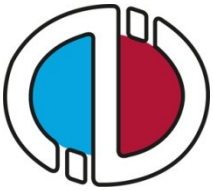

ANADOLU ÜNİVERSİTESİ

BİLECİK ŞEYH EDEBALİ ÜNİVERSİTESİ

Fen Bilimleri Enstitüsü
Matematik Anabilim Dalı

BAZI DİOPHANTİNE DENKLEMLERİNİN ÇÖZÜMLERİ ÜZERİNE

Mehmet KILIÇ
Yüksek Lisans

Tez Danışmanı
Doç. Dr. İlker İNAM

BİLECİK, 2016

Ref.No: 10115784

ANADOLU ÜNİVERSİTESİ

BİLECİK ŞEYH EDEBALİ ÜNİVERSİTESİ

Fen Bilimleri Enstitüsü
Matematik Anabilim Dalı

BAZI DİOPHANTİNE DENKLEMLERİNİN ÇÖZÜMLERİ ÜZERİNE

Mehmet KILIÇ
Yüksek Lisans

Tez Danışmanı
Doç. Dr. İlker İNAM

BİLECİK, 2016

ANADOLU UNIVERSITY

BILECIK SEYH EDEBALI UNIVERSITY

Graduate School of Sciences
Department of Mathematics

ON THE SOLUTIONS OF SOME DIOPHANTINE EQUATIONS

Mehmet KILIÇ
Master's Thesis

Thesis Advisor
Assoc. Prof. Dr. Ilker INAM

BILECIK, 2016

BİLECİK ŞEYH EDEBALİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS
JÜRİ ONAY FORMU

Bilecik Şeyh Edebali Üniversitesi Fen Bilimleri Enstitüsü Yönetim Kurulunun ..... tarih ve ..... sayılı kararıyla oluşturulan jüri tarafından 23.06.2016 tarihinde tez savunma sınavı yapılan Mehmet Kılıç'ın "Bazı Diophantine Denklemlerinin Çözümleri Üzerine" başlıklı tez çalışması Matematik Anabilim Dalında YÜKSEK LİSANS tezi olarak oy birliği ile kabul edilmiştir.

JÜRİ

ÜYE
(TEZ DANIŞMANI) : Doç. Dr. İlker İNAM

ÜYE : Doç. Dr. Ercan ALTINIŞIK

ÜYE : Doç. Dr. Nülifer ÖZDEMİR

MATEMATİK ANABİLİM DALI BAŞKANI: Doç. Dr. Sıddıka Ö. KARAKUŞ

ONAY

Bilecik Şeyh Edebali Üniversitesi Fen Bilimleri Enstitüsü Yönetim Kurulunun .../.../..... tarih ve ...../..... sayılı kararı.

TEŞEKKÜR

Yüksek Lisans eğitimimin tez hazırlama süreci boyunca yardımlarını benden esirgemeyen, yoğun mesaisine rağmen beni ihmal etmeyen kıymetli hocam, Sayın Doç. Dr. İlker İNAM'a, zaman zaman kaynakların çevirilerinde bana yardımcı olan değerli mesai arkadaşım, Uzman Tevide ZÜGÜL'e katkılarından dolayı teşekkürlerimi sunarım.

Ayrıca her zaman kahrımı çeken ve sürekli bana destek olan çok kıymetli eşim Gonce KILIÇ'a teşekkürü bir borç bilirim ve bu tez çalışmasını da hayatımıza neşe kaynağı olan minik kızım Rana KILIÇ'a armağan ederim.

Mehmet KILIÇ

ÖZET

Altı bölümden oluşan bu çalışmada Sayılar Teorisi'nin yüzyıllardır popülerliğini kaybetmemiş konusu olan Diophantine denklemleri çalışılmıştır. İlk bölümde ilerleyen bölümlerde kullanılacak temel kavramlar tanımlanmış ve bu kavramlarla ilgili bazı özellikler ele alınmıştır. İkinci bölümde C bir tamsayı olmak üzere $x^2 + C = y^n$ Diophantine denkleminin tamsayı çözümleri için genel bir metot incelenmiştir. Üçüncü bölümde $x^2 + 2^k = y^n$ Diophantine denkleminde k'nın tek olması durumu, dördüncü bölümde $x^2 + 3^k = y^n$ Diophantine denklemi, beşinci bölümde $x^2 + 5^k = y^n$ Diophantine denklemi ve son olarak altıncı bölümde Ramanujan-Nagell denklemi olarak da adlandırılan $x^2 + 7 = 2^n$ Diophantine denkleminin tamsayı çözümleri aranmıştır. Çalışma derleme niteliğindedir.

Anahtar Kelimeler

Diophantine Denklemleri; Lebesgue-Nagell Denklemi; Ramanujan-Nagell Denklemi

ABSTRACT

In this work consisting of six chapters, we study one of the subjects of the Number Theory, Diophantine equations that has been popular for centuries. In the first section, the basic concepts, used later in the next chapters, are defined and some of the features related to these concepts are discussed. In the second part, general method for finding integer solutions of Diophantine equation $x^2 + C = y^n$ where C is an integer is examined. In the third chapter $x^2 + 2^k = y^n$ Diophantine equation where k is odd, in the fourth chapter $x^2 + 3^k = y^n$ Diophantine equation, fifth chapter $x^2 + 5^k = y^n$ Diophantine equations, and finally in the sixth chapter Ramanujan-Nagell equation, also called $x^2 + 7^k = 2^n$ Diophantine integer solutions of the equation are sought. The work is a compilation.

Key Words

Diophantine Equations; Lebesgue-Nagell Equation; Ramanujan-Nagell Equation

İÇİNDEKİLER

JÜRİ ONAY SAYFASI
TEŞEKKÜR
ÖZET ……... i
ABSTRACT ……..……ii
İÇİNDEKİLER ……..iii
SİMGELER VE KISALTMALAR.....…….....…….iv
1. TEMEL KAVRAMLAR.....……...1
1.1 Tanımlar, Temel Kavramlar ve Bazı Önemli Teoremler.....…….....1
2. $x^2 + C = y^n$ DİOPHANTİNE DENKLEMİNİN GENEL HALİ…….....…..13
2.1 Metod ve Teknik.....…….....14
2.2. $\pm x + \sqrt{-C} = (a + b\sqrt{-C})^p$ Denkleminin İncelenmesi.....18
3. $x^2 + 2^k = y^n$ DİOPHANTİNE DENKLEMİ.....…….....……...23
4. $x^2 + 3^m = y^n$ DİOPHANTİNE DENKLEMİ…….……27
4.1 m-nin Tek Sayı Olma Durumu.....…….....…….27
4.2 m-nin Çift Sayı Olma Durumu.…….....…….....……31
4.2.1 $4|n$ durumu.…….....…….33
4.2.2 $4 \nmid n$ durumu.…….....…….....34
5. $x^2 + 5^m = y^n$ DİOPHANTİNE DENKLEMİ…….....……38
5.1 $5x^2 + 1 = y^n$ Denklemi .....…….40
5.2 $x^2 + 5^{2m+1} = y^n$ Denklemi.....…….....……40
5.3 $x^2 + 5^{2m} = y^n$ Denklemi.....…….....……41
6. RAMANUJAN-NAGELL DİOPHANTİNE DENKLEMİ.....….....44
KAYNAKLAR ……..50
ÖZGEÇMİŞ

SİMGELER VE KISALTMALAR

Simgeler

$\mathbb{N}$: Doğal Sayılar Kümesi

$\mathbb{Z}$: Tam Sayılar Kümesi

$\mathbb{Q}$: Rasyonel Sayılar Kümesi

$\mathbb{R}$: Reel Sayılar Kümesi

$\mathbb{C}$: Kompleks Sayılar Kümesi

Σ : Toplam Sembolü

$a|b$: a, b yi böler

$a \nmid b$: a, b yi bölmez

$p^{\alpha}\|q$: $p^{\alpha}|q$ fakat $p^{\alpha+1} \nmid q$

$\binom{a}{b}$: a nın, b ye göre kombinasyonu

$\left(\frac{a}{b}\right)$: Legendre Sembolü

(a,b) : a ile b nin en büyük ortak böleni

$a \equiv b\ (mod\ m)$: a, m modülüne göre b ye denktir

$a \equiv b, c\ (mod\ m)$: $a \equiv b\ (mod\ m)$ veya $a \equiv c\ (mod\ m)$

$a \not\equiv b\ (mod\ m)$: a, m modülüne göre b ye denk değildir

$\mathbb{Z}_m$: m modülüne göre kalan sınıflarının kümesi

N : Çarpımsal norm

h_K : K cisminin sınıf sayısı (class number)

$ord_p g$: g'nin modülo p mertebesi

O_K : Tamlık halkası

TİB : Temel İdeal Bölgesi

TÇAB : Tektürlü Çarpanlarına Ayırma Bölgesi

1. TEMEL KAVRAMLAR

Bu bölümde çalışmanın ilerleyen bölümlerinde kullanılacak olan bazı temel kavramlar tanıtılacaktır. Kavramlarla ilgili ayrıntılar tanımların alındığı (Çallıalp, 2009), (Çallıalp, 2013), (Ireland ve Rosen, 1990) ve (Asar, vd., 2012) kaynaklarında bulunabilir.

1.1. Tanımlar, Temel Kavramlar ve Bazı Önemli Teoremler

Tanım 1.1.1. $m > 0$ bir tamsayı olsun. $a, b \in \mathbb{Z}$ için;

$$a \equiv b \ (mod\ m) \Leftrightarrow m|a-b$$

ile tanımlanır. Bu durumda a *ve* b, $mod\ m$ *kongrüent (denk)* denir. Böyle bir ifadeye de *kongrüans* denir (Çallıalp, 2009).

Önerme 1.1.2. Yukarıda tanımlanan "≡" bağıntısı $\mathbb{Z}$ üzerinde bir denklik bağıntısıdır (Çallıalp, 2013).

Tanım 1.1.3. $\mathbb{Z}$'deki "≡" denklik bağıntısının belirttiği denklik sınıflarına, m modülüne göre $(mod\ m)$ *kalan sınıfları* denir ve tüm kalan sınıfları kümesi $\mathbb{Z}_m$ ile gösterilir. $a \in \mathbb{Z}$ nın denklik sınıfı, $\bar{a} = \{x \in \mathbb{Z}: m|a-x\}$ dir (Çallıalp, 2013).

Tanım 1.1.4. $\mathbb{Z}_m$'de her sınıftan bir ve yalnız bir eleman alarak elde edilen sisteme *tam temsilciler sistemi* denir (Çallıalp, 2009).

Tanım 1.1.5. $\mathbb{Z}_m$'de kendileri $\bar{0}$ dan farklı olduğu halde çarpımları $\bar{0}$ olan sınıflara *sıfır bölen sınıfları* denir. Örneğin $\mathbb{Z}_6$'nın sıfır bölenleri; $\bar{2}, \bar{3}, \bar{4}$ olup, $\mathbb{Z}_{10}$'un sıfır bölenleri; $\bar{2}, \bar{4}, \bar{5}, \bar{6}, \bar{8}$ olur (Çallıalp, 2013).

Tanım 1.1.6. $\bar{a} \in \mathbb{Z}_m$ sınıfı için, $(a, m) = 1$ ise $\bar{a}$ sınıfına bir *asal kalan sınıfı* denir. $\mathbb{Z}_m$ nin tüm asal kalan sınıfları $\mathbb{Z}_m^*$ ile gösterilir ve bir tam temsilciler sistemine de *indirgenmiş tam temsilciler sistemi* denir (Çallıalp, 2009).

Tanım 1.1.7. Pozitif n tamsayısı için $1 \leq a \leq n$ ve $(a,n) = 1$ olan a tam sayılarının sayısı $\Phi(n)$ ile gösterilir ve *Euler Φ-Fonksiyonu* denir (Asar, vd., 2012).

Dikkat edilirse $\mathbb{Z}_m^*$'ın eleman sayısı $\Phi(m)$ Euler fonksiyonu yardımıyla verilir.

Teorem 1.1.8. (Euler Teoremi) $m \in \mathbb{Z}$ olsun. $(a,m) = 1$ olan her $a \in \mathbb{Z}$ için $a^{\Phi(m)} \equiv 1\ (mod\ m)$ veya $\bar{a}^{\Phi(m)} = \bar{1}$ dir (Çallıalp, 2013).

Teorem 1.1.9. (Fermat'ın Küçük Teoremi) Özel olarak $m = p$ asal sayısı için her $a \in \mathbb{Z}$ ve $p \nmid a$ için, $a^{p-1} \equiv 1\ (mod\ p)$ veya her $a \in \mathbb{Z}$ için, $a^p \equiv a\ (mod\ p)$ dir (Çallıalp, 2009).

Tanım 1.1.10. p bir asal sayı olmak üzere; $g^0 = 1, g, \dots, g^{p-2}$ indirgenmiş (sıfırdan farklı) tam temsilciler sistemi olacak şekilde bir $g \in \mathbb{Z}$ varsa g'ye modulo p bir *primitif (ilkel) kök* denir. g nin modulo p bir primitif kök olması için gerek ve yeter şart

$$g^k \equiv 1\ (mod\ p)$$

olacak şekilde en küçük k sayısının $p-1$ olmasıdır. Başka değişle $\mathbb{Z}_p^*$ çarpımsal grubunu alırsak, $\bar{g}$ nin mertebesinin $p-1$ olmasıdır (Çallıalp, 2009).

Tanım 1.1.11. $g \not\equiv 0\ (mod\ p)$, $(\bar{g} \neq 0)$ olmak üzere; $g^k \equiv 1\ (mod\ p)$ sağlayan en küçük $k > 0$ tamsayısına g'nin modülo p *mertebesi* denir ve $ord_p g$ ile gösterilir. $ord_p g$ nin $\bar{g} \in \mathbb{Z}_p^*$ nin çarpımsal mertebesi olduğu açıktır (Çallıalp, 2009).

Tanım 1.1.12. $n, m \in \mathbb{Z}^+$ olmak üzere, $x^n \equiv a\ (mod\ m)$ kongrüansının bir çözümü varsa a'ya *n-inci kuvvet rezidüsü (kalıntı)* denir. Özel olarak $n = 2$ ise *kuadratik rezidü* denir (Çallıalp, 2009).

Önerme 1.1.13. p asal sayı ve $p \nmid a$ olsun. g, modülo p bir primitif kök ve $a \equiv g^b\ (mod\ p)$ ise $x^n \equiv a\ (mod\ p)$ kongrüansının çözümü olması için gerek ve yeter şart $(n, p-1) | b$ olmasıdır (Çallıalp, 2009).

Teorem 1.1.14. (Euler Kriteri) p asal tam sayı ve $p \nmid a$, $n > 0$ olsun. $x^n \equiv a\ (mod\ p)$ nin bir çözümü olması için gerek ve yeter şart $(n, p-1) = s$ ise $a^{\frac{p-1}{s}} \equiv 1\ (mod\ p)$ olmasıdır. Özel olarak $p \neq 2$ asal ve $p \nmid a$ olsun. $x^2 \equiv a\ (mod\ p)$ nin bir çözümü olması için gerek ve yeter şart $a^{\frac{p-1}{2}} \equiv 1\ (mod\ p)$ olmasıdır (Çallıalp, 2009).

Tanım 1.1.15. $p \neq 2$ asal tam sayı olsun.

$$\left(\frac{a}{p}\right) = \begin{cases} 1, \text{eğer } p \nmid a \text{ ve } a \text{ kuadratik rezidü ise,} \\ -1, \text{eğer } p \nmid a \text{ ve } a \text{ kuadratik rezidü değil ise,} \\ 0, \text{eğer } p|a. \end{cases}$$

ile tanımlanır ve $\left(\frac{a}{p}\right)$ ye *Legendre Sembolü* denir (Çallıalp, 2009).

Önerme 1.1.16. Çallıalp'a (2009) göre Legendre Sembolü için aşağıdaki önermeler doğrudur:

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

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

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

iv. $p \nmid c$ ise $\left(\frac{ac^2}{p}\right) = \left(\frac{a}{p}\right)$ dir.

Örnek 1.1.17. $p \neq 2$ asal tamsayı olsun. Euler Kriteri yardımıyla

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1, \text{eğer } p \equiv 1\ (mod\ 4) \text{ ise} \\ -1, \text{eğer } p \equiv 3\ (mod\ 4) \text{ ise} \end{cases}$$

olduğu kolayca görülür (Çallıalp, 2009).

Uyarı 1.1.18. Çallıalp'a (2009) göre, $p \neq q$ farklı asal tek sayılar olduğunda,

$$x^2 \equiv p\ (mod\ q) \text{ ile } x^2 \equiv q\ (mod\ p)$$

kongrüanslarının çözülebilirlikleri arasında bir ilişki vardır ve bu ilişki *"Kuadratik Karşılıklılık (Quadratic Reciprocity)"* olarak bilinir.

Uyarı 1.1.19. (Kuadratik Karşılıklılık Kuralı) $p \neq q$ farklı asal tek sayılar ise,

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

dir (Çallıalp, 2009).

Tanım 1.1.20. R birimli bir halka $(0_R \neq 1_R)$ ve $0_R \neq a \in R$ olsun. Eğer $ab = 1_R$ olacak biçimde $b \in R$ varsa b'ye a nın *sağ tersi* ve $ca = 1_R$ olacak şekilde $c \in R$ varsa c ye a nın *sol tersi* denir. Eğer $d \in R$ olmak üzere $ad = da = 1_R$ ise d'ye a nın *tersi* ve a'ya *tersinir (birimsel) eleman* denir (Asar, vd., 2012).

Tanım 1.1.21. R birimli değişmeli bir halka ve $0_R \neq 1_R$ olsun. Eğer R sıfır bölensiz ise R ye bir *tamlık bölgesi* denir (Asar, vd., 2012).

Tanım 1.1.22. R birimli değişmeli bir halka ve $0_R \neq 1_R$ olsun. Eğer R nin sıfırdan farklı her elemanı tersinir ise R'ye bir *bölme halkası* denir. Değişmeli bir bölme halkasına *cisim* denir (Asar, vd., 2012).

Örnek 1.1.23. $(\mathbb{Z}, +, \cdot)$ tamlık bölgesidir. Çünkü $\mathbb{Z}$ birimli ve değişmelidir ve $m, n \in \mathbb{Z}$ için $mn = 0$ iken $m = 0$ ya da $n = 0$ dır. Ancak $\mathbb{Z}$ cisim değildir; çünkü $\mathbb{Z}$ içinde, örneğin 2'nin çarpmaya göre tersi yoktur. Buna karşın $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ ve $(\mathbb{C}, +, \cdot)$ halkaları cisimdir (Asar, vd., 2012).

Teorem 1.1.24. Her sonlu tamlık bölgesi bir cisimdir (Asar, vd., 2012).

Tanım 1.1.25. R bir halka ve I, R nin bir toplamsal altgrubu olsun. Eğer her $a \in I$ ve $r \in R$ için $ra \in I$ ise I ya R nin bir *sol ideali*, $ar \in I$ ise I ya R nin bir *sağ ideali* denir. Eğer I hem sol ideal hem de sağ ideal ise I ya R nin bir *ideali* denir (Asar, vd., 2012).

Teorem 1.1.26. R bir halka ve S, R nin boş olmayan bir alt kümesi olsun. S nin bir ideal olması için gerek ve yeter şart her $a, b \in S$ için $a + b, -a, ar, ra \in S$ olmasıdır (Asar, vd., 2012).

Tanım 1.1.27. R bir halka ve $X \subseteq R$ olsun. R nin X i içeren bütün ideallerinin kesişimine *X tarafından üretilen ideal* denir ve bir karışıklık olmadığı sürece, $\langle X \rangle$ ile gösterilecektir. Eğer $X=\{x_1, x_2, \dots, x_n\}$ ise $\langle \{x_1, x_2, \dots, x_n\} \rangle = \langle x_1, x_2, \dots, x_n \rangle$ ile gösterilir ve buna $x_1, x_2, \dots, x_n$ tarafından üretilen ideal denir. $n = 1$ için $\langle x_1 \rangle$ idealine x_1 tarafından üretilen *temel ideal* denir. Her ideali temel ideal olan bir tamlık bölgesine *temel ideal bölgesi* denir ve kısaca TİB ile gösterilir (Asar, vd., 2012).

Tanım 1.1.28. $f(x) = \sum_{i=0}^{m} a_i x^i$ polinomunda $a_m \neq 0_R$ olsun. a_m ye *başkatsayı* ve $a_m = 1_R$ ise $f(x)$'e *monik polinom* denir (Asar, vd., 2012).

Tanım 1.1.29. D bir tamlık bölgesi ve $a, b \in D$ olsun. Eğer $b = au$ olacak biçimde bir u birimsel elemanı varsa b, a ile *bağdaşıktır* denir (Asar, vd., 2012).

Tanım 1.1.30. D bir tamlık bölgesi ve $c \in D$ olsun. Eğer

i. $c \neq 0_D$ ise ve c birimsel değilse ve

ii. $a, b \in D$ olmak üzere $c = ab$ iken a ya da b birimsel ise,

o zaman c'ye *indirgenmez eleman* denir (Asar, vd., 2012).

Tanım 1.1.31. D bir tamlık bölgesi ve $p \in D$ olsun. Eğer

i. $p \neq 0_D$ ve p birimsel değilse ve

ii. $a, b \in D$ olmak üzere $p|ab$ iken $p|a$ ya da $p|b$ ise,

o zaman p'ye bir *asal eleman* denir (Asar, vd., 2012).

Lemma 1.1.32. D bir tamlık bölgesi ve $0_D \neq p \in D$ olsun. p'nin asal olması için gerek ve yeter şart pD idealinin asal olmasıdır (Asar, vd., 2012).

Lemma 1.1.33. D bir tamlık bölgesi olsun. D'nin her asal elemanı indirgenmezdir (Asar, vd., 2012).

Lemma 1.1.34. D bir TİB ve $0_D \neq c \in D$ olsun. c'nin indirgenmez olması için gerek ve yeter şart cD idealinin maksimal olmasıdır (Asar, vd., 2012).

Teorem 1.1.35. D bir TİB olsun. D'nin indirgenmez her elemanı asaldır (Asar, vd., 2012).

Tanım 1.1.36. D bir tamlık bölgesi olsun. Eğer;

i. D nin birimsel olmayan her elemanı sonlu sayıda indirgenmezin çarpımı ise ve

ii. $c_1, c_2, \dots, c_m, d_1, d_2, \dots, d_n$ D'nin indirgenmez elemanları olmak üzere

$$c_1 c_2 \dots c_m = d_1 d_2 \dots d_n$$

iken $m = n$ ve $d_1, d_2, \dots, d_m$ nin uygun indekslenmesinden sonra her $1 \leq i \leq m$ için c_i ile d_i bağdaşık ise, o zaman D ye bir *Tek Türlü Çarpanlara Ayırma Bölgesi* denir ve kısaca TÇAB ile gösterilir (Asar, vd., 2012).

Teorem 1.1.37. D bir TİB olsun. D nin sıfırdan farklı ve birimsel olmayan her elemanı sonlu sayıda indirgenmezin çarpımıdır (Asar, vd., 2012).

Teorem 1.1.38. Her TİB bir TÇAB dir (Asar, vd., 2012).

Lemma 1.1.39. D bir TÇAB olsun. D nin bir elemanının asal olması için gerek ve yeter şart indirgenmez olmasıdır (Asar, vd., 2012).

Lemma 1.1.40. D bir TÇAB olsun. Bu durumda aşağıdakiler sağlanır.

i. $a, b \in D$ ve $a \neq 0_D$ olsun. O zaman a ile b nin bir en büyük ortak böleni vardır. Daha genel olarak $a_1, a_2, \dots, a_n \in D$ en az biri sıfırdan farklı olan n eleman olsun. O zaman $a_1, a_2, \dots, a_n$ nin bir en büyük ortak böleni vardır.

ii. $a, b, c \in D$ olsun. Eğer $a|bc$ ve a ile b aralarında asal ise $a|c$ dir (Asar, vd., 2012).

Tanım 1.1.41. D bir tamlık bölgesi ve $\delta: D\backslash\{0_D\} \to \mathbb{N}$ fonksiyonu verilsin. Eğer;

i. her $a, b \in D$ ve $a \neq 0_D$ için $b = aq + r$ ve ya $r = 0_D$ ya da $\delta(r) < \delta(a)$ olacak biçimde $q, r \in D$ varsa,

ii. her $a, b \in D \backslash \{0_D\}$ için $\delta(a) \leq \delta(ab)$ ise,

o zaman D ye bir *Öklid bölgesi* denir ve kısaca ÖB ile gösterilir. Öte yandan δ'ya bir *Öklid fonksiyonu* denir (Asar, vd., 2012).

Örnek 1.1.42. δ, $\mathbb{Z}$ üzerinde mutlak değer fonksiyonu olsun. Her $z \in \mathbb{Z}$ için $|z| \in \mathbb{N}$ dir. $a, b \in \mathbb{Z}$ ve $a \neq 0$ olsun. Bölüm algoritmasından dolayı $b = qa + r$ ve $0 \leq r < |a|$ olacak biçimde $q, r \in \mathbb{Z}$ vardır. Ayrıca $b \neq 0$ iken $|b| \geq 1$ olduğundan $|a| \leq |a||b| = |ab|$ dir. Dolayısıyla $\mathbb{Z}$ bir ÖB dir (Asar, vd., 2012).

Teorem 1.1.43. F bir cisim olsun. O zaman $F[x]$ bir ÖB'dir (Asar, vd., 2012).

Teorem 1.1.44. $\mathbb{Z}[i] = \{a + ib: a, b \in \mathbb{Z}\}$ bir Öklid bölgesidir (Asar, vd., 2012).

Teorem 1.1.45. Her Öklid bölgesi bir TİB ve böylece bir TÇAB dır (Asar, vd., 2012).

Tanım 1.1.46. D bir tamlık bölgesi olsun ve bir $N: D \to \mathbb{N}$ fonksiyonu verilsin. Eğer

i. her $a, b \in D$ için $N(ab) = N(a)N(b)$ ve

ii. her $a \in D$ için $a = 0_D$ olması $N(a) = 0$ olması için gerek ve yeter şart ise

o zaman N'ye D üzerinde bir *çarpımsal norm* denir (Asar, vd., 2012).

Teorem 1.1.47. D bir tamlık bölgesi ve N, D üzerinde çarpımsal norm olsun. Bu durumda aşağıdakiler sağlanır.

i. $N(1_D) = 1$ dir. $u \in D$ olsun. Eğer u birimsel ise $N(u) = 1$ dir.

ii. Her $u \in D$ için eğer $N(u) = 1$ ise u birimsel olsun. Eğer $a \in D$ ve p bir asal sayı olmak üzere $N(a) = p$ ise o zaman a indirgenmezdir.

Sonuç 1.1.48. n hiçbir asal sayının karesiyle bölünmeyen pozitif bir tamsayı olsun. $\mathbb{Z}[\sqrt{-n}] = \{a + b\sqrt{-n}: a, b \in \mathbb{Z}\}$ tamlık bölgesi üzerinde bir N fonksiyonu her $a + b\sqrt{-n}$ için $N(a + b\sqrt{-n}) = a^2 + nb^2$ olarak tanımlansın. Bu durumda aşağıdakiler sağlanır.

i. N çarpımsal bir normdur.

ii. $u \in \mathbb{Z}[\sqrt{-n}]$ nin birimsel olması için gerek ve yeter şart $N(u) = 1$ olmasıdır. $\mathbb{Z}[i]$ nin birimselleri ± 1, $\pm i$ ve $n > 1$ için $\mathbb{Z}[\sqrt{-n}]$ nin birimselleri ± 1 dir.

iii. $\mathbb{Z}[\sqrt{-n}]$ nin sıfırdan farklı ve birimsel olmayan her elemanı sonlu sayıda indirgenmezin çarpımıdır.

Örnek 1.1.49. $\mathbb{Z}[\sqrt{-5}]$ bir TÇAB değildir (Asar, vd., 2012).

Tanım 1.1.50. D bir TÇAB ve $0_D \neq f(x) \in D[x]$ olsun. O zaman $f(x)$'in katsayılarının en büyük ortak bölenine $f(x)$'in bir *içeriği (kapsamı)* denir ve $C(f(x))$ ile gösterilir. $C(f(x))$ birimsel ise $f(x)$'e bir *ilkel polinom* denir. Özel olarak her monik polinom ilkeldir (Asar, vd., 2012).

Lemma 1.1.51. D bir TÇAB ve $f(x) = a_0 + a_1x + \ ... \ + a_nx^n \in D[x]$ sabit olmayan bir polinom olsun. Bu durumda aşağıdakiler sağlanır.

i. $f(x) = C\big(f(x)\big)g(x)$ olacak biçimde $D[x]$ in bir $g(x)$ ilkel polinomu vardır.

ii. $0_D \neq a \in D$ olsun. O zaman $C\big(af(x)\big)$ ile $aC\big(f(x)\big)$, D içinde bağdaşıktır (Asar, vd., 2012).

Lemma 1.1.52. D bir TÇAB ve $f(x), g(x) \in D[x]$ sıfırdan farklı polinomlar olsun. O zaman $C\big(f(x)g(x)\big)$ ile $C\big(f(x)\big)C\big(g(x)\big)$, D içinde bağdaşıktır. Özel olarak iki ilkel polinomun çarpımı ilkeldir (Asar, vd., 2012).

Teorem 1.1.53. D bir TÇAB olsun. O zaman $D[x]$ bir TÇAB dir (Asar, vd., 2012).

Tanım 1.1.54. Kendinden başka hiçbir alt cismi olmayan bir cisme *asal cisim* denir (Çallıalp, 2013).

Örnek 1.1.55. $\mathbb{Q}$ rasyonel sayılar cismi bir asal cisimdir. Gerçekten S, $\mathbb{Q}$ nun bir alt cismi olsa, $1 \in S$ olacağından, $\mathbb{Z} \subset S$ ve sıfırdan farklı her tam sayının tersini de

kapsayacağından, çarpma işleminin kapalılığından dolayı her rasyonel sayıyı da kapsar (Çallıalp, 2013).

Tanım 1.1.56. F cismi bir E cisminin alt cismi ise E'ye, F nin bir *genişlemesi* denir (Çallıalp, 2013).

Lemma 1.1.57. F bir cisim ve E, F'nin bir cisim genişlemesi olsun. Bu durumda E, F üzerinde bir vektör uzayıdır (Çallıalp, 2013).

Tanım 1.1.58. E, F nin bir genişlemesi ise bu durumda E'nin F-uzayı olarak boyutuna E'nin F üzerindeki *derecesi* denir ve $[E:F]$ ile gösterilir (Çallıalp, 2013).

Tanım 1.1.59. E, F nin bir genişlemesi ve $[E:F]$ sonlu ise genişlemeye *sonlu genişleme* denir (Çallıalp, 2013).

Tanım 1.1.60. E, F nin bir genişlemesi olsun. Bir $\alpha \in E$ için, $f(\alpha) = 0$ olacak şekilde, sıfır polinomdan farklı bir

$$f(x) = a_0 + a_1 x + \ \ldots + a_n x^n \in F[x]$$

polinomu varsa α'ya, F üzerinde bir *cebirsel eleman* denir (Çallıalp, 2013).

Tanım 1.1.61. E, F nin bir genişlemesi ve her $\alpha \in E$, F üzerinde cebirsel ise E'ye F'nin bir *cebirsel genişlemesi* denir (Çallıalp, 2013).

Önerme 1.1.62. Her sonlu genişleme bir cebirsel genişlemedir (Çallıalp, 2013).

Tanım 1.1.63. $\mathbb{Q}$ rasyonel sayılar cisminin bir sonlu genişlemesine *sayı cismi* denir. Özel olarak ikinci dereceden bir sayı cismine de *kuadratik sayı cismi* denir (Çallıalp, 2009).

Uyarı 1.1.64. $[K:\mathbb{Q}] = 2$ ise d, kare çarpansız bir tamsayı olmak üzere, $K = \mathbb{Q}(\sqrt{d})$ olarak alınabilir. Bu durumda $\{1, \sqrt{d}\}$ de K'nın $\mathbb{Q}$ üzerinde bir tabanı olur. Yani her $\alpha \in \mathbb{Q}(\sqrt{d})$ elemanı $a, b \in \mathbb{Q}$ olmak üzere $\alpha = a + b\sqrt{d}$ şeklinde yazılabilir ve bu yazılış tek türlüdür. Eğer; $d > 0$ ise $\mathbb{Q}(\sqrt{d})$ ye, *reel kuadratik sayı cismi*, $d < 0$ ise *sanal kuadratik sayı cismi* denir (Çallıalp, 2009).

Tanım 1.1.65. $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ olsun. $\bar{\alpha} = a + b\sqrt{d}$ ye $\alpha = a + b\sqrt{d}$ nin *eşleniği* denir. $N(\alpha) = \alpha\bar{\alpha} = a^2 - db^2$ ve $\text{İz}(\alpha) = \alpha + \bar{\alpha} = 2a$ ile tanımlı $\mathbb{Q}(\sqrt{d}) \to \mathbb{Q}$ ye fonksiyonlarına sırasıyla *norm* ve *iz* denir (Çallıalp, 2009).

Önerme 1.1.66. Norm ve İz fonksiyonlarının aşağıdaki özellikleri vardır. Her $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$ için,

- **i.** $\text{İz}(\alpha + \beta) = \text{İz}(\alpha) + \text{İz}(\beta)$,
- **ii.** $N(\alpha\beta) = N(\alpha)N(\beta)$,
- **iii.** $N(\alpha) = 0 \Leftrightarrow \alpha = 0$
- **iv.** α, $X^2 - \text{İz}(\alpha)X + N(\alpha) \in \mathbb{Q}[X]$ polinomunun bir köküdür (Çallıalp, 2009).

Tanım 1.1.67. Bir kompleks sayı $\mathbb{Q}$ üzerinde cebirsel ise bu sayıya bir cebirsel sayı denir (Çallıalp, 2013).

Tanım 1.1.68. α bir cebirsel sayı olsun. $f(\alpha) = 0$ olacak şekilde bir,

$$f(x) = x^n + a_1x^{n-1} + \ \ldots + a_n \in \mathbb{Z}[x]$$

polinomu varsa α'ya *cebirsel tamsayı* denir (Çallıalp, 2013).

Önerme 1.1.69. Bir rasyonel sayının, cebirsel tamsayı olması için gerek ve yeter koşul tamsayı olmasıdır (Çallıalp, 2013).

Teorem 1.1.70. d kare çarpansız bir tam sayı ve $K = \mathbb{Q}(\sqrt{d})$ nin cebirsel tam sayılar kümesi O_K olsun. Bu durumda,

$$w_d = \begin{cases} \sqrt{d}; \text{eğer } d \equiv 2,3\ (mod\ 4) \text{ ise,} \\ \dfrac{1+\sqrt{d}}{2};\ \text{eğer } d \equiv 1\ (mod\ 4) \text{ ise} \end{cases}$$

olmak üzere O_K nin her elemanı, $x, y \in \mathbb{Z}$ için $x + yw_d$ şeklinde yazılabilir (Çallıalp, 2009).

Sonuç 1.1.71. O_K cebirsel tamsayılar kümesi, $\mathbb{Q}(\sqrt{d})$ nin bir alt halkasını ve şu halde bir alt tamlık bölgesini oluşturur (Çallıalp, 2009).

Tanım 1.1.72. O_K'ya $K = \mathbb{Q}(\sqrt{d})$ nin *tamlık halkası* ve $\{1, w_d\}$ ye de bir *tamlık tabanı* denir (Çallıalp, 2009).

Tanım 1.1.73. $u \in O_K$ ve $u|1$ ise u ya, $\mathbb{Q}(\sqrt{d})$ cisminin veya O_k halkasının bir *aritmetik birimi* veya *birimsel elemanı* denir. Birimsel elemanlar kümesi O_K^* ile gösterilir (Çallıalp, 2009).

Önerme 1.1.74. O_K halkasının birimsel elemanlar kümesi O_K^*, çarpımsal bir gruptur. Bu gruba K nın *birim grubu* denir (Çallıalp, 2009).

Önerme 1.1.75. $u \in O_K^*$ ise $\pm u, \pm\bar{u} \in O_K^*$ dır. $\alpha \in O_K$nın birimsel olması için gerek ve yeter şart $N(\alpha) = \pm 1$ olmasıdır (Çallıalp, 2009).

Önerme 1.1.76. $d < 0$, $d \neq 1$, $d \neq 3$ ise $\mathbb{Q}(\sqrt{d})$ sanal kuadratik sayı cisminin birimsel elemanları yalnız ± 1 dir. $\mathbb{Q}(\sqrt{-1})$ cisminin birimsel elemanları 4 tane $\{\pm 1, \mp i\}$ ve $\mathbb{Q}(\sqrt{-3})$ cisminin birimsel elemanları 6 tane olup $\left\{\pm 1, \frac{\pm 1 \mp i\sqrt{-3}}{2}\right\}$ dir (Çallıalp, 2009).

Tanım 1.1.77. $A, B \subset O_K$ iki ideal olmak üzere $\langle\alpha\rangle A = \langle\beta\rangle B$ olacak şekilde sıfırdan farklı $\alpha, \beta \in O_K$ elemanları bulunabiliyorsa A ve B ideallerine *denk idealler* denir ve $A \sim B$ ile gösterilir. Bu bir denklik bağıntısıdır. Burada tanımlanan denklik sınıfları,

ideal sınıfları olarak adlandırılır. İdeal sınıflarının sayısına K cisminin *sınıf sayısı* denir ve h_K ile gösterilir (Ireland ve Rosen, 1990)

Teorem 1.1.78. K bir sayı cismi ve O_K, K cisminin tamlık halkası olsun. Bu durumda; O_K tamlık halkasının bir TİB olması için gerek ve yeter şart $h_K = 1$ olmasıdır (Ireland ve Rosen, 1990)

Teorem 1.1.79. K bir sayı cismi ve h_K bu sayı cisminin sınıf sayısı olsun. h_K sonlu bir tam sayıdır (Ireland ve Rosen, 1990).

Teorem 1.1.80. K bir sayı cismi ve h_K bu sayı cisminin sınıf sayısı olsun. Her idealin h_K-inci kuvveti bir temel idealdir (Kılıçlı, 2014).

Tanım 1.1.81. $m > 1$ kare-çarpansız olsun ve $\mathbb{Q}(\sqrt{m})$ kuadratik sayı cismi ve O_m bu sayı cisminin tamsayı halkası olsun. $\epsilon \in O_m$'nin bir birimi olmak üzere $N(\epsilon) = \pm 1$ eşitliği sağlansın. Bu durumda eğer $\epsilon > 1$ ise ϵ'a *temel birim* denir ve bunun dışındaki her birim $n \in \mathbb{Z}$ için $\pm\epsilon^n$ biçimindedir (Finch, 2005).

2. $x^2 + C = y^n$ DİOPHANTİNE DENKLEMİ

Bu bölümde *C* bir tamsayı olmak üzere $x^2 + C = y^n$ denkleminin çözümü için genel teorik metot verilecektir. Burada Cohn (1993a), makalesinden faydalanılmıştır. Daha genel olarak, güzel bir literatür taraması Vîrgolici (2013) çalışmasında bulunabilir. Öte yandan bu bölümde verilen sonuçlar teorik olduğu için bu tezde yer alan Diophantine denklemlerinden farklı denklemlerin çalışıldığı Kılıçlı (2014) yüksek lisans teziyle benzerlik taşımaktadır.

Bu denklemde *n*'nin çift sayı yani $k \in \mathbb{Z}$ olmak üzere $n = 2k$ olması durumunda *C* sayısı,

$$x^2 + C = y^{2k} \Rightarrow y^{2k} - x^2 = C \Rightarrow (y^k - x)(y^k + x) = C$$

olarak yazılabildiğinden problem oldukça kolaylaşır.

n'nin tek sayı olması durumunda gerektiği yerde uygun değişken değişimi yapılarak genellik bozulmadan *p* tek asal olmak üzere $n = p$ durumu göz önüne alınabilir.

$p = 3$ durumunda denklem $x^2 + C = y^3$ halini alır ki bu denklem bir eliptik eğri belirtir detaylar için Silverman (1986), kitabına bakılabilir. Mordell (1969) bu denklemin tamsayı çözümlerini bir araya getirmiştir.

$p = 5$ için Blass (1976) ve Wren (1973), $p = 7$ için Blass ve Steiner (1978) çalışmalarında bazı sonuçlar bilinmektedir. Burada Hipereliptik Eğriler Teorisi de kullanılabilir. Temel referans olarak Bugeaud, vd. (2008) göz önüne alınabilir.

$C = 1, 2$ ve 4 için metot iki aşamadan oluşmaktadır. İlk olarak $\mathbb{Q}[\sqrt{-1}]$ ve $\mathbb{Q}[\sqrt{-2}]$ cisimleri birer TİB ve böylece Teorem 1.45. gereği TÇAB olduğundan bu özellik kullanılarak, belli a değerleri için $y = a^2 + C$ olduğu gösterilir. O halde ikinci adımda $\mathbb{Q}[\sqrt{a^2 + C}\,]$ cismindeki temel birim, a cinsinden basitçe ifade edilir.

C'nin diğer değerleri için ilk aşama geçilse bile ikincisi sağlanamaz bu yüzden ispatı tamamlamak için farklı bir metot gereklidir. Nagell (1954a), $C = 8$ için böyle bir metot buldu ve bu durumda denklemin bir çözümünün olmadığını ispatladı.

Literatürde genel p değerleri için oldukça az sonuç bulunabilmektedir. İlgili yıllarda dergilere ulaşım sınırlı olduğundan sonuçların tekrarlandığı çok fazla durum vardır. Örneğin $C = 2$ için ilk kez Ljunggren (1943a) çalışmasında verilen ispat, Nagell (1954b) çalışmasında tekrarlanmıştır. $C = 3$ için ilk defa Nagell (1923) tarafından ispatlanan sonucu, Brown (1975) ve ardından da Cohn (1993a) tekrarlamıştır. İlk çalışmalarda çoğunlukla C'nin incelenen değerleri için deneme-yanılma metotu kullanılmıştır.

2.1. Metod ve Teknik

Doğal olarak öncelik denklemin sol tarafını $\sqrt{-C}$ sayısının elemanı olduğu imajiner kuadratik sayı cisminde $\left(x + \sqrt{-C}\right)\left(x - \sqrt{-C}\right) = y^p$ şeklinde çarpanlara ayırmak olacaktır ki, bu durumda belli a ve b tamsayıları için eğer;

$$\pm x + \sqrt{-C} = (a + b\sqrt{-C})^p \tag{2.1}$$

ise, gerçekten de x, $y = a^2 + b^2C$ ile bir çözüm belirtir. Aşağıdaki koşullarla birlikte (2.1) çözüm için yeterli koşul olur. Eğer;

(1) $C \not\equiv 3\ (mod\ 4)$ ise,

(2) Birim eleman sorunu çıkmazsa,

(3) Cisim tek türlü çarpanlarına ayrılabilirse,

(4) C kare çarpansız ise,

(5) $\pm x + \sqrt{-C}$ çarpanları aralarında asal ise,

fakat her durumda (2.1) koşulunun çözüm için yeter şart olduğu doğrudur. Bu olasılık her C için dikkate alınması gerektiğinden bununla ilgili bazı sonuçları bir sonraki bölümde çözeceğiz. Buna geçmeden önce yukarıdaki maddeleri inceleyelim.

İlk olarak, $C \equiv 3\ (mod\ 4)$ ise (2.1)'e ek olarak gerekli şart, $y = \frac{1}{4}(A^2 + B^2C)$ olmak üzere,

$$\pm x + \sqrt{-C} = (\tfrac{1}{2}\left(A + B\sqrt{-C}\right))^p,\ A \equiv B \equiv 1\ (mod\ 2) \tag{2.2}$$

elde edilir. Bu yalnızca $p = 3$ ise olabilir. (2.2)'de imajiner kısımları eşitlersek,

$$2^p = B\sum_{r=0}^{\frac{p-1}{2}}\binom{p}{2r+1}A^{p-2r-1}(-B^2C)^r \tag{2.3}$$

eşitliğini elde ederiz. Bundan dolayı B tek olduğundan, $B = \pm 1$ dir. Böylece

$$\pm 2 \equiv \pm 2^p \equiv (-C)^{\frac{p-1}{2}} \equiv \left(\frac{-C}{p}\right) \equiv 0, \pm 1\ (mod\ p) \tag{2.4}$$

olur ki bu da $p = 3$ olduğunu gösterir ve bu değerler (2.3)'te yerine yazılarak $\pm 8 = 3A^2 - C$ elde edilir. Daha ayrıntılı açıklamak gerekirse, (2.4)'te, ilk denklik Fermat'ın Küçük Teoremi (Teorem 1.1.9.), ikinci denklik Eşitlik (2.3)'ün mod p'ye göre hesaplanması, üçüncü ve dördüncü denklik Legendre sembolünün özellikleri yardımıyla elde edilmiştir. Böylece aşağıdaki lemma ispatlanmış olur.

Lemma 2.1.1. (2.2)'deki durum ancak ve ancak $C = 3A^2 \pm 8$ iken gerçekleşir ve sadece $p = 3$, durumunda çözüm vardır ve bu çözüm $x = A^3 \pm 3A$ şeklindedir (Cohn, 1993a).

Dikkat edilirse $C = 3d^2$ ise altı birim vardır. ± 1, $\pm w$ ve $\pm w^2$ dir. (2.1) veya (2.2)'den başka, yeni bir durum daha söz konusudur, bu da

$$\pm x + d\sqrt{-3} = w\left(\frac{1}{2}\left(A + Bd\sqrt{-3}\right)\right)^3,\ A \equiv B\ (mod\ 2) \tag{2.5}$$

olmasıdır.

Lemma 2.1.2. (2.5)'teki durum ancak ve ancak $C = 48D^6$, $x = 4D^3$, $p = 3$ olduğunda geçerlidir (Cohn, 1993a).

Uyarı 2.1.3. Eğer $C < 0$ durumu hesaba katılsaydı bu durumda birimleri bulma problemi oldukça karmaşık bir hal alacaktı. Bu ise $C > 0$ kısıtlamasının önemini gösterir. Teorem 1.1.78. gereği bir kuadratik sayı cisminin tamlık halkasının TÇAB olması için gerekli koşul sınıf sayısının 1 olmasıdır. Buna göre Sanal kuadratik sayı cisimleri için sınıf sayısının 1 olduğu durumlar, bu cisimlerin sonlu sayıda ve $C = 1, 2, 3, 7, 11, 19, 43, 67, 163$ değerlerine karşılık gelen $\mathbb{Q}[\sqrt{-C}]$ cisimleri olduğu bilinmektedir Sadece 9 durumun ortaya çıkması problemin kapsamının daralması gibi gözükse de durum böyle değildir. Örneğin, $C = 6$ için $\mathbb{Q}[\sqrt{-6}]$ cisminin sınıf sayısı $h = 2$ dir.

Denklemin herhangi bir olası çözümü için, $(x, 6) = 1$ ve p tektir. Bu durumda $x + \sqrt{-6}$ tarafından oluşturulan temel ideal π eşleniği π', $[y]^p$ ile aralarında asaldır. Böylece bazı ξ idealleri için $\pi = \xi^p$ dir. Fakat istediğimiz sonuç, $x + \sqrt{-6} = \left(a + b\sqrt{-6}\right)^p$, ξ'nın bir temel ideal olup olmadığı bilinmediği için doğrudan doğruya istenilen sonuç elde edilmez. Ancak $h = 2$ olduğundan, ξ^2'nin temel ideal olduğu sonucu çıkar ve dolayısıyla $\left(x + \sqrt{-6}\right)^2$ sayısı bu cisimde bir elemanın p-inci kuvvetine eşit olmalıdır. p tek olduğundan, o zaman bu elde edilir ki $x + \sqrt{-6}$ kendisi de bu özellikte bir kuvvettir. Bu durumda aşağıda Lemma 2.2.2 ve Lemma 2.2.3 den, eğer $C = 6$ ise denklemin hiçbir durumda çözümünün olmadığı elde edilecektir.

Aynı argümanlar diğer durumlar için de kullanılabilir. Burada $h = 1$ olması önemli değil fakat önemli olan $p \nmid h$ olmasıdır. h, ancak 2'nin bir kuvveti olursa bu her tek asal sayı için geçerli olacaktır. h'nin diğer değerleri için yine bu durum geçerli olduğundan sadece sınıf sayısını bölmeyen sonlu sayıda asal değerler için bu metod kullanabilirdir. Diğer istisnai durumlar ise farklı metodlarla çözülmelidir. Böylece örneğin $C = 26$ için, $h = 6$ olur ve bu nedenle $p = 3$ olmadıkça yukarıdaki metod uygulanabilirdir ve $p = 3$ durumu ayrı olarak ele alınmalıdır (Cohn, 1993a).

Eğer C kare-çarpansız değilse $C = cd^2$ yazılabilir, burada c kare-çarpansızdır. Bu durumda (2.1) koşuluna ek olarak;

$$\pm x + d\sqrt{-c} = \left(a + b\sqrt{-c}\right)^p \tag{2.6}$$

elde edilir ve ayrıca $c \equiv 3 \ (mod\ 4)$ ise

$$\pm x + d\sqrt{-c} = \left(\frac{1}{2}\left(A + B\sqrt{-c}\right)\right)^p, A \equiv B \equiv 1 \ (mod\ 2) \tag{2.7}$$

dir (Cohn, 1993a).

Bu denklem üzerinde gerekli analiz yapılarak aşağıdaki teorem elde edilir.

Teorem 2.1.4. $C > 0$, $C = cd^2$, c kare-çarpansız, $p \not\equiv 7 \ (mod\ 8)$ olsun. Eğer p asal tek sayı ve $x^2 + C = y^p$ ise bu durumda aralarında asal x ve y pozitif tamsayıları için aşağıdaki önermelerden en az birisi doğrudur.

(a) Öyle a ve b tamsayıları vardır ki $b|d$ olmak üzere $y = a^2 + b^2c$ ve $\pm x + d\sqrt{-c} = \left(a + b\sqrt{-c}\right)^p$ dir.

(b) $c \equiv 3 \ (mod\ 8)$, $p = 3$ ve $B|d$ olmak üzere A ve B tek tamsayıları vardır, $y = \frac{1}{4}(A^2 + B^2c)$, $\pm x + d\sqrt{-c} = \frac{1}{8}\left(A + B\sqrt{-c}\right)^3$ tür.

(c) $p|h$, $\mathbb{Q}[\sqrt{-c}]$ cisminin sınıf sayısıdır.

(d) $C = 3A^2 \pm 8$, $p = 3$, $x = A^3 \pm 3A$ dır.

(e) $C = 48D^6$, $p = 3$, $x = 4D^3$ tür (Cohn, 1993a).

2.2. $\pm x + \sqrt{-C} = (a + b\sqrt{-C})^p$ Denkleminin İncelenmesi

Verilen denklemde imajiner kısımlar eşitlenirse,

$$1 = b\sum_{r=0}^{\frac{p-1}{2}} \binom{p}{2r+1} a^{p-2r-1}.(-Cb^2)^r$$

ve dolayısıyla $b = \pm 1$ olduğu elde edilir. Böylece

$$\pm 1 \equiv \sum_{r=0}^{\frac{p-1}{2}} \binom{p}{2r+1} a^{p-2r-1}.(-C)^r \tag{2.8}$$

olur ve bundan geri kalan sonuçlar izleyecektir. (2.8) den açık olarak a ve C nin biri çift iken diğeri tek biri tek iken diğeri çift olduğu anlaşılır. Eğer a ve C her ikisi de çift olsaydı (2.8) denkleminin sağ tarafı da çift olacaktı. Dolayısıyla eğer her ikisi de tek olsaydı bu durumda

$$\pm 1 \equiv \sum_{r=0}^{\frac{p-1}{2}} \binom{p}{2r+1} = 2^{p-1} \equiv 0 \ (mod\ 2)$$

denkliği elde edilmeliydi. (2.8) denklemiyle ilgili Cohn (1993a) çalışmasında verilen ayrıntılı sonuçlar aşağıda sıralanmıştır.

Lemma 2.2.1. q, (2.8) denklemini sağlayan a nın herhangi bir asal tek böleni olsun. Bu durumda $C^{q-1} \equiv 1 \ (mod\ q^2)$; $p = q = 3$ olmadıkça, $q^{\alpha} \| a$ ise bu durumda $q^{2\alpha} \| (C^{q-1})$ dir (Cohn, 1993a).

Lemma 2.2.2. (2.8) denkleminde negatif işaret durumu sadece $p \equiv 3 \ (mod\ 4)$ ise gerçekleşebilir ve aşağıdaki şartların her ikisi de (2.8) denklemini karşılar;

1. Ya,

(a) $C \equiv 1$ veya $13 \ (mod\ 16)$, veya

(b) $C \equiv 0 \ (mod\ 8)$ ve $p \equiv 7 \ (mod\ 8)$ veya

(c) $C \equiv 4 \ (mod\ 8)$ ve $p \equiv 3 \ (mod\ 8)$

dir.

2. Ya da,

(a) $C \equiv 1 \ (mod\ 9)$ veya

(b) $C \equiv 0 \ (mod\ 3)$ ve $p \equiv 2 \ (mod\ 8)$ veya

(c) $C \equiv 4$ veya $7 \ (mod\ 9)$ ve $p \equiv 3 \ (mod\ 8)$

dir (Cohn, 1993a).

Lemma 2.2.3. (2.8) denkleminde pozitif işaret durumu sadece aşağıdaki durumların her ikisi de sağlandığında gerçekleşebilir.

1. Ya,

(a) $C \equiv 3 \ (mod\ 4)$, veya

(b) $C \equiv 1 \ (mod\ 4)$, $2^{2\gamma} \| (C-1)$ ve $p \equiv 1 \ (mod\ 4)$, veya

(c) $C \equiv 2 \ (mod\ 8)$ ve $p \equiv 3 \ (mod\ 8)$, veya

(d) $C \equiv 6 \ (mod\ 8)$ ve $p \equiv 7 \ (mod\ 8)$

dir .

2. Ya da,

(a) $C \equiv 2 \ (mod\ 3)$, veya

(b) $C \equiv 4$ veya $7 \ (mod\ 9)$ ve $p \equiv 1$ veya $7 \ (mod\ 8)$, veya

(c) $C \equiv 1 \ (mod\ 9)$ ve $p \not\equiv 3 \ (mod\ 8)$, veya

(d) $C \equiv 21 \ (mod\ 27)$ ve $p \equiv 1 \ (mod\ 3)$

tür (Cohn, 1993a).

Lemma 2.2.4. P, C sayısını bölen bir asal tek sayı olsun. Bu durumda (2.8) denkleminin pozitif eşitliği mevcut iken $pa^{p-1} \equiv 1 \ (mod\ P)$, $\left(\frac{p}{P}\right) = 1$ dir ve $P \neq 3$ ise

$p \not\equiv 1\ (mod\ P)$ bulunur. Buna karşılık (2.8) denkleminin negatif eşitliği mevcut iken $pa^{p-1} \equiv -1\ (mod\ P)$, $\left(\frac{-p}{P}\right) = 1$ ve $p \not\equiv 1\ (mod\ P)$ dir (Cohn, 1993a).

Lemma 2.2.5. (2.8) eşitliğinde $p = 3$ olması için gerek ve yeter şart $C = 3a^2 \pm 1$ ve $x = 8a^3 \pm 3a$ olmasıdır. $p = 5$ olması için gerek ve yeter şart $C = 19$, $x = 22434$ ya da $C = 341$, $x = 2759646$ olmasıdır. $p = 7$ iken denklemin bir çözümü yoktur (Cohn, 1993a).

Bazı durumlarda örneğin; $C = 6$ olduğunda çözümün olmadığını söyleyebilmek için (2.8) denkleminin her iki işaret içinde mümkün olmadığını göstermek yeterlidir. Bu eşitliğin her iki işaret için de imkansız olduğu gösterilemediği durumlarda nasıl hareket edilecektir? Şimdi verilecek metot kullanılırken bir çok hesaplamanın bir arada kullanılması gerekebilir. Bununla birlikte bu metot yardımıyla çoğunlukla bir çözüm elde edilmesine rağmen, her durumda bir çözüme ulaşılabileceğinin garantisi yoktur.

a ve $m \geq 0$ tam sayıları için bir tam sayı fonksiyonu;

$$f_m(a) = \frac{\left(a + \sqrt{-C}\right)^m - \left(a - \sqrt{-C}\right)^m}{2\sqrt{-C}} \tag{2.9}$$

şeklinde tanımlansın. Dolayısıyla (2.8) denklemi $f_p(a) = \mp 1$ formunda yazılabilir. Bu durumda C yi bölmeyen q asal tek sayıları tek tek denklemde yerine konulabilir ya da (2.9) denkleminin daha önceki lemmalar tarafından dışarıda bırakılmamış p değerleri için $mod\ q$ ya göre imkansız olduğu gösterilerek bir çözüm olmadığı ispatlanabilir.

Öncelikle m nin bir fonksiyonu olarak $\{f_m(a)\}$ dizisi $mod\ q$ ya göre periyodik olur. Gerçekten de bu periyot $\left(\frac{-C}{q}\right) = \mp 1$ Legendre sembolünün işaretine göre değişen ve sırasıyla $-C$ bir kuadratik rezidü iken $\mathrm{Q} = q - 1$, değil iken $\mathrm{Q} = q^2 - 1$ şeklinde alan Q sayısının bir katıdır. Burada;

$$\left(a+\sqrt{-C}\right)^{q} \equiv a^{q} + (-C)^{(q-1)/2}\sqrt{-C} \equiv a + \left(\frac{-C}{q}\right)\sqrt{-C}\ (mod\ q)$$

olup benzer şekilde eşleniği için de $\left(\frac{-C}{q}\right) = -1$ ise aynı işlem sürdürülerek

$$\left(a+\sqrt{-C}\right)^{q^2} \equiv \left(a-\sqrt{-C}\right)^{q} \equiv \left(a+\sqrt{-C}\right)\ (mod\ q)$$

elde edilir. Böylece her iki durumda da $f_{m+\mathrm{Q}}(a) \equiv f_m(a)\ (mod\ q)$ bulunur. Dolayısıyla bu fonksiyon $mod\ q$ ya göre periyodik bir fonksiyondur. Ayrıca (2.9)'ye göre bu fonksiyonun tanımından $f_0(a) = 0$ ve $f_1(a) = 1$ şeklindedir ve $m \geq 0$ sayısı için;

$$f_{m+2}(a) \equiv 2af_{m+1}(a) - (a^2 + C)f_m(a) \tag{2.10}$$

eşitliği mevcuttur. Bunun yanı sıra a nın fonksiyonu olarak $f_m(a)$ bir polinomdur ve m tek sayı iken bu polinom a'nın yalnızca çift kuvvetlerini içerir. Bu nedenle $f_p(a) \equiv \pm 1\ (mod\ q)$ kongrüansını çözebilmek için $1 \leq m \leq \mathrm{Q} - 1$ ve $0 \leq a \leq \frac{q}{2}$ aralığındaki değerler için yalnızca $p \equiv m\ (mod\ \mathrm{Q})$ kongrüansını ele almak yeterlidir. Lemma 2.2.3 kullanılarak $q^2 \nmid (C^{q-1} - 1)$ olduğu kontrol edilmek şartıyla $a = 0$ değeri değerlendirme dışı tutulabilir. Kullanılacak olan q asal sayılarından bu koşulu sağlamayanları eleyebiliriz.

Metodun uygulanma süreci şu şekilde işleyecektir. İlk olarak verilen bir C sayısı için, C yi bölmeyen q asal sayılarından Lemma 2.2.3'ten a sayısını bölmeyenler seçilir. Bu asal sayılardan her biri için, (2.10) eşitliği kullanılarak $1 \leq a \leq {}^{q}/_{2}$ aralığındaki her a sayısı ve $1 \leq m \leq \mathrm{Q} - 1$ aralığındaki her m tek sayısı için $f_m(a)$ değerlerinin $mod\ q$'ya göre kalanları hesaplanır. Bu metot yardımıyla her a sayısı için kongrüansın sağlandığı aralıktaki m değerleri listelenir. Böylelikle p, $mod\ \mathrm{Q}$'nun kalan sınıflarından birinin elemanı olmak durumunda kalır. Ayrıca bu listeden p'nin asal olmadığı kalanlar çıkartılabilir. Örneğin; $\mathrm{Q} = 66$ sayısı için 15 değeri listeden çıkartılabilir. İşlemler bu şekilde devam ettirilerek istenilen şekilde, yeterli sayıda kongrüans koşulları bulunur ve

bu kongrüanslar Lemma 2.2.4 ve Lemma 2.2.5 ile birlikte düşünülerek bir çözüm elde edilmeye çalışılır.

(2.8) denkleminde pozitif işaretin olduğu durumda üstteki metodun kullanışlı olup olmayacağı konusunda endişe duyulabilir, çünkü $f_1(a) = 1$ olduğundan $p \equiv 1\ (mod\ Q)$ durumu önceki tartışmalardan dolayı hariç bırakılmaz. Bu nedenle, $p \equiv 1\ (mod\ 4)$ durumu Lemma 2.2.5 tarafından çıkarılmadıkça, ne kadar çok sayıda q asalı için metot tekrar edilirse $(p-1)$ in o kadar sayıda farklı çarpanının olması gerektiği görülür. Bununla birlikte, eğer C sayısı 5 yada 5'ten büyük bir P asal çarpanına sahipse Q sayısını bölen P asal sayılarına karşılık uygun q asalları seçilerek $p \equiv 1\ (mod\ P)$ olduğunu ispatlamak gerekir. Ancak bu Lemma 2.2.5'e göre mümkün değildir. Bu işlem direkt olarak yapılabildiği gibi, bazen de örneğin; $C = 21$ için pozitif eşitlik mümkün olmadığında C sayısını bölen 3'ten büyük P asal sayıları için $(P-1)|(p-1)$ olduğu ispatlanarak yapılabilir. Bununla birlikte, bazı durumlarda örneğin; $C = 17$ için bu iki yöntemin aynı anda kullanılması gerekebilir. Ayrıca Lemma 2.2.5'ten dolayı (2.8) denkleminin negatif eşitliği C'nin yalnızca 2 ve 3 çarpanlarını içerdiği durumlarda gerçeklenmeyecektir (Cohn, 1993a).

3. $x^2 + 2^k = y^n$ DİOPHANTİNE DENKLEMİ

Bu bölümde k sayının tek sayı olması durumu incelenerek bu Diophantine denkleminin en genel tamsayı çözümleri verilecektir.

Teorem 3.1 k tek sayı olsun. Bu durumda $x^2 + 2^k = y^n$ denkleminin tüm tamsayı çözümleri x, y pozitif sayılar, $n \geq 3$ ve $\alpha \geq 0$ olmak üzere aşağıdaki gibidir (Cohn, 1992).

k	x	y	n
$6\alpha + 1$	$5.2^{3\alpha}$	$3.2^{2\alpha}$	3
$4\alpha + 5$	$7.2^{2\alpha}$	3.2^{α}	4
$10\alpha + 5$	$11.2^{5\alpha+3}$	$3.2^{2\alpha+1}$	5

Uyarı 3.2. Yukarıda verilen çözümlere dikkat edilirse, α'nın her bir değeri için farklı bir çözüm elde edilir. Bu ise çözüm kümesinin üç sonsuz aileden oluştuğunu gösterir. Bu ailelerin birbirinden farklı olduğu açıktır.

Bu denklemin çözümü 2. bölümde verilen metotlar yardımıyla elde edilecektir. k tek sayı yani $K \in \mathbb{Z}$ olmak üzere $k = 2K + 1$ olsun. k = 3 durumu için Nagell (1955) tarafından bir metot verilmiştir. Cohn (1992) aşağıdaki lemmayla birlikte Nagell'in sonucunu genelleştirmiştir.

Lemma 3.3. x, y pozitif tamsayılar ve $n \geq 3$ olmak üzere $2x^2 + 1 = y^n$ denkleminin $x = 11$, $y = 3$, $n = 5$ dışında bir çözümü yoktur (Cohn, 1992).

Teorem 3.1'in İspatı. Lemma 3.3 gereği $k = 1$ için, $K > 0$ olduğu kabul edilecektir.
İlk olarak x ve n tek sayı olsun. O halde $y \equiv 1 \ (mod\ 8)$ dir. Bundan dolayı $\mathbb{Q}[\sqrt{-2}]$ cisminde tek türlü asal çarpanlara ayırma yardımıyla

$$\left(x + 2^K\sqrt{-2}\right)\left(x - 2^K\sqrt{-2}\right) = y^n \tag{3.1}$$

yazılabilir ve burada sol taraftaki çarpanların ortak böleni yoktur. Böylece bazı a ve b tamsayıları için

$$\left(x + 2^K\sqrt{-2}\right) = \left(a + b\sqrt{-2}\right)^n \tag{3.2}$$

ve $y = a^2+2b^2 \equiv 1\ (mod\ 8)$ olarak elde edilir. Böylece a tek ve b çift sayı olur. (3.2)'de imajiner kısımlar eşitlenerek

$$2^K = b\sum_{r=0}^{\frac{n-1}{2}} \binom{n}{2r+1} a^{n-2r-1}(-2b^2)^r \tag{3.3}$$

ve bundan dolayı sağ taraftaki ikinci çarpan tek olduğundan $b = \pm 2^K$ dır. Böylece $y = a^2+2^{2K+1}$ dir. Burada a tek ve

$$\pm 1 = \sum_{r=0}^{\frac{n-1}{2}} \binom{n}{2r+1} a^{n-2r-1}(-2^{2K+1})^r \tag{3.4}$$

olur. Şimdi ya $3|a$'dır ve bu durumda (3.4) nin sağ tarafı $mod\ 3$ te 1'e denktir ya da $a^2 \equiv 1\ (mod\ 3)$'tür ve bu durumda

$$\sum_{r=0}^{\frac{n-1}{2}} \binom{n}{2r+1} = 2^{n-1} \equiv 1\ (mod\ 3) \tag{3.5}$$

olur. Böylece (3.4)'te negatif işaret alınmaz ve $n \equiv 1\ (mod\ 8)$ sonucunu elde edilir. O halde $\varrho \geq 3$ ve t tek sayı olmak üzere $n - 1 = 2^{\varrho}.t$ olsun. Bu durumda $\{u_m\}$ ve $\{v_m\}$ dizileri $u_m + 2^K v_m\sqrt{-2} = (a + 2^K\sqrt{-2})^{2^m}$ ile tanımlanır. Buradan görülür ki $u_1 = a^2 - 2^{2K+1} \equiv 1\ (mod\ 8)$, $v_1 = 2a \equiv 2\ (mod\ 4)$ ve bu durumda $v_{m+1} = 2u_m v_m$ ve $u_{m+1} = u_m^2 - 2^{2K+1}v_m^2$ olduğundan tümevarımla kolayca görülebilir ki $u_{\varrho} \equiv 1\ (mod\ 2^{\varrho+2})$, $v_{\varrho} \equiv 2^{\varrho}\ (mod\ 2^{\varrho+1})$ olur. Böylece,

$$(a + 2^K\sqrt{-2})^{n-1} = (u_\varrho + v_\varrho 2^K\sqrt{-2})^t$$
$$= U + V2^K\sqrt{-2}$$

olur. Burada $U = u_\varrho^t \ (mod\ 2^{2K+1}v_\varrho^2)$'dir ve bundan dolayı $U = 1\ (mod\ 2^{\varrho+2})$ ve benzer şekilde $V = 2^\varrho\ (mod\ 2^{\varrho+1})$ elde edilir. Böylece (3.2)'den $x + 2^K\sqrt{-2} = (U + V2^K\sqrt{-2})(\ a + 2^K\sqrt{-2})$ olur ve dolayısıyla $1 = U + aV \equiv 1 + 2^\varrho\ (mod\ 2^{\varrho+1})$ olur ki bu bir çelişkidir.

Şimdi x tek olmak üzere, n sayısının çift olduğu durum göz önüne alınsın. Bu durumda $n = 4$ için incelemek yeterli olacaktır. O halde

$$(y^2 + x)(y^2 - x) = 2^{2K+1} \tag{3.6}$$

eşitliğini bulmalıydık. Dolayısıyla $\lambda > k$ olmak üzere $y^2 + x = 2^\lambda$, $y^2 - x = 2^{2K+1-\lambda}$ olur. Böylece $y^2 = 2^{\lambda-1} + 2^{2K-\lambda}$ ve y tek olduğundan $\lambda = 2K$ dır. Dolayısıyla $(y-1)(y+1) = 2^{2K-1}$ dir. Böylece $y \pm 1$, 2'nin bir kuvvetidir ve bundan dolayı $y = 3$ ve böylece elde edilen tek çözüm $x = 7$, $n = 4$, $k = 5$ olur.

Son olarak x sayısının çift olduğu kabul edilsin. O halde y kesinlikle çift olacaktır. Bu durumda $x = 2^a X$ ve $y = 2^b Y$ olduğu kabul edilsin. Burada $a > 0$, $b > 0$ ve X ve Y tek sayıdır. Bunlar denklemde yazılırsa

$$2^{2a}X^2 + 2^{2K+1} = 2^{nb}Y^n \tag{3.7}$$

olur ve bundan dolayı $nb = \min(2a, 2K+1)$ olur. Şimdi $2a$ ve $2K+1$ den hangisinin daha büyük olduğuna bağlı olarak iki durum ortaya çıkar.

1. Durum. $a \leq K$ ise o halde $nb = 2a$ dır. Buna göre her iki tarafı 2^{2a} ile bölünürse $X^2 + 2^{2K+1-2a} = Y^n$ olur. Böylece iki durum söz konusu olur.

1. $K = a$ ise $\alpha \geq 1$ için $x = 5.2^{3\alpha}$, $y = 3.2^{2\alpha}$, $n = 3$, $k = 6\alpha + 1$ olur.

2. $K = a + 2$ olduğunda ise $\alpha \geq 1$ için $x = 7.2^{2\alpha}$, $y = 3.2^{\alpha}$, $k = 4\alpha + 5$ elde edilir.

Yukarıdaki her iki durumda da $\alpha = 0$ için bilinen sonuçlara karşılık gelir.

2. Durum. $a \geq K + 1$ ise o halde $nb = 2K + 1$ dir. Bu durumda bunları denklemde yerine yazıp düzenlersek denklem $2Z^2 + 1 = Y^n$ haline gelir. Burada $Z = 2^{a-K-1}.X$ tir. Lemma 3.1.3 gereği bu denklemin tek çözümü $Z = 11$, $Y = 3$, $n = 5$'tir. Dolayısıyla $5b = 2K + 1$ ve bundan dolayı $K = 5\alpha + 2$, $k = 10\alpha + 5$, $b = 2\alpha + 1$, $a = 5\alpha + 3$ ve böylece son olarak $x = 11.2^{5\alpha+3}$, $y = 3.2^{\alpha+1}$, $k = 10\alpha + 5$, $n = 5$, $\alpha \geq 0$ olur. Bu da ispatı tamamlar (Cohn, 1992).

4. $x^2 + 3^m = y^n$ DİOPHANTİNE DENKLEMİ

Bu bölümde $x^2 + 3^m = y^n$ Diophantine denkleminin çözümleri araştırılacaktır. Tıpkı bir önceki denklemde olduğu gibi burada da m sayısının tek veya çift olması durumuna göre farklı sonuçlar söz konusudur.

4.1. m'nin Tek Sayı Olma Durumu

Bu kısımda Arif ve Abu Muriefah (1998) çalışmasında yer alan sonuçlar verilecektir. Buna göre bu kısmın ana teoremi aşağıdaki gibidir.

Teorem 4.1.1. m tek sayı, $n \geq 3$ olmak üzere $x^2 + 3^m = y^n$ denkleminin pozitif tam sayılarda bir tek çözümü vardır ve bu çözüm $m = 5 + 5M$, $x = 10.3^{3M}$, $y = 7.3^{2M}$ ve $n = 3$ şeklindedir (Arif ve Abu Muriefah, 1998). Teoremin ispatı için aşağıdaki lemma gerekli olacaktır.

Lemma 4.1.2. $n \geq 3$ ve n tek sayı olmak üzere $3x^2 + 1 = y^n$ denkleminin y tek sayı ve $y \geq 1$ için tamsayılarda çözümü yoktur (Nagell, 1955).

Teorem 4.1.1'in İspatı. Nagell (1923) çalışmasına göre $m = 1$ için denklemin çözümünün olmadığını biliniyor. O halde $m = 2k + 1$ olsun. x in tek olduğu varsayılırsa bu durumda y çift olmalıdır. $x^2 + 3^m = y^n$ denklemini mod 8'de incelersek $x^2 + 3^m \equiv 4\ (mod\ 8)$ ve $y^n \equiv 0\ (mod\ 8)$ olmalıdır. Bu ise çelişkidir. O halde x çift ve y tek sayı olmalıdır.

Teoremin ispatını $(3, x) = 1$ ve $3|x$ olmak üzere iki durumda incelemek kolaylık sağlayacaktır.

1.Durum. $(3, x) = 1$ olsun. İlk olarak n'nin tek sayı olduğu kabul edilsin. p bir tek asal sayı olmak üzere genellik bozulmadan $n = p$ olduğu düşünülebilir. O halde Teorem 2.1.4'ten iki olasılık söz konusu olur. a ve b tam sayı olmak üzere

$$x + 3^k\sqrt{-3} = (a + b\sqrt{-3})^p \tag{4.1}$$

olur ve burada $y = a^2 + 3b^2$ dir. Ya da

$$x + 3^k\sqrt{-3} = \left(\frac{a+b\sqrt{-3}}{2}\right)^3 \tag{4.2}$$

olur ki burada $a \equiv b \equiv 1\ (mod\ 2)$ ve $y = \frac{a^2+3b^2}{4}$'tür. (4.1) ifadesinde $y = a^2 + 3b^2$ ve y tek sayıdır. Bundan dolayı a ve b den biri tek ve diğeri çifttir. Burada sanal kısımları eşitlenirse,

$$3^k = b\sum_{r=0}^{\frac{p-1}{2}} \binom{p}{2r+1} a^{p-2r-1}(-3b^2)^r$$

eşitliği elde edilir. Bundan dolayı b tek sayıdır. $\sum$ toplam sembolü içerisindeki terim 3'e bölünmediğinden dolayı $b = \pm 3^k$ elde edilir. Dolayısıyla

$$\pm 1 = \sum_{r=0}^{\frac{p-1}{2}} \binom{p}{2r+1} a^{p-2r-1}(-3^{2k+1})^r$$

olur. Lemma 2.2.2 ve Lemma 2.2.3 gösterir ki burada her iki işaret de imkansızdır. Dolayısıyla (4.1) denkleminin hiçbir çözümü yoktur.

Şimdi (4.2) denklemi göz önüne alınsın. Aynı şekilde burada da sanal kısımlar eşitlenirse

$$8.3^k = b(3a^2 - 3b^2) \tag{4.3}$$

eşitliği elde edilir. Eğer $b = \pm 1$ ise (4.3)'te yerine yazılırsa

$$\pm 8.3^k = 3a^2 - 3$$

olur. $k = 1$ olduğu durum kolayca elenebilir. Bu nedenle $k > 1$ olduğunu kabul edilsin. O halde $a = \pm 5$, $k = 2$ çözümü vardır. Bundan dolayı $y = 7$ dir. Dolayısıyla (4.2) den $x = 10$ dur.

Eğer $b = \pm 3^{\lambda}$, $0 < \lambda < k$ ise o halde (4.3) denklemi $\pm 8.3^{k-\lambda-1} = a^2 - 3^{2\lambda}$ haline gelir ve bu eşitlik mod 3'te incelenirse, $k - \lambda - 1 > 0$ olduğu durumda eşitliğin çözümü yoktur. Bu nedenle $k - \lambda - 1 = 0$ ve $k - 1 = \lambda$ olmalıdır. Böylece $\pm 8 = a^2 - 3^{2(k-1)}$ olur. Burada $+8 = a^2 - 3^{2(k-1)}$ eşitliği mod 3'te incelenirse bu eşitliğin doğru olmayacağı açıkça görülür. Bundan dolayı $-8 = a^2 - 3^{2(k-1)}$ olur. Bu denklemin sadece $k = 2$ için $a = \pm 1$ çözümü vardır. Böylece $b = \pm 3$ olur ve buradan $x = 10$ ve $y = 7$ çözümü elde edilir.

Son olarak eğer $b = \pm 3^{k}$ ise o halde (4.3) denklemi $\pm 8 = 3a^2 - 3^{2k+1}$ halini alır fakat bu eşitlik mod 3'e göre doğru değildir.

Şimdi eğer n eğer çift ise bu durumda $x^2 + 3^m = y^n$ denklemini $n = 4$ için incelemek yeterli olacaktır. Dolayısıyla denklem $(y^2 - x)(y^2 + x) = 3^{2k+1}$ şeklinde çarpanlarına ayrılırsa $(3, x) = 1$ olduğundan

$$y^2 - x = 1 \text{ ve } y^2 + x = 3^{2k+1}$$

olmalıdır. Bu iki denklem taraf tarafa toplanarak

$$2y^2 = 3^{2k+1} + 1$$

eşitliği elde edilir ki bu da mod 3'e göre doğru değildir.

2.Durum. $3|x$ olsun. O halde kesinlikle $3|y$ olmalıdır. $x = 3^{u}X$ ve $y = 3^{v}Y$ olduğu kabul edilsin. Burada $u > 0, v > 0$ ve $(3, X) = (3, Y) = 1$ dir. O halde bu eşitlikler $x^2 + 3^{2k+1} = y^n$ denkleminde yerine yazılırsa denklem

$$3^{2u}X^2 + 3^{2k+1} = 3^{nv}Y^n$$

haline gelir. Burada $2u$, $2k+1$ ve nv'den hangisinin daha küçük olduğuna bağlı olarak üç durum karşımıza çıkar.

İlk olarak $2u = min(2u, 2k+1, nv)$ olsun. Bu durumda en son elde edilen denklemin her iki tarafını 3^{2u} ile bölünürse

$$X^2 + 3^{2(k-u)+1} = 3^{nv-2u}Y^n$$

eşitliği elde edilir. Bu denklem mod 3'e göre incelenirse $nv - 2u = 0$ sonucuna varılır. Bu durumda $(3, X) = 1$ olduğundan

$$X^2 + 3^{2(k-u)+1} = Y^n$$

eşitliği elde edilir. Eğer $k - u = 0$ ise bu denklemin bir çözümü yoktu. Eğer $k - u > 0$ ise bundan dolayı yukarıdaki çözüme göre bu denklemin yalnızca $k - u = 2$ ve $n = 3$ ise yalnızca bir çözümü vardır. Bundan dolayı $nv = 3v = 2u$ ve $3|u$ dur. $u = 3M$ olduğu kabul edilsin. Bu durumda $k = 2 + 3M$ ve $m = 5 + 6M$'dir. Bundan dolayı bu denklemin sadece $m = 5 + 6M$ olduğunda bir çözümü vardır ve bu çözüm $X = 10$ ve $y = 7$ dir. Dolayısıyla denklemin genel çözümü $x = 10.3^u = 10.3^{3M}$ ve $y = 7.3^v = 7.3^{2M}$ olur.

İkinci olarak $2k + 1 = min(2u, 2k+1, nv)$ ise bu durumda denklem

$$3^{2u-2k-1}X^2 + 1 = 3^{nv-2k-1}Y^n$$

olur. Bu denklemi mod 3'te incelenirse $nv - 2k - 1 = 0$ olmalıdır. Bu nedenle n tek sayı ve

$$3(3^{u-k-1})^2X^2 + 1 = Y^n$$

olur ki Lemma 4.1.2'den dolayı bu denklemin çözümü yoktur.

Son olarak, $nv = min(2u, 2k+1, nv)$ ise budurumda denklem

$$3^{2u-nv}X^2 + 3^{2k+1-nv} = Y^n$$

halini alır ve bu mod 3'e göre sadece $2u - nv = 0$ veya $2k + 1 - nv = 0$ olduğunda mümkündür. Zaten bu durumların her ikiside yukarıda ele alındı ve böylece ispat tamamlanmıştır.

4.2. *m*'nin Çift Sayı Olma Durumu.

Bu kısımda $x^2 + 3^m = y^n$ Diophantine denkleminde m'nin çift sayı olması durumunda Luca (2000) çalışmasında elde edilen sonuçlar verilecektir. Buna göre verilen denklemin aşağıdaki şekilde tamsayı çözümleri vardır.

Teorem 4.2.2. m çift sayı, $n \geq 3$ ve $x > 0$ olmak üzere

$$x^2 + 3^m = y^n \tag{4.4}$$

denkleminin tüm pozitif tamsayı çözümleri $t \in \mathbb{Z}$ olmak üzere $m = 4 + 6t$, $x = 46.3^{3t}$, $y = 13.3^{2t}$ ve $n = 3$ şeklindedir (Luca, 2000).

İspat. $(3, x) = 1$ durumu için denklemi incelenmesi yeterli olacaktır. Gerçekten de $a \geq 1$ ve $(3, x_1) = 1$ için $x = 3^a x_1$ olsun. Bu durumda $b \geq 0$ ve $(3, y_1) = 1$ için $y = 3^b y_1$ yazılabilir. Bu ifadeler (4.4) denkleminde yerine yazılırsa

$$3^{2a}{x_1}^2 + 3^m = 3^{nb}{y_1}^n \tag{4.5}$$

halini alır. Bu durumda (4.5) denklemi üç durumda incelenir.

1. Durum. $2a > m$ ise bu durumda (4.5) denkleminin her iki yanını 3^m ile bölünürse denklem

$$\left(3^{a-\frac{m}{2}}x_1\right)^2 + 1 = 3^{nb-m}{y_1}^n \tag{4.6}$$

haline gelir. (4.6) denklemi mod 3'e göre incelenirse eşitlik sadece $nb - m = 0$ için doğru olacaktır. Bu denklemde $X = 3^{a-\frac{m}{2}}x_1$ ve $Y = y_1$ yazılırsa

$$X^2 + 1 = Y^n \tag{4.7}$$

olarak bulunur ki bu denklemin çözümünün olmadığı bilinmektedir.

2. Durum. $2a = m$ ise (4.5) denkleminin her iki tarafını 3^m ile bölünürse denklem

$${x_1}^2 + 1 = 3^{nb-m}{y_1}^n \tag{4.8}$$

halini alır. (4.8) eşitliği mod 3'te incelenirse ${x_1}^2 + 1 \equiv 0\ (mod\ 3)$ olur. -1 mod 3'te bir kuadratik rezidü olmadığından $nb = m$ olmalıdır. Dolayısıyla (4.8) denklemi

$${x_1}^2 + 1 = {y_1}^n$$

haline gelir ki tekrar Lebesgue denklemi olur ve bu denklemin tamsayı çözümü yoktur.

3. Durum: $2a < m$ ise (4.5) denkleminin her iki tarafı 3^{2a} ile bölünürse denklem

$${x_1}^2 + 3^{m-2a} = 3^{nb-2a}{y_1}^n \tag{4.9}$$

halini alır. (4.9) denklemi mod 3'te incelenirse $(3, x_1) = 1$ olduğundan dolayı $nb - 2a = 0$ olmalıdır. Burada $m - 2a = m_1$ yazılabilir. Bu durumda m_1 çift olmak üzere (4.9) denklemi

$${x_1}^2 + 3^{m_1} = {y_1}^n \tag{4.10}$$

halini alır. m_1 çift sayı ve $(3, x_1) = 1$ olmak üzere (4.10) denklemi tam olarak (4.4) denklemidir.

Bundan sonra $(3, x) = 1$ olmak üzere (x, y, m, n), (4.4) denkleminin bir çözümü olduğu kabul edilsin. Burada dikkat edilirse x çift ve y tek sayıdır. Gerçekten de eğer x tek sayı ise (4.4) denklemi mod 8'de incelenirse $x^2 + 3^m \equiv 2\ (mod\ 8)$ ve $y^n \equiv 0\ (mod\ 8)$ olur. Bu ise bir çelişkidir. Bu durumda y^n ne bir çift sayının ne de bir tek sayının kuvveti olamaz. Burada iki durum oluşur.

4.2.1. $4|n$ durumu

Bu durumda genellik bozulmadan $n = 4$ olduğu kabul edilebilir. (4.4) denklemi tekrardan yazıp çarpanlarına ayrılırsa

$$(y^2 - x)(y^2 + x) = 3^m \tag{4.11}$$

denklemini elde edilir. Burada $(y^2 - x)$ ve $(y^2 + x)$ aralarında asal olduğundan

$$y^2 + x = 3^m \quad \text{ve} \quad y^2 - x = 1$$

eşitlikleri elde edilir. Bu iki denklemi taraf tarafa toplanırsa $2y^2 = 3^m + 1$ olur veya

$$\left(3^{\frac{m}{2}}\right)^2 - 2y^2 = -1 \tag{4.12}$$

şeklinde yazılabilir. (4.12)'da $X = 3^{\frac{m}{2}}$ ve $Y = y$ yazılırsa

$$X^2 - 2Y^2 = -1$$

denklemi bir Pell denklemi haline gelir. Bu denklemin çözümleri

$$X_1 = 1, Y_1 = 1, X_2 = 7, Y_2 = 5, X_n = 6X_{n-1} - X_{n-2}, Y_n = 6Y_{n-1} - Y_{n-2} \tag{4.13}$$

şeklindedir. Bundan dolayı $(3, X_n) = 1$ olur ki bu $X = 3^{m/2}$ olmasıyla çelişir.

Böylece (4.4) denkleminin $4|n$ için hiç bir çözümü yoktur.

4.2.2. $4 \nmid n$ durumu

$n \geq 3$ ve $4 \nmid n$ olduğunda p gibi bir tek asal sayı vardır ki $p|n$ olur. $n = p$ olduğu varsayılsın. Bu durumda (4.4) denklemi

$$x^2 + 3^m = y^p \tag{4.14}$$

halini alır. $x^2 \equiv y^2 \equiv 1\ (mod\ 3)$ olduğundan $y \equiv 1\ (mod\ 3)$ elde edilir. (4.14) denklemi düzenlenip kompleks çarpanlarına ayrılarak

$$\left(x + i3^{m/2}\right)\left(x - i3^{m/2}\right) = y^p$$

olur. $\mathbb{Z}[i]$'nin sınıf sayısı 1 ve $\left(x + i3^{m/2}, x - i3^{m/2}\right) = 1$ olduğundan a ve b gibi öyle iki tamsayı vardır ki $y = a^2 + b^2$ dir ve

$$\begin{cases} x + i3^{m/2} = (a + ib)^p \\ x - i3^{m/2} = (a - ib)^p \end{cases} \tag{4.15}$$

olur. Burada $a.b \neq 0$ olduğuna dikkat edilmelidir. (4.15) çözüm sisteminden

$$\begin{cases} x = \frac{(a+ib)^p + (a-ib)^p}{2} \\ 3^{m/2} = \frac{(a+ib)^p - (a-ib)^p}{2i} \end{cases} \tag{4.16}$$

eşitlikleri elde edilir. p tek sayı olduğundan (4.16)'dan $a|x$ sonucu çıkar. Özellikle $3 \nmid a$ dır. (4.16)'nın ikinci denkleminden $b|3^{m/2}$ elde edilir.

İlk olarak $p = 3$ durumu göz önüne alınsın. Bu durumda (4.16)'nın ikinci kısmı

$$3^{m/2} = b(3a^2 - b^2) \tag{4.17}$$

haline gelir. (4.17) denklemi mod 3'te incelenirse $3|b$ olduğu elde edilir. Özellikle $9|b(3a^2 - b^2)$ dir ki buradan $^m/_2 \geq 2$ olur. Eğer $^m/_2 = 2$ ise o halde

$$9 = b(3a^2 - b^2)$$

ve $b = \pm 3$ olur. Bu da $a = 2$ ve $b = 3$ olmasına neden olur. Böylece bulunan a ve b değerlerini (4.15)'te yerine yazarsak $(x, y, m, n) = (46,13,4,3)$ çözümü elde edilir.

(4.17) denkleminin $m > 4$ için hiçbir çözümü yoktur. Gerçekten de u tamsayı ve $0 < u < {}^m/_2$ olmak üzere $b = \pm 3^u$ olsun. (4.17) denklemi

$$3a^2 - 3^{2u} = \pm 3^{\frac{m}{2}-u}$$

ve ya

$$a^2 = 3^{2u-1} \pm 3^{\frac{m}{2}-u-1} \tag{4.18}$$

haline gelir. $3 \nmid a$ olduğundan, $u = \frac{m}{2} - 1$ elde edilir ve

$$a^2 = 3^{m-3} \pm 1 \tag{4.19}$$

dir. Denklemde -1 durumu göz önüne alındığında $m \geq 6$ için

$$a^2 + 1 = 3^{m-3} \tag{4.20}$$

olur ki önceki argümanlar gereği bu denklemin çözümü yoktur. Denklem $+1$ ile birlikte $m \geq 6$ için

$$a^2 = 3^{m-3} + 1 \tag{4.21}$$

eşitliğine dönüşür. Cho Ko (1965) çalışması gereği

$$X^2 = Y^n + 1$$

denkleminin belli $n \geq 3$ için en az bir tane sıfırdan farklı çözümü vardır ve bu çözüm $X = 3,\ Y = 2$ ile verilir. Dolayısıyla (4.21) denkleminin çözümü yoktur.

Bundan sonra $p > 3$ olduğu kabul edilsin. İlk olarak $b = \pm 3^{m/2}$ olsun. Bu durumda dikkat edilirse $b \neq \pm 1$ değildir. Gerçekten de, eğer $b = \pm 1$ ise o halde $y = a^2 + b^2 = a^2 + 1$ olur. $y \equiv 1\ (mod\ 3)$ olduğundan buradan $a \equiv 0\ (mod\ 3)$ sonucu çıkar ki bu da çelişkidir. Dolayısıyla belli u tamsayıları için $0 < u \leq {}^{m}/_{2}$ olsun bu durumda $u < {}^{m}/_{2}$ için $b = \pm 3^u$ olduğunu kabul edelim. (4.16)'da ikinci denklem b ile sadeleştirilip $mod\ 3$'e indirgenirse, $pa^{p-1} \equiv 0\ (mod\ 3)$ denkliği elde edilir. p asal sayı ve $p > 3$ olmak üzere $3 \nmid a$ için bu denklik doğru olmaz. Dolayısıyla $b = \pm 3^{m/2}$ dir. İkinci bölümdeki Lemma 2.2.2 ve Lemma 2.2.3'ten $b = -3^{m/2}$, $C = 3^m \equiv 1\ (mod\ 16)$, $p \equiv -1\ (mod\ 12)$, sonucu elde edilir. Özel olarak $4|m$'dir. Lemma 2.2.1'den ayrıca biliniyor ki a çift sayı ve eğer q, a nın herhangi bir tek asal böleni ise o halde

$$3^{m(q-1)} \equiv 1\ (mod\ q^2) \tag{4.22}$$

dir ve $q^{\alpha} \| a$ ise bu durumda $q^{2\alpha} \| (3^{m(q-1)} - 1)$ dir.

Şimdi (4.16)'nın ikinci denklemi göz önüne alınsın, $\varepsilon = a + ib$ ve $\bar{\varepsilon} = a - ib$ olsun. $b = -3^{m/2}$ olduğundan

$$\frac{\varepsilon^p - \bar{\varepsilon}^p}{\varepsilon - \bar{\varepsilon}} = -1 \tag{4.23}$$

eşitliği elde edilir. Dikkat edilirse, her $k \geq 0$ için

$$u_k = \frac{\varepsilon^k - \bar{\varepsilon}^k}{\varepsilon - \bar{\varepsilon}} \tag{4.24}$$

dizisi bir Lucas dizisidir. Bilu, vd. (2001) çalışmasından her $k > 13$ asal değerleri için u_k nın bir ilkel böleninin var olduğu biliniyor. Üstelik, $k \in \{5,7,11,13\}$ için kesinlikle u_k nın ilkel böleninin olmadığı 10 Lucas dizisi vardır. Bu dizilerin $\mathbb{Z}[i]$'de karakteristik denkleminin kökünün olmadığı kolayca görülebilir.

Dolayısıyla, $|u_p| > 1$ olurki bu da (4.23) ile çelişir. Buradan da $p > 3$ için hiç bir çözümün olmadığı sonucuna varılır.

Böylece (4.4) denkleminin genel çözümleri $x = 46.3^{3t}$, $m = 4 + 6t$, $y = 13.3^{2t}$ ve $n = 3$ olarak elde edilmiş olur.

5. $x^2 + 5^m = y^n$ DİOPHANTİNE DENKLEMİ

Bu bölümde Tao (2009) çalışmasında yer alan sonuçlar ışığında $y > 2$ ve $m > 0$ olmak üzere $x^2 + 5^m = y^n$ Diophantine denklemi incelenmiştir. Burada $2 \nmid m$ olduğunda ve de $2|m$ olduğunda, $(x, y) = 1$ koşulu altında denklemin pozitif tamsayı çözümü olmadığı görülecektir. İspatta Bilu, vd. (2001) çalışmasında yer alan önemli sonuçlar kullanılmıştır.

Bu bölümün ana teoremi aşağıdaki gibidir:

Teorem 5.1. $n > 2$ ve $m > 0$ tamsayılar olmak üzere $x^2 + 5^m = y^n$ denkleminin ne $2 \nmid m$ olduğunda ne de $(x, y) = 1$ koşulu altında, $2|m$ olduğu durum için pozitif tamsayı çözümü yoktur (Tao, 2009).

Teorem 5.1'in ispatında aşağıdaki yardımcı teoremlere ihtiyaç duyulacaktır.

Lemma 5.2. F, sınıf sayısı h_F olan bir sayı cismi ve O_F de F'nin bir tamsayılar halkası olsun. O_F'nin bir A ideali için, eğer A^n bir temel ideal ve $(h_F, n) = 1$ ise bu durumda A da bir temel idealdir. Özellikle $\mathbb{Q}(\sqrt{-5})$ kuadratik sayı cisminin sınıf sayısı 2 olduğu gibi herhangi n tek sayısı için eğer A^n temel ideal ise o halde A da temel idealdir (Tao, 2009).

Lemma 5.3. $d \equiv 3\ (mod\ 4)$ ve kare çarpansız bir tamsayı olmak üzere $\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, $K = \mathbb{Q}(\sqrt{d})$ kuadratik cisminin bir cebirsel sayısı ve $(a, bd) = 1$ ve $2|ab$ olsun. Bu durumda $\mathbb{Z}[\sqrt{d}]$ halkasının iki ideali $\langle\alpha\rangle$ ve $\langle\bar{\alpha}\rangle$ aralarında asaldır. Burada $\bar{\alpha} = a - b\sqrt{d}$, α'nın cebirsel eşleniğidir (Tao, 2009).

Uyarı 5.4. $d \equiv 3\ (mod\ 4)$ için Lemma 5.3'e benzer bir sonuç kolayca elde edebilir.

Şimdi Teorem 5.1'in ispatında kullanılacak bazı kavramlar aşağıda tanıtılacaktır.

Tanım 5.5. α ve β, $\alpha+\beta$ ve $\alpha\beta$ sıfırdan farklı aralarında asal sayı olacak ve $\frac{\alpha}{\beta}$ birimin kökü olmayacak şekilde iki cebirsel sayı olsun. O halde (α,β) ikilisi bir *Lucas çifti* olarak adlandırılır ve *Lucas sayı dizisi*

$$u_n = u_n(\alpha,\beta) = \frac{\alpha^n - \beta^n}{\alpha-\beta}\,, \qquad n = 0,1,2\ldots$$

olarak tanımlanır.

Tanım 5.6. (α,β) bir Lucas çifti olsun. p bir asal sayı olmak üzere eğer p, u_n'yi bölüyor ancak $(\alpha-\beta)^2 u_1 u_2 \ldots u_{n-1}$'i bölmüyorsa p'ye $u_n(\alpha,\beta)$-nin bir *ilkel böleni* adı verilir.

Tanım 5.7. Bir Lucas ikilisi olan $u_n(\alpha,\beta)$'nın ilkel böleni olmayacak şekildeki (α,β) çiftine bir *n-kusurlu Lucas çifti* denir. Eğer n-kusurlu Lucas ikilisi yoksa o halde n *tamamen kusursuz* olarak adlandırılır.

Lemma 5.8. $n > 30$ olmak üzere her n tamsayısı tamamen kusursuzdur (Bilu, vd. 2001).

Tao (2009) çalışmasında, $x^2 + 5^m = y^n,\ \ n > 2,\ \ m > 0,\ \ x,y,m,n \in \mathbb{N}$ denklemi üzerinde gerekli analiz yapılarak denklemin tamsayı çözümlerini ararken aşağıdaki gibi 4 durumun söz konusu olacağı gösterilmiştir.

i. $5x^2 + 1 = y^n$, n tek sayı olması durumu

ii. $x^2 + 5^{2m'+1} = y^n$, $(x,y) = 1$ olması durumu

iii. $x^2 + 1 = 5^r y^n$, $1 \le r \le n$ durumu.

iv. $x^2 + 5^{2m'} = y^n,\ \ (x,y) = 1$ durumu.

Dikkat edilirse, böylece $(x,y) \neq 1$ durumu $(x,y) = 1$ durumuna indirgenir. Tao (2009) çalışmasında iii. durumu hariç tüm durumlar için ispat verilmiştir. Bahsedilen durumda ise ispat oldukça teknik olduğu için atlanmıştır.

5.1. $5x^2 + 1 = y^n$ Denklemi

Burada n'nin tek olduğu durumu incelemek yeterlidir.

Teorem 5.1.1. $n > 2$ olmak üzere $5x^2 + 1 = y^n$ denkleminin sadece bir pozitif tamsayı çözümü vardır ve bu çözüm $(x, y, n) = (4,3,4)$ tür (Tao, 2009).

İspat. (x, y, n) verilen denklemin bir tamsayı çözümü olsun. İlk olarak $2|x$ ve $2 \nmid y$ olduğu kolayca görülür. x ve y nin her ikisi de aynı anda tek veya çift olamaz. Bunun yanında $y^n \equiv 2\ (mod\ 4)$ olması imkansız olduğundan x tek olamaz. Teoremi elde etmek için aşağıdaki iki teoremi ispatlamak yeterlidir.

Teorem 5.1.2. $5x^2 + 1 = y^4$ denkleminin sadece bir pozitif tamsayı çözümü vardır ve bu çözüm $(x, y) = (4,3)$ tür (Tao, 2009).

Bu teoremin ispatında Cohn'un bir sonucu kullanılmaktadır.

Teorem 5.1.3. p bir asal tek sayı olmak üzere $5x^2 + 1 = y^p$ denkleminin pozitif tamsayı çözümü yoktur (Tao, 2009).

Bu teoremin ispatında Lemma 5.2 ve Lemma 5.3 kullanılmakta olup bazı teknik detaylar barındırmaktadır.

Uyarı 5.1.4. Teorem 5.1.1'den $5x^2 + 1 = y^n,\ n > 2,$ denkleminin sadece $n = 4$ olduğunda bir pozitif tamsayı çözümü olduğu görülmektedir. İlk durumda n tek olduğundan, bu durumda denklemin pozitif tamsayı çözümü olmadığı görülür.

5.2. $x^2 + 5^{2m+1} = y^n$ Denklemi

Bu bölümde ii. durum ele alınacaktır.

Teorem 5.2.1. $x^2 + 5^{2m+1} = y^n,\ (x, y) = 1,\ n > 2,\ m \geq 0$ denkleminin tamsayı çözümü yoktur (Tao, 2009).

İspat. (x, y, m, n) verilen denklemin bir tamsayı çözümü olsun. Bu durumda $2|x$ ve $2 \nmid y$ dir. x, y her ikisi aynı anda çift veya tek olamaz. Eğer $2 \nmid x$ ve $2|y$ ise, o halde $x^2 + 5^{2m+1} \equiv 6 \ (mod\ 8)$ iken $y^n \equiv 0 \ (mod\ 8)$ olur. Nagell'e (1923) göre verilen denklemi $m \geq 1$ için incelemek yeterlidir. Bunun için de Tao (2009) çalışmasında aşağıdaki üç teorem ispatlanmıştır.

Teorem 5.2.3. $x^2 + 5^{2m+1} = y^4,\ (x, y) = 1,\ m \geq 1$ denkleminin tamsayı çözümü yoktur (Tao, 2009).

Bu teoremin ispatında çarpanlara ayırma metotu kullanılmış ve olmayana ergi metotuyla sonuca ulaşılmıştır.

Teorem 5.2.4. $p \neq 5$ bir tek asal sayı olmak üzere $x^2 + 5^{2m+1} = y^p,\ (x, y) = 1,$ $m \geq 0$ denkleminin çözümü yoktur (Tao, 2009).

Bu teoremin ispatında Lemma 5.3 ve Teorem 5.1.3 kullanılmış olup 2. Bölüm'de yer alan teknikler kullanılarak bazı hesaplamalarla sonuca gidilmiştir.

Teorem 5.2.5. $x^2 + 5^{2m+1} = y^5,\ (x, y) = 1,\ m \geq 0$ denkleminin tamsayı çözümü yoktur (Tao, 2009).

Bu teoremin ispatında bazı basit hesaplamalarla sonuca gidilmiştir.

5.3. $x^2 + 5^{2m} = y^n$ Denklemi

Aşağıdaki teorem iv. durumu kapsayacak şekilde verilmiştir. Böylece Teorem 5.1'in ispatı tamamlanmış olacaktır.

Teorem 5.3.1. m herhangi bir tamsayı olmak üzere $m \geq 0$ için $x^2 + 5^{2m} = y^n, n > 2,$ $(x, y) = 1$ denkleminin tamsayı çözümü yoktur. Sadece $(x, m) = (0,0)$ bir tamsayı çözümü olur (Tao, 2009).

İspat. x'in çift olduğu açıktır. Gerçekten de, aksi halde x tek olursa, bu durumda $y^n = x^2 + 5^{2m} \equiv 2\ (mod\ 8)$ olur ki $n > 2$ için bu durum mümkün değildir. Verilen denklemi sadece $m > 0$ için incelemek yeterlidir. Bu ise Tao (2009) çalışmasında aşağıdaki beş teorem yardımıyla yapılmış ve böylece Teorem 5.2.5'in ispatına ulaşılmıştır.

Teorem 5.3.2. $x^2 + 5^{2m} = y^4$, $m > 0$, $(x, y) = 1$ denkleminin tamsayı çözümü yoktur (Tao, 2009).

Bu teoremin ispatında Lemma 5.2 kullanılmış olup, 2. Bölüm'de verilen teknikle sonuca gidilmiştir.

Teorem 5.3.3. $x^2 + 5^{2m} = y^5$, $m > 0$, $(x, y) = 1$ denkleminin tamsayı çözümü yoktur (Tao, 2009).

Bu teoremin ispatında Fermat'ın Küçük Teoremi'ni (Teorem 1.1.9) içine alan bazı hesaplamalarla sonuca gidilmiştir.

Teorem 5.3.4. $x^2 + 5^{2m} = y^p$, $m > 0$, $(x, y) = 1$, $p \equiv 1\ (mod\ 20)$ denkleminin tamsayı çözümü yoktur (Tao, 2009).

Bu teoremin ispatı Teorem 5.3.2'nin ispatına benzerdir.

Teorem 5.3.5. $x^2 + 5^{2m} = y^p$, $m > 0$, $(x, y) = 1$, $p \equiv 11\ (mod\ 20)$ denkleminin tamsayı çözümü yoktur (Tao, 2009).

Bu teoremin ispatı da Teorem 5.3.2'nin ispatına benzerdir.

Teorem 5.3.6. $x^2 + 5^{2m} = y^p$, $m > 0$, $(x, y) = 1$, $p \equiv 19\ (mod\ 20)$ denkleminin tamsayı çözümü yoktur (Tao, 2009).

Bu teoremin ispatında yukarıda tanıtılan Lucas çiftlerinin özellikleri kullanılmıştır.

6. $x^2 + 7 = 2^n$ RAMANUJAN-NAGELL DENKLEMİ

Çalışmanın altıncı ve son bölümünde özel bir Diophantine denklemi olan ve Ramanujan-Nagell denklemi olarak adlandırılan $x^2 + 7 = 2^n$ Diophantine denkleminin tamsayı çözümleri araştırılacaktır. Bu bölümde verilen sonuç uzun zamandır bilinmesine rağmen ispatı oldukça anlaşılır şekilde verilen De Chenne (2016) kaynağından faydalanılmıştır. İspatta cisim genişlemelerinden ve tek türlü çarpanlara ayırma özelliklerinden faydalanılacaktır.

Bu kısmın ana sonucu aşağıdaki gibidir.

Teorem 6.1. (Ramanujan-Nagell), $x, n \in \mathbb{Z}$ olmak üzere $x^2 + 7 = 2^n$ denkleminin çözümleri sadece $(x, n) = (\pm 1,3), (\pm 3,4), (\pm 5,5), (\pm 11,7), (\pm 81,15)$ dir (Spencer, 2016).

İspat: Burada önceki bölümlerde verilen metotların kullanılabilmesi adına $\mathbb{Q}(\sqrt{-7})$ cismi üzerinde çalışılacaktır. $\mathbb{Q}(\sqrt{-7})$ cisminin tamsayılar halkası TÇAB'dir. Aşikar olarak, x tek sayı olmalıdır ve (x, n) denklemin bir çözümü ise $(-x, n)$ de denklemin çözümüdür. Bu nedenle x'in pozitif olduğu kabul edilsin.

İlk olarak n çift olsun. O halde verilen denklem

$$\begin{aligned} 7 &= 2^n - x^2 \\ &= \left(2^{n/2} - x\right)\left(2^{n/2} + x\right) \end{aligned}$$

şeklinde çarpanlarına ayrılabilir. Aşikar olarak hem $2^{n/2} - x$ hem de $2^{n/2} + x$ ifadesi tamsayı olmalıdır. Çünkü kabul gereği x pozitif ve $n > 0$ dır, o halde $2^{n/2} + x > 2^{n/2} - x$ olur ve buradan,

$$\begin{aligned} 7 &= 2^{n/2} + x \\ 1 &= 2^{n/2} - x \end{aligned}$$

eşitlikleri bulunur. Bu iki eşitlik taraf tarafa toplanırsa

$$8 = 2^{1+(n/2)}$$

elde edilir ve buradan $n = 4$ ve $x = 3$ olarak bulunur.

Şimdi n tek sayı ve $n > 3$ olsun. $\mathbb{Q}(\sqrt{-7})$ cisminde 2 sayısı,

$$2 = \left(\frac{1+\sqrt{-7}}{2}\right)\left(\frac{1-\sqrt{-7}}{2}\right)$$

şeklinde yazılırsa bunun $\mathbb{Q}(\sqrt{-7})$ üzerinde bir çarpanlara ayırma yöntemi olduğu görülebilir. x tek sayı olduğundan $x = 2k + 1$ alarak denklemde yazarsak $x^2 + 7 = 4k^2 + 4k + 8$ olur ve sağ taraf 4 ile tam bölünebilirdir. Burada $m = n - 2$ alıp denklem yeniden yazılırsa

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

olur. Bundan dolayı bu son eşitlik,

$$\left(\frac{x+\sqrt{-7}}{2}\right)\left(\frac{x-\sqrt{-7}}{2}\right) = \left(\frac{1+\sqrt{-7}}{2}\right)^m \left(\frac{1-\sqrt{-7}}{2}\right)^m,$$

şeklinde çarpanlarına ayrılabilir. Burada sağ taraf asal çarpanlarına ayrılmıştır. Ne $\frac{1+\sqrt{-7}}{2}$ çarpanı ne de $\frac{1-\sqrt{-7}}{2}$ çarpanı sol tarafın bir ortak böleni değildir, çünkü böyle bir çarpan sol tarafın çarpanlarının farkı olan $\sqrt{-7}$'yi bölecektir ki bu durum söz konusu olamaz. $\mathbb{Q}(\sqrt{-7})$'nin çarpımsal tersleri ± 1 olduğundan, çarpanları karşılaştırarak,

$$\frac{x \pm \sqrt{-7}}{2} = \pm\left(\frac{1+\sqrt{-7}}{2}\right)^m$$

olduğu bulunur. Buradan,

$$\frac{x+\sqrt{-7}}{2}=\left(\frac{1+\sqrt{-7}}{2}\right)^m,$$
$$\frac{x-\sqrt{-7}}{2}=\left(\frac{1+\sqrt{-7}}{2}\right)^m,$$
$$\frac{x+\sqrt{-7}}{2}=\left(\frac{1-\sqrt{-7}}{2}\right)^m,$$
$$\frac{x-\sqrt{-7}}{2}=\left(\frac{1-\sqrt{-7}}{2}\right)^m,$$

olduğu görülür. Bu denklemlerin farkları alınarak

$$\pm\sqrt{-7}=\left(\frac{1+\sqrt{-7}}{2}\right)^m-\left(\frac{1-\sqrt{-7}}{2}\right)^m$$

elde edilir. İddia ediliyor ki

$$+\sqrt{-7}\neq\left(\frac{1+\sqrt{-7}}{2}\right)^m-\left(\frac{1-\sqrt{-7}}{2}\right)^m$$

dir. Burada daha kısa olması için $a=\frac{1+\sqrt{-7}}{2}$ ve $b=\frac{1-\sqrt{-7}}{2}$ alınsın. Bu durumda $a-b=\sqrt{-7}$ olur. Böylece,

$$a-b=a^m-b^m$$

elde edilir. O halde $ab=2$ olduğundan

$$a^2\equiv(1-b)^2\equiv 0\ (mod\ b^2)$$

olur ve bundan dolayı

$$a^m\equiv a(a^2)^{(m-1)/2}\equiv a\ (mod\ b^2)$$

dir. Dolayısıyla

$$a \equiv a - b \ (mod\ b^2)$$

olur ki bu bir çelişkidir. Dolayısıyla işaret negatif olmalıdır. Bu göz önünde tutulup ilk ifade tekrardan,

$$\begin{aligned} -2^m\sqrt{-7} &= \left(1+\sqrt{-7}\right)^m - \left(1-\sqrt{-7}\right)^m \\ &= \sum_{i=0}^{m} \binom{m}{i} \left(\sqrt{-7}\right)^i - \sum_{i=0}^{m} \binom{m}{i} \left(-\sqrt{-7}\right)^i \end{aligned}$$

olarak yazılabilir. i tek sayı olsun. O halde eşitliğin sağ tarafı

$$\begin{aligned} \binom{m}{i} \left(\sqrt{-7}\right)^i - \binom{m}{i} \left(-\sqrt{-7}\right)^i &= \binom{m}{i} \left(\sqrt{-7} + \sqrt{-7}\right) \\ &= 2\binom{m}{i} \left(\sqrt{-7}\right)^{i+1} \end{aligned}$$

halini alır. i çift sayı olsun. Bu durumda denklemin sağ tarafı,

$$\begin{aligned} \binom{m}{i} \left(\sqrt{-7}\right)^i - \binom{m}{i} \left(-\sqrt{-7}\right)^i &= \binom{m}{i} \left(\sqrt{-7} - \sqrt{-7}\right) \\ &= 0 \end{aligned}$$

olur. Böylece,

$$-2^{m-1} = \binom{m}{1} - \binom{m}{3} 7 + \binom{m}{5} 7^2 - \cdots \pm \binom{m}{m} 7^{(m-1)/2}$$

olduğu elde edilir ve

$$-2^{m-1} \equiv m \ (mod\ 7)$$

olur. Şimdi, $2^6 \equiv 1 \ (mod\ 7)$ dir ve buradan hareketle sadece $m \equiv 3, 5$ veya $13 \ (mod\ 42)$ sonuçları elde edilir.

Burada, sadece $m = 3, 5$ ve 13 için olabileceği gösterilip, çözümün tekliği için mod 42'de Ramanujan-Nagell denkleminin iki çözümünün birbirine denk olduğunu göstermek yeterlidir. Bu nedenle kabul edilsin ki m ve m_1 farklı iki çözüm olsun ve 7^l, $m - m_1$'i bölen 7'nin en büyük kuvveti olsun. O halde

$$a^{m_1} = a^m a^{m_1-m} = a^m \left(\frac{1}{2}\right)^{m_1-m} \left(1+\sqrt{-7}\right)^{m_1-m}$$

dir. Şimdi

$$\left(\frac{1}{2}\right)^{m_1-m} = \left[\left(\frac{1}{2}\right)^6\right]^{\frac{m_1-m}{6}} \equiv 1 \ (mod\ 7^{l+1})$$

ve

$$\left(1+\sqrt{-7}\right)^{m_1-m} \equiv 1 + (m_1 - m)\sqrt{-7} \ (mod\ 7^{l+1})$$

olur, o halde $7|(m_1 - m)$ dir.

$$a^m = \frac{1 + m\sqrt{-7}}{2^m} \ (mod\ 7)$$

olduğundan yukarıda yerine yazılarak

$$a^{m_1} \equiv a^m + \frac{m_1 - m}{2}\sqrt{-7} \ (mod\ 7^{l+1})$$

ve

$$b^{m_1} \equiv b^m + \frac{m_1 - m}{2}\sqrt{-7} \ (mod\ 7^{l+1})$$

olur. Fakat $a^m - b^m = a^{m_1} - b^{m_1}$ olduğundan $(m_1 - m)\sqrt{-7} \equiv 0\ (mod\ 7^{l+1})$ dir. Fakat m_1 ve m tamsayılar olduğundan

$$m_1 \equiv m\ (mod\ 7^{l+1})$$

dir ve bu da l-nin tanımıyla çelişir. Böylece $m = 3, 5$ veya 13 dir ki bu $n = 5, 7$ veya 15 olduğunu ifade eder ve bu da ispatı bitirir.

KAYNAKLAR

Arif, S. A., Abu Muriefah, F. S., "On the Diophantine equation $x^2 + 2^k = y^n$", ***International Journal of Mathematics and Mathematical Sciences***, 20: 299-304 (1997).

Arif, S. A., Abu Muriefah, F. S., "On the Diophantine equation $x^2 + 2^k = y^n$", ***International Journal of Mathematics and Mathematical Sciences***, 21: 610-620 (1998a).

Arif, S. A., Abu Muriefah, F. S., "On A Diophantine Equation" ***Bulletin of The Australian Mathematical Society***, 57: 189-198 (1998b).

Arıkan, A., Asar A. O., Arıkan, A., "Cebir 2. Baskı", ***Gazi Kitabevi,*** Ankara (2012).

Bilu, Y. F., Hanrot, G., Voutier, P. M. with an appendix by M. Mignotte, "Existence of primitive divisors of Lucas and Lehmer sequences", ***J. Reine Angew. Math.*** 539: 75-122 (2001).

Blass, J., "A note on diophantine equation $Y^2 + k = x^5$", ***Math. Comp.*** 30: 638–640 (1976).

Blass, J. and Steıner, R., "On the equation $y^2 + k = X^7$", ***Utilitas Math***., 13: 293-297 (1978).

Brown, E., "Diophantine equations of the form $x^2 + D = y^n$", ***J. Reine Angew. Math.***, 274/275: 385–389 (1975).

Brown, E., "Diophantine equations of the form $ax^2 + Db^k = y^p$", ***J. Reine Angew. Math.*** 291: 118–127 (1977).

Bugeaud, Y., Mignotte, M., Siksek, S., "Classical and modular approaches to exponential Diophantine equations II. The Lebesgue-Nagell equation". ***Compos. Math.*** 142: 31–62 (2006).

Bugeaud, Y., Mignotte, M., Siksek, S., Stoll, M., Tengely, S., "Integral Points on Hyperelliptic Curves". ***Algebra&Number Theory***, 2(8): 859-885 (2008).

Cohn, J. H. E., "The Diophantine equation $x^2 + 2^k = y^n$", ***Archiv der Mathematik***, 59: 341-344 (1992)

Cohn, J. H. E., "The Diophantine equation $x^2 + C = y^n$", ***Acta Arithmetica***, 65: 367-381 (1993a).

Cohn, J. H. E., "The Diophantine equation $x^2 + 2^k = y^n$", ***Glasgow Mathematical Journal***, 35: 203–206 (1993b).

KAYNAKLAR (Devam ediyor)

Cohn, J. H. E., "The Diophantine equation $x^2 + 2^k = y^n$", II, ***International Journal of Mathematics and Mathematical Sciences***, 22: 459-462 (1999).

Çallıalp, F., "Sayıların Teorisi", ***Birsen Yayınevi,*** İstanbul (2009).

Çallıalp, F., "Örneklerle Soyut Cebir", ***Birsen Yayınevi,*** İstanbul (2013).

De Chenne, S., "The Ramanujan-Nagell Theorem: Understanding the Proof". http://buzzard.ups.edu/courses/2013spring/projects/spencer-ant-ups-434-2013.pdf , (Ziyaret edilme tarihi, 18.05.2016).

Feng, K., "Algebraic Number Theory", ***Science Press***, Beijing (2000).

Finch, S., "Class Number Theory", 2005.
http://www.people.fas.harvard.edu/~sfinch/csolve/clss.pdf
(Ziyaret edilme tarihi: 27.05.2016)

Ireland, K., Rosen, M., "A Classical Introduction to Modern Number Theory 3rd ed.", ***Springer-Verlag***, New York (1990).

Kılıçlı, S., "Lebesgue-Nagell Diophantine Denklemlerinin Çözümleri", Yüksek Lisans Tezi, *Ondokuz Mayıs Üniversitesi Fen Bilimleri Enstitüsü*, Samsun (2014).

Ko, Chao, "On the diophantine equation $x^2 = y^n + 1$, $xy \neq 0$", ***Sci. Sinica***, 14:457-460 (1965).

Korhonen, O., "On the Diophantine equation $Ax^2 + 8B = y^n$", ***Acta Univ. Oulu. Ser. A Sci. Rerum Natur. Math.***, 16 (1979a).

Korhonen, O., "On the Diophantine equation $Ax^2 + 2B = y^n$", ***ibid.***, 17 (1979b).

Korhonen, O., "On the Diophantine equation $Cx^2 + D = y^n$", ***ibid.***, 25 (1981).

Lebesgue, V. A., "Sur l'impossibilitè en nombres entiers de l'èquation $x^n = y^2 + 1$", ***Nouvelles Annales des Mathèmatiques***, 1(9): 178-181 (1850).

Le, M., Guo, Y., "On the Diophantine equation $x^2 + 2^k = y^n$", ***Chin. Sci. Bull.*** 42: 1255–1257 (1997).

Ljunggren, W., "On the diophantine equation $x^2 + p^2 = y^n$", ***Norske Vid. Selsk. Forh. Trondheim***, 16(8):27–30 (1943a).

Ljunggren, W., "Über einige Arcustangensgleichungen die auf interessante unbestimmte Gleichungen führen", ***Ark. Mat. Astr. Fys.***, 29A(13) (1943b).

KAYNAKLAR (Devam ediyor)

Ljunggren, W., "On the diophantine equation $x^2 + D = y^n$", ***Norske Vid. Selsk. Forh. Trondheim***, 17(23): 93-96 (1944).

Luca, F., "On a Diophantine equation", ***Bulletin of The Australian Mathematical Society*** 61: 241-246 (2000).

Mordell, L.J., "Diophantine Equations". ***Academic Press***, London (1969).

Nagell, T. , Sur l'impossibilitè de quelques èquations àdeux indèterminèes, ***Norsk. Mat. Forensings Skrifter***, 13: 65–82 (1923).

Nagell, T., "On the Diophantine equation $x^2 + 8D = y^n$", ***Ark. Mat.*** 3: 103–112 (1954a).

Nagell, T., Verallgemeinerung eines Fermatschen Satzes, ***Arch. Math. (Basel)***, 5: 153–159 (1954b).

Nagell, T., "Contributions to the theory of a category of diophantine equations of the second degree with two unknowns", ***Nova Acta Regtae Soc. Sc. Upaliensls***, Ser. 4, 16(2): 1-38 (1955).

Silverman, J., "The Arithmetic of Elliptic Curves", ***Springer-Verlag***: New York (1986).

Stewart, I.N. and Tall, D.O., "Algebraic Number Theory", ***Chapman and Hall***: London (1987).

Tao, L., "On the Diophantine Equation $x^2 + 5^m = y^n$", ***The Ramanujan Journal***, 19: 325-338 (2009).

Vîrgolici, H., "On the Exponential Diophantine Equation $x^2 + D = y^n$: a brief survey", ***Annals Of Spiru Haret University Mathematics-Informatics Series***, 9: 45-54, (2013).

Wren, B. M. E., "$y^2 + D = x^5$", ***Eureka***, 36: 37–38 (1973).

ÖZGEÇMİŞ

Kişisel Bilgiler

Adı Soyadı : Mehmet KILIÇ

Doğum Yeri ve Tarihi : Gölhisar /BURDUR-1986

Eğitim Durumu

Lisans Öğrenimi : Afyon Kocatepe Üniversitesi, Matematik

Bildiği Yabancı Diller : İngilizce

Bilimsel Faaliyetleri :

İş Deneyimi

Stajlar :

Projeler :

Çalıştığı Kurumlar : Bilecik Şeyh Edebali Üniversitesi, Uluslararası İlişkiler Ofisi

İletişim

Adres : Bilecik Şeyh Edebali Üniversitesi, Uluslararası İlişkiler Ofisi, Eski Rektörlük Binası Zemin Kat

Tel : (228) 214 14 10

E-Posta Adresi : mehmet.kilic@bilecik.edu.tr

Akademik Çalışmaları

i. ……

Yabancı Dil Bilgisi **:** İngilizce (Orta Seviye)

Tarih:23/06/2016