklerinden her C için bu koşulun sağlandığı bilinmektedir. Yani D nin bir tam kare olması durumunda (1.10) in her p asalı için çözümü vardır.

D bir tam kare değil ise, $D_1 \neq 1$ tam kare olmayan bir sayı olmak üzere $D = C^2 D_1$ şeklinde yazılabilir. $x^2 \equiv C^2 D_1 \pmod{p}$ çözülebilir olsun. Bu durumda,

$$\left(\frac{C^2 D_1}{p}\right) = \left(\frac{C^2}{p}\right) \cdot \left(\frac{D_1}{p}\right) = 1$$

olmalı. $\left(\frac{C^2}{p}\right) = 1$ olduğu biliniyor. O halde $\left(\frac{D_1}{p}\right) = 1$ olmalı.

Yani $x^2 \equiv D_1 \pmod{p}$ yi incelemek gerekir.

Yardımcı Teorem 1.6.1. $p > 2$ asal, $(D, p) = 1$ olmak üzere $x^2 \equiv D \pmod{p}$ kongrüansı çözülebilir ise modülo p birbirine kongrü olmayan iki tane çözüm vardır

İspat. α, $x^2 \equiv D \pmod{p}$ nin bir çözümü olsun.

$$\alpha^2 \equiv D \pmod{p} \text{ olur.}$$

$\beta = p - \alpha$ da, $x^2 \equiv D \pmod{p}$ nin bir diğer çözümü olsun.

$$(p - \alpha)^2 \equiv (-\alpha)^2 \equiv \alpha^2 \equiv D \pmod{p} \text{ olur.}$$

$\alpha \equiv \beta \pmod{p}$ olsun. $(p - \alpha) \equiv \alpha \pmod{p}$ olur.

$$\Rightarrow -\alpha \equiv \alpha \pmod{p}$$

$$\Rightarrow 2\alpha \equiv 0 \pmod{p}$$

$$\Rightarrow \alpha \equiv 0 \pmod{p}$$

Buradan $D \equiv 0 \pmod{p}$ elde edilir. Bu ise $(D, p) = 1$ olmasıyla çelişir. O halde kabulümüz yanlıştır. $\alpha \not\equiv \beta \pmod{p}$ dir.

Ayrıca; (1.10) kongrüansında p bir tek asal olarak düşünülecektir.

Son olarak, kuadratik polinomların asal bölenlerini belirlemeye yarayan durumlara geçmeden önce bazı teoremlere ihtiyaç vardır.

Yardımcı Teorem 1.6.2. $r \geq 2$ olmak üzere $n_1, n_2, ..., n_r$ doğal sayıları ikişer ikişer aralarında asal sayılar ise;

$$x \equiv a_1 \pmod{n_1}, x \equiv a_2 \pmod{n_2}, ..., x \equiv a_r \pmod{n_r} \qquad (1.12)$$

kongrüanslarının daima x gibi bir ortak çözümü vardır. Bu çözüm $N = n_1.n_2...n_r$ olmak üzere modülo N tek türlü belirlidir (*Nagell, 1964, sy 78*).

İspat. $N = n_1 n_2 ... n_r$ olmak üzere $N = n_i v_i$; $(i = 1, 2, ..., r)$ diyelim.

$(n_1, n_2, ..., n_r) = 1$ olduğundan $i = 1, 2, ..., r$ olmak üzere v_i ler de $(v_1, v_2, ..., v_r) = 1$ koşulunu sağlar. $y_i \in \mathbb{Z}$ olmak üzere,

$$v_1 y_1 + v_2 y_2 + ... + v_r y_r = 1$$

yazılabilir.

Bu eşitlikte de $v_i y_i = z_i$ $(i = 1, 2, ..., r)$ dersek;

$$z_1 + z_2 + ... + z_r = 1$$

olur.

$N = n_1 n_2 ... n_r = n_i v_i$ almıştık. Mesela, $i = 1$ için $n_2 ... n_r = v_1$ elde edilir. $z_1 = v_1 y_1 = n_2 ... n_r . y_1$ olur. Buradan,

$$z_1 \equiv 0 \pmod{n_i} \ (i \neq 1)$$

elde edilir. Benzer şekilde $i \neq j$ olmak üzere,

$$z_j \equiv 0 \pmod{n_i}$$

kongrüansı elde edilir. $i = j$ için ise,

$$z_i \equiv 0 \pmod{n_i}$$

olur. Dolayısıyla (1.12) sistemi için aşağıdaki gibi bir ortak çözümden bahsedilebilir:

$$x \equiv a_1 z_1 + a_2 z_2 + \ldots + a_r z_r \pmod{N}$$

(1.12) sistemini sağlar. Gerçekten de;

$$x - a_1 z_1 - a_2 z_2 - \ldots - a_r z_r = Nk$$

olacak şekilde $k \in \mathbb{Z}$ vardır.

$$x - \underbrace{a_1 z_1}_{\equiv a_1 \pmod{n_1}} - \underbrace{a_2 z_2}_{\equiv a_2 \pmod{n_2}} - \ldots - \underbrace{a_r z_r}_{\equiv a_r \pmod{n_r}} = \underbrace{n_1 . n_2 \ldots n_r}_{\equiv 0 \pmod{n_1}}$$

$$x \equiv a_1 \pmod{n_1} \text{ olur.}$$

$$x - \underbrace{a_1 z_1}_{\equiv 0 \pmod{n_2}} - \underbrace{a_2 z_2}_{\equiv a_2 \pmod{n_2}} - \ldots - \underbrace{a_r z_r}_{\equiv 0 \pmod{n_2}} = \underbrace{n_1 . n_2 \ldots n_r}_{\equiv 0 \pmod{n_2}}$$

……

$$x - \underbrace{a_1 z_1}_{\equiv 0 \pmod{n_r}} - \underbrace{a_2 z_2}_{\equiv 0 \pmod{n_r}} - \ldots - \underbrace{a_r z_r}_{\equiv a_r \pmod{n_r}} = \underbrace{n_1 . n_2 \ldots n_r}_{\equiv 0 \pmod{n_r}}$$

$$x \equiv a_r \pmod{n_r}$$

Teorem 1.6.1. $P > 1$, tam kare içermeyen bir tek tam sayı; m, modülo P ye göre indirgenmiş rezidü sisteminin elemanları olsun. $\left(\frac{m}{P}\right)$ de modülo P ye göre m nin Jacobi sembolü olmak üzere;

$$S = \sum_{m} \left(\frac{m}{P}\right) = 0$$

dır (*Nagell, 1964, sy 150*).

İspat. $\left(\frac{b}{P}\right) = -1$ koşulunu sağlayan bir b tam sayısı daima vardır. Öncelikle bunu görelim:

p, P nin bir asal böleni olsun ve $\frac{P}{p} = P'$ diyelim.

β da p nin bir kuadratik non rezidüsü olsun.

Bu durumda, Çinlilerin Kalan Teoremi' nden aşağıdaki kongrüanslar gerçeklenir.

$$b \equiv \beta \pmod{p}\,; b \equiv 1 \pmod{P'}$$

Çünkü $(p, P') = 1$ dir. Zira $(p, P') \neq 1$ olsaydı $P' = p.k$ yazılabilirdi. Bu ise P nin tam kare içermemesiyle çelişir.

$$\left(\frac{b}{P}\right) = \left(\frac{b}{p}\right).\left(\frac{b}{P'}\right) = \left(\frac{\beta}{p}\right).\left(\frac{1}{P'}\right) = -1$$

dir. Jacobi sembolünün tanımından $(b, P) = 1$ olmalı. Biliyoruz ki $(b, P) \neq 1$ için $\left(\frac{b}{P}\right) = 0$ dır. Bu durumda $(b, P) = 1$ olduğundan, $(m, P) = 1$ ise $(mb, P) = 1$ olur. Dolayısıyla m, P nin indirgenmiş rezidü sistemini tarıyor ise, mb de P nin indirgenmiş rezidü sistemini tarar.

$$\Rightarrow S = \sum_m \left(\frac{m}{P}\right) = \sum_m \left(\frac{mb}{P}\right) = \left(\frac{b}{P}\right)\sum_m \left(\frac{m}{P}\right) = -\sum_m \left(\frac{m}{P}\right)$$

$$\Rightarrow S = \sum_m \left(\frac{m}{P}\right) = 0$$

dır.

Sonuç1.6.1. μ, modülo P ye göre birbirine kongrü olmayan ve $\left(\frac{a}{P}\right) = 1$ koşulunu sağlayan sayıların sayısını göstersin.

ν, modülo P ye göre birbirine kongrü olmayan ve $\left(\frac{b}{P}\right) = -1$ koşulunu sağlayan sayıların sayısını göstersin.

Bu durumda Teorem 1.6.1. e göre;

$$\mu = \nu = \frac{1}{2}\varphi(P)$$

dir, çünkü $\varphi(P)$ ile zaten indirgenmiş rezidü sisteminin eleman sayısını gösteriyoruz. Yani modülo P ile aralarında asal olan kalan sınıflarından oluşan kümenin sayısını gösteriyoruz. Teorem 1.6.1 e göre bu kümenin elemanlarının tamamının modülo P ye

göre Jacobi sembollerinin toplamı sıfırı veriyor. Bu da ancak $\mu = \nu = \frac{1}{2}\varphi(\mathrm{P})$ ile sağlanır.

Teorem 1.6.1. ve Sonuç 1.6.1. den aşağıdaki durumlar ortaya çıkar. Bu durumların her birinde $\mathrm{D} \neq 1$, tam kare olmayan bir tam sayıyı göstermektedir:

1. Durum: $\mathrm{D} = \pm\mathrm{P} \equiv 1 \pmod 4;\ \mathrm{P} > 0$ olmak üzere,

$$a_1, a_2, ..., a_v$$

$0 - 2\mathrm{P}$ aralığında $\left(\frac{a_i}{\mathrm{P}}\right) = +1$ koşulunu sağlayan $\frac{1}{2}\varphi(\mathrm{P})$ tane tek tam sayıyı,

$$b_1, b_2, ..., b_v$$

$0 - 2\mathrm{P}$ aralığında $\left(\frac{b_i}{\mathrm{P}}\right) = -1$ koşulunu sağlayan $\frac{1}{2}\varphi(\mathrm{P})$ tane tek tam sayıyı göstersin.

Bu durumda $\mathrm{p} \nmid 2\mathrm{D}$ koşulunu sağlayan bir p asalının, $\mathrm{x}^2 - \mathrm{D}$ kuadratik polinomunun bir böleni olması için gerek ve yeter koşul, $\mathrm{i} = 1, 2, ..., \mathrm{v}$ olmak üzere

$$\mathrm{p} \equiv a_i \pmod{2\mathrm{P}}$$

olmasıdır (*Nagell, 1964, sy 151;Mollin,1998, sy 205*).

2. Durum: $\mathrm{D} = \pm\mathrm{P} \equiv 3 \pmod 4;\ \mathrm{P} > 0$ olmak üzere,

$$a_1, a_2, ..., a_v$$

$0 - 4\mathrm{P}$ aralığında $\left(\frac{a_i}{\mathrm{P}}\right) = +1$ ve $a_i \equiv 1 \pmod 4$ koşulunu sağlayan $\frac{1}{2}\varphi(\mathrm{P})$ tane tam sayıyı,

$$b_1, b_2, ..., b_v$$

$0 - 4\mathrm{P}$ aralığında $\left(\frac{b_i}{\mathrm{P}}\right) = -1$ ve $b_i \equiv 3 \pmod 4$ koşulunu sağlayan $\frac{1}{2}\varphi(\mathrm{P})$ tane tam sayıyı göstersin.

Bu durumda $\mathrm{p} \nmid 2\mathrm{D}$ koşulunu sağlayan bir p asalının, $\mathrm{x}^2 - \mathrm{D}$ kuadratik polinomunun bir böleni olması için gerek ve yeter koşul, $\mathrm{i} = 1, 2, ..., \mathrm{v}$ ve $\mathrm{j} = 1, 2, ..., \mathrm{v}$ olmak üzere,

$$\mathrm{p} \equiv a_i \pmod{4\mathrm{P}} \quad \text{veya} \quad \mathrm{p} \equiv b_j \pmod{4\mathrm{P}}$$

Olmasıdır (*Nagell, 1964, sy 152;Mollin,1998, sy 205-206*).

3. Durum: $D = \pm 2P \equiv 2 \pmod 8; P > 0$ olmak üzere,

$$a_1, a_2, ..., a_\mu$$

$0-8P$ aralığında $\left(\frac{a_i}{P}\right) = +1$ ve $a_i \equiv \pm 1 \pmod 8$ koşulunu sağlayan $\varphi(P)$ tane tam sayıyı,

$$b_1, b_2, ..., b_\mu$$

$0-8P$ aralığında $\left(\frac{b_j}{P}\right) = -1$ ve $b_j \equiv \pm 3 \pmod 8$ koşulunu sağlayan $\varphi(P)$ tane tam sayıyı göstersin.

Bu durumda $p \nmid D$ koşulunu sağlayan bir p asalının, $x^2 - D$ kuadratik polinomunun bir böleni olması için gerek ve yeter koşul, $i = 1, 2, ..., \mu$ ve $j = 1, 2, ..., \mu$ olmak üzere,

$$p \equiv a_i \pmod{8P} \quad \text{veya} \quad p \equiv b_j \pmod{8P}$$

olmasıdır (*Nagell, 1964, sy 152;Mollin,1998, sy 206*).

Örnek 1.6.1. $D = -6$ için $x^2 + 6$ polinomunun 2 ve 3 dışındaki asal bölenleri,

$$p \equiv 1, 5, 7, 11 \pmod{24}$$

kongrüanslarından herhangi birini gerçekler.

4. Durum: $D = \pm 2P \equiv 6 \pmod 8$; $P > 0$ olmak üzere,

$$a_1, a_2, ..., a_\mu$$

$0-8P$ aralığında $\left(\frac{a_i}{P}\right) = +1$ ve $a_i \equiv 1 \pmod 8$ veya $a_i \equiv 3 \pmod 8$ koşulunu sağlayan $\varphi(P)$ tane tam sayıyı,

$$b_1, b_2, ..., b_\mu$$

$0-8P$ aralığında $\left(\frac{b_j}{P}\right) = -1$ ve $b_j \equiv 5 \pmod 8$ veya $b_j \equiv 7 \pmod 8$ koşulunu sağlayan $\varphi(P)$ tane tam sayıyı göstersin.

Bu durumda $p \nmid D$ koşulunu sağlayan bir p asalının, $x^2 - D$ kuadratik polinomunun bir böleni olması için gerek ve yeter koşul, $i = 1, 2, ..., \mu$ ve $j = 1, 2, ..., \mu$ olmak üzere,

$$p \equiv a_i \pmod{8P} \quad \text{veya} \quad p \equiv b_j \pmod{8P}$$

olmasıdır (*Nagell, 1964, sy 153;Mollin,1998, sy 207*).

Bu temel bilgiler doğrultusunda Pell Denklemlerini incelemeye geçmeden önce, özellikle 2. Bölümde bazı temel teoremlerin ispatında kullanılacak olan bir ilkeyi verelim:

1.7. DİRİCHLET' NİN ÇEKMECE İLKESİ

$m, n \in \mathbb{N}$ ve $m > n$ olmak üzere, n tane kutuya m tane nesne yerleştirilmek istense, kutulardan en az birine en az iki tane nesne düşer (*Nagell, 1964, sy 36-38*).

Anlaşılması oldukça basit olsa da, bu ilkenin birçok ilginç uygulamaları vardır. Bu çalışmada, kimi teoremlerin ispatında bu ilkenin kullanımı söz konusu olacaktır.

2.GENEL KISIMLAR

2.1. TAM SAYILARIN TAM KARELER TOPLAMI ŞEKLİNDE İFADE EDİLMESİ

Teorem 2.1.1.(THUE) $n>1$ bir doğal sayı ve e de $\sqrt{n}$ den büyük en küçük tam sayı olsun. $x, y \le e-1$ birer doğal sayı olmak üzere n ile aralarında asal olan herhangi bir tam sayı için $ay \equiv x \pmod{n}$ veya $ay \equiv -x \pmod{n}$ kongrüansları gerçeklenir (*Nagell, 1964, sy 122-123*).

İspat. $ay + x$ biçimindeki tüm sayıları düşünelim:

x ve y doğal sayıları $x, y \le e-1$ eşitsizliğini sağladığından $x, y \in \{0,1,2,...,e-1\}$ dir.

Böylelikle $ay + x$ biçiminde ne kadar sayı olduğu hesaplanabilir:

$x \to e$ tane farklı değer alabilir $\quad$ $y \to e$ tane farklı değer alabilir

Bu durumda; $x = y$ olacak şekilde toplam "e tane" $ay + x$ biçiminde sayı,

$x \neq y$ olacak şekilde toplam "$e(e-1)$ tane" $ay + x$ biçiminde sayı vardır.

O halde $x = y$ veya $x \neq y$ için toplam $e + e(e-1) = e + e^2 - e = e^2$ tane $ay + x$ biçiminde sayı olur.

İşte bu e^2 tane $ay + x$ biçimindeki sayıyı, n modülüne göre bir tam rezidü sistemi olan $\{0,1,2,...,n-1\}$ kümesine yerleştirmek istersek, Dirichlet' nin Çekmece İlkesi gereğince bu kalan sınıflarından en az birine en az iki tane $ay + x$ biçiminde sayı düşer. Yani $ay + x$ biçimindeki sayılardan en az iki tanesi n modülüne göre aynı kalan sınıfı içerisinde olur.

$$ay_1 + x_1 \equiv ay_2 + x_2 \pmod{n}; \quad x_1, y_1, x_2, y_2 \le e-1$$

$$a(y_1 - y_2) \equiv x_2 - x_1 \pmod{n} \qquad (2.1)$$

(2.1) in çözümüne bakalım:

$(a,n)=1 ve\ 1|(x_2-x_1)$ olduğundan kongrüansın çözümü vardır ve bir tanedir.

$x_1, y_1, x_2, y_2 \le e-1$ olduğundan;

$$0<|y_1-y_2| \le e-1 \text{ ve } 0<|x_1-x_2| \le e-1$$

dir. $|y_1-y_2|$ ve $|x_1-x_2|$ değerleri sıfırdan farklıdır. Aksi halde $y_1=y_2$ ve $x_1=x_2$ eşitlikleri elde edilir ki bu durum Dirichlet'nin Çekmece İlkesi ile çelişir.

$$|x_1-x_2|=x \qquad \text{ve} \qquad |y_1-y_2|=y \quad \text{diyelim.}$$

$x_1-x_2>0 \rightarrow x_1-x_2=x \ ; \quad y_1-y_2>0 \rightarrow y_1-y_2=y$ (i)

$x_1-x_2>0 \rightarrow x_1-x_2=x \ ; \quad y_1-y_2<0 \rightarrow y_1-y_2=-y$ (ii)

$x_1-x_2<0 \rightarrow x_1-x_2=-x \ ; \quad y_1-y_2>0 \rightarrow y_1-y_2=y$ (iii)

$x_1-x_2<0 \rightarrow x_1-x_2=-x \ ; \quad y_1-y_2<0 \rightarrow y_1-y_2=-y$ (iv)

(i) $ay \equiv x \pmod n$

(ii) $a(-y) \equiv x \pmod n \rightarrow ay \equiv -x \pmod n$

(iii) $ay \equiv -x \pmod n$

(iv) $a(-y) \equiv -x \pmod n \rightarrow ay \equiv x \pmod n$

Yani verilen koşullar altında $ay \equiv x \pmod n$ ve $ay \equiv -x \pmod n$ kongrüanslarından biri gerçeklenir.

Sonuç 2.1.1. Teorem 2.1.1 de n nin asal olması halinde $(x,y)=1$ olduğunu varsayabiliriz.

İspat . n asal ve $(x,y)=d>1$ olsun.

$d|x$ ve $d|y$ dir. Ayrıca $d|ay$ dir. Bu durumda $d|ay+x$ veya $d|ay-x$ olur.

$ay+x \equiv 0 \pmod n$ veya $ay-x \equiv 0 \pmod n$ olduğundan;

$n|ay+x$ veya $n|ay-x$ elde edilir.

$ay+x=d.s=n.r$ veya $ay-x=d.s=d.r$ koşulunu sağlayan $r,s \in \mathbb{N}$ vardır.

$(x,y)=d$ olduğundan $d<x$ ve $d<y$ dir.

Teorem 2.1.1. den $x<n$ ve $y<n$ dir. Buradan da $d<n$ eşitsizliği elde edilir. O halde $r<s$ olmalıdır.

$ay - x = d.s = n.r$ eşitliğinden $n = d.(s \mid r)$ yazılabilir. $\frac{s}{r} \in \mathbb{N}$ veya $\frac{s}{r} \in \mathbb{Q}$ olabilir.

$\frac{s}{r} \in \mathbb{N}$ ise $r < s$ olduğundan, $\frac{s}{r} > 1$ olur. Kabülümüzden $d > 1$ olduğu biliniyor. Böylelikle n sayısı 1 den büyük iki sayının çarpımı şeklinde yazılmış oldu. Bu ise n nin asal olmasıyla çelişir.

$\frac{s}{r} \in \mathbb{Q}$ ise $\frac{r}{d} \in \mathbb{N}$ olmalıdır. O halde $r < d$ dir. $d > 1$ ve $d < n$ olduğu biliniyor. Buradan $1 < \frac{d}{r} < n$ olur. Bu da yine n nin asallığıyla çelişir.

O halde kabülümüz yanlıştır. $(x, y) = 1$ olmalıdır.

Teorem 2.1.2. 1) $p \equiv 1 \pmod 4$ koşulunu sağlayan her asal, $p = x^2 + y^2$ biçiminde ifade edilebilir. (Başka hiçbir $p > 2$ asalı bu özelliği sağlamaz.)($x, y \in \mathbb{N}$)

2) $p \equiv 1 \pmod 6$ koşulunu sağlayan her asal, $p = x^2 + 3y^2$ biçiminde ifade edilebilir. (Başka hiçbir asal bu özelliği sağlamaz.)

3) $p \equiv 1 \pmod 8$ veya $p \equiv 3 \pmod 8$ koşulunu sağlayan her asal, $p = x^2 + 2y^2$ biçiminde ifade edilebilir. (Başka hiçbir asal bu özelliği sağlamaz.)

4) $p \equiv 1,9$ veya $11 \pmod{24}$ koşulunu sağlayan her asal, $p = x^2 + 7y^2$ biçiminde ifade edilebilir. (Başka hiçbir asal bu özelliği sağlamaz.)

5) $p \equiv 5$ veya $11 \pmod{24}$ koşulunu sağlayan her asal, $p = 2x^2 + 3y^2$ biçiminde ifade edilebilir. (Başka hiçbir asal bu özelliği sağlamaz.)

(*Nagell, 1964, sy 188-190*)

İspat. Bu teoremin ispatında Teorem 2.1.1 den yararlanacağız:

Kuadratik polinomların asal bölenleri incelenirken $x^2 - D$ biçimindeki polinomları incelemenin yeterli olduğu görülmüştü. Hipotezde geçen kuadratik polinomları bu biçime benzetmeye çalışıp, oradan ispata geçeceğiz:

$z = \frac{x}{y};\ x, y \in \mathbb{N}$ alalım:

1) $p = x^2 + y^2 \Rightarrow \frac{p}{y^2} = \frac{x^2}{y^2} + 1$

$$\Rightarrow \frac{x^2}{y^2}+1-\frac{p}{y^2}=0$$

$$\Rightarrow z^2+1\equiv 0 \pmod{p} \quad (p>2)$$

2) $p=x^2+3y^2 \Rightarrow \frac{p}{y^2}=\frac{x^2}{y^2}+3$

$$\Rightarrow \frac{x^2}{y^2}+3-\frac{p}{y^2}=0$$

$$\Rightarrow z^2+3\equiv 0 \pmod{p} \quad (p>2)$$

3) $p=x^2+2y^2 \Rightarrow \frac{p}{y^2}=\frac{x^2}{y^2}+2$

$$\Rightarrow \frac{x^2}{y^2}+2-\frac{p}{y^2}=0$$

$$\Rightarrow z^2+2\equiv 0 \pmod{p} \quad (p>2)$$

4) $p=x^2+7y^2 \Rightarrow \frac{p}{y^2}=\frac{x^2}{y^2}+7$

$$\Rightarrow \frac{x^2}{y^2}+7-\frac{p}{y^2}=0$$

$$\Rightarrow z^2+7\equiv 0 \pmod{p} \quad (p>2)$$

Teoremin ilk 4 maddesi için $z^2+d\equiv 0 \pmod{p}$ $(d=1,2,3$ veya $7)$ $(p>2)$ kongrüanslarını incelemek yeterlidir.

1) $z, z^2+1\equiv 0 \pmod{p}$ kongrüansının bir çözümü olsun.

$z^2\equiv -1 \pmod{p}$ yazılabilir. O halde bu kongrüansın bir çözümü varsa, kuadratik rezidü tanımından, $\left(\frac{-1}{p}\right)=1$ olmalı.

Hipotez gereği p asal ve z de $z^2+d\equiv 0 \pmod{p}$ nin bir çözümü ise, Teorem 2.1.1 den; $zy\equiv x \pmod{p}$ veya $zy\equiv -x \pmod{p} \Rightarrow z\equiv \frac{x}{y} \pmod{p}$ veya $z\equiv \frac{-x}{y} \pmod{p}$ yazılabilir.

Bu durumda; $z^2+d\equiv 0 \pmod{p}$ kongrüansı $x^2+dy^2\equiv 0 \pmod{p}$ halini alır.

Buradan $x^2 + dy^2 = mp\,; m \in \mathbb{N}$ eşitliği elde edilir. Burada $m \leq d$ dir.

$m > d$ olsun :

$x, y < \sqrt{p} \Rightarrow x^2, y^2 < p$ olur.

$\Rightarrow y^2 < p \Rightarrow dy^2 < dp \ (d > 0)$

$\Rightarrow x^2 + dy^2 < p + dp = p(d+1)$

$\Rightarrow mp < p(d+1)$ ($p > 0$ olduğundan eşitliğin her iki yanını p ile bölebiliriz.)

$\Rightarrow m < d+1$

Buradan $d < m < d+1$ eşitsizliği elde edilir. Yani ardışık iki doğal sayı arasına başka bir doğal sayı girmiş oldu. Bu ise mümkün değildir. O halde kabulümüz yanlıştır. Yani $m \leq d$ dir.

Tekrar $z^2 + 1 \equiv 0 \pmod{p}$ kongrüansına dönecek olursak;

$z \equiv x / y \pmod{dp}$ veya $z \equiv -x / y \pmod{dp}$ olmak üzere $x^2 + y^2 \equiv 0 \pmod{p}$ kongrüansı elde edilir.

$\Rightarrow x^2 + dy^2 = mp \ ; \ m \leq d = 1$

$\Rightarrow p = x^2 + y^2$

2) Bu durum için $z^2 + 2 \equiv 0 \pmod{p}$ kongrüansını incelemeliyiz:

$z^2 + 2 \equiv 0 \pmod{p}$ nin çözümü varsa $\left(\frac{-2}{p}\right) = 1$ olmalıdır. $\Rightarrow \left(\frac{2}{p}\right).\left(\frac{-1}{p}\right) = 1$ olmalı

$\left(\frac{-2}{p}\right) = 1 \Rightarrow \left(\frac{2}{p}\right) = 1$ ve $\left(\frac{-1}{p}\right) = 1$ dir.

O halde Teorem 1.2.1. den,

$$\left(\frac{-1}{p}\right) = 1 \Rightarrow p \equiv 1 \pmod{4}$$

dir.

Teorem 1.3.1. den,

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1, & p \equiv \pm 1 \pmod{8} \text{ ise} \\ -1, & p \equiv \pm 3 \pmod{8} \text{ ise} \end{cases}$$

olur.

Bu durumda;

$$p \equiv \mp 1 \pmod 8 \Rightarrow \frac{p^2-1}{8} = \frac{(8m \mp 1)^2 - 1}{8} = 8m^2 \mp 2m \quad (m \in \mathbb{Z})$$

$$\Rightarrow \left(\frac{2}{p}\right) = 1$$

olur.

$$p \equiv \mp 3 \pmod 8 \Rightarrow \frac{p^2-1}{8} = \frac{(8m \mp 3)^2 - 1}{8} = 8m^2 \mp 6m + 1$$

$$\Rightarrow \left(\frac{2}{p}\right) = -1$$

olur.

$$\Rightarrow \left(\frac{-2}{p}\right) = 1 \Rightarrow \begin{Bmatrix} \text{i) } p \equiv 1 \pmod 4 \text{ ve } p \equiv 1 \pmod 8 \text{ veya } p \equiv 7 \pmod 8 \\ \text{ii) } p \equiv 3 \pmod 4 \text{ ve } p \equiv 3 \pmod 8 \text{ veya } p \equiv 5 \pmod 8 \end{Bmatrix}$$

$\Rightarrow$ i) $\left[p \equiv 1 \pmod 4 \text{ ve } p \equiv 1 \pmod 8\right]$ veya $\left[p \equiv 1 \pmod 4 \text{ ve } p \equiv 7 \pmod 8\right]$

$\Rightarrow$ ii) $\left[p \equiv 3 \pmod 4 \text{ ve } p \equiv 3 \pmod 8\right]$ veya $\left[p \equiv 3 \pmod 4 \text{ ve } p \equiv 5 \pmod 8\right]$

Çinlilerin Kalan Teoreminden,

$\Rightarrow \left.\begin{matrix} p \equiv 1 \pmod 4 \\ p \equiv 1 \pmod 8 \end{matrix}\right\}$ $(4,8) = 4$ ve $1 \equiv 1 \pmod 4$ olduğundan çözüm var.

$$p \equiv 1 \pmod 8 \tag{2.2}$$

$\Rightarrow \left.\begin{matrix} p \equiv 1 \pmod 4 \\ p \equiv 7 \pmod 8 \end{matrix}\right\}$ $(4,8) = 4$ ve $1 \not\equiv 7 \pmod 4$ olduğundan çözüm yoktur.

$\Rightarrow \left.\begin{matrix} p \equiv 3 \pmod 4 \\ p \equiv 3 \pmod 8 \end{matrix}\right\}$ $(4,8) = 4$ ve $3 \equiv 3 \pmod 4$ olduğundan çözüm var.

$p = 4k + 3 \Rightarrow 4k + 3 \equiv 3 \pmod 8$

$\Rightarrow 4k \equiv 0 \pmod 8$

$\Rightarrow k \equiv 2 \pmod 8$

$\Rightarrow 4k + 3 = 4(8u + 2) + 3 \Rightarrow 4k + 3 = 32u + 11$

$$p \equiv 3 \pmod 8 \tag{2.3}$$

$$\Rightarrow \left.\begin{matrix} p \equiv 3 \pmod 4 \\ p \equiv 5 \pmod 8 \end{matrix}\right\} \qquad (4,8) = 4 \quad \text{ve} \quad 3 \not\equiv 5 \pmod 4 \quad \text{olduğundan}$$

çözüm yoktur. O halde,

$$\left(\frac{-2}{p}\right) = 1 \Rightarrow p \equiv 1 \pmod 8 \text{ veya } p \equiv 3 \pmod 8 \qquad (2.4)$$

Teorem 2.1.1. den $z^2 + 2 \equiv 0 \pmod p$ kongrüansı için $z \equiv \mp \frac{x}{y} \pmod p$ alınabilir.

Ayrıca p asal olduğundan (x,y)=1 dir.

Buradan $x^2 + 2y^2 \equiv 0 \pmod p$ elde edilir.

$$\Rightarrow x^2 + 2y^2 = mp \ ; \ m \le 2 \text{ olur.}$$

$$\Rightarrow m = 1 \text{ veya } m = 2 \text{ dir.}$$

$m = 1$ için $p = x^2 + 2y^2$ olur.

$m = 2$ için $2p = x^2 + 2y^2$ olur.

$x = 2x_1$ alalım,

$$\Rightarrow 4x_1^2 + 2y^2 = 2p$$

$$\Rightarrow p = 2x_1^2 + y^2 \text{ olur.}$$

Bu da ispatı tamamlar.

3) Bu durum için $z^2 + 3 \equiv 0 \pmod p$ kongrüansını incelemeliyiz:

Bu kongrüansın çözümü var ise $\left(\frac{-3}{p}\right) = 1$ olmalı. $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right).\left(\frac{3}{p}\right)$ olduğundan,

$$\left(\frac{-3}{p}\right) = 1 \Rightarrow \begin{cases} \text{i)} \left(\frac{-1}{p}\right) = 1 \text{ ve } \left(\frac{3}{p}\right) = 1 \\ \text{ii)} \left(\frac{-1}{p}\right) = -1 \text{ ve } \left(\frac{3}{p}\right) = -1 \end{cases}$$

$$\left(\frac{-1}{p}\right) = 1 \Rightarrow p \equiv 1 \pmod 4 \quad \text{ve} \quad \left(\frac{-1}{p}\right) = -1 \Rightarrow p \equiv 3 \pmod 4$$

Bu durumda öncelikle 3 ün hangi asallar için kuadratik rezidü ve kuadratik-non rezidü olduğunu görmeliyiz:

$\left(\frac{3}{p}\right)=1$ koşulunu sağlayan p asallarını bulalım:

Teorem 1.4.1. den,

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

dir.

Eşitliğin her iki tarafını $\left(\frac{p}{3}\right)$ ile çarpalım:

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

$$\Rightarrow\left(\frac{3}{p}\right)=1\Rightarrow\begin{cases}\left(\frac{p}{3}\right)=1 \text{ ve } (-1)^{\frac{p-1}{2}}=1\\ \left(\frac{p}{3}\right)=-1 \text{ ve } (-1)^{\frac{p-1}{2}}=-1\end{cases}$$

$$(-1)^{\frac{p-1}{2}}=1\Rightarrow\frac{p-1}{2}=2k\Rightarrow p=4k+1\Rightarrow p\equiv 1\pmod 4$$

$$(-1)^{\frac{p-1}{2}}=-1\Rightarrow\frac{p-1}{2}=2k+1\Rightarrow p=4k+3\Rightarrow p\equiv 3\pmod 4$$

$\left(\frac{p}{3}\right)=1$ ise $p,3$ ün bir kuadratik rezidüsüdür. Dolayısıyla, 1.Bölümde verilen Legendre Sembolü özelliklerinden p, 3 ün bir kuadratik rezidüsüne kongrü olmalıdır. 3 bir tek asal olduğuna göre Teorem 1.2.2. den 3 ün $\frac{3-1}{2}$ tane, yani 1 tane kuadratik rezidüsü ve 1 tane kuadratik-non rezidüsü vardır.

Yani $x^2\equiv a\pmod 3$ kongrüansını sağlayan 3 ile aralarında asal olan bir tane a sayısı vardır. Modülo 3 tam rezidü sistemi $\{0,1,2\}$ olduğundan, $a=1$ için $x=1$ çözümdür. Ancak $a=2$ için böyle bir x bulunamaz. O halde 1 modülo 3 için kuadratik rezidü, 2 modülo 3 için kuadratik-non rezidüdür. ($a=0$ olma durumunu düşünmüyoruz. Çünkü kuadratik rezidü tanımına göre $x^2\equiv D\pmod n$ kongrüansında $(D,n)=1$ olmalı)

Bu durumda;

$$\left.\begin{array}{l}\left(\frac{p}{3}\right)=1 \text{ ise } p\equiv 1 \pmod 3\\ \left(\frac{p}{3}\right)=-1 \text{ ise } p\equiv 2 \pmod 3\end{array}\right\}$$

elde edilir. Buradan da,

$$\left(\frac{3}{p}\right)=1\Rightarrow\begin{cases}p\equiv 1 \pmod 4 \text{ ve } p\equiv 1 \pmod 3\\ p\equiv 3 \pmod 4 \text{ ve } p\equiv 2 \pmod 3\end{cases}$$

kongrüans sistemleri elde edilir. Bu kongrüans sistemlerinin çözümü için Yardımcı Teorem 1.6.2. yi kullanacağız:

$$\text{(i)}\ \begin{cases}p\equiv 1 \pmod 4\\ p\equiv 1 \pmod 3\end{cases}\Rightarrow (4,3)=1 \text{ ve } 1\mid 1-1$$

olduğundan çözüm var ve bu çözüm;

$$p\equiv 1 \pmod{12} \text{ dir…(IV)}$$

$$\text{(ii)}\ \begin{cases}p\equiv 3 \pmod 4\\ p\equiv 2 \pmod 3\end{cases}\Rightarrow (4,3)=1 \text{ ve } 1\mid 3-2$$

olduğundan çözüm var ve bu çözüm;

$$p\equiv 3 \pmod 4 \Rightarrow p=4k+3$$

$$4k+3\equiv 2 \pmod 3$$

$$4k+3=4(3u+2)+3=12u+11\Rightarrow p\equiv 11 \pmod{12}\ldots(V)$$

$$\Rightarrow \left(\frac{3}{p}\right)=1 \Rightarrow p\equiv 1 \pmod{12} \text{ veya } p\equiv 11 \pmod{12} \ldots(VI)$$

bulunur.

$$\left(\frac{3}{p}\right)=-1 \Rightarrow \begin{cases}\left(\frac{p}{3}\right)=1 \text{ ve } (-1)^{\frac{p-1}{2}}=-1\\ \left(\frac{p}{3}\right)=-1 \text{ ve } (-1)^{\frac{p-1}{2}}=1\end{cases} \Rightarrow \begin{cases}p\equiv 1 \pmod 3 \text{ ve } p\equiv 3 \pmod 4\\ p\equiv 1 \pmod 3 \text{ ve } p\equiv 3 \pmod 4\end{cases}$$

$$\left.\begin{array}{l}p\equiv 1 \pmod 3\\ p\equiv 3 \pmod 4\end{array}\right\}\Rightarrow (3,4)=1 \text{ ve } 1\mid 3-1$$

olduğundan çözüm var ve bu çözüm;

$$p\equiv 1 \pmod 3 \Rightarrow p=3k+1$$

$$\Rightarrow 3k+1\equiv 3 \pmod 4$$

$$\Rightarrow\ k \equiv 2 \pmod 4 \Rightarrow k = 4u+2$$

$$\Rightarrow\ 3k+1 = 3(4u+2)+1 \Rightarrow 12u+7$$

$$\Rightarrow\ p \equiv 7 \pmod{12} \ldots \text{(VII)}$$

$$\left.\begin{array}{l} p \equiv 2 \pmod 3 \\ p \equiv 1 \pmod 4 \end{array}\right\} \Rightarrow (3,4) = 1 \text{ ve } 1 \mid 2-1$$

olduğundan çözüm var ve bu çözüm;

$$p \equiv 2 \pmod 3 \Rightarrow p = 3k+2$$

$$\Rightarrow\ 3k+2 \equiv 1 \pmod 4 \Longrightarrow k \equiv 1 \pmod 4 \Longrightarrow k = 4u+1$$

$$\Rightarrow\ p = 3(4u+1)+2 = 12u+5$$

$$\Rightarrow\ p \equiv 5 \pmod{12} \ldots \text{(VIII)}$$

$\Rightarrow$ i) $p \equiv 1 \pmod 4$ ve $\left[p \equiv 1 \pmod{12} \text{ veya } p \equiv 11 \pmod{12}\right]$

$\Rightarrow$ ii) $p \equiv 3 \pmod 4$ ve $\left[p \equiv 7 \pmod{12} \text{ veya } p \equiv 5 \pmod{12}\right]$

i) $\left[\underbrace{p \equiv 1 \pmod 4 \text{ ve } p \equiv 1 \pmod{12}}_{(1)}\right]$ veya $\left[\underbrace{p \equiv 1 \pmod 4 \text{ ve } p \equiv 11 \pmod{12}}_{(2)}\right]$

ii) $\left[\underbrace{p \equiv 3 \pmod 4 \text{ ve } p \equiv 7 \pmod{12}}_{(3)}\right]$ veya $\left[\underbrace{p \equiv 3 \pmod 4 \text{ ve } p \equiv 5 \pmod{12}}_{(4)}\right]$

(1): $(4,12) = 4$ ve $4 \mid 1-1$ olduğundan çözüm var ve bu çözüm: $p \equiv 1 \pmod{12} \ldots \text{(IX)}$

(2): $(4,12) = 4$ ve $4 \nmid 11-1$ olduğundan çözüm yoktur.

(3): $(4,12) = 4$ ve $4 \mid 7-3$ olduğundan çözüm var ve bu çözüm: $p \equiv 3 \pmod 4$

$$\Rightarrow\ 4k+3 \equiv 7 \pmod{12}$$

$$\Rightarrow\ p \equiv 7 \pmod{12} \ldots \text{(X)} \text{ dir.}$$

(4): $(4,12) = 4$ ve $4 \nmid 5-3$ olduğundan çözüm yoktur.

(IX) ve (X) dan ; $p \equiv 1 \pmod{12}$ veya $p \equiv 7 \pmod{12}$ olur. Buradan da,

$$p \equiv 1 \pmod 6$$

olur. $z^2+3 \equiv 0 \pmod p$ için,

$$\Rightarrow\ x^2+3y^2 = mp \text{ olacak şekilde } m \in \mathbb{N} \text{ vardır ve } m \le 3$$

$$\Rightarrow\ m = 1,2 \text{ veya } 3 \text{ olabilir. } (p > 3)$$

$m=1$ için $p=x^2+3y^2$ olur.

$m=2$ için $2p=x^2+3y^2$ olur. $\Rightarrow$ x^2+3y^2 bir çift sayıdır.

$\Rightarrow$ x^2 ve y^2 çift olabilir $\Rightarrow$ x ve y çifttir.

Teorem 2.1.1. den $(x,y)=1$ olduğu biliniyor. Dolayısıyla x ve y aynı anda çift olamaz.

$\Rightarrow$ x^2 ve y^2 tek olabilir.

$\Rightarrow$ $x=2r_1+1$ ve $y=2r_2+1$ olacak şekilde $r_1, r_2 \in \mathbb{N}$ var.

$$\Rightarrow (4r^2_1+4r_1+1)+3(4r^2_2+4r_2+1)=4r^2_1+4r_1+1+3.4r^2_2+3.4r_2+3$$
$$=4(r^2_1+r_1+3r^2_2+3r_2+1)$$
$$=2p$$

$\Rightarrow p=2(r^2_1+r_1+3r^2_2+3r_2+1)$ olur ki bu p nin bir tek asal olmasıyla çelişir.

$\therefore$ $m=2$ için $2p=x^2+3y^2$ eşitliği gerçeklenmez.

$m=3$ için $3p=x^2+3y^2$ olur. $\Rightarrow$ $x=3x_1$ alınırsa

$\Rightarrow$ $3p=9x^2_1+3y^2$

$\Rightarrow$ $p=3x^2_1+y^2$ elde edilir.

Böylelikle ispat tamamlanmış olur.

4) Bu durum için $z^2+7\equiv 0 \pmod p$ kongrüansını incelemeliyiz:

Bunun için $p\equiv 1,9 \text{ veya } 11 \pmod{14}$ olması gerektiği bir önceki maddedekilere benzer şekilde gösterilir.

z, $z^2+7\equiv 0 \pmod p$ için bir çözüm ise p de asal olduğundan $z=\mp\frac{x}{y} \pmod p$ gerçeklenir. Buradan $x^2+7y^2\equiv 0 \pmod p$ kongrüansı elde edilir. Bu kongrüanstan eşitliğe geçecek olursak,

$$x^2+7y^2=mp$$

bulunur. $m=1,2,3,4,5,6 \text{ veya } 7$ olabilir.

m çift ise; x ve y aynı anda ya çift ya da tek olmalıdır. Ancak x ve y nin çift olması $(x,y)=1$ ile çelişir.O halde $x=2k_1+1$ ve $y=2k_2+1$ oalacak şekilde $k_1, k_2 \in \mathbb{Z}$ vardır. x ve y nin bu değerleri $x^2+7y^2=mp$ de yerine yazılırsa mp nin 8 in bir katı olduğu

görülür. $m = 2, 4$ veya 6 olduğundan bu durumda mp nin 8 in bir katı olabilmesi için p nin kesinlikle bir çift sayı olması gerekir. Bu ise p nin bir tek asal olmasıyla çelişir. $m = 3$ için,

$$x^2 + 7y^2 = 3p \Rightarrow x^2 + 7y^2 \equiv 0 \pmod 3$$

Bu kongrüans çözülebilir olsa 3 asal bir sayı olduğundan $z \equiv \mp \frac{x}{y}$ sağlanır.Bu kongrüansın çözülebilir olması için gerek ve yeter koşul $\left(\frac{-7}{3}\right) = 1$ olmasıdır.

$$\left(\frac{-7}{3}\right) = \underbrace{\left(\frac{7}{3}\right)}_{=1}\underbrace{\left(\frac{-1}{3}\right)}_{=-1} = -1$$

olduğundan $m = 3$ için de istenen eşitlik gerçeklenmez. Benzer şekilde $m = 5$ için de eşitliğin gerçeklenmediği görülür.

Bu durumda tek durum $m = 1$ olmasıdır. O halde,

$$p = x^2 + 7y^2$$

olur. Yani istenen eşitlik elde edilir.

5) Bu durum için $p > 3$ bir asal olmak üzere,

$$2z^2 + 3 \equiv 0 \pmod p \tag{2.5}$$

kongrüansını inceleyelim.

z, (2.5) için bir çözüm ise p de asal olduğundan Teorem 2.1.1. gereği,

$$z \equiv \mp \frac{x}{y} \pmod p \tag{2.6}$$

sağlanır. (2.6) yı (2.5) de yerine yazarsak;

$$2x^2 + 3y^2 \equiv 0 \pmod p \tag{2.7}$$

elde edilir.

(2.7) kongrüansını $x^2 - D \equiv 0 \pmod p$ biçimine indirgeyelim:

$p > 3$ bir asal olduğundan, $(p, 2) = 1$ dir. Dolayısıyla (2.7) nin her iki yanını 2 ile çarpabiliriz.

$$4x^2 + 6y^2 \equiv 0 \pmod p$$

olur. $x' = 2x$ alalım:

$$(x')^2 + 6y^2 \equiv 0 \pmod{p}$$

olur. Buradan da,

$$\left(\frac{x'}{y}\right) + 6 \equiv 0 \pmod{p} \qquad (2.8)$$

elde edilir.

Bu ise 1.bölüm de yer alan " Kuadratik Polinomların Asal Bölenleri" bölümündeki 3. Durum a tekabül eder. $[D = -6 \equiv 2 \pmod 8]$ Bu durumdan ve Örnek 1.6.1. den (2.8) in çözülebilir olması için gerek ve yeter koşulun $p \equiv 1,5,7$ veya $11 \pmod{24}$ olması gerektiği biliniyor.

Teorem 2.1.1. den, $z \equiv \mp\frac{x}{y} \pmod{p}$ kongrüansının varlığı; p asal olduğu için $(x,y) = 1$ ve $x, y < \sqrt{p}$ olduğu biliniyor.

$\Rightarrow 2x^2 + 3y^2 \equiv 0 \pmod{p}$ kongrüansından eşitliğe geçelim.

$\Rightarrow 2x^2 + 3y^2 = mp$ olacak şekilde $m \in \mathbb{N}$ vardır.

$\Rightarrow 2x^2 + 3y^2 < 2p + 3p = 5p \Rightarrow mp < 5p$

p asal olduğundan;

$\Rightarrow m < 5$

$\Rightarrow m = 1,2,3$ veya 4 olabilir.

$m = 1 \Rightarrow 2x^2 + 3y^2 = p$ olur, ispat biter.

$m = 2 \Rightarrow 2x^2 + 3y^2 = 2p$ olur. Bu durumda; y çift ve x tek olur. [$(x,y) = 1$ olduğundan y çift iken x çift olamaz.] $y = 2y_1$ alınırsa;

$\Rightarrow 2x^2 + 3y^2 = 2p \Rightarrow x^2 + 6y_1 = p$

olur. x tek olduğundan $x = 2k+1$ olacak şekilde $k \in \mathbb{N}$ vardır. $y_1 = 2m$ veya $y_1 = 2m+1\ (m \in \mathbb{N})$ olur. $y_1 = 2m$ alınırsa;

$\Rightarrow (2k+1)^2 + 6(4m^2) = p \Rightarrow 4k^2 + 4k + 1 + 6.4m^2 = p$

$\Rightarrow 4k^2 + 4k + 24m^2 + 1 = p$

$\Rightarrow 4.2n + 24m^2 + 1 = p$

$\Rightarrow p = 24m^2 + 8n + 1$

$$\Rightarrow\ p \equiv 1 \pmod 8$$

$y_1 = 2m+1$ alınırsa;

$$\Rightarrow (2k+1)^2 + 6(4m^2+4m+1) = p$$

$$\Rightarrow\ 4k^2+4k+1+6.4m^2+6.4m+6 = p$$

$$\Rightarrow\ 4k^2+4k+24m^2+24m+7 = p$$

$$\Rightarrow\ 8n+24(m^2+m)+7 = p$$

$$\Rightarrow\ p \equiv -1 \pmod 8 \Rightarrow\ p \equiv 7 \pmod 8$$

$m = 3 \Rightarrow\ 2x^2+3y^2 = 3p$ olur. Bu durumda $x = 3x_1$ ve $y = 2k+1$ olur.

$x_1 = 2m$ alınırsa;

$$\Rightarrow\ p = 6.4m^2+4k^2+4k+1 \Rightarrow\ p \equiv 1 \pmod 8$$

$x_1 = 2m+1$ alınırsa;

$$\Rightarrow p = 6(4m^2+4m+1)+4k^2+4k+1$$

$$\Rightarrow\ p \equiv -1 \pmod 8 \Rightarrow p \equiv 7 \pmod 8$$

İspatın başında (2.8) in çözülebilir olması için gerek ve yeter koşulun $p \equiv 1,5,7$ veya $11 \pmod{24}$ olması gerektiği belirtilmişti.

$p \equiv 1 \pmod{24} \Rightarrow p \equiv 1 \pmod 8$ ve $p \equiv 7 \pmod{24} \Rightarrow p \equiv 7 \pmod 8$

olduğu biliniyor.

O halde $m = 2$ ve $m = 3$ hallerinde istediğimiz biçimi elde edemiyoruz ve bu haller $p \equiv 1 \pmod 8$ veya $p \equiv 7 \pmod 8$ için gerçeklendiğinden $p \equiv 1 \pmod{24}$ ve $p \equiv 7 \pmod{24}$ durumlarını eliyoruz.

$m = 4 \Rightarrow\ 2x^2+3y^2 = 4p$ olur. O halde $x = 2x_1$ ve $y = 4y_1$ olur. Bu ise $(x,y) = 1$ olmasıyla çelişir.

$\therefore$ (2.8) kongrüansı $p \equiv 5$ veya $11 \pmod{24}$ için gerçeklenir.

Böylelikle Teorem 2.1.2 nin ispatı tamamlanmış olur.

Şimdi Teorem 2.1.2 de elde ettiklerimizi genelleştirmemize yarayacak aşağıdaki teoremi verelim:

Teorem 2.1.3. $x, y, c, d \in \mathbb{N}$ olmak üzere p asal sayısı en çok bir şekilde $p = cx^2 + dy^2$ biçiminde ifade edilebilir (*Nagell, 1964, sy 190-191*).

İspat. p yi; $u, v \in \mathbb{N}$ olmak üzere,

$$p = cx^2 + dy^2 \tag{2.9}$$

ve

$$p = cu^2 + dv^2 \tag{2.10}$$

şeklinde iki ayrı biçimde ifade edebildiğimizi varsayalım. $x = u$ ve $y = v$ olduğu gösterilirse ispat tamamlanmış olur:

$$p = cx^2 + dy^2 \Rightarrow d = \frac{p - cx^2}{y^2} \tag{2.11}$$

$$p = cu^2 + dv^2 \Rightarrow d = \frac{p - cu^2}{v^2} \tag{2.12}$$

(2.11) ve (2.12) den;

$$(p - cx^2)v^2 = (p - cu^2)y^2$$

olur. Buradan da,

$$pv^2 - cx^2v^2 = py^2 - cu^2y^2 \Longrightarrow p(v^2 - y^2) = c(x^2v^2 - u^2y^2)$$

$$\Longrightarrow c(x^2v^2 - u^2y^2) \equiv 0 \pmod{p}$$

$c < p$ olduğundan,

$$xv \equiv \mp uy \pmod{p} \tag{2.13}$$

olur.

(2.9) ve (2.10) taraf tarafa çarpıldığında,

$$p^2 = (cx^2 + dy^2)(cu^2 + dv^2) = c^2x^2u^2 + cdx^2v^2 + dcy^2u^2 + d^2y^2v^2$$

olur. Buradan da,

$$p^2 = (cxu \mp dyv)^2 + cd(uy \pm vx)^2 \tag{2.14}$$

bulunur.

$uy = vx$ olsun. Teorem 2.1.1, (2.9) ve (2.10) dan $(x, y) = 1$ ve $(u, v) = 1$ olduğu görülür. Bu durumda $x = u$ ve $y = v$ elde edilir.

$uy \neq vx$ olsun. (2.13) ve (2.14) den $p = |uy \pm vx|$ $c = d = 1$ ve $cxu \mp dyv = 0$ olur.

Buradan da $xu \mp yv = 0$ olur. $(x, y) = 1$ ve $(u, v) = 1$ olduğundan bu da ancak $x = u$ ve $y = v$ olduğunda mümkündür.

Böylelikle ispat tamamlanmış olur.

2.2. BACHET TEOREMİ

Teorem 2.2.1. (Bachet) Her doğal sayı dört tane tam karenin toplamı şeklinde yazılabilir (*Nagell, 1964, sy 191-192*).

Teorem 2.2.1 in ispatına geçmeden önce Euler Özdeşliği diye bilinen eşitliği ve ardından da iki tane yardımcı teoremi vereceğiz:

$$\begin{cases} \left(a^2 + b^2 + c^2 + d^2\right)\left(\alpha^2 + \beta^2 + \gamma^2 + \delta^2\right) \\ = \left(a\alpha + b\beta + c\gamma + d\delta\right)^2 + \left(a\beta - b\alpha - c\delta + d\gamma\right)^2 \\ + \left(a\gamma + b\delta - c\alpha - d\beta\right)^2 + \left(a\delta - b\gamma + c\beta - d\alpha\right)^2 \end{cases} \tag{2.15}$$

(2.15) in gerçeklendiği kolaylıkla gösterilebilir.

Yardımcı Teorem 2.2.1. p bir tek asalsa; $x_1^2 + x_2^2 + x_3^2 + x_4^2 = mp$ eşitliğini sağlayan $x_1, x_2, x_3, x_4 \in \mathbb{Z}$ vardır ve m, p den küçük bir doğal sayıdır (*Nagell, 1964, sy 192*).

İspat. $0 \leq x \leq \frac{p-1}{2}$ eşitsizliğini sağlayan x leri düşünelim. p bir tek asal olduğundan $\frac{p-1}{2}$ bir tam sayıdır. Bu aralıkta toplam $\frac{p-1}{2} + 1 = \frac{p+1}{2}$ tane tam sayı vardır. Bu sayıların modülo p ye göre birbirlerine kongrü olmadığı açıktır. O halde; $0 \leq x^2 \leq \left(\frac{p-1}{2}\right)^2$ eşitsizliği sağlanır. Aynı şekilde,

$$\frac{p+1}{2} \text{ tane } x^2 \tag{2.16}$$

sayısı da modülo p ye göre birbirlerine kongrü değillerdir.

Benzer şekilde $0 \le y \le \frac{p-1}{2}$ eşitsizliğini sağlayan $\frac{p+1}{2}$ tane y sayısı ve $0 \le y^2 \le \left(\frac{p-1}{2}\right)^2$ eşitsizliğini sağlayan $\frac{p+1}{2}$ tane y^2 sayısı da modülo p ye göre birbirlerine kongrü değillerdir. O halde

$$\frac{p+1}{2} \text{ tane } -1-y^2 \tag{2.17}$$

sayılarından bahsedilebilir.

Bu durumda (2.16) ve (2.17) kümelerinin birlikte $p+1$ tane elemanı vardır. Bu $p+1$ tane sayı modülo p ye göre p tane kalan sınıfının içerisine yerleştirilirse, Dirichlet'nin Çekmece İlkesi gereğince bu sayılardan en az iki tanesi aynı kalan sınıfının içerisine düşer.

$$\Rightarrow x^2 \equiv -1-y^2 \pmod{p}$$

$$\Rightarrow x^2+y^2+1 \equiv 0 \pmod{p}$$

$$\Rightarrow x^2+y^2+1 \equiv 0 \pmod{p}$$

$$\Rightarrow x^2+y^2+1+0^2 = mp$$

olacak şekilde $m \in \mathbb{N}$ vardır. $m < p$ olduğu gösterilirse ispat tamamlanmış olur.

$$x < \frac{p-1}{2} < \frac{p}{2} \Rightarrow x^2 < \frac{p^2}{4} \quad \text{ve} \quad y < \frac{p-1}{2} < \frac{p}{2} \Rightarrow y^2 < \frac{p^2}{4}$$

olduğundan

$$\Rightarrow m = \frac{1}{p}(x^2+y^2+1) < \frac{1}{p}\left(\frac{p^2}{2}+1\right) < \frac{1}{p}\left(\frac{p^2}{2}+\frac{p^2}{2}\right) = p$$

Yardımcı Teorem 2.2.2. Her p asalı dört tane tam karenin toplamı şeklinde yazılabilir (*Nagell, 1964, sy 193-194*).

İspat. $p = 2$ için ispat açıktır. $(2 = 1^2+1^2+0^2+0^2)$

p bir tek asal olsun ve m de; $x_1, x_2, x_3, x_4 \in \mathbb{Z}$ olmak üzere

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = mp \tag{2.18}$$

Eşitliğini sağlayan en küçük doğal sayı olsun.

Yardımcı Teorem 2.2.1. den $m < p$ olduğu biliniyor. $m = 1$ olduğu gösterilirse ispat tamamlanmış olur.

(2.18) şu şekilde de yazılabilir:

$$\left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2 = \frac{1}{2}mp$$

m çift olsun, yani $m = 2k; k \in \mathbb{N}$ şeklinde yazılabilsin.Karşımıza üç farklı durum çıkar:

Durum I) $i = 1,2,3,4$ *olmak üzere* x_i *lerin hepsi çifttir.*

$x_i = 2k_i$ olmak üzere;

$$x_1 + x_2 , x_1 - x_2, x_3 + x_4, x_3 - x_4 \tag{2.19}$$

sayılarının hepsi çift olur. Dolayısıyla,

$$\left(\frac{x_1 + x_2}{2}\right), \left(\frac{x_1 - x_2}{2}\right), \left(\frac{x_3 + x_4}{2}\right), \left(\frac{x_3 - x_4}{2}\right) \tag{2.20}$$

sayıları birer tam sayıdır. Bu durumda p nin bir katı yine dört tane tam sayının kareleri toplamı şeklinde yazıldı. Ancak $k < m$ olduğundan bu durum, m nin tanımıyla çelişir.

Durum II) x_i *lerin hepsi tektir.*

$x_i = 2k_i + 1$ olmak üzere; (2.19) sayılarının hepsi çift sayı ve (2.20) sayılarının her biri tam sayı olur. Dolayısıyla Durum I) deki çelişki elde edilir.

Durum III) x_i *lerin ikisi tek, ikisi çifttir.*

Örneğin x_1 ve x_2 çift, x_3 ve x_4 tek olsun. Yine (2.19) sayılarının hepsi çift sayı ve (2.20) sayılarının her biri tam sayı olur. Dolayısıyla, burada da Durum I) deki çelişki elde edilir.

O halde m tek sayıdır. $m \geq 3$ olsun. $k = 1,2,3,4$ olmak üzere her k sayısı için $|y_k| < \frac{1}{2}m$ bir tam sayı olmak üzere;

$$y_k \equiv x_k \pmod{m} \tag{2.21}$$

olsun. Bu durumda $y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod{m}$ olur. Dolayısıyla,

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = mr \tag{2.22}$$

dir.

$r = 0$ *olsun.* $y_1 = y_2 = y_3 = y_4 = 0$ olur. Dolayısıyla (2.21) den x_i lerin her biri m ile bölünebilir. $\left(\frac{x_i}{m}\right)$ ler birer tam sayı olur. (2.18) den;

$$p = m\left[\left(\frac{x_1}{m}\right)^2 + \left(\frac{x_2}{m}\right)^2 + \left(\frac{x_3}{m}\right)^2 + \left(\frac{x_4}{m}\right)^2\right]$$

yazılabilir. Yardımcı Teorem 2.2.1. den $m < p$ olduğu biliniyor. Böylelikle $1 < m < p$ eşitsizliğinden bahsedilebilir. Bu ise p nin asallığıyla çelişir.

$r > 0$ olsun. $|y_k| < \frac{1}{2}m$ olduğundan (2.22) den;

$$\frac{1}{4}m^2 + \frac{1}{4}m^2 + \frac{1}{4}m^2 + \frac{1}{4}m^2 > mr$$

olur. Buradan da $r < m$ elde edilir.

(2.18) ve (2.22) eşitlikleri terim terime çarpılır ve Euler Özdeşliği'i kullanılırsa

$$mr.mp = (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 +$$

$$(x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2 + (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2$$

olur. (2.21) den;

$$mr.mp = \underbrace{(x_1^2 + x_2^2 + x_3^2 + x_4^2)^2}_{\equiv 0 \pmod{m}} + \underbrace{(x_1x_2 - x_2x_1 + x_3x_4 - x_4x_3)^2}_{\equiv 0 \pmod{m}} +$$

$$\underbrace{(x_1x_3 - x_3x_1 + x_4x_2 - x_2x_4)^2}_{\equiv 0 \pmod{m}} + \underbrace{(x_1x_4 - x_4x_1 + x_2x_3 - x_3x_2)^2}_{\equiv 0 \pmod{m}}$$

$$\Rightarrow mr.mp = (mz_1)^2 + (mz_2)^2 + (mz_3)^2 + (mz_4)^2$$

olur. Son olarak;

$$pr = z_1^2 + z_2^2 + z_3^2 + z_4^2$$

elde edilir. Bu durum ise, $r < m$ ve $i = 1, 2, 3, 4$ olmak üzere $z_i \in \mathbb{Z}$ olduğundan m nin tanımıyla çelişir.

O halde $m = 1$ dir.

Böylelikle Yardımcı Teorem 2.2.2 nin ispatı biter.

Şimdi bu iki yardımcı teoremi ve Euler özdeşliğini kullanarak Bachet Teoremini ispatlayalım:

Her $n \in \mathbb{N}$ alalım. $n = p_1 p_2 ... p_k$ şeklinde asal çarpanlarına ayrılsın.

$k = 1$ için ispat açıktır.

$k = m$ için iddia doğru olsun. $n = p_1 p_2 ... p_m = x_1^2 + x_2^2 + x_3^2 + x_4^2 \; ; \; x_i \in \mathbb{Z}$

$k = m+1$ için iddia doğru mudur?

$$n = p_1 p_2 ... p_m . p_{m+1} = (x_1^2 + x_2^2 + x_3^2 + x_4^2) p_{m+1}$$

Yardımcı Teorem 2.2.2 den

$$n = p_1 p_2 ... p_m . p_{m+1} = (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2)$$

Euler Özdeşliğinden bu ifadenin dört tam karenin toplamı şeklinde yazılabildiği biliniyor.

Böylelikle Bachet Teoreminin ispatı tamamlanmış olur.

Yardımcı Teorem 2.2.3. $n, N \in \mathbb{N}$ olmak üzere, N herhangi bir doğal sayının $n.$ kuvvetinden farklıysa , $\sqrt[n]{N}$ bir irrasyonel sayıdır.

İspat. $\sqrt[n]{N}$ rasyonel olsun. Bu durumda;

$$\sqrt[n]{N} = \frac{a}{b} \text{ dir. } (b \neq 0 \text{ ve } (a,b) = 1; a, b \in \mathbb{Z} \;)$$

$$\Rightarrow N = \frac{a^n}{b^n} \text{ olur.}$$

$N \in \mathbb{N}$ olduğundan; i) $b = 1$ olabilir.

$\Rightarrow N = a^n$ olur ki bu, N nin tanımıyla çelişir.

ii)$b \neq 1$ ve $b \mid a$ olabilir.

$\Rightarrow$ Bu ise $(a,b) = 1$ olmasıyla çelişir.

O halde kabulümüz yanlıştır. $\sqrt[n]{N}$ irrasyoneldir.

Şimdi aşağıda Dirichlet'nin Çekmece İlkesi'ni kullanarak Teorem 2.2.2. nin ispatı için gerekli olan bir eşitsizliği elde edeceğiz:

a , herhangi bir reel sayı olsun. $0-1$ aralığını t tane eşit parçaya bölelim. Oluşan her bir alt aralık için aralığın sol uç noktası aralığa dahildir, sağ uç nokta dahil değildir.

$$\left[0,\frac{1}{t}\right)\cup\left[\frac{1}{t},\frac{2}{t}\right)\cup\left[\frac{2}{t},\frac{3}{t}\right)\cup\ldots\cup\left[\frac{t-1}{t},1\right)$$

$y\geq 0$ bir tam sayı, x de $x\geq ay$ eşitsizliğini sağlayan en küçük tam sayı olsun. Bu durumda;

$$0\leq x-ay<1$$

olur. Yani $0-1$ aralığının içine $x-ay$ biçiminde sayılar düştüğü görülür.

y tam sayısına $\{0,1,\ldots,t\}$ kümesinden değerler verilirse, toplamda $t+1$ tane $x-ay$ biçiminde sayı elde edilmiş olur..

Bu durumda t tane eşit alt aralıktan oluşan $0-1$ aralığına bu $t+1$ tane sayı yerleştirilmek istenirse, bu alt aralıklardan en az bir tanesi, $t+1$ tane sayıdan en az iki tanesini içerir. Dolayısıyla, $h\leq t$ olacak şekilde bir h doğal sayısı; x',y' ve x'',y'' tam sayı çiftleri vardır ki aşağıdaki eşitsizlikler sağlanır:

$$\frac{h-1}{t}\leq x'-ay'<\frac{h}{t}\quad ;\quad \frac{h-1}{t}\leq x''-ay''<\frac{h}{t}$$

Bu iki eşitsizlik de aynı aralığa düşen iki sayıyı gösteriyor. Bu sayıların farkı yine bu aralığa düşecektir. Her bir alt aralığın boyu $\frac{1}{t}$ olduğundan, bu sayıların farkı aşağıdaki eşitsizliği sağlar:

$$\frac{-1}{t}\leq x''-x'+a(y'-y'')<\frac{1}{t}$$

$x''-x'=x$ ve $y''-y'=y$ diyelim. O halde,

$$|x-ay|<\frac{1}{t} \qquad (2.23)$$

yazılabilir. y ye $\{0,1,\ldots,t\}$ kümesinden değerler verildiği belirtilmişti.

$y''>y'$ olduğu varsayılırsa; $y''-y'=y$ olduğundan y sayısı $\{1,2,\ldots,t\}$ kümesinden değerler alır.

Böylelikle şu sonuç elde edilir:

Herhangi bir a reel sayısına ve her t doğal sayısına $|x-ay|<\frac{1}{t}$ eşitsizliğini sağlayan en az bir tane x ve y tam sayı çifti karşılık gelir. Buradan ayrıca aşağıdaki eşitsizlik elde edilir:

$$y \le t \Rightarrow \frac{1}{t} \le \frac{1}{y} \Rightarrow |x-ay| < \frac{1}{y} \Rightarrow \left|\frac{x}{y} - a\right| < \frac{1}{y^2} \qquad (2.24)$$

Burada (2.23) ve (2.24) eşitsizliklerinden (x,y)=1 dir.

(x,y)=d>1 olsun. $x = md$ ve $y = nd$ olacak şekilde $m, n \in \mathbb{Z}$ vardır.

$x \ge ay \ge \|a\| y$ yazılabilir. $\|a\| y = x - 1$

$\|a\| = s;\ s \in \mathbb{Z}$

$x - 1 = sy \Rightarrow md - 1 = snd$

$\Rightarrow d(m - sn) = 1$ olur. Böylelikle çelişki elde edilir.

$\Rightarrow (x, y) = 1$ olmalı.

a keyfi bir reel sayı olarak alınmıştı. Eğer a rasyonel bir sayı ise;

$b > 0$ ve $(\alpha, b) = 1$ olmak üzere $a = \frac{\alpha}{b}$ yazılabilir.

$$\Rightarrow \left|\frac{x}{y} - \frac{\alpha}{b}\right| = \frac{|bx - \alpha y|}{yb}$$

$\Rightarrow a = \frac{\alpha}{b} \ne \frac{x}{y}$ ve $y > 0$ olmak üzere

$\Rightarrow \frac{|bx - \alpha y|}{yb} \ge \frac{1}{yb}$ olur.

(2.24) den $\frac{1}{yb} < \frac{1}{y^2}$ olur. $\Rightarrow \frac{1}{b} < \frac{1}{y} \Rightarrow y < b$ olur.

O halde (2.24) için (x,y)=1 olmak üzere sonlu tane x ve y tam sayı çiftine bağlı çözüm vardır.

Buradan, (2.24) eşitsizliği sağlanıyorsa, $y < b$ sonucu da elde edilir.

Teorem 2.2.2. a bir irrasyonel sayı ise, (2.24) in $(x, y) = 1$ olmak üzere sonsuz tane x, y tam sayı çözümü vardır (*Nagell, 1964, sy 37*).

İspat. $t_1 \in \mathbb{N}$ olsun. Yukarıda elde edilen sonuçtan $(x_1, y_1) = 1$ olacak şekilde $x_1, y_1 \in \mathbb{Z}$ tam sayı çifti belirlenebilir, öyleki;

$$\eta_1 = \left| \frac{x_1}{y_1} - a \right| < \frac{1}{y_1 t_1} \quad (1 \le y_1 \le t_1)$$

olur. a irrasyonel olduğundan $\frac{x_1}{y_1} \neq a$ dır. Dolayısıyla, $\eta_1 \neq 0$ dır.

Bu durumda $t_2 > \frac{1}{\eta_1}$ koşulunu sağlayan bir $t_2 \in \mathbb{N}$ seçilebilir ve $(x_2, y_2) = 1$ koşulunu sağlayan $x_2, y_2 \in \mathbb{Z}$ belirlenebilir, öyleki;

$$\eta_2 = \left| \frac{x_2}{y_2} - a \right| < \frac{1}{y_2 t_2} \le \frac{1}{t_2} < \eta_1 \quad (1 \le y_2 \le t_2)$$

Bu şekilde devam edilirse;

$\eta_1 > \eta_2 > \ldots > \eta_i > \ldots$ şeklinde azalan bir sonsuz dizi elde edilir (azalan pozitif sayı zinciri de denebilir).

$$\eta_i = \left| \frac{x_i}{y_i} - a \right| \Rightarrow \eta_i < \frac{1}{y_i^2}$$

O halde sonsuz tane (x_i, y_i) tam sayı çifti bulunur. Böylelikle ispat tamamlanmış olur.

Not: Bu ispatla, aynı zamanda bir irrasyonel sayıya $\frac{x_i}{y_i}$ rasyonel sayılarıyla yaklaşma yöntemi verilmiş olur.

2.3. $x^2 - Dy^2 = 1$ DİOFANT DENKLEMİ

Yardımcı Teorem 2.3.1. D, tam kare olmayan herhangi bir doğal sayı ise, aşağıdaki eşitsizliği sağlayan sonsuz tane x ve y doğal sayı çifti vardır.

$$\left| x^2 - Dy^2 \right| < 1 + 2\sqrt{D}$$

(*Nagell, 1964, sy 195*).

İspat. Yardımcı Teorem 2.2.3. i hatırlayalım. $n=2$ ve D tam kare olamayan bir doğal sayı. O halde $\sqrt{D}$ bir irrasyoneldir.

Teorem 2.2.2. den de şu söylenebilir:

$$\left|\frac{x}{y}-\sqrt{D}\right|<\frac{1}{y^2}$$

Eşitsizliğini sağlayan sonsuz tane x ve y tam sayı çifti vardır. Ayrıca,

$$\left|\frac{x}{y}+\sqrt{D}\right|=\left|\frac{x}{y}-\sqrt{D}+2\sqrt{D}\right|<\frac{1}{y^2}+2\sqrt{D}$$

yazılabilir. Dolayısıyla,

$$\begin{aligned}\left|x^2-Dy^2\right| &= \left|x-y\sqrt{D}\right|\left|x+y\sqrt{D}\right| \\ &< \frac{1}{y}\left(\frac{1}{y}+2y\sqrt{D}\right) \\ &= \frac{1}{y^2}+2\sqrt{D} \\ &\le 1+2\sqrt{D}\end{aligned}$$

olur. Böylelikle ispat tamamlanmış olur.

Teorem 2.3.1. $D\in\mathbb{N}$ tam kare değil ise $x^2-Dy^2=1$ denklemini sağlayan en az bir tane x,y doğal sayı çifti vardır (*Nagell, 1964, sy 195-197*).

İspat. $x^2-Dy^2<1+2\sqrt{D}$ eşitsizliğini sağlayan sonsuz tane x,y tam sayı çifti olduğunu görmüştük. Bu durumda en az bir tane $k\neq 0$ tam sayısı için aşağıdaki eşitlik sağlanır:

$$x^2-Dy^2=k \tag{2.25}$$

Bu eşitliği sağlayan sonsuz tane x_i, y_i tam sayı çiftinden en az iki tanesi şu koşulu sağlar:

$$\left.\begin{aligned}x_1 &\equiv x_2 \pmod{|k|} \\ y_1 &\equiv y_2 \pmod{|k|}\end{aligned}\right\} \tag{2.26}$$

x_1, x_2, y_1, y_2 sayılarının modülo $|k|$ ya göre olası kalanları teker teker incelendiğinde toplam k^4 farklı durum ortaya çıkar.

$x^2 - Dy^2 = k$ eşitliğini sağlayan x_1, y_1 tam sayı çifti alınırsa,

$$x_1^2 - Dy_1^2 = k$$

olur. (2.26) kongrüans sisteminden de yararlanarak k^4 tane farklı durumdan $x_1 = x_2$ ve $y_1 = y_2$ durumu da göz önüne alındığında,

$$x_2^2 - Dy_2^2 = k$$

Olacak şekilde x_2, y_2 tam sayı çifti vardır.

$$x_1^2 - Dy_1^2 = x_2^2 - Dy_2^2 = k \tag{2.27}$$

$$(x_1 - y_1\sqrt{D})(x_2 + y_2\sqrt{D}) = x_1x_2 - y_1y_2D + (x_1y_2 - x_2y_1)\sqrt{D} \tag{2.28}$$

(2.26) ve (2.27) den,

$$x_1x_2 - y_1y_2D \equiv x_1^2 - y_1^2D \equiv 0 \pmod{|k|}$$

ve

$$x_1y_2 - x_2y_1 \equiv x_1y_1 - x_1y_1 \equiv 0 \pmod{|k|}$$

yazılabilir. Dolayısıyla;

$$x_1x_2 - y_1y_2D = ku$$

$$x_1y_2 - x_2y_1 = kv$$

olacak şekilde $u, v \in \mathbb{Z}$ vardır.

Elde edilen bu son iki eşitlik (2.28) de yerine yazılırsa,

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

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

eşitlikleri elde edilir. Bu son iki eşitlik terim terime çarpılırsa,

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

olur.

O halde;

$$(u^2 - Dv^2) = 1$$

dir. (Böylelikle en az bir tane x, y tam sayısı bulunmuş olur.)

Burada $v \neq 0$ dır. $v = 0$ olsa;

$$x_1y_2 = x_2y_1 \quad \text{ve} \quad k^2 = k^2u^2 \Rightarrow u = \mp 1$$

olur.

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

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

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

olur. Buradan $|x_1| = |x_2|$ ve $|y_1| = |y_2|$ elde edilir.

Yani sadece bu eşitlikler için iddianın sağlandığı sonucu bulunur. Oysa sonsuz tane x, y tam sayısı olduğu biliniyor ve bunlar arasından $|x_1| \neq |x_2|$ ve $|y_1| \neq |y_2|$ koşullarına göre de seçim yapılabilir. O halde $v \neq 0$ dır.

Böylelikle ispat tamamlanmış olur.

Tanım 2.3.1. $D, k \in \mathbb{Z}$ olmak üzere $x^2 - Dy^2 = k$ tipindeki denklemlere "Pell Denklemleri" denir.

$x^2 - Dy^2 = 1$ biçimindeki Pell Denklemlerini incelerken D tam kare olmayan bir doğal sayı olarak alınacaktır.

$x = u$ ve $y = v$ tam sayıları $x^2 - Dy^2 = k$ denklemini sağlıyorsa $u + v\sqrt{D}$ bu denklemin bir çözümüdür. $u = u'$ ve $v = v'$ olmak üzere $u + v\sqrt{D}$ ile $u' + v'\sqrt{D}$ çözümleri eşittir.

$u + v\sqrt{D} > u' + v'\sqrt{D}$ ise 1. çözüm 2. çözümden büyüktür.

Tanım 2.3.2.(Temel Çözüm)

$$x^2 - Dy^2 = 1 \tag{2.29}$$

denkleminin tüm $x + y\sqrt{D}$ çözümleri arasından x ve y nin pozitif olduğu çözümler alınsın. Bu çözümlerden en küçüğü

$$x_1 + y_1\sqrt{D}$$

ile gösterilsin. Bu çözüme (2.29) ın temel çözümü denir.

Şimdi, (2.29) ile verilen Pell Denkleminin, temel çözümü yardımıyla tüm çözümlerini bulmaya yönelik bir teorem ispatlanacaktır.

Teorem 2.3.2. (2.29) ın sonsuz tane $x+y\sqrt{D}$ çözümü vardır. x ve y pozitif tam sayılar olmak üzere bu çözümlerin hepsi aşağıdaki formülden elde edilir.

$$x_n + y_n\sqrt{D} = (x_1 + y_1\sqrt{D})^n \tag{2.30}$$

(2.30) da $x_1 + y_1\sqrt{D}$ ile (2.29) ın temel çözümü gösterilmektedir. Ayrıca $n \in \mathbb{N}$ olmak üzere;

$$\left.\begin{aligned} x_n &= x_1^{\,n} + \sum_{k=1} \binom{n}{2k} x_1^{\,n-2k} y_1^{\,2k} D^k \\ y_n &= \sum_{k=1} \binom{n}{2k-1} x_1^{\,n-2k+1} y_1^{\,2k-1} D^{k-1} \end{aligned}\right\}$$

dir (*Nagell, 1964, sy 198-199*).

İspat. (2.30) dan,

$$x_n - y_n\sqrt{D} = (x_1 - y_1\sqrt{D})^n \tag{2.31}$$

(2.30) ile (2.31) terim terime çarpıldığında,

$$\begin{aligned} x_n^{\,2} - y_n^{\,2} D &= (x_1 - y_1\sqrt{D})^n (x_1 + y_1\sqrt{D})^n \\ &= \left[(x_1 - y_1\sqrt{D})(x_1 + y_1\sqrt{D}) \right]^n \end{aligned}$$

olur. $x_1 + y_1\sqrt{D}$ (2.29) ın temel çözümü olduğundan;

$$x_n^{\,2} - D y_n^{\,2} = 1$$

olur. Bu durumda $x_n + y_n\sqrt{D}$ (2.29) ın bir çözümüdür.

Böylelikle (2.30) kullanılarak (2.29) ın bir çözümü elde edildi.

Şimdi $n \in \mathbb{N}$ ve $x_n, y_n \in \mathbb{N}$ olmak üzere, (2.30) dan elde edilemeyen bir $x_n + y_n\sqrt{D}$ çözümünün olmadığı gösterilecektir:

u ve v birer doğal sayı olmak üzere $u + v\sqrt{D}$ nin (2.29) için (2.30) dan elde edilmemiş bir çözüm olduğunu varsayalım:

Bu durumda aşağıdaki eşitsizliği sağlayan bir $n \in \mathbb{N}$ vardır.

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

(2.30) dan;

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

olur. Eşitsizliğin her üç tarafını $x_n - y_n\sqrt{D}$ ile çarpalım:

(Bunun için $x_n - y_n\sqrt{D} > 0$ olmalı. $x_n + y_n\sqrt{D} = (x_1 + y_1\sqrt{D})^n$ dir.

$x_1 + y_1\sqrt{D}$ (2.29) ın temel çözümü olduğundan $x_1, y_1 > 0$ dır. Buradan $x_n + y_n\sqrt{D} > 0$ olur.($x_n^2 - Dy_n^2 = (x_n - \sqrt{D}y_n)\underbrace{(x_n + \sqrt{D}y_n)}_{>0} = 1$ olduğundan $x_n - y_n\sqrt{D} > 0$ olmalıdır.)

Buradan,

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

$$1 < \left(u + v\sqrt{D}\right)\left(x_n - y_n\sqrt{D}\right) < \left(x_1 - y_1\sqrt{D}\right) \qquad (2.32)$$

$(u + v\sqrt{D})\ (x_n - y_n\sqrt{D}) = x + y\sqrt{D}$ diyelim. O halde,

$$x = ux_n - vy_n D \text{ ve } y = vx_n - uy_n$$

olur. O halde bu eşitliklerden yararlanarak aşağıdaki eşitlik de yazılabilir:

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

Bu iki eşitlik taraf tarafa çarpılırsa,

$$\underbrace{(u^2 - Dv^2)}_{=1}\ \underbrace{(x_n^2 - Dy_n^2)}_{=1} = x^2 - Dy^2 = 1$$

olur. Bu durumda $x + y\sqrt{D}$ de (2.29) ın bir çözümüdür. (2.32) den

$$x + y\sqrt{D} > 1$$

olduğu görülür. Öte yandan; (2.29) dan;

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

olur. Bu eşitsizliklerden $x > 0$ ve $y > 0$ olduğu görülür, şöyle ki

$$\left.\begin{array}{l} x + \sqrt{D}y > 0 \\ x - \sqrt{D}y > 0 \end{array}\right\} \Rightarrow\ 2x > 0 \Rightarrow x > 0$$

$$\left.\begin{array}{l} x + \sqrt{D}y > 1 \\ x - \sqrt{D}y < 1 \end{array}\right\} \Rightarrow\ \sqrt{D}y - x > -1 \Rightarrow 2\sqrt{D}y > 0 \Rightarrow y > 0$$

olur. Son olarak; (2.32) den,

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

olur. Bu ise $x_1 + y_1\sqrt{D}$ nin (2.29) ın temel çözümü olmasıyla çelişir.

Böylelikle Teorem 2.3.2. nin ispatı tamamlanmış olur.

D sayısı verildiğinde (2.29) ın $x_1 + y_1\sqrt{D}$ temel çözümü denemeyle bulunabilir. Örneğin (2.29) ,

$$x^2 = 1 + Dy^2$$

şeklinde yazılabilir. y ye değerler vererek (1,2,3,…) eşitliğin sağ tarafında tam kare bir ifade yakalanıncaya kadar olası minimum x ve y değerleri bulunabilir. Ancak bu, görüldüğü gibi, kullanışlı bir yöntem değildir. Örnek vermek gerekirse;

$D = 94$ için (2.29) ın temel çözümü,

$$2143295 + 221064\sqrt{94}$$

dir. Dolayısıyla daha başka yöntemler ortaya çıkmıştır. Mesela Euler; gösterdiği yöntemde temel çözümü bulmak için $\sqrt{D}$ nin sonlu sürekli kesir açılımını kullanır. Bu yöntem diğerine göre oldukça kullanışlıdır. Bu yöntemin nasıl uygulandığına yönelik detaylı bilgi 3. Bölüm'de incelenecektir.

D nin belli değerleri için ise temel çözüm hemen bulunabilir. Örneğin, $u > 1$ bir tam sayı olmak üzere,

$$x^2 - (u^2 - 1)y^2 = 1$$

denklemini düşünelim:

$$x^2 = 1 + (u^2 - 1)y^2$$

olur.

$y_1 = 1$ için,

$$x^2 = 1 + (u^2 - 1) \Rightarrow x_1 = u$$

$$\Rightarrow x_1 + y_1\sqrt{D} = u + \sqrt{u^2 - 1}$$

bulunur.

Sıradaki teoremle, daha genel bir yöntem verilecektir:

Teorem 2.3.3. D tam kare olmayan bir doğal sayı olsun. ξ ve η,

$$\xi > \frac{1}{2}\eta^2 - 1 \tag{2.33}$$

eşitsizliğini sağlayan doğal sayılar ve $a = \xi + \eta\sqrt{D}$,

$$x^2 - Dy^2 = 1 \tag{2.34}$$

nin bir çözümü ise, a sayısı (2.34) in temel çözümüdür (*Nagell, 1964, sy 200*).

.

İspat. $\eta = 1$ için,

$$a = \xi + \eta\sqrt{D}$$

(2.34) in bir çözümü ise,

$$(\xi + \eta\sqrt{D})(\xi - \eta\sqrt{D}) = 1$$

olur. O halde,

$$\xi^2 - D\eta^2 = 1 \Rightarrow \xi^2 = 1 + D\eta^2$$

$$\Rightarrow \xi^2 = 1 + D$$

dir. Buradan, tam kare olmayan $D \in \mathbb{N}$ belli olduktan sonra ξ bulunabilir.

$\eta > 1$ için,

Kabul edelim ki,

$$\xi + \eta\sqrt{D}$$

(2.34) in temel çözüm olmayan bir çözümü olsun ve $1 \le y_1 < \eta$ olmak üzere $x_1 + y_1\sqrt{D}$ (2.34) in temel çözümü olsun. Bu durumda;

$$x_1^{\,2} - y_1^{\,2}D = 1 \quad \text{ve} \quad \xi^2 - \eta^2 D = 1$$

olur.

$$\Rightarrow D = \frac{x_1^{\,2} - 1}{y_1^{\,2}} = \frac{\xi^2 - 1}{\eta^2}$$

$$\Rightarrow x_1^{\,2}\eta^2 - \eta^2 = \xi^2 y_1^{\,2} - y_1^{\,2}$$

$$\Rightarrow x_1^{\,2}\eta^2 - \xi^2 y_1^{\,2} = \eta^2 - y_1^{\,2} = d$$

$y_1 < \eta$ olduğundan $d > 0$ dır.

$$\Rightarrow \underbrace{(x_1\eta + \xi y_1)}_{=d_1}\underbrace{(x_1\eta - \xi y_1)}_{=d_2} > 0 \quad (x_1, y_1, \xi, \eta \in \mathbb{N})$$

O halde $d_1, d_2 \in \mathbb{N}$ olmak üzere $d = d_1 d_2$ olur.

Buradan; $x_1\eta + \xi y_1 - x_1\eta + \xi y_1 = 2\xi y_1$ olduğundan $d_1 - d_2 \in \mathbb{N}$ dir.

$$\Rightarrow \xi = \frac{d_1 - d_2}{2y_1} \text{ olur.}$$

$$\Rightarrow d_1 - d_2 < d_1 < d_1 d_2$$

$$\Rightarrow d_1 - d_2 + 1 \le d_1 d_2 \Rightarrow d_1 - d_2 \le \underbrace{d_1 d_2}_{=d} - 1$$

$$\Rightarrow \xi = \frac{d_1 - d_2}{2y_1} \le \frac{d-1}{2y_1} = \frac{\eta^2 - y_1^{\,2} - 1}{2y_1} = \frac{\eta^2}{2y_1} - \underbrace{\left(\frac{y_1^{\,2}+1}{2y_1}\right)}_{\ge 1} \le \frac{\eta^2}{2} - 1$$

Bu ise (2.33) ile çelişir. $\eta = y_1$ ve $\xi = x_1$ olmalıdır. Böylelikle ispat tamamlanmış olur.

2.4. $x^2 - Dy^2 = -1$ DİOFANT DENKLEMİ

D tam kare olmayan bir doğal sayı ise,

$$x^2 - Dy^2 = 1 \tag{2.35}$$

Diofant denklemi her zaman çözülebilirdir. Ancak,

$$\xi^2 - D\eta^2 = -1 \tag{2.36}$$

Diofant denklemi belli D değerleri için çözülebilirdir.

Tanım 2.4.1. Bir D tam sayısı için (2.36) çözülebilir ise bu Diofant denkleminin ξ ve η ya bağlı pozitif çözümleri arasından en küçüğü olan $\xi_1 + \eta_1\sqrt{D}$ sayısına (2.36) in temel çözümü denir.

Önerme 2.4.1. (2.36) in herhangi bir çözümünün karesi (2.35) in bir çözümüdür.

İspat. $\xi + \eta\sqrt{D}$ (2.36) in bir çözümü olsun. Bu durumda;

$$(\xi + \eta\sqrt{D})(\xi - \eta\sqrt{D}) = -1$$

dir. Bu eşitlikte her iki tarafın karesi alınırsa,

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

olur. Yani $(\xi + \eta\sqrt{D})^2$ (2.35) in bir çözümüdür.

Teorem 2.4.1. D tam kare olmayan bir doğal sayı olsun. (2.36) in çözülebilir olduğunu, $\xi_1 + \eta_1\sqrt{D}$ nin de (2.36) in temel çözümü olduğunu varsayalım. Bu durumda;

$$x_1 + y_1\sqrt{D} = (\xi_1 + \eta_1\sqrt{D})^2 = \xi_1^2 + D\eta_1^2 + 2\xi_1\eta_1\sqrt{D} \tag{2.37}$$

sayısı (2.35) in temel çözümüdür. Ayrıca;

$$\left.\begin{aligned} \xi_n &= \xi_1^n + \sum_{k=1}\binom{n}{2k}\xi_1^{n-2k}\,\eta_1^{2k}\,D^k \\ \eta_n &= \sum_{k=1}\binom{n}{2k-1}\xi_1^{n-2k+1}\,\eta_1^{2k-1}\,D^{k-1} \end{aligned}\right\} \tag{2.38}$$

olmak üzere;

$$\xi_n + \eta_n\sqrt{D} = (\xi_1 + \eta_1\sqrt{D})^n \tag{2.39}$$

eşitliğinden;

1) n tek tam sayı ise (2.36) nin ξ ve η pozitif sayılarına bağlı tüm çözümleri elde edilir.
2) n çift tam sayı ise (2.35) nin $x = \xi_n$ ve $y = \eta_n$ pozitif sayılarına bağlı tüm çözümleri elde edilir.

(*Nagell, 1964, sy 201-203*).

İspat. (2.39) dan $\xi_n - \eta_n\sqrt{D} = (\xi_1 - \eta_1\sqrt{D})^n$ olduğu görülür. (2.39) ile bu eşitliği taraf tarafa çarpalım:

$$\xi_n^2 - D\eta_n^2 = (-1)^n$$

olur. Dolayısıyla n nin tekliğine ya da çiftliğine bağlı olarak $\xi_n + \eta_n\sqrt{D}$ sayısı (2.35) in ya da (2.36) nin bir çözümüdür.

$$(\xi_1^2 - \eta_1^2 D) = -1 \Rightarrow -\xi_1^2 + \eta_1^2 D = 1$$

$$(\eta_1\sqrt{D} - \xi_1)(\eta_1\sqrt{D} + \xi_1) = 1$$

olur. Buradan $-\xi_1 + \eta_1\sqrt{D}$ sayısının 1 den küçük bir pozitif sayı olduğu görülür.

Şimdi (2.35) ile (2.36) nin temel çözümlerinin (2.37) ile ilişkili olmadığını varsayalım.

$$1 < x_1 + y_1\sqrt{D} < (\xi_1 + \eta_1\sqrt{D})^2$$

olur. $(\xi_1 + \eta_1\sqrt{D})^2$ sayısının (2.35) in bir çözümü olduğu Önerme 2.4.1. de gösterildi. Dolayısıyla (2.37) eşitliğinin gerçeklenmemesi halinde, yukarıdaki eşitsizlik elde edilir. Bu eşitsizliğin her üç tarafını $-\xi_1 + \eta_1\sqrt{D}$ pozitif sayısıyla çarpalım:

$$\xi_0 = -\xi_1 x_1 + \eta_1 y_1 D \quad \text{ve} \quad \eta_0 = \eta_1 x_1 - \xi_1 y_1$$

olmak üzere,

$$-\xi_1 + \eta_1\sqrt{D} < \xi_0 + \eta_0\sqrt{D} < \xi_1 + \eta_1\sqrt{D} \tag{2.40}$$

eşitsizliği elde edilir.

$$(\xi_0 + \eta_0\sqrt{D})(\xi_0 - \eta_0\sqrt{D}) = (-\xi_1 x_1 + \eta_1 y_1 D)^2 - D(\eta_1 x_1 - \xi_1 y_1)^2$$

$$= (\xi_1 x_1)^2 - 2\xi_1 x_1 \eta_1 y_1 D + (\eta_1 y_1 D)^2 - D(\eta_1 x_1)^2 + 2\eta_1 x_1 \xi_1 y_1 D - D(\xi_1 y_1)^2$$

$$= (\xi_1 x_1)^2 + (\eta_1 y_1 D)^2 - D(\eta_1 x_1)^2 - D(\xi_1 y_1)^2$$

$$= \xi_1^2 \underbrace{(x_1^2 - D y_1^2)}_{=1} - D\eta_1^2 \underbrace{(x_1^2 - D y_1^2)}_{=1}$$

$$= \xi_1^2 - D\eta_1^2 = -1$$

olur. Dolayısıyla ξ_0 ve η_0 (2.36) yi sağlar.

(2.40) eşitsizliğine dönecek olursak $-\xi_1 + \eta_1\sqrt{D}$ sayısı (2.36) nin negatif ξ ve pozitif η lara bağlı çözümleri arasından en büyük olanıdır. (Bu durum $\xi_1 + \eta_1\sqrt{D}$ sayısının (2.36) nin temel çözümü olmasının doğal bir sonucudur.)

$-\xi_1 + \eta_1\sqrt{D}$ ile $\xi_1 + \eta_1\sqrt{D}$ sayılarının özelliklerinden (2.40) eşitsizliği ile ilgili şu çelişkiler elde edilir:

i) $\xi_0 > 0$, $\eta_0 > 0$: $\xi_1 + \eta_1\sqrt{D}$ sayısının (2.36) nin temel çözümü olmasıyla çelişilir.

ii) $\xi_0 < 0$, $\eta_0 > 0$: $-\xi_1 + \eta_1\sqrt{D}$ sayısının (2.36) nin negatif ξ ve pozitif η lara bağlı çözümleri arasından en büyük olmasıyla çelişilir.

iii) $\xi_0 < 0$, $\eta_0 < 0$: ($\eta_1^2 D > \xi_1^2$ eşitsizliğiyle çelişilir.)

iv) $\xi_0 > 0$, $\eta_0 < 0$: ($x_1^2 > y_1^2 D$ eşitsizliğiyle çelişilir.)

v) $\xi_0 = 0$ ve $\eta_0 \neq 0$ olsun: $-\eta_0^2 D = -1$ olur. D tam kare olmayan bir doğal sayı, η_0 da bir tam sayı olduğundan bu eşitlik gerçeklenmez.

$\xi_0 \neq 0$ ve $\eta_0 = 0$ olsun: $\xi_0^2 = -1$ çelişkisi elde edilir.

vii) $\xi_0 = \eta_0 = 0$ olsun: Bu durum da ξ_0 ile η_0 ın (2.36) nin çözümü olmasıyla çelişir.

O halde kabulümüz yanlıştır. (2.37) eşitliği gerçeklenir. Yani (2.36) nin temel çözümünün karesi (2.35) in herhangi bir çözümü olmakla kalmaz, özel olarak (2.35) in temel çözümüdür.

Şimdi, u ve v pozitif sayılar olmak üzere $u+v\sqrt{D}$ nin (2.36) nin (2.39) eşitliğinden elde edilemeyen bir çözümü olduğunu varsayalım.

Bu durumda aşağıdaki eşitsizliği sağlayan bir m doğal sayısı vardır:

$$(\xi_1+\eta_1\sqrt{D})^{2m-1} < u+v\sqrt{D} < (\xi_1+\eta_1\sqrt{D})^{2m+1}$$

$(\xi_1-\eta_1\sqrt{D})^{2m}=\xi_{2m}-\eta_{2m}\sqrt{D}$ pozitif sayısını eşitliğin her üç tarafıyla çarpalım:

$$\xi_0 = u\xi_{2m}-v\eta_{2m}D \text{ ve } \eta_0 = v\xi_{2m}-u\eta_{2m}$$

olmak üzere,

$$-\xi_1+\eta_1\sqrt{D} < \xi_0+\eta_0\sqrt{D} < \xi_1+\eta_1\sqrt{D} \tag{2.41}$$

olur. Burada (2.40) eşitsizliğinde olduğu gibi ξ_0 ve η_0 ın (2.36) yi sağladığı gösterilebilir. (2.41) in gerçeklenmeyeceğini gösterilmişti. O halde kabulümüz yanlıştır. Böylelikle ispat tamamlanmış olur.

Teorem 2.4.2. p, $p\equiv 1 \pmod 4$ koşulunu sağlayan bir asal sayı ise,

$$\xi^2-p\eta^2=-1 \tag{2.42}$$

Diofant Denklemi ξ ve η tam sayılarına göre çözülebilirdir (*Nagell, 1964, sy 203-204*).

İspat. $x_1+y_1\sqrt{p}$ **;** $x^2-py^2=1$ in temel çözümü olsun.

$$x_1^{\,2}-py_1^{\,2}=1 \Rightarrow x_1^{\,2}-1=py_1^{\,2} \tag{2.43}$$

olur. x_1 sayısı ya tek ya da çift bir doğal sayıdır.

x_1 çift olsa; $x_1=2k$ olacak şekilde $k\in\mathbb{N}$ vardır.

$x_1^{\,2}-py_1^{\,2}=1$ olduğundan x_1 ile y_1 in aynı anda çift olamayacağı görülür. Dolayısıyla $y_1=2m+1$ olacak şekilde $m\in\mathbb{Z}$ vardır. Buradan,

$$4k^2-(2m+1)^2p=1 \Rightarrow 4k^2-(4m^2+4m+1)p=1$$

$$\Rightarrow 4k^2-4m^2p-4mp-p=1$$

olur. Burada modülo 4 için kongrüansa geçecek olursak;

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

olur. Bu ise hipotezle çelişir.

$y_1=1$ için, $4k^2-1=p$ olur. Buradan da $p\equiv -1 \pmod 4$ koşulu elde edilir. Tekrar hipotezle çelişki elde edilir. O halde x_1 tek olur. Bu durumda,

$(x_1-1),(x_1+1)$ sayıları ardışık çift sayılardır.

$\xi^2-p\eta^2=-1$ çözülebilir ise temel çözümü olan $\xi+\sqrt{p}\eta$ sayısının karesi $x^2-py^2=1$ in temel çözümünü verir.

$$x_1+y_1\sqrt{p}=(\xi+\eta\sqrt{p})^2 \Rightarrow x_1=\xi^2+p\eta^2\ ;\ y_1=2\xi\eta$$

olur. Bu eşitliklerden,

$$x_1-1=2\xi^2\ ;$$

$$x_1+1=2\xi^2+2=2(\xi^2+1)=2p\eta^2$$

$$(x_1-1)(x_1+1)=2\xi^2.2p\eta^2=2p\eta^2.2\xi^2$$

bulunur.

Bu durumda, $x_1\pm1=2\xi^2$ ve $x_1\mp1=2p\eta^2$ olur. Bu iki eşitlikte x_1 i yok edecek olursak,

$$\xi^2-p\eta^2=\pm1$$

eşitliği bulunur.

$\xi^2-p\eta^2=1$ olsa; $\xi+\sqrt{p}\eta$ sayısı $x^2-py^2=1$ in pozitif bir çözümü olur. $y_1=2\xi\eta$ eşitliğinden $\eta<y_1$ olduğundan bu durum $x_1+y_1\sqrt{p}$ in temel çözüm olmasıyla çelişir. Yani $\xi^2-p\eta^2=-1$ olmalıdır, bu da ispatı tamamlar.

Örnek 2.4.1. $\xi^2-34\eta^2=-1$ Diofant denkleminin çözümünün olmadığını inceleyelim (*Nagell, 1964, sy 204*).

$x^2-34y^2=1$ in temel çözümünü bulmak için $x^2=34y^2-1$ eşitliğinde y ye sırasıyla 1,2,… değerleri verilir, ta ki eşitliğin sağ tarafı bir tam kare oluncaya kadar. Bu yöntemle $35+6\sqrt{34}$ in temel çözüm olduğu bulunur.

Teorem 2.4.1 den;

$$35+6\sqrt{34}=(\xi_1+\eta_1\sqrt{34})^2$$

dir.

$$\Rightarrow 35+6\sqrt{34}=\xi_1^{\,2}+2\sqrt{34}\xi_1\eta_1+34\eta_1^{\,2}$$

$$\Rightarrow 35=\xi_1^{\,2}+34\eta_1^{\,2}\ ;\ \ 6=2\xi_1\eta_1\Rightarrow\xi_1\eta_1=3$$

$$\xi_1=1,\eta_1=3\Rightarrow 35\neq1+34.9$$

$$\xi_1 = 3, \eta_1 = 1 \Rightarrow 35 \neq 9 + 34.1$$

Dolayısıyla çözüm yoktur.

Şu ana kadar, $k \in \mathbb{Z}$ ve D tam kare olmayan bir doğal sayı olmak üzere $x^2 - Dy^2 = k$ eşitliğiyle verilen Pell Denklemlerinde $k = \mp 1$ olma durumu incelendi. Bu denklemler için Teorem 2.4.1. ve Teorem 2.3.2. nin önemi vurgulandı, çünkü bu teoremler ile temel çözümün bilinmesi halinde diğer tüm çözümlerin bulunmasına yarayan (2.30), (2.37), (2.39) eşitlikleri verildi. Şimdi ise $C \in \mathbb{Z} - \{0\}$ olmak üzere $u^2 - Dv^2 = C$ denklemini inceleyeceğiz.

2.5. $u^2 - Dv^2 = C$ DİOFANT DENKLEMİ

D tam kare olmayan bir doğal sayı olsun. $C \in \mathbb{Z} - \{0\}$ olmak üzere,

$$u^2 - Dv^2 = C \tag{2.44}$$

Diofant Denklemini düşünelim. Denklemin çözülebilir olduğunu ve $u + v\sqrt{D}$ nin de bir çözüm olduğunu varsayalım. Eğer $x + y\sqrt{D}$,

$$x^2 - Dy^2 = 1 \tag{2.45}$$

denkleminin herhangi bir çözümü ise,

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

sayısı da (2.44) in bir çözümüdür. Bu sayıya $u + v\sqrt{D}$ ile ilgili çözüm denir.

Birbiriyle ilgili olan tüm çözümlerin kümesi (2.44) in bir çözüm sınıfını oluşturur. Teorem 2.3.2. den, her sınıf sonsuz çözüm içerir.

(2.44) in $u + v\sqrt{D}$ ve $u' + v'\sqrt{D}$ gibi herhangi iki çözümü verildiğinde aynı sınıfa ait olup olmadıklarına karar vermek mümkündür. Bu iki çözümün birbiriyle ilgili olmaları için gerek ve yeter koşul,

$$\frac{uu' - vv'D}{C} \text{ ve } \frac{vu' - uv'}{C}$$

sayılarının birer tam sayı olmasıdır.

Tanım 2.5.1. Eğer K, (2.44) için; $i=1,2,...$ olmak üzere $u_i+v_i\sqrt{D}$ çözümlerinden oluşan bir sınıf ise; $i=1,2,...$ olmak üzere $u_i-v_i\sqrt{D}$ çözümleri de bir sınıf oluşturur. Bu sınıf $\overline{K}$ ile gösterilir. K ve $\overline{K}$ sınıflarına eşlenik sınıflar denir.

Tanım 2.5.2. Eşlenik sınıflar genellikle farklıdır ancak bazen çakıştıkları olur. Çakışmaları halinde bu sınıflara belirsiz sınıflar adı verilir.

Bir K sınıfındaki tüm $u+v\sqrt{D}$ çözümleri arasından $u^*+v^*\sqrt{D}$ çözümünü alalım: v^*, K da yer alan v nin en küçük negatif olmayan değeri olsun. K belirsiz değilse (yani K ile $\overline{K}$ çakışmıyorsa) u^* tek türlü belirlidir, çünkü $-u^*+v^*\sqrt{D}$ $\overline{K}$ eşlenik sınıfına dahildir. K belirsiz ise, $u^*\geq 0$ eşitsizliğini belirterek tek türlü belirli u^* sayısı elde edilir.

Tanım 2.5.3. Yukarıdaki koşullara bağlı oluşturulan $u^*+v^*\sqrt{D}$ çözümüne, K sınıfının temel çözümü denir.

Uyarı 2.5.1. i) $u+v\sqrt{D}$, K sınıfına ait bir çözüm ve bu sınıfa ait temel çözüm $u^*+v^*\sqrt{D}$ olmak üzere, $|u^*|$ sayısı $|u|$ nun mümkün olan en küçük değerini alır.

ii) u^* ya da v^* sayısının sıfır olması durumu, yalnızca sınıfın belirsiz olması durumunda ortaya çıkar.

iii) $C=\pm 1$ ise sadece bir sınıf vardır ve o da belirsizdir (yani bu sınıf eşleniği ile çakışır).

Şimdi; (2.44) deki C sayısının pozitif olduğu durum için, $C=N$ alarak, aşağıdaki teoremi inceleyelim.

Teorem 2.5.1. Eğer $u+v\sqrt{D}$,

$$u^2-Dv^2=N \tag{2.46}$$

eşitliğiyle verilen Diofant Denkleminin K sınıfına ait temel çözümü ve $x_1+y_1\sqrt{D}$ de (2.45) in temel çözümü ise aşağıdaki eşitsizlikler vardır:

$$0\leq v\leq \frac{y_1}{\sqrt{2(x_1+1)}}.\sqrt{N} \tag{2.47}$$

$$0 < |u| \le \sqrt{\frac{1}{2}(x_1 + 1)N} \tag{2.48}$$

(*Nagell, 1964, sy 205-206*).

İspat. (2.47) ve (2.48) eşitsizlikleri bir K sınıfı için doğruysa, aynı eşitsizlikler eşlenik sınıf $\overline{K}$ için de doğrudur. Dolayısıyla u sayısı pozitif alınabilir. Buradan,

$$ux_1 - Dvy_1 = ux_1 - \sqrt{(u^2 - N)(x_1^2 - 1)} > 0 \tag{2.49}$$

olduğu görülür. Ayrıca, $u + v\sqrt{D}$ ile aynı sınıfta olan,

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

çözümünü düşünelim. $u + v\sqrt{D}$, K sınıfının temel çözümü, (2.49) dan $ux_1 - Dvy_1$ sayısı pozitif olduğundan aşağıdaki eşitsizlik vardır:

$$ux_1 - Dvy_1 \ge u \tag{2.50}$$

Bu eşitsizlikten,

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

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

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

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

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

Böylelikle (2.48) in sağlandığı görülür. (2.48) den, (2.47) nin de gerçeklendiği görülür.

Şimdi ise; (2.44) deki C sayısının negatif olduğu durum için, $C = -N$ alarak, aşağıdaki teoremi inceleyelim.

Teorem 2.5.2. Eğer $u + v\sqrt{D}$,

$$u^2 - Dv^2 = -N \tag{2.51}$$

eşitliğiyle verilen Diofant Denkleminin K sınıfına ait temel çözümü ve $x_1 + y_1\sqrt{D}$ de (2.45) in temel çözümü ise aşağıdaki eşitsizlikler gerçeklenir:

$$0 \le v \le \frac{y_1}{\sqrt{2(x_1 - 1)}}.\sqrt{N} \tag{2.52}$$

$$0 < |u| \le \sqrt{\frac{1}{2}(x_1 - 1)N} \tag{2.53}$$

(*Nagell, 1964, sy 206-207*).

İspat. Eğer (2.52) ve (2.53) eşitsizlikleri bir K sınıfı için doğruysa, aynı eşitsizlikler eşlenik sınıf $\overline{K}$ için de doğrudur. Dolayısıyla $u \ge 0$ alınabilir. Buradan da aşağıdaki eşitsizlikler yazılabilir:

$$(x_1 v)^2 = \left(y_1^2 + \frac{1}{D}\right)(u^2 + N) > y_1^2 u^2$$

$$\Rightarrow x_1 v - y_1 u > 0 \tag{2.54}$$

Ayrıca, $u + v\sqrt{D}$ ile aynı sınıfta olan,

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

çözümünü düşünelim. $u + v\sqrt{D}$, K sınıfının temel çözümü, (2.54) den $ux_1 - Dvy_1$ sayısı pozitif olduğundan aşağıdaki eşitsizlik vardır:

$$x_1 v - y_1 u \ge v \tag{2.55}$$

Bu eşitsizlikten,

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

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

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

bulunur. Böylelikle (2.53) nin gerçeklendiği görülür. (2.53) den, (2.52) nin de gerçeklendiği görülür.

Teorem 2.5.1. ve Teorem 2.5.2. in bir sonucu olarak aşağıdaki teorem verilebilir:

Teorem 2.5.3. $D, N \in \mathbb{N}$ olmak üzere D tam kare değil ise, (2.46) ve (2.51) Diofant denklemlerinin sonlu sayıda çözüm sınıfları vardır. Bu sınıfların temel çözümleri Teorem 2.5.1. ve Teorem 2.5.2. deki eşitsizlikler yoluyla sonlu sayıda denemeyle bulunabilir. Eğer $u^*+v^*\sqrt{D}$, K sınıfının temel çözümü ise, K nın tüm $u+v\sqrt{D}$ çözümleri aşağıdaki eşitlikten elde edilir:

$$u+v\sqrt{D}=\left(u^*+v^*\sqrt{D}\right)\left(x+y\sqrt{D}\right)$$

Burada $\left(x+y\sqrt{D}\right)$; ± 1 dahil, (2.45) in tüm çözümlerini tarar. (2.46) ya da (2.51) Diofant Denklemlerinin; (2.47) ve (2.48) ya da (2.51) ve (2.52) eşitsizliklerini sağlayan bir çözümü yoksa, hiç çözümü yoktur (*Nagell, 1964, sy 208*).

Teorem 2.5.1. ve Teorem 2.5.2. ye ek olarak aşağıdaki teorem verilebilir:

Teorem 2.5.4. p bir asal sayı ise,

$$u^2-Dv^2=\pm p \tag{2.56}$$

Diofant Denkleminin en çok bir tane $u+v\sqrt{D}$ çözümü vardır. Burada u ve v sırasıyla, $u\geq 0$ olmak üzere, (2.47) ve (2.48) ya da (2.52) ve (2.53) eşitsizliklerini sağlar.

(2.56) çözülebilir ise, p nin $2D$ yi bölüp bölmemesine göre, 1 ya da 2 tane çözüm sınıfı vardır (*Nagell, 1964, sy 208-209*).

İspat. Varsayalım ki, $u+v\sqrt{D}$ ve $u_1+v_1\sqrt{D}$ (2.56) nın Teorem 2.5.4. in ilk kısmını sağlayan çözümleri olsun. Dolayısıyla u, v, u_1 ve v_1 negatif değildir. Aşağıdaki denklemlerde D yok edilirse;

$$u^2-Dv^2=\pm p\,;\, {u_1}^2-D{v_1}^2=\pm p \tag{2.57}$$

olur. Buradan da,

$$u^2{v_1}^2-{u_1}^2v^2=\pm p\left({v_1}^2-v^2\right)$$

elde edilir. Dolayısıyla,

$$uv_1\equiv \pm u_1 v \pmod p \tag{2.58}$$

kongrüansı gerçeklenir. Ayrıca (2.57) deki eşitlikler terim terime çarpılırsa;

$$\left(uu_1 \mp Dvv_1\right)^2-D\left(uv_1 \mp u_1 v\right)^2=p^2$$

elde edilir. Buradan,

$$\left(\frac{uu_1 \mp Dvv_1}{p}\right)^2 - D\left(\frac{uv_1 \mp u_1 v}{p}\right)^2 = 1 \tag{2.59}$$

olur. Bu eşitlikte işaret (2.58) sağlanacak şekilde seçilir. Bu durumda (2.59) ın sol tarafındaki kare ifadeler tam sayıdır.

$$uv_1 \mp u_1 v \neq 0$$

ise, (2.59) dan,

$$\left|uv_1 \mp u_1 v\right| \geq y_1 p \tag{2.60}$$

bulunur.

Öte yandan; (2.47) ve (2.48) ya da (2.52) ve (2.53) eşitsizliklerinden,

$$\left|uv_1 \mp u_1 v\right| < y_1 p$$

bulunur ki bu eşitsizlik (2.60) ile çelişir.

$$uv_1 \mp u_1 v = 0$$

ise, bu eşitsizlik sadece $u = u_1$ ve $v = v_1$ için geçerlidir. Sonuç olarak; en çok iki tane çözüm sınıfı vardır. Şimdi de $u + v\sqrt{D}$ ile $u - v\sqrt{D}$ nin sırasıyla (2.47) ve (2.48) ya da (2.52) ve (2.53) eşitsizliklerini sağlayan çözümler olduğunu varsayalım. Bu çözümlerin ilgili olması için gerek ve yeter koşul p nin $2uv$ ve $u^2 + Dv^2 = 2Dv^2 \pm p$ sayılarını bölmesidir. $p \nmid v$ olduğundan $p \mid 2u$ ve $p \mid 2D$ dir. Ancak $p \mid 2u$ olması için de $p \mid 2D$ olması gerekir. Dolayısıyla, $u + v\sqrt{D}$ ile $u - v\sqrt{D}$ çözümlerinin aynı sınıfta olabilmesi için gerek ve yeter koşul $2D$ nin p nin bir katı olmasıdır.

Örnek 2.5.1.

$$u^2 - 2v^2 = 119 \tag{2.61}$$

Diofant Denklemini inceleyelim (*Nagell, 1964, sy 209*).

$$x^2 - 2y^2 = 1 \tag{2.62}$$

denkleminin temel çözümü $3 + 2\sqrt{2}$ dir. (2.62) in

$$11 + \sqrt{2}, -11 + \sqrt{2}, 13 + 5\sqrt{2}, -13 + 5\sqrt{2}$$

çözümleri (2.47) ve (2.48) eşitsizliklerini sağlar. Bu çözümlerin her birinin farklı sınıflara ait temel çözümler olduğu görülür. Dolayısıyla (2.61) in 4 tane çözüm sınıfı vardır.

Örnek 2.5.2.

$$u^2 - 6v^2 = -29 \tag{2.63}$$

Diofant Denklemini inceleyelim (*Nagell, 1964, sy 210*).

$$x^2 - 6y^2 = 1$$

denkleminin temel çözümü $5 + 2\sqrt{6}$ dır. (2.52) ve (2.53) eşitsizliklerinden,

$$5 + 3\sqrt{6}\,, -5 + 3\sqrt{6}$$

temel çözümleri elde edilir.

Örnek 2.5.3.

$$u^2 - 6v^2 = -2 \tag{2.64}$$

Diofant Denkleminin yalnız bir tane temel çözümü vardır. Bu çözüm $2 + \sqrt{6}$ dır, çünkü $2 + \sqrt{6}$ ve $-2 + \sqrt{6}$ çözümleri aynı belirsiz sınıfa aittir (*Nagell, 1964, sy 210*).

Örnek 2.5.4.

$$u^2 - 82v^2 = 23 \tag{2.65}$$

Diofant Denklemini inceleyelim (*Nagell, 1964, sy 210*).

$$x^2 - 82y^2 = 1 \tag{2.66}$$

denkleminin temel çözümü $163 + 18\sqrt{82}$ dir. (2.47) den

$$v < \frac{9}{2}\sqrt{\frac{46}{41}} < 5$$

eşitsizliği bulunur. (2.65) in $v = 1, 2, 3$ ya da 4 için çözümü yoktur. Dolayısıyla çözüm yoktur.

Teorem 2.5.5. $p; p \equiv 1$ ya da $-1 \pmod 8$ koşulunu sağlayan bir asal sayı ise

$$u^2 - 2v^2 = p \tag{2.67}$$

$$u < \sqrt{2p}, v < \sqrt{\frac{1}{2}p} \tag{2.68}$$

eşitlik ve eşitsizliklerini sağlayan $u, v \in \mathbb{N}$ vardır. Ayrıca,

$$u^2 - 2v^2 = -p \tag{2.69}$$

$$u < \sqrt{p}, v < \sqrt{p} \tag{2.70}$$

eşitlik ve eşitsizliklerini sağlayan $u, v \in \mathbb{N}$ vardır (*Nagell, 1964, sy 211*).

İspat. $p \equiv \pm 1 \pmod 8$ için $z^2 \equiv 2 \pmod p$ kongrüansı çözülebilir. O halde z bir çözüm ise Teorem 2.1.1. den,

$$z \equiv \pm \frac{x}{y} \pmod p$$

kongrüansı, $x, y \in \mathbb{N}$ ve $x, y < \sqrt{p}$ koşulları altında gerçeklenir. Buradan,

$$x^2 - 2y^2 = -p$$

bulunur. Bu eşitlikten,

$$(x + 2y)^2 - 2(x + y)^2 = p$$

yazılabilir. Dolayısıyla, (2.67) ve (2.69) denklemlerinin her ikisi de çözülebilirdir.

$$x^2 - 2y^2 = 1$$

denklemini düşünelim. Temel çözümün $3 + 2\sqrt{2}$ olduğu görülür. Teorem 2.5.1. ve Teorem 2.5.2. den (2.67) ve (2.69) eşitlikleri bulunur. Bu denklemlerin çözümlerinin de (2.68) ve (2.70) eşitsizliklerini sağladığı görülür.

Teorem 2.5.6. $p; p \equiv 1 \pmod{12}$ koşulunu sağlayan bir asal sayı ise,

$$u^2 - 3v^2 = p \tag{2.71}$$

$$u < \sqrt{\frac{3}{2}p}\,, v < \sqrt{\frac{1}{6}p} \tag{2.72}$$

eşitlik ve eşitsizliklerini sağlayan $u, v \in \mathbb{N}$ vardır.

$p; p \equiv -1 \pmod{12}$ koşulunu sağlayan bir asal sayı ise,

$$u^2 - 3v^2 = -p \tag{2.73}$$

$$u < \sqrt{\frac{1}{2}p}\,, v < \sqrt{\frac{1}{2}p} \tag{2.74}$$

eşitlik ve eşitsizlikleri vardır (*Nagell, 1964, sy 212*).

İspat. $p \equiv \pm 1 \pmod{12}$ için $z^2 \equiv 3 \pmod{p}$ kongrüansı çözülebilirdir. O halde z bir çözüm ise Teorem 2.1.1. den,

$$z \equiv \pm \frac{x}{y} \pmod{p}$$

kongrüansı, $x, y \in \mathbb{N}$ ve $x, y < \sqrt{p}$ koşulları altında gerçeklenir. Buradan,

$$x^2 - 3y^2 = -mp$$

bulunur. $m = 1$ ya da 2 dir.

$m = 2$ için,

$$x^2 - 3y^2 = -2p$$

eşitliği vardır ve x , y tek doğal sayılardır. Buradan,

$$\left(\frac{x+3y}{2}\right)^2 - 3\left(\frac{x+y}{2}\right)^2 = p$$

eşitliği yazılabilir ve $\frac{1}{2}(x+3y), \frac{1}{2}(x+y)$ sayılarının tam sayı olduğu görülür. Bu yüzden (2.71) eşitliği, $p \equiv 1 \pmod{12}$ ve (2.73) eşitliği $p \equiv -1 \pmod{12}$ için çözülebilirdir.

$$x^2 - 3y^2 = p$$

eşitliğini inceleyelim. Bu Diofant Denkleminin temel çözümünün $2+\sqrt{3}$ olduğu bulunur. Teorem 2.5.1. ve Teorem 2.5.2. den, (2.71) ve (2.73) denklemlerinin çözümlerinin, (2.72) ve (2.74) eşitsizliklerini sağladığı kolayca gerçeklenir.

3. SÜREKLİ KESİRLER

Bu bölümde 2. bölümde ayrıntılı bir şekilde incelediğimiz Pell Denklemleri'nin temel çözümünü bulmaya yönelik oldukça etkili bir yöntemden bahsedeceğiz. Bunun için sürekli kesirlerle ilgili bazı temel tanım ve teoremlerin bilinmesi gerekmektedir. Bu bilgilerin ardından son olarak asıl amacımıza yönelik bir teoremle 2. bölümle ilgili daha genel bir bakış açısı kazanmış olacağız.

3.1. SONLU (BASİT) SÜREKLİ KESİRLER

Tanım 3.1.1. Bir $\frac{r}{s}\left(s>0; r,s\in\mathbb{Z}\right)$ kesrini göz önüne alalım. $i=0,1,2,...,n$ olmak üzere $i=0$ hariç her i için $a_i\in\mathbb{N}$ ve $a_0\in\mathbb{Z}$ olsun.

$$\frac{r}{s}=a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{\ddots a_{n-1}+\cfrac{1}{a_n}}}} \tag{3.1}$$

(3.1) eşitliğinin sağ tarafına bir sonlu (basit) sürekli kesir denir. Başka bir ifadeyle eşitliğin sağ tarafına $\frac{r}{s}$ kesrinin sonlu (basit) sürekli kesir açılımı denir.

Bu kesri yukarıdaki eşitlikten yararlanarak kısaca ifade etmenin birkaç yolu vardır. Bunlardan en çok kullanılan gösterim,

$$\frac{r}{s}=\left[a_0,a_1,...,a_n\right]$$

dir. Bu gösterime ek olarak;

$$[a_0, a_1, ..., a_n] = \left[a_0, a_1, ..., a_{n-2}, a_{n-1} + \frac{1}{a_n} \right]$$

ya da

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

gibi farklı gösterimler kullanmak mümkündür.

Şimdi $(r,s) = 1; s > 0; r, s \in \mathbb{Z}$ olmak üzere bir $t = \frac{r}{s}$ kesri verildiğinde bu kesrin sonlu sürekli kesir açılımının nasıl bulunduğunu görelim:

$r = a_0 s + t_0 \quad ; \quad 0 < t_0 < s$

$s = a_1 t_0 + t_1 \quad ; \quad 0 < t_1 < t_0$

$t_0 = a_2 t_1 + t_2 \quad ; \quad 0 < t_2 < t_1$

……

$t_{n-3} = a_{n-1} t_{n-2} + t_{n-1}; \quad 0 < t_{n-1} < t_{n-2}$

$t_{n-2} = a_n t_{n-1} + 0; \quad \ldots\ldots$

Yukarıda açıkça görülüyor ki r, s tam sayı çiftine Öklid Bölüm Algoritması uygulanmaktadır. Bu şekilde elde edilen denklemlerden aşağıdaki eşitlikler bulunur:

$$t = \frac{r}{s} = a_0 + \frac{t_0}{s} = a_0 + \frac{1}{s / t_0} \qquad (1)$$

$$\frac{s}{t_0} = a_1 + \frac{t_1}{t_0} = a_1 + \frac{1}{t_0 / t_1} \qquad (2)$$

… …… …

$$\frac{t_{n-3}}{t_{n-2}} = a_{n-1} + \frac{t_{n-1}}{t_{n-2}} = a_{n-1} + \frac{1}{t_{n-2} / t_{n-1}} \qquad (n)$$

$$\frac{t_{n-2}}{t_{n-1}} = a_n \qquad (n+1)$$

(1) denkleminde $\frac{s}{t_0}$ yerine, (2) denklemindeki eşitini yazıp ardından bu şekilde devam edilirse t rasyonel sayısının

$$t = [a_0, a_1, ..., a_n]$$

sonlu sürekli kesirlere açılımı elde edilir.

Bir $t = \frac{r}{s}$ kesri verildiğinde bunun sonlu sürekli kesir açılımının tek türlü olmadığı kolayca gösterilebilir. t nin sonlu sürekli kesir açılımı

$$t = [a_0, a_1, ..., a_n]$$

olsun. $t = [a_0, a_1, ..., a_n] = [a_0, a_1, ..., a_n - 1, 1]$ olduğuna dikkat edelim.

Teorem 3.1.1. Sonlu bir sürekli kesir rasyonel sayıdır. Tersine her rasyonel sayının tam iki türlü sürekli kesirlere açılımı vardır (*Hardy and Wright, 1938, sy 128-129; Wright, 1948, sy 16-17*).

Örnek 3.1.1. $63/13$ in sürekli kesirlere açılımını, Öklid Algoritmasından yararlanarak bulalım:

$$63 = 13.4 + 11$$

$$13 = 11.1 + 2$$

$$11 = 2.5 + 1$$

$$2 = 1.2$$

Bu durumda kısmi bölümler 4, 1, 5, 2 dir. Yani,

$$63/13 = [4,1,5,2] = [4,1,5,1,1]$$

bulunur.

Tanım 3.1.2. Bir $\frac{r}{s} = [a_0, a_1, ..., a_n]$ kesrinin $k.$yaklaşık kesri

$$\frac{p_k}{q_k} = [a_0, a_1, ..., a_k]$$

dır.

Tanımın bir sonucu olarak $\frac{r}{s}=[a_0,a_1,...,a_n]$ kesrinin $n.$ yaklaşık kesri; $\frac{p_n}{q_n}=\frac{r}{s}$,

0. yaklaşık kesri ise $\frac{p_0}{q_0}=a_0$ dır.

$$\frac{p_0}{q_0}=a_0 \Rightarrow p_0=a_0, q_0=1$$

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

$$\vdots$$

$$\begin{cases} p_{k+2}=a_{k+2}p_{k+1}+p_k \\ q_{k+2}=a_{k+2}q_{k+1}+q_k \end{cases} \quad (k\in\mathbb{Z}) \qquad (3.2)$$

$k=0$ alındığında $p_{-2}=q_{-1}=0$ ve $p_{-1}=q_{-2}=1$ olduğu görülür.

Teorem 3.1.2. $a_0\in\mathbb{Z}$ dışında her biri birer pozitif tam sayı olan $a_0,a_1,...,a_n$ tam sayılar dizisi için (3.2) ile p_k ve q_k tam sayılarını tanımlayalım. Bu takdirde her $x\in\mathbb{R}-\{0\}$ ve her $k\geq 0$ tam sayısı için;

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

dır (*Çallıalp, 2009, sy 116*).

İspat. n ye göre indüksiyonla yapılır:

$[a_0,x]=a_0+\frac{1}{x}=\frac{a_0x+1}{x}=\frac{xp_0+p_{-1}}{x_{\ 0}+qq_1}$ olduğundan $n=1$ için iddia doğrudur.

$n=k$ için iddia doğru olsun. O halde,

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

olur.

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

$$=\frac{xa_kp_{k-1}+xp_{k-2}+p_{k-1}}{xa_kq_{k-1}+xq_{k-2}+q_{k-1}}=\frac{x\left(a_kp_{k-1}+p_{k-2}\right)+p_{k-1}}{x\left(a_kq_{k-1}+q_{k-2}\right)+q_{k-1}}$$

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

olur. Yani iddia $n=k+1$ için doğrudur. Dolayısıyla ispat biter.

Teorem 3.1.3. Her $k\geq -1$ için,

$$p_kq_{k-1}-p_{k-1}q_k=(-1)^{k-1} \tag{3.3}$$

dır (*Çallıalp, 2009, sy 117*).

İspat. p_k ve q_k sayıları (3.2) bağıntısı ile verilmişti. İspat için bu bağıntıdan yararlanacağız:

$$p_kq_{k-1}-p_{k-1}q_k=(a_kp_{k-1}+p_{k-2})q_{k-1}-p_{k-1}(a_kq_{k-1}+q_{k-2})$$

$$=a_kp_{k-1}q_{k-1}+p_{k-2}q_{k-1}-p_{k-1}a_kq_{k-1}-p_{k-1}q_{k-2}$$

$$=p_{k-2}q_{k-1}-p_{k-1}q_{k-2}$$

$$=-(p_{k-1}q_{k-2}-p_{k-2}q_{k-1})$$

parantez içindeki bu ifade, eşitliğin sol tarafına k yerine $k-1$ yazmakla elde edilir. Bundan sonraki adımda ise p_{k-1} ve q_{k-1} sayılarının eşitlerini yazacağız ve bu şekilde bu indirgeme işlemine devam edeceğiz. Böylece toplamda $k-1$ kere bu işlemi tekrar ettiğimizde ;

$$p_kq_{k-1}-p_{k-1}q_k=(-1)^{k-1}(p_0q_{-1}-p_{-1}q_0)=(-1)^{k-1}$$

bulunur.

Sonuç 3.1.2. Her $k\geq 0$ için $(p_k,q_k)=1$ olur (*Çallıalp, 2009, sy 117*).

İspat. (3.3) eşitliğinden 1 in p_k ve q_k ların bir lineer toplamı şeklinde yazılabildiğini görüyoruz. Dolayısıyla p_k ve q_k aralarında asaldır.

Yardımcı Teorem 3.1.1. $a,b,c \in \mathbb{Z}$; a veya b sıfırdan farklı olmak üzere, $ax+by=c$ Diofant denkleminin bir çözümü olması için gerek ve yeter koşul $d=(a,b)$ ise $d \mid c$ olmasıdır. Bu takdirde sonsuz çözüm var ve bir çözüm (x_0, y_0) ise herhangi bir çözüm, $k \in \mathbb{Z}$ olmak üzere;

$$x = x_0 + \frac{b}{d}.k \quad \text{ve} \quad y = y_0 - \frac{a}{d}.k$$

ile bir parametreye bağlı olarak belirlidir (*Çallıalp, 2009, sy 10*).

Sonuç 3.1.3. $(a,b)=1$ olmak üzere, $ax+by=c$ Diofant denkleminin bir çözümü,

$$\frac{a}{b} = [a_0, a_1, ..., a_n] = \frac{p_n}{q_n} \tag{3.4}$$

denirse, n tek iken; $x = q_{n-1}, y = -p_{n-1}$ ve n çift iken; $x = -q_{n-1}, y = p_{n-1}$ olarak alınabilir (*Wright,1948, sy 20-21*).

İspat. $(a,b)=1$, $b>0$ ve $(p_n, q_n)=1, q_n>0$ olduğundan, $\frac{a}{b} = \frac{p_n}{q_n} \Rightarrow a = p_n$, $b = q_n$ olur. (3.3) eşitliğinden,

$$aq_{n-1} - p_{n-1}b = (-1)^{n-1}$$

olur. Bu eşitliğin her iki yanını $(-1)^{n-1}c$ ile çarpalım:

$$a\left[(-1)^{n-1} cq_{n-1}\right] + \left[(-1)^{n} cp_{n-1}\right] b = c$$

olacağından, n tek ise; $x = cq_{n-1}, y = -cp_{n-1}$ ve n çift ise; $x = -cq_{n-1}$, $y = cp_{n-1}$ verilen Diofant denkleminin bir çözümü olur. Dolayısıyla, Yardımcı Teorem 3.1.1. den $ax+by=c$ Diofant denkleminin tüm çözümlerini bulmak mümkün olur.

Örnek 3.1.2. $63x+13y=1$ denkleminin bir çözümünü bulalım. Örnek 3.1.1. de $\frac{63}{13} = [4,1,5,2]$ olduğunu bulmuştuk.

k	-2	-1	0	1	2	3
a_k			4	1	5	2
p_k	0	1	4	5	29	63
q_k	1	0	1	1	6	13

(3.2) eşitliklerinden yararlanılarak yukarıdaki tablo oluşturulmuştur. $n = 3$ olduğundan Sonuç 3.1.4. den $x = q_2 = 6, y = -p_2 = 2$ verilen denklemin bir çözümü olur. Böylece Yardımcı Teorem 3.1.1. den aynı denklemin diğer çözümlerini bulmak da mümkün olur.

Ayrıca, $\frac{63}{13} = [4,1,5,2] = [4,1,5,1,1]$ olduğu biliniyor. Yani verilen denklemin çözümlerini bulmak için bu açılım da kullanılabilir.

Tanım 3.1.3. $a_0 \in \mathbb{Z}$ dışında her biri birer pozitif tam sayı olmak üzere $a_0, a_1, \ldots$ tam sayılar dizisi verilsin. (3.2) eşitlikleriyle beraber $\{p_k\}$ ile $\{q_k\}$ dizilerini tanımlayalım.

$$c_k = [a_0, a_1, \ldots, a_k] \tag{3.5}$$

olmak üzere, c_k ya $k.$yaklaşım denir.

Tanımda belirtilen c_k, $k+1$ terimli bir sonlu sürekli kesirdir. Dolayısıyla $c_k = \frac{p_k}{q_k}$ bir rasyonel sayıdır. Şimdi aşağıdaki yardımcı teoremle, $\lim_{k\to\infty} c_k$ nın her zaman var olduğunu göstereceğiz:

Yardımcı Teorem 3.1.2. i) Çift yaklaşımlar dizisi artan;

$$c_0 < c_2 < c_4 < \ldots$$

ii) Tek yaklaşımlar dizisi azalan;

$$c_1 < c_3 < c_5 < \ldots$$

iii) Her tek yaklaşım, her çift yaklaşımdan büyüktür.

(*Çallıalp, 2009, sy 119*).

İspat. i) Her çift $k \geq 2$ için, (3.4) den,

$$\frac{p_k}{q_k}=\frac{p_{k-2}}{q_{k-2}}+\frac{a_k}{q_kq_{k-2}}\Rightarrow c_k=c_{k-2}+\frac{a_k}{q_kq_{k-2}} \tag{3.6}$$

olur. Her $k>0$ için q_k ve a_k sayıları pozitif olduğundan, $c_{k-2}<c_k$ elde edilir.

ii) Her tek $k\geq 1$ için, (3.4) den, benzer şekilde, $c_k=c_{k-2}-\frac{a_k}{q_kq_{k-2}}$ olur. q_k ve a_k sayıları pozitif olduğundan, $c_{k-2}>c_k$ elde edilir.

iii) (3.3) den, her $t\geq 0$ ve $k=2t+1$ için,

$$\frac{p_{2t+1}}{q_{2t+1}}-\frac{p_{2t}}{q_{2t}}=\frac{1}{q_{2t}q_{2t+1}}\Rightarrow c_{2t+1}=c_{2t}+\frac{1}{q_{2t}q_{2t+1}}$$

olur. Buradan da $c_{2t+1}>c_{2t}$ bulunur.

Şimdi her $r,s\geq 0$ için, $c_{2r+1}>c_{2s}$ olduğunu gösterelim:

$r=s$ olsun. (i) den;

$$c_{2r+1}>c_{2r}>c_{2s}$$

$r<s$ olsun. (ii) den;

$$c_{2r+1}>c_{2s+1}>c_2$$

olur. Böylelikle istenen elde edilmiş olur.

Teorem 3.1.4. Her $k\geq 1$ için, $a_k>0$ olmak üzere; $a_0,a_1,...$ tam sayılar dizisi verildiğinde, $c_k=[a_0,a_1,...,a_k]$ ise $\lim_{k\to\infty}c_k$ mevcuttur. Her $r,s\geq 0$ tam sayısı için

$$c_{2r}<\lim_{k\to\infty}c_k<c_{2s+1}$$

dir (*Çallıalp, 2009, sy 119-120*).

İspat. Yardımcı Teorem 3.1.1. den, $\{c_{2k}\}$ artan ve herhangi bir tek yaklaşım ile üstten sınırlı olduğundan,

$$\lim_{k\to\infty}c_{2k}$$

vardır. Benzer şekilde,

$$\lim_{k\to\infty}c_{2k+1}$$

de vardır. (3.5) eşitliklerinden

$$\lim_{k\to\infty} c_{2k+1} = \lim_{k\to\infty} c_{2k} + \lim_{k\to\infty} \frac{1}{q_{2k}q_{2k+1}}$$

bulunur. $\{q_k\}$ artan dizi ve $q_k \geq k$ olduğu göz önünde tutularak, son limit sıfır olacağından ,

$$\lim_{k\to\infty} c_{2k+1} = \lim_{k\to\infty} c_{2k}$$

olur. Yani çift ve tek yaklaşımlar dizisinin limitleri aynı olduğundan,

$$\lim_{k\to\infty} c_k = \lim_{k\to\infty} c_{2k} = \lim_{k\to\infty} c_{2k+1}$$

bulunur. Teoremin ifadesindeki eşitsizlik de, ispatın başında verilen nedenden sağlanır.

Tanım 3.1.4. $a_0 \in \mathbb{Z}$ dışında, her biri birer pozitif tam sayı olan bir $a_0, a_1, ...$ tam sayılar dizisi, $c_k = [a_0, a_1, ..., a_k]$ olmak üzere, değeri

$$[a_0, a_1, ..., a_k, ...] = \lim_{k\to\infty} c_k$$

olan bir sonsuz sürekli kesir tanımlar. c_k lara yaklaşım ve a_k lara da kısmi bölümler denir.

Teorem 3.1.5. $\alpha = [a_0, a_1, ...]$ ise $\|\alpha\| = a_0$ ve

$$\alpha = a_0 + \frac{1}{[a_1, a_2, ...]}$$

dır (*Çallıalp, 2009, sy 120*).

Sonuç 3.1.5. $\alpha = [a_0, a_1, ...]$ sonsuz sürekli kesri bir tam sayı olamaz (*Çallıalp, 2009, sy 121*).

İspat. Yukarıdaki teoremden $a_0 < \alpha < a_0 + 1$ eşitsizliğinin varlığı görülür. Dolayısıyla $\alpha \in \mathbb{Z}$ olamaz.

Teorem 3.1.6. $\alpha = [a_0, a_1, ...] = [b_0, b_1, ...]$ ise her $k > 0$ için, $a_k = b_k$ dır (*Çallıalp, 2009, sy 121*).

İspat. Teorem 3.1.5. den,

$$a_0 + \frac{1}{[a_1, a_2, ..., a_k]} = b_0 + \frac{1}{[b_1, b_2, ..., b_k]}$$

olduğundan, k ya göre indüksiyonla istenen eşitlik elde edilir.

Teorem 3.1.7. Her sonsuz sürekli kesrin değeri bir irrasyonel sayıdır (*Çallıalp, 2009, sy 121-122*).

İspat. $\alpha = [a_0, a_1, ...]$ ve α bir rasyonel sayı olsaydı, Teorem 3.1.1 e göre, sonlu sürekli kesirlere açılımı olurdu. Bu takdirde,

$$\alpha = [a_0, a_1, ...] = [b_0, b_1, ..., b_n]$$

ve $\|\alpha\| = a_0 = b_0$ olur. Teorem 3.1.5. e göre,

$$a_0 + \frac{1}{[a_1, a_2, ...]} = b_0 + \frac{1}{[b_1, b_2, ..., b_n]}$$

dir. Buradan,

$$[a_0, a_1, ...] = [b_0, b_1, ..., b_n],$$

bu şekilde devam ederek,

$$[a_n, ...] = [b_n] = b_n \in \mathbb{Z}$$

bulunurdu. Fakat sonsuz sürekli kesir bir tam sayı olamayacağından, bu bize bir çelişki verir. Böylelikle ispat tamamlanmış olur.

Şimdi bir α irrasyonel sayısının sonsuz sürekli kesir açılımının nasıl bulunacağını açıklayalım:

$\alpha = \alpha_0$ ve $a_0 = \|\alpha_0\| \in \mathbb{Z}$ olsun. $\alpha = \alpha_0$ bir irrasyonel sayı olduğundan,

$$0 < \alpha_0 - a_0 < 1 \Rightarrow \alpha_1 = \frac{1}{\alpha_0 - a_0}$$

$\alpha_1 < 1$ de bir irrasyonel sayı olur.

$$\alpha_0 = a_0 + \frac{1}{\alpha_1}$$

dır. α_0 için yaptığımız işlemi α_1 için de uygularsak bir $\{a_k\}$ sonsuz dizisi elde edilir.

$$\alpha_0 = a_0 + \frac{1}{\alpha_1},\ a_0 = \|\alpha_0\| \in \mathbb{Z}$$

$$\alpha_1 = a_1 + \frac{1}{\alpha_2},\ 0 < a_1 = \|\alpha_1\| \in \mathbb{Z}$$

…….

$$\alpha_{k-1} = a_{k-1} + \frac{1}{\alpha_k}, 0 < a_{k-1} = \|\alpha_{k-1}\| \in \mathbb{Z} \tag{3.7}$$

…….

Burada α_{k-1} irrasyonel bir sayı olduğundan, α_k da irrasyonel ve $a_0 \in \mathbb{Z}$ dışında a_k $(k > 0)$ lar pozitif tam sayılardır. Böylece

$$\alpha = [a_0, a_1, ..., a_{k-1}, \alpha_k] \tag{3.8}$$

olur ve $[a_0, a_1, ...]$ sonsuz sürekli kesri bulunmuş olur.

Teorem 3.1.8. α bir irrasyonel sayı ve α_k lar (3.7) eşitlikleri ile tanımlanmış olsun. $a_k = \|\alpha_k\| \in \mathbb{Z}$ olmak üzere $\alpha = [a_0, a_1, ...]$ dir (*Çallıalp, 2009, sy 122-123*).

Teorem 3.1.9. Her $k \geq 0$ için,

$$\alpha_k = [a_k, a_{k+1}, ...]$$

dır (*Çallıalp, 2009, sy 123*).

Tanım 3.1.5. (3.7) eşitlikleri ile tanımlı $\alpha_k = [a_k, a_{k+1}, ...]$ lara, $\alpha = \alpha_0 = [a_0, a_1, ...]$ sonsuz sürekli kesrinin tam bölümleri denir.

Teorem 3.1.10. $1 < \beta$ bir irrasyonel sayı ve

$$\beta = [b_0, b_1, ...]$$

olsun. $a_0 \in \mathbb{Z}$ dışında her $k > 0$ için, $a_k > 0$ olmak üzere, $a_0, a_1, ..., a_{n-1}$ $(n > 0)$ tam sayıları verildiğinde

$$[a_0, a_1, ..., a_{n-1}, \beta] = [a_0, a_1, ..., a_{n-1}, b_0, b_1, ...]$$

dır (*Çallıalp, 2009, sy 123*).

Teorem 3.1.11. $\alpha = [a_0, a_1, ...]$ olmak üzere her $n \geq 1$ için,

$$\left| \alpha - \frac{p_n}{q_n} \right| < \left| \alpha - \frac{p_{n-1}}{q_{n-1}} \right|$$

dır (*Çallıalp, 2009, sy 125*).

Teorem 3.1.11. de $c_k = \frac{p_k}{q_k}$ yaklaşımlarının α irrasyonel sayısına uzaklıkları ele alınmaktadır. Daha detaylı belirtmek gerekirse bu önermenin ispatında; $c_0, c_1, ...$ dizisinin gittikçe α ya yakınsadığı görülür. Burada, paydası q_n den küçük olan rasyonel sayılar arasında α ya en yakın olan rasyonel sayı $\frac{p_n}{q_n}$ dir .

Teorem 3.1.12. $(c,d)=1$, $d>0$ ve

$$\left|\alpha - \frac{c}{d}\right| < \left|\alpha - \frac{p_n}{q_n}\right| \Rightarrow d > q_n$$

dır (*Çallıalp, 2009, sy 125*).

Teorem 3.1.13. α irrasyonel bir sayı, $(c,d)=1, d>0$ olmak üzere

$$\left|\alpha - \frac{c}{d}\right| < \frac{1}{2d^2}$$

ise $\frac{c}{d}$, α nın sürekli kesirlere açılımında bir yaklaşımdır (*Çallıalp, 2009, sy 126-127*).

3.2. KUADRATİK İRRASYONELLER

Tanım 3.2.1. $u, v \in \mathbb{Q}$, $v \neq 0$ ve $D>0$ tam kare olmayan bir tam sayı ise $u + v\sqrt{D}$ reel sayısına bir kuadratik irrasyonel sayı denir.

$$\mathbb{Q}(\sqrt{D}) = \left\{ u + v\sqrt{D} \mid u, v \in \mathbb{Q} \right\}$$

kümesi $\mathbb{Q}$ rasyonel sayılar cisminin 2. dereceden bir genişlemesidir. Kuadratik irrasyonel sayılar, bu cismin irrasyonel sayılarıdır.

Tanım 3.2.2. $\alpha = u + v\sqrt{D} \in \mathbb{Q}(\sqrt{D})$ ise $\alpha' = u - v\sqrt{D}$ ye, α nın eşleniği denir.

Teorem 3.2.1. Her α kuadratik irrasyonel sayısı, $D>0$ tam kare olmayan bir doğal sayı ve $r, s \in \mathbb{Z};\ s \neq 0;\ s \mid D - r^2$ olmak üzere,

$$\alpha = \frac{r + \sqrt{D}}{s}$$

şeklindedir (*Çallıalp, 2009, sy 129*).

Tanım 3.2.3. $n \geq 0$, $m \geq 0$ olmak üzere;

$$\left[b_0, b_1, ..., b_{n-1}, \overline{c_0, c_1, ..., c_{m-1}} \right]$$

şeklindeki bir sonsuz sürekli kesire periyodik denir. Böyle m ve n lerin en küçüğünü aldığımızda m ye periyot uzunluğu; $c_0, c_1, ..., c_{m-1}$ e bir periyot denir. Eğer $n = 0$ ise pür periyodik denir.

Teorem 3.2.2. Her periyodik sürekli kesir bir kuadratik irrasyonel sayıdır (*Çallıalp, 2009, sy 130-131*).

Şimdi tersine olarak, bir kuadratik irrasyonel sayının sürekli kesirlere açılımının periyodik olacağını görelim. Bir α kuadratik irrasyonel sayısı verildiğinde, (3.7) eşitlikleri ile $\alpha = \alpha_0$, $\|\alpha_k\| = a_k$ ve $k \geq 0$ için, $\alpha_k = a_k + \frac{1}{\alpha_{k+1}}$ tanımlayalım. Teorem 3.2.1. den $r_0, s_0 \in \mathbb{Z}$ ve $s_0 \mid (D - r_0^2)$ olmak üzere, $\alpha = \alpha_0 = \frac{r_0 + \sqrt{D}}{s_0}$ şeklinde yazalım. Her a_k tam bölümü de benzer şekilde yazılabilir. r_k ve s_k dizilerini aşağıdaki şekilde tanımlayıp, bunların α_k tam bölümlerini verdiğini ispatlayalım. r_0 ve s_0 verildiğinde her $k \geq 0$ için,

$$r_{k+1} = a_k s_k - r_k \quad ; \quad s_{k+1} = \frac{D - r^2_{k+1}}{s_k} \tag{3.9}$$

diyelim. Bu gösterimleri kullanarak aşağıdaki teoremi ispatlayabiliriz.

Teorem 3.2.3. Her $k \geq 0$ tam sayısı için,

(i) $r_k, s_k \in \mathbb{Z}$ ve $s_k \neq 0$,

(ii) $s_k \mid (D - r_k^2)$,

(iii) $\alpha_k = \frac{r_k + \sqrt{D}}{s_k}$ dır.

(*Çallıalp, 2009, sy 131-132*).

İspat. $k=0$ için yukarıdaki eşitliklerin sağlandığı açıktır. Bu üç iddianın da k için doğru olduğunu kabul edip, $k+1$ için doğru olduğunu görelim.

(3.9) eşitliklerinden;

$r_{k+1} \in \mathbb{Z}$ ve D de tam kare olmayan bir doğal sayı olduğundan $D \neq r^2_{k+1}$ dır. Dolayısıyla $s_k \neq 0$ gerçeklenir.(i) nin ispatı biter.

$$s_{k+1} = \frac{D - r^2_{k+1}}{s_k} = \frac{D-(a_k s_k - r_k)^2}{s_k} = \frac{D - r^2_k}{s_k} - a_k{}^2 s_k + 2a_k r_k \qquad (3.10)$$

olur. Herbir iddianın k için gerçeklendiğini kabul etmiştik. Dolayısıyla $s_k \mid (D - r_k{}^2)$ sağlanır. Bu durumda (3.10) dan, $s_k \mid (D - r_{k+1}{}^2) = s_k s_{k+1}$ olur. Buradan da $s_{k+1} \mid (D - r_{k+1}{}^2)$ elde edilir. (ii) nin ispatı biter.

$$\begin{aligned} \alpha_{k+1} = \frac{1}{\alpha_k - a_k} &= \frac{s_k}{r_k + \sqrt{D} - a_k s_k} \\ &= \frac{s_k}{\sqrt{D} - r_{k+1}} \cdot \frac{\sqrt{D} + r_{k+1}}{\sqrt{D} + r_{k+1}} \\ &= \frac{\sqrt{D} + r_{k+1}}{(\sqrt{D} - r^2_{k+1})/s_k} \\ &= \frac{\sqrt{D} + r_{k+1}}{s_{k+1}} \end{aligned}$$

olur. (iii) nin ispatı biter. Böylelikle önermenin ispatı tamamlanmış olur.

Bu ispat aynı zamanda bir kuadratik irrasyonel sayının sürekli kesirlere açılımını bulmaya yönelik kullanışlı bir yöntemdir. Şimdi bu yöntemi kullanacağımız aşağıdaki örneği inceleyelim.

Örnek 3.2.1. $\sqrt{13}$ in sürekli kesirlere açılımını bulalım.

$\sqrt{13} = \dfrac{\sqrt{13}+0}{1}$ olmak üzere $r_0 = 0, s_0 = 1$ alalım. O halde $a_0 = \left\| \sqrt{13} \right\| = 3$ dır.

(3.9) eşitliklerinden ve Teorem 3.2.3. den yararlanarak sırasıyla r_1, s_1 ve a_1 değerlerini hesaplayalım:

$r_1 = a_0 s_0 - r_0 = 3.1 - 0 = 3$, $s_1 = \frac{13-3^2}{1} = 4$ olur. $\alpha_1 = \frac{3+\sqrt{13}}{4} \Rightarrow \|\alpha_1\| = a_1 = 1$ bulunur.

Bu şekilde devam edildiğinde sonuç olarak aşağıdaki tablo elde edilir.

k	0	1	2	3	4	5
r_k	0	3	1	2	1	3
s_k	1	4	3	3	4	1
a_k	3	1	1	1	1	6

Böylece $\sqrt{13} = \left[3, \overline{1,1,1,6}\right]$ olarak bulunur.

Teorem 3.2.2. Kuadratik irrasyonel bir sayının sürekli kesirlere açılımı periyodiktir (*Çallıalp, 2009, sy 134*).

Tanım 3.2.3. α bir kuadratik irrasyonel sayı ve $\alpha > 1$, $-1 < \alpha' < 0$ ise α ya indirgenmiş kuadratik irrasyonel sayı denir.

Örnek 3.2.2. $\alpha = \sqrt{2}+1 > 1$ ve $-1 < \alpha' = 1-\sqrt{2} < 0$ olduğundan, $\sqrt{2}+1$ bir indirgenmiş kuadratik irrasyonel sayıdır.

Teorem 3.2.3. Bir kuadratik irrasyonel sayı olan α nın sürekli kesirlere açılımının pür periyodik olması için gerek ve yeter koşul indirgenmiş kuadratik irrasyonel sayı olmasıdır (*Çallıalp, 2009, sy 135-136*).

Teorem 3.2.4. $D > 0$ tam kare olmayan bir doğal sayı ise,

$$\sqrt{D} = \left[a_0, \overline{a_1, a_2, ..., a_{m-1}, 2a_0}\right]$$

eşitliği vardır. Yani, $\sqrt{D}$ nin sürekli kesirlere açılımı bir terim sonra periyodiktir ve periyodun son terimi $a_m = 2a_0$ dır (*Çallıalp, 2009, sy 136-137*).

Teorem 3.2.5. $D > 0$ tam kare olmayan bir doğal sayı ve

$$\sqrt{D} = \left[a_0, \overline{a_1, a_2, ..., a_m}\right], (a_m = 2a_0)$$

m periyot uzunlukta olsun. Bu durumda her $k \geq 0$ için;

(i) $p^2_{k-1} - Dq^2_{k-1} = (-1)^k s_k$,

(ii) $s_k > 0$

(iii) $s_k = 1 \Leftrightarrow m \mid k$ dır.

önermeleri gerçeklenir (*Çallıalp, 2009, sy 137-139*).

Teorem 3.2.4. $\sqrt{D}$ nin periyot uzunluğu m ve yaklaşımları $\frac{p_k}{q_k}$ lar olsun.

i) Eğer m çift ise $x^2 - Dy^2 = 1$ Pell denkleminin bir çözümünün $p_i + q_i\sqrt{D}$ olması için gerek ve yeter koşul, $\exists k \in \mathbb{N}$ için $i = km - 1$ olmasıdır.

ii) Eğer m tek ise $x^2 - Dy^2 = 1$ Pell denkleminin bir çözümünün $p_i + q_i\sqrt{D}$ olması için gerek ve yeter koşul, $\exists k \in \mathbb{N}$ için $i = 2km - 1$ olmasıdır.

(*Çallıalp, 2009, sy 141-142*).

İspat. $x^2 - Dy^2 = 1$ Pell denkleminin bir çözümünün $p_i + q_i\sqrt{D}$ olması için gerek ve yeter koşulun,

$$(-1)^{i+1} s_{i+1} = 1 \Leftrightarrow i + 1 = mk = \text{çift}, \exists k \in \mathbb{N}$$

olduğu Teorem 3.2.5. de gösterildi. Buradan açıkça görülür ki,

m çift ise; $i = mk - 1, \exists k \in \mathbb{N}$ dir.

m tek ise; $i = 2mk - 1, \exists k \in \mathbb{N}$ dir.

Teorem 3.2.5. $\sqrt{D}$ nin periyot uzunluğu m ve yaklaşımları $\frac{p_k}{q_k}$ lar olsun.

(i) Eğer m çift ise $x^2 - Dy^2 = -1$ denkleminin hiçbir çözümü $p_i + q_i\sqrt{D}$ olamaz.

(ii) Eğer m tek ise $x^2 - Dy^2 = -1$ denkleminin bir çözümünün $p_i + q_i\sqrt{D}$ olması için gerek ve yeter koşul $i = (2k-1)m - 1, \exists k \in \mathbb{N}$ olmasıdır.

(*Çallıalp, 2009, sy 142*).

İspat. Teorem 3.2.4. e benzer şekilde, $x^2 - Dy^2 = -1$ Pell denkleminin bir çözümünün $p_i + q_i\sqrt{D}$ olması için gerek ve yeter koşul,

$$(-1)^{i+1}s_{i+1} = -1 \Leftrightarrow i+1 = mk = tek, \exists k \in \mathbb{N}$$

olmasıdır. Eğer m çift ise bu koşul hiç gerçeklenmez. Eğer m tek ise $k = 2n+1 (n = 0,1,2,...)$ olmalıdır.

Sonuç 3.2.1. $x^2 - Dy^2 = 1$ denkleminin sonsuz çözümü vardır. $x^2 - Dy^2 = -1$ denkleminin ise çözümü olmayabilir ancak varsa sonsuz çözümü vardır.

Teorem 3.2.6. $p + q\sqrt{D}$, $x^2 - Dy^2 = \pm 1$ denkleminin bir pozitif çözümü ise $\frac{p}{q}$, $\sqrt{D}$ nin sürekli kesirlere açılımında bir yaklaşımdır (*Çallıalp, 2009, sy 142*).

İspat. $p^2 - Dq^2 = 1$ ise $(p + q\sqrt{D})(p - q\sqrt{D}) = 1$ olur. Buradan,

$$\left|\frac{p}{q} - \sqrt{D}\right| = \frac{1}{q(p + q\sqrt{D})}$$

bulunur. $p^2 = 1 + Dq^2$ olduğundan $p > q$ olur. Ayrıca,

$$p + q\sqrt{D} > q + q\sqrt{D} > 2$$

dir. O halde;

$$\left|\frac{p}{q} - \sqrt{D}\right| = \frac{1}{q(p + q\sqrt{D})} < \frac{1}{q.2q} = \frac{1}{2q^2}$$

bulunur.

Bu durumda Teorem 3.1.13. e göre $\frac{p}{q}, \sqrt{D}$ nin sürekli kesirlere açılımında bir yaklaşımdır.

Sonuç 3.2.2. $\sqrt{D}$ nin periyot uzunluğu m olmak üzere,

i) $x^2 - Dy^2 = 1$ denkleminin temel çözümü;

m çift ise (p_{m-1}, q_{m-1}), m tek ise (p_{2m-1}, q_{2m-1}) dir.

ii) $x^2 - Dy^2 = -1$ denkleminin temel çözümü;

m tek ise (p_{m-1}, q_{m-1}) dir.

Örnek 3.2.3. $x^2 - 13y^2 = 1$ denkleminin temel çözümünü bulalım:

Öncelikle $\sqrt{13}$ in sürekli kesirlere açılımını bulmak gerekir. Örnek 3.2.1. den $\sqrt{13} = [3, \overline{1,1,1,6}]$ olduğu biliniyor. Açıkça görülüyor ki $m = 5$ dir. Sonuç 3.2.2. ye göre verilen Pell Denkleminin temel çözümü (p_9, q_9) dır. Tablo oluşturarak p_9 , q_9 değerleri bulunabilir.

k	-2	-1	0	1	2	3	4	5	6	7	8	9
a_k			3	1	1	1	1	6	1	1	1	1
p_k	0	1	3	4	7	11	18	119	137	256	393	649
q_k	1	0	1	2	3	5	8	53	61	114	175	289

O halde $x^2 - 13y^2 = 1$ denkleminin temel çözümü, $(p_9, q_9) = (649, 289)$ olmak üzere,

$$649 + 289\sqrt{13}$$

dır. Bu tablodan yararlanarak $x^2 - 13y^2 = -1$ denkleminin temel çözümü ise $(p_4, q_4) = (18, 8)$ olmak üzere,

$$18 + 8\sqrt{13}$$

olarak bulunur.

Her iki denklem için de temel çözüm bulunduğundan, Teorem 2.3.2. ve Teorem 2.4.1. de gösterildiği üzere artık diğer tüm pozitif çözümler de bulunabilir.

$x_1 + y_1\sqrt{D}$, $x^2 - Dy^2 = 1$ denkleminin temel çözümü ve $r_0 + s_0\sqrt{D}$, $x^2 - Dy^2 = N$ denkleminin bir çözümü ise

$$r_n + s_n\sqrt{D} = \left(r_0 + s_0\sqrt{D}\right)\left(x_1 + y_1\sqrt{D}\right)^n$$

eşitliğiyle belirli $r_n + s_n\sqrt{D}$ sayıları da $x^2 - Dy^2 = N$ denkleminin çözümü olur. Ancak tüm çözümler bu şekilde olmayabilir. 2. Bölümde $u^2 - Dv^2 = C$ denklemi ele alınırken, bu durum derinlemesine incelenmiştir.

4. MALZEME VE YÖNTEM

1.Bölümde 2. Dereceden bazı Diofant Denklemleri'nin incelenebilmesi için gerekli olan temel Sayılar Teorisi bilgileri üzerinde durulmuştur. Bu amaçla genel olarak Legendre Sembolü ve Jacobi Sembollerinin tanım ve özellikleri ile bunlara bağlı Gauss Lemması, Euler Kriteri gibi bazı temel teoremler incelenmiştir. Son olarak 2. Bölümde yer alan bazı teoremlerin ispatı için gerekli olan Dirichlet' nin Çekmece İlkesi verilmiştir.

2. Bölümde Pell Denklemleri' nin incelenmesine geçmeden önce Thue Teoremi, Teorem 2.1.2. ve Bachet Teoremi derinlemesine incelenmiştir. Ardından Pell Denklemlerinin çözümüne yönelik temel teorem ve tanımlar verilerek, bazı durumlar örneklerle açıklanmıştır.

3. Bölümde ise Pell Denklemleri'nin temel çözümünü bulmaya yönelik kullanışlı bir yöntem vermek üzere Sürekli Kesirler ile ilgili temel tanım ve teoremler verilmiştir ve bazı özel durumlar örneklendirilmiştir.

5.BULGULAR

Bu Yüksek Lisans tez çalışmasında temel olarak,

$$x^2 - Dy^2 = k$$

denkleminin x, y tam sayı çözümlerinin nasıl bulunacağı araştırılmıştır. Burada x, y birer tam sayıyı, D ise tam kare olmayan bir doğal sayıyı göstermektedir.

$k = 1$ olması durumunda, tam kare olmayan D doğal sayısı için Pell denkleminin her zaman çözümünün olduğu, hatta sonsuz adet x, y doğal sayı çözümünün olduğu ve $x_1 + y_1\sqrt{D}\ (x_1, y_1 \in \mathbb{N})$ ile gösterilen temel çözümün bilinmesi halinde diğer tüm pozitif çözümlerin bulunabileceği gösterildi.

$k = -1$ olması durumunda ise D nin belli değerleri için çözümün var olduğu yani her zaman çözümün olmadığı, ancak çözümün olması halinde yine denklemi gerçekleyen sonsuz adet x, y doğal sayısının olduğu ve temel çözüm yardımıyla pozitif diğer tüm çözümlerin bulunabileceği gösterildi. Bunun dışında, $x^2 - Dy^2 = -1$ in herhangi bir çözümünün karesinin $x^2 - Dy^2 = 1$ in bir çözümünü verdiği; özel olarak ise, $\xi_1 + \eta_1\sqrt{D}\ ;(\xi_1, \eta_1 \in \mathbb{N})$ $x^2 - Dy^2 = -1$ in temel çözümü olmak üzere bu çözümün karesinin $x^2 - Dy^2 = 1$ in temel çözümünü verdiği gösterildi.

$k = 1$ ve $k = -1$ durumlarında temel çözüme bağlı olarak diğer tüm pozitif çözümlerin bulunabileceği eşitlikler verildi ve bu eşitlikleri kullanmadan başka hiçbir çözümün bulunamayacağı gösterildi.

Bu durumlar haricinde $k = C; \left(C \in \mathbb{Z} - \{0\}\right)$ durumu incelendi ve burada diğer iki durumdaki eşitliklerden yararlanarak çözüm bulunabileceği ancak bu eşitlikleri kullanmadan elde edilebilen farklı biçimdeki çözümlerin de varlığı gösterildi ve bazı durumlar örneklerle açıklandı.

Sonuç olarak Pell Denklemleri'nde denklemin x, y çözümlerini bulmak için temel çözüm tanımının önemi gözlendi ve bu çözümü bulmaya yönelik Euler'in geliştirdiği yöntem üzerinde duruldu. Sürekli Kesirler yardımıyla verilen bu yöntemin nasıl uygulandığı bir örnekle açıklandı.

6. TARTIŞMA VE SONUÇ

Bu Yüksek Lisans Tez Çalışması' nda,

i) $x^2+y^2 = n$ (n bir doğal sayı)

ii) $x^2 - Dy^2 = k$ (k , D doğal sayılar)

biçimindeki 2. Dereceden Diofant Denklemleri incelenmiştir.

Bu denklemlerde karşılaşılan en büyük zorluk, denklemlerin çözümünü bulmaya yönelik genel bir yöntem verilememesi, aşağı yukarı her denklemin kendine has bir çözüm yönteminin olmasıdır.

Bu çalışmada ii) de verilen Pell Denklemleri ; esas olarak Dirichlet' nin, tam sayılı çözümleri verirken de Euler' in verdiği yöntemle derinlemesine incelenmiştir.

KAYNAKLAR

1. ÇALLIALP, FETHİ, 2009, *Sayıların Teorisi*, Birsen Yayınevi, İstanbul.

2. DICKSON, LEONARD EUGENE, 1939, *Modern Elementary Theory of Numbers*, The University of Chicago Press, Chicago.

3. HARDY, G.H. and WRIGHT, E.M. , 1938, *An Introduction to the Theory of Numbers*, Oxford University Press, U.K.

4. KAYA, ARİF, 1988, *Sayılar Kuramına Giriş*, Ege Üniversitesi Fen Fakültesi Yayınları, İzmir.

5. MOLLIN, RICHARD A. , 1998, *Fundamental Number Theory with Applications*, CRC Press LLC, U.S.A.

6. NAGELL, TRYGVE, 1964, *Introduction to Number Theory*, Chelsea Publishing Company, New York.

7. WRIGHT, HARRY N. , 1948, *First Course in Theory of Numbers*, John Wiley and Sons, Inc. , New York.

ÖZGEÇMİŞ

Duygu ÖZDEN 11.06.1984 yılında Ankara'da doğmuştur. İlköğrenimini Şanlıurfa Vatan İlkokulu'nda tamamlamıştır. Orta ve lise öğrenimini Ankara Gazi Anadolu Lisesi'nde tamamladıktan sonra 2002 yılında Ankara Üniversitesi Fen Fakültesi Matematik Bölümü'ne girmeye hak kazanmıştır. Bu bölümden Haziran 2007 de mezun olmuş, Şubat 2008 de İstanbul Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı'nda Yüksek Lisans öğrenimine başlamıştır. Ocak 2009 da İstanbul Üniversitesi Fen Fakültesi Matematik Bölümü Cebir ve Sayılar Teorisi Anabilim Dalı' na Araştırma Görevlisi olarak atanmıştır. Halen bu görevine devam etmektedir.