T.C.

BURSA ULUDAĞ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

TERAI SANISI HAKKINDAKİ DIOPHANT DENKLEMLER

Elif KIZILDERE

Prof. Dr. Gökhan SOYDAN
(Danışman)

YÜKSEK LİSANS TEZİ
MATEMATİK ANABİLİM DALI

BURSA – 2019

TEZ ONAYI

Elif KIZILDERE tarafından hazırlanan "Terai Sanısı Hakkındaki Diophant Denklemler" adlı tez çalışması aşağıdaki jüri tarafından oy birliği/~~oy çokluğu~~ ile Bursa Uludağ Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı'nda **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Danışman : Prof. Dr. Gökhan SOYDAN

Üye: Prof. Dr. Gökhan SOYDAN — İmza
Bursa Uludağ Üniversitesi Fen Edebiyat Fakültesi,
Matematik Anabilim Dalı

Üye: Prof. Dr. Refik KESKİN — İmza
Sakarya Üniversitesi Fen Edebiyat Fakültesi,
Matematik Anabilim Dalı

Üye: Doç. Dr. Musa DEMİRCİ — İmza
Bursa Uludağ Üniversitesi Fen Edebiyat Fakültesi,
Matematik Anabilim Dalı

Yukarıdaki sonucu onaylarım

Prof. Dr. Hüseyin Aksel EREN
Ensititü Müdürü
.. / .. / 2019

B. U. Ü. Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu,
- başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- atıfta bulunduğum eserlerin tümünü kaynak olarak gösterdiğimi,
- kullanılan verilerde herhangi bir tahrifat yapmadığımı,
- ve bu tezin herhangi bir bölümünü bu üniversite veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı

beyan ederim.

12 / 06 / 2019

İmza

Elif KIZILDERE

Bu tez çalışması TÜBİTAK tarafından 3001 Başlangıç Ar-Ge Projeleri Destekleme Programı kapsamında 117F287 nolu proje ile desteklenmektedir.

ÖZET

Yüksek Lisans Tezi

TERAI SANISI HAKKINDAKİ DIOPHANT DENKLEMLER

Elif KIZILDERE

Bursa Uludağ Üniversitesi
Fen Bilimleri Enstitüsü
Matematik Anabilim Dalı

Danışman: Prof. Dr. Gökhan SOYDAN

Bu tez üç bölümden oluşmaktadır. Birinci bölümde ilk olarak sayılar teorisinden, cebirden ve cebirsel sayılar teorisinden bilinen bazı temel kavramlar verilmiştir. Sonrasında ikinci mertebeden tekrarlama bağıntılı diziler, ilkel bölen teoremi, logaritmalarda lineer formlar gibi Diophant denklemlerin modern teorisinde önemli yer tutan kavramlar hakkında bilgiler verilmiştir.

Tezin ikinci bölümünde $((c+1)m^2+1)^x + (cm^2-1)^y = (am)^z$ Diophant denkleminin bazı koşullar altında tek çözümünün $(x,y,z) = (1,1,2)$ olduğu gösterilmiştir. Dolayısıyla bu denklem için Terai sanısı doğrulanmıştır.

Tezin son bölümünde ise Nagell'in $2^x + 5^y = 3^z$ ve $4^x + 7^y = 5^z$ Diophant denklemlerinin genellemesi olan $(n-1)^x + (n+2)^y = n^z$ Diophant denkleminin tüm pozitif tamsayı çözümleri bulunmuştur. İspatlarda kullanılan materyaller, sayılar teorisindeki elemanter yöntemler, Baker teorisi ve Lucas dizilerinin ilkel bölen teoremidir.

Anahtar Kelimeler: Diophant denklem, Jacobi sembolü, Baker'in teorisi, Lucas dizilerinin ilkel bölenleri

2019, viii + 65 sayfa.

ABSTRACT

Msc Thesis

DIOPHANTINE EQUATIONS CONCERNING TERAI'S CONJECTURE

Elif KIZILDERE

Bursa Uludağ University
Graduate School of Natural and Applied Sciences
Department of Mathematics

Supervisor: Prof. Dr. Gökhan SOYDAN

This thesis consists of three chapters. In the first chapter, firstly some fundamental known notions from number theory, algebra and algebraic number theory are recalled. Then the notions such as the second order linear recurrence sequences, primitive divisor theorem and linear forms in logarithms which have and important place in the modern theory of Diophantine equations are given.

In the second chapter of the thesis, it was shown that the Diophantine equation $((c+1)m^2+1)^x + (cm^2-1)^y = (am)^z$ under some conditions has only the positive integer solution $(x,y,z) = (1,1,2)$. So, Terai's conjecture is confirmed for this equation.

In the last chapter of the thesis, all positive integer solutions of the Diophantine equation $(n-1)^x + (n+2)^y = n^z$ which is generalisation of Nagell's Diophantine equations $2^x + 5^y = 3^z$ and $4^x + 7^y = 5^z$ were found. The main tools which are used on the proofs are elementary methods of number theory, Baker's theory and primitive divisor theorem of Lucas sequences.

Key Words: Diophantine equation, Jacobi symbol, Baker's theory, primitive divisors of Lucas sequences.

2019, viii + 65 pages.

TEŞEKKÜR

Bu tez çalışmasındaki her aşamada büyük emeği olan, karşılaştığım zorluklarda bana yol gösteren, sabırla sorularımı cevaplayan, yardım ve desteğini üzerimden esirgemeyen, olumlu yaklaşımlarıyla teşvik eden, tecrübesi ve bilgisi ile yönlendiren, kullandığı her kelimenin hayatıma kattığı önemini asla unutmayacağım Danışman hocam Prof. Dr. Gökhan Soydan'a içtenlikle teşekkür ederim.

TÜBİTAK-3001 Başlangıç Ar-Ge Projeleri Destekleme Programı kapsamında 117F287 nolu projeden aldığım destek için TÜBİTAK'a teşekkür ederim.

Üniversiteye başladığım andan itibaren desteğini esirgemeyen, kazandığı tecrübe ve bilgiler ile yol gösteren, motive eden hocam Prof. Dr. İsmail Naci Cangül'e ve üstümde emeği olan tüm hocalarıma teşekkür ederim.

Bu yaşıma gelene kadar maddi ve manevi desteklerini benden esirgemeyen, her zaman yanımda olan canım anneme, babama ve kardeşime candan teşekkür ederim.

PARI-GP programındaki hesaplamalarıyla ve verdiği önerilerle bizi aydınlatan Dr. Paul Voutier'e içtenlikle teşekkür ederim.

Beni hep güzel şeyler yapacağıma inanarak teşvik eden her zaman yanımda olduğunu hissettiğim en büyük destekçilerimden biri olan Can Anıl Mutlu'ya kalpten teşekkür ederim.

Elif KIZILDERE
12 / 06 / 2019

İÇİNDEKİLER

Sayfa

SİMGELER ve KISALTMALAR DİZİNİ

Simgeler	**Açıklama**
$\mathbb{C}$	Kompleks sayılar kümesi
$\mathbb{R}$	Reel sayılar kümesi
$\mathbb{Q}$	Rasyonel sayılar kümesi
$\mathbb{Z}$	Tamsayılar kümesi
$\mathbb{Z}^+$	Pozitif tamsayılar kümesi
$\mathbb{N}$	Doğal sayılar kümesi
$\mathbb{Z}_n$	$\{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{n-1}\}$ (n modundaki kalan sınıfları kümesi)
$\mathbb{Z}_n^*$	$\{\overline{1}, \overline{2}, \cdots, \overline{n-1}\}$
$\mathbb{Q}(\alpha)$	Rasyonel sayılar cismine α cebirsel sayısının katılmasıyla elde edilen cisim genişlemesi
Q_m	m modülüne göre ikinci dereceden kalanların kümesi
Q_m^*	$Q_m \backslash \{0\}$
$\mathbb{F}[x]$	Katsayıları $\mathbb{F}$ cisminden alınan x belirsizine göre polinomlar halkası
$a \mid b$	a, b sayısını böler
$a \nmid b$	a, b sayısını bölmez
$p^u \parallel a$	$p^u \mid a$ ancak $p^{u+1} \nmid a$
$\left(\frac{a}{n}\right)$	a sayısının n modunda Jacobi Sembolü
$a \sim b$	a, b'ye denktir
$[E : \mathbb{F}]$	$\mathbb{F}$ cisminin E cismi üzerindeki derecesi
F_n	n. Fibonacci sayısı
L_n	n. Lucas sayısı
$H(\alpha)$	α cebirsel sayısının büyüklüğü
$der(\alpha)$	α cebirsel sayısının derecesi
$ind(\alpha, \mathbb{F})$	α cebirsel sayısının $\mathbb{F}$ cismi üzerindeki indirgenmez polinomu
$h(\beta)$	β cebirsel sayısının mutlak logaritmik büyüklüğü
$\log a$	a sayısının logaritması

(a, b)	a ve b tamsayılarının en büyük ortak böleni
$[a, b]$	a ve b tamsayılarının en küçük ortak katı
$a \equiv b \pmod{m}$	a ve b, m modunda birbirine kongrüanttır
$a \not\equiv b \pmod{m}$	a ve b, m modunda birbirine kongrüant değildir
$[\![a]\!]$	a sayısının tam kısmı
$0_{\mathbb{F}}$	$\mathbb{F}$ cisminin sıfır elemanı
$w(n)$	n'nin farklı asal bölenlerinin sayısı

ÇİZELGELER DİZİNİ

Sayfa

1. GİRİŞ VE TEMEL KAVRAMLAR

Bu bölümde cebir, sayılar teorisi ve cebirsel sayılar teorisinden iyi bilinen bazı temel tanım ve teoremler verilecektir. Ayrıca tezin 2. ve 3. bölümlerinde gerekli olacak literatürden bilinen bazı teoremler ve yardımcı teoremler de bu bölümde ifade edilecektir.

1.1 Tarihsel Giriş

Günümüzde birçok amatör ve profesyonel matematikçi Diophant denklemler hakkında, hatta Diophant analizi hakkında bile bilgiye sahiptirler. Yirminci yüzyılın ikinci yarısında matematiğin bu alanı, cebirsel geometriye yakınlığından ve matematiksel düşüncenin açık bir odağı haline gelmesinden dolayı çok popüler olmuştur. Bu denklemler ismini, "cebirin babası" olarak bilinen "İskenderiyeli Diophantus" tan alır. Diophantus bilim tarihinin en zor bilmecelerinden birini temsil eder. Ne zaman yaşamış olduğu ve onunla aynı alanda çalışmış olanların kimler olduğu net olarak bilinmez. Diophantus'un çalışmaları da zifiri karanlıkta parlayan bir ateşe benzer.

Diophantus'un 500 yıllık bir dönemde herhangi bir zaman diliminde yaşamış olduğu tahmin edilir. Yaşamış olduğu dönemin alt sınırını belirlemek kolaydır. Çünkü çokgenler üzerine yazdığı kitabında M.Ö. 2. yüzyılda yaşamış olan İskenderiyeli matematikçi Hypsicles'den bahsedilir. Diğer yandan ise İskenderiyeli Theon'un büyük astronom Ptolemy'nin "Almopest" adlı eserine yaptığı yorumda Diophantus'un çalışmalarından bahseder. Theon'un M.S. 4. yüzyılın ortalarında yaşamış olduğu bilindiğinden Diophantus'un yaşadığı 500 yıllık dönemin bu dönem olduğu tahmin edilir. Çoğu tarihçi de onun çalışmalarının çoğunu M.S. 250 civarında yaptığına inanır. Diophantus'un hayatı hakkında en önemli bilgi M.S. 500 civarında Metradorus tarafından yazılan bilmecelerin kurgusal birleşiminden gelir. Bunlardan biri şu şekildedir:

> "Diophantus hayatının $\frac{1}{6}$ sında çocukluk çağını geçirmiş; $\frac{1}{7}$ sinden sonra evlenmiş; $\frac{1}{12}$ sinden sonra sakalları uzamış; oğlu evlendikten 5 yıl sonra doğmuş; oğlu babasının yaşının yarısı kadar yaşamış ve baba oğlundan 4 yıl sonra ölmüştür."

Bu bilmeceden Diophantus'un 84 yıl yaşadığını hesaplamak kolaydır.

Diophantus antik Yunan zamanında cebirde sembolleri ilk kullanan matematikçi idi. O, matematikte bilinmeyen niceliğini sembolize etmiş, negatif sayıları tanıtmış, cebirsel işlemler ve üslü ifadeler için semboller kullanmıştır. Ayrıca sayılar teorisindeki önemli sonuçları 13 ciltlik "Arithmetica" isimli eserinde ifade etmiştir. Bu eserde üçüncü dereceye kadar olan denklemlerin çözümlerini içeren yaklaşık 150 tane problem yer alır. Ancak 13 ciltlik bu eserin sadece 6 cildi günümüze kadar korunabilmiştir.

1.2 Diophant Denklemler

Aritmetik en eski matematik aktivitelerinden biridir. Aritmetik alanındaki gelişmelerde Diophantus, sayılar teorisinde notasyon kullanımına yenilik getirmekle kalmamış, önemli problemler önermiş ve bunları çözmüştür.

Kendi ismiyle anılan Diophantus'un denklemleri şöyle tanımlanır:
$n \geq 2$ ve f, n değişkenli bir fonksiyon olmak üzere

$$f(x_1, x_2, \cdots, x_n) = 0 \tag{1.2.1}$$

formundaki denklem *Diophant denklem* olarak adlandırılır. f tamsayı katsayılı bir polinom ise (1.2.1) denklemi *cebirsel bir Diophant denklem* olarak adlandırılır. (1.2.1) denklemini sağlayan $(x_1', x_2', \cdots, x_n') \in \mathbb{Z}^n$ n'lisi (1.2.1) denkleminin bir *çözümüdür*. Bir veya daha çok çözüme sahip olan denklem *çözülebilir* olarak adlandırılır. Bir Diophant denklemi hakkında üç temel problem düşünülür:

1. Denklem çözülebilir mi?
2. Denklem çözülebilir ise çözümlerin sayısı sonlu mu yoksa sonsuz çoklukta mıdır?
3. Denklem çözülebilir ise tüm çözümlerin belirlenmesi.

Diophantus'un (1.2.1) tipindeki denklemler hakkındaki çalışmalarına 3. yüzyılda Çinliler, 8 ile 12. yüzyıllarda Araplar devam etmişlerdir. Fermat, Euler, Lagrange, Gauss ve diğer

matematikçiler de bu denklemler hakkında daha derinlemesine çalışmışlardır.

Sayılar teorisi tarihindeki ilk Diophant denklemlerden biri

$$x^2 + y^2 = z^2 \tag{1.2.2}$$

denklemidir. Bu denklem, kenarları tamsayı olan tüm dik üçgenlerin belirlenmesi probleminden ortaya çıkmıştır. (1.2.2) denklemini sağlayan (x, y, z) üçlüleri *Pisagor üçlüleri* olarak adlandırılır. $(3, 4, 5),\ (5, 12, 13),\ (8, 15, 17)$ bu Pisagor üçlülerinden bazılarıdır. Ancak bu üçlüler sonlu tane olmadığından hepsi bunlardan ibaret değildir. Tüm Pisagor üçlüleri şu şekilde elde edilebilir: Eğer (x, y, z) üçlüsü, (1.2.2) denklemi için bir çözüm ise, bu denklemde eşitliğin her iki tarafı z^2 ile bölündüğünde $\left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1$ birim çemberi elde edilir ve buna karşılık gelen çözümler $\left(\frac{x}{z}, \frac{y}{z}\right)$ rasyonel ikilileridir. $t \in \mathbb{Q}$ olmak üzere $\cos\theta = \frac{1-t^2}{1+t^2},\ \sin\theta = \frac{2t}{1+t^2},\ t = \tan(\theta/2)$ parametreleri yardımıyla yukarıdaki birim çemberin üzerindeki tüm rasyonel çözümleri, dolayısıyla (1.2.2) denkleminin tüm tamsayı çözümleri bulunabilir. Başka bir örnek de $a, b, c \in \mathbb{Z}$ sabitler ve $x, y \in \mathbb{Z}$ değişkenler olmak üzere $ax + by = c$ lineer Diophant denklemidir.

Yine en meşhur Diophant denklemlerden biri (1.2.2) denkleminin genellemesi olan Fermat'nın denklemi $x^n + y^n = z^n, (n \geq 3)$ tür.

Diophant denklemlerin çalışılması modern sayılar teorisinde birçok tekniğin gelişmesine sebep olmuştur. Örneğin "Fermat'nın Son Teoremi"nin ispatı ile cebirsel geometri, eliptik eğri teorisi ve cebirsel sayılar teorisi gibi birçok alanda önemli gelişmeler sağlanmıştır.

1900 yılında David Hilbert'in önerdiği 23 problem arasındaki 10'uncu problem Diophant denklemler hakkında idi. Hilbert tüm Diophant denklemleri çözmek için genel bir metodun olup olmayacağını sorgulamıştır. Hilbert'in 10'uncu problemi şöyle ifade edilir:

"Tamsayı katsayılı, sonlu sayıda değişkene sahip olan bir Diophant denklemin çözümünün olup olmayacağına karar verebilecek bir genel algoritma mümkün müdür?"

1970'te Yuri Matiyasevich, Hilbert'in 10'uncu problemine olumsuz bir cevap vererek aşağıdaki sonucunu ifade etmiştir:

Teorem 1.2.1 Verilen keyfi bir Diophant denklem için bir tamsayı çözümü olup olmayacağına karar verebileceğimiz bir algoritma mümkün değildir (Matiyasevich 1970).

Uyarı 1.2.2 Hilbert'in 10'uncu probleminin benzeri, yani bir Diophant denklemin rasyonel çözümünün olup olmayacağına karar verebilecek bir algoritmanın varlığı henüz ispatlanmış değildir, yani halen açık bir problemdir.

Diophant denklemleri çözmek için genel bir metot olmadığından Diophant denklemlerin bazı tiplerini çözmek için birçok teknik bulunmuştur. Fermat, Euler, Lagrange ve Poincaré gibi birçok matematikçi bu konu üzerinde çalışmıştır. Transandant sayı teori ve hesaplamaya dayalı sayı teori gibi alanlardaki gelişmeler de Diophant denklemlerin çözümünde önemli bir araç olmuştur.

Bu tezde, modern sayı teorisinin yukarıda bahsedilen teknikleri kullanılarak bazı üstel denklemlerin tüm çözümlerinin belirlenmesi üzerine çalışılmıştır.

1.3 Kongrüanslar

Tanım 1.3.1 $a, b \in \mathbb{Z}$ ve $m \in \mathbb{Z}^+$ olsun. Eğer $m \mid a - b$ ise a, b'ye m *modülüne göre denktir* denir ve $a \equiv b \pmod{m}$ şeklinde gösterilir. Eğer $m \nmid a - b$ ise o zaman a, b'ye m *modülüne göre denk değil* denir ve $a \not\equiv b \pmod{m}$ ile gösterilir (Asar ve Arıkan 2012).

$a \equiv b \pmod{m}$ ifadesine bir kongrüans ve b'ye a'nın m *modülüne göre bir kalanı* denir. Böylece m ile $\mathbb{Z}$ üzerine tanımlanmış olan bağıntıya da m *modülüne göre kongrüans* denir.

Teorem 1.3.2 $a, b, c \in \mathbb{Z}$ ve $m \in \mathbb{Z}^+$ olsun. Aşağıdakiler sağlanır.

i. m modülüne göre kongrüans $\mathbb{Z}$ üzerinde bir denklik bağıntısıdır.

ii. $a \equiv b \pmod{m}$ ve $c \equiv d \pmod{m}$ ise her $x, y \in \mathbb{Z}$ için $ax + cy \equiv bx + dy \pmod{m}$ dir.

iii. $a \equiv b \pmod{m}$ ve $c \equiv d \pmod{m}$ ise $ac \equiv bd \pmod{m}$ dir.

iv. $a \equiv b \pmod{m}$ ve $t \mid m$ ise $a \equiv b \pmod{t}$ dir (Asar ve Arıkan 2012).

Teorem 1.3.3 $a, x, y \in \mathbb{Z}$ ve $m \in \mathbb{Z}^+$ olsun. Aşağıdakiler sağlanır.

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

ii. $ax \equiv ay \pmod{m}$ ve $(a, m) = 1$ ise $x \equiv y \pmod{m}$ dir.

iii. $m_1, m_2, \cdots, m_r$ her biri sıfırdan farklı tamsayılar olmak üzere $i = 1, 2, \cdots, r$ için, $x \equiv y \pmod{m_i}$ olması için gerek ve yeter şart $x \equiv y \pmod{[m_1, m_2, \cdots, m_r]}$ olmasıdır (Asar ve Arıkan 2012).

1.4 İkinci Dereceden Kalanlar

Tanım 1.4.1 $(a, m) = 1$ olsun. Eğer $x^2 \equiv a \pmod{m}$ kongrüansının bir çözümü varsa a sayısına m *modülüne göre ikinci dereceden bir kalan* denir. Eğer çözüm yoksa a sayısı m modülüne göre ikinci dereceden bir kalan değildir. m modülüne göre ikinci dereceden kalanların kümesi Q_m ile gösterilir (Asar ve Arıkan 2012).

Tanım 1.4.2 (Legendre Sembolü) p bir tek asal ve a bir tamsayı olsun. Legendre sembolü

$$\left(\frac{a}{p}\right) = \begin{cases} 0\,, & p \mid a \text{ ise,} \\ 1\,, & a \in Q_p \text{ ise,} \\ -1\,, & a \notin Q_p \text{ ise} \end{cases}$$

şeklinde tanımlanır. Burada $x^2 \equiv a \pmod{n}$ kongrüansının bir çözümü varsa $\left(\frac{a}{n}\right) = 1$ şeklinde ifade edilir (Menezes ve ark. 1996).

Jacobi sembolü de, Legendre sembolünün daha geneli olan bir fonksiyondur. Şöyle tanımlanır:

Tanım 1.4.3 $p_1, p_2, \cdots, p_k$ asal sayılar, $e_1, e_2, \cdots, e_k \in \mathbb{Z} \cup \{0\}$ olmak üzere $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ (≥ 3) bir tek tamsayı olsun. Jacobi sembolü

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \left(\frac{a}{p_2}\right)^{e_2} \cdots \left(\frac{a}{p_k}\right)^{e_k}$$

şeklinde tanımlanır (Menezes ve ark. 1996).

Eğer n bir asal ise Jacobi sembolü aslında Legendre sembolüdür.

1.4.1 Jacobi Sembolü ve Özellikleri

$m \geq 3, n \geq 3$ tek tamsayılar ve $a, b \in \mathbb{Z}$ olsun. Jacobi sembolünün özellikleri aşağıdaki gibidir:

i. $\left(\frac{a}{n}\right) = 0, 1$ veya -1 dir. Ayrıca $\left(\frac{a}{n}\right) = 0$ olması için gerek ve yeter şart $(a, n) \neq 1$ olmasıdır.

ii. $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right) \cdot \left(\frac{b}{n}\right)$ dir. Eğer $a \in \mathbb{Z}_n^*$ ise $\left(\frac{a^2}{n}\right) = 1$ dir.

iii. $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right) \cdot \left(\frac{a}{n}\right)$ dir.

iv. $a \equiv b \pmod{n}$ ise $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$ dir.

v. $\left(\frac{1}{n}\right) = 1$ dir.

vi. $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$ dir. Yani $n \equiv 1 \pmod{4}$ ise $\left(\frac{-1}{n}\right) = 1$, $n \equiv 3 \pmod{4}$ ise $\left(\frac{-1}{n}\right) = -1$ dir.

vii. $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$ dir. Yani $n \equiv 1$ veya $7 \pmod{8}$ ise $\left(\frac{2}{n}\right) = 1$, $n \equiv 3$ veya $5 \pmod{8}$ ise $\left(\frac{2}{n}\right) = -1$ dir.

viii. $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right) \cdot (-1)^{(n-1)(m-1)/4}$ tür. Diğer bir ifade ile m ve n'nin her ikiside 4 modunda 3'e denk ise $\left(\frac{m}{n}\right) = -\left(\frac{n}{m}\right)$, aksi takdirde $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)$ dir.

ix. n ve a_1 tek sayılar iken $a = 2^e \cdot a_1$ ise,

$$\left(\frac{a}{n}\right) = \left(\frac{2^e}{n}\right)\left(\frac{a_1}{n}\right) = \left(\frac{2}{n}\right)^e \cdot \left(\frac{n \pmod{a_1}}{a_1}\right) \cdot (-1)^{(n-1)(a_1-1)/4}$$

tür (Menezes ve ark. 1996).

Örnek 1.4.4 $a = 158$ ve $n = 235$ için $\left(\frac{a}{n}\right)$'yi hesaplayalım.

$$\left(\frac{a}{n}\right) = \left(\frac{158}{235}\right) = \left(\frac{2}{235}\right)\left(\frac{79}{235}\right) = (-1)^{(235^2-1)/8}\left(\frac{235}{79}\right)(-1)^{(79-1)(235-1)/4} = \left(\frac{77}{79}\right)$$

$$= \left(\frac{79}{77}\right)(-1)^{78\cdot 76/4} = \left(\frac{2}{77}\right) = \left(\frac{2}{11}\right)\left(\frac{2}{7}\right) = (-1)^{(11^2-1)/8}(-1)^{(7^2-1)/8} = -1$$

dir.

1.4.2 Kronecker Sembolü ve Özellikleri

Tanım 1.4.5 $m > 0$, $d \equiv 0$ veya $1 \pmod 4$ olsun ve d bir tam kare olmasın. $\left(\frac{d}{m}\right)$ Kronecker sembolü

$$\left(\frac{d}{p}\right) = 0, \quad p \mid d \text{ ise;}$$

$$\left(\frac{d}{2}\right) = \begin{cases} 1\,, & d \equiv 1 \pmod 8 \text{ ise,} \\ -1\,, & d \equiv 5 \pmod 8 \text{ ise;} \end{cases}$$

$$\left(\frac{d}{p}\right) = \text{Legendre sembolü}, p \text{ tek asal ve } p \nmid d \text{ ise}$$

şeklinde tanımlanır. Eğer p_r asal iken $m = \prod_{r=1}^{v} p_r$ ise,

$$\left(\frac{d}{m}\right) = \prod_{r=1}^{v}\left(\frac{d}{p_r}\right)$$

dir (Hua 1982).

Aşağıdakileri göstermek kolaydır;
(i) $(d, m) > 1$ ise $\left(\frac{d}{m}\right) = 0$ dır.
(ii) $(d, m) = 1$ ise $\left(\frac{d}{m}\right) = \pm 1$ dir.
(iii) Eğer $m_1 > 0,\ m_2 > 0$ ise

$$\left(\frac{d}{m_1 m_2}\right) = \left(\frac{d}{m_1}\right)\left(\frac{d}{m_2}\right)$$

dir.

Teorem 1.4.6 $m > 0,\ (m, d) = 1$ ise Kronecker sembolü

$$\left(\frac{d}{m}\right) = \begin{cases} \left(\frac{m}{|d|}\right), & d \text{ tek iken,} \\ \left(\frac{2}{m}\right)^b (-1)^{\frac{u-1}{2}\frac{m-1}{2}} \left(\frac{m}{|u|}\right), & d = 2^b u,\ 2 \nmid u \text{ iken} \end{cases}$$

şeklinde verilir. Burada $\left(\frac{m}{|d|}\right),\ \left(\frac{2}{m}\right)$ ve $\left(\frac{m}{|u|}\right)$ birer Jacobi sembolüdür (Hua 1982).

Teorem 1.4.7 $\left(\frac{d}{m}\right)$ Kronecker sembolü, $(\mathrm{mod}\ |d|)$'de reel karakterdir (yani sadece ± 1 ve 0 değerlerini alır) (Hua 1982).

Teorem 1.4.8 $m > 0,\ n > 0$ ve $m \equiv -n\ (\mathrm{mod}\ |d|)$ olsun. O halde

$$\left(\frac{d}{m}\right) = \begin{cases} \left(\frac{d}{m}\right), & d > 0 \text{ ise,} \\ -\left(\frac{d}{n}\right), & d < 0 \text{ ise} \end{cases}$$

dir (Hua 1982).

1.5 Sürekli Kesirler

Tanım 1.5.1 $q_0, q_1, \cdots, q_k, \cdots$ terimleri reel sayılar ve q_0 dışındaki bütün terimleri pozitif olan bir (sonlu ya da sonsuz) dizi olsun. O halde

$$q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots + q_k + \cfrac{1}{q_{k+1} + \cfrac{1}{\ddots}}}}}$$

ifadesine bir *sürekli kesir* denir ve bu sürekli kesir $< q_0, q_1, \cdots, q_k, \cdots >$ ile gösterilir. Bundan başka verilen dizinin sonlu ya da sonsuz olmasına göre bu sürekli kesre *sonlu sürekli kesir* ya da *sonsuz sürekli kesir* denir. Ayrıca eğer her $i \geq 0$ için q_i bir tamsayı ve $q_{i+1} \geq 1$ ise o zaman bu sürekli kesre *basit sürekli kesir* denir (Asar ve Arıkan 2012).

Şimdi de $\alpha \neq 0$ bir irrasyonel sayı olsun. α'nın tam kısmı $[\![\alpha]\!]$, α'nın tam değeridir. O halde $\alpha = [\![\alpha]\!] + (\alpha - [\![\alpha]\!])$ olur. Burada $\alpha_1 = \dfrac{1}{\alpha - [\![\alpha]\!]}$ olsun. O halde $\alpha_1 > 1$ ve $\alpha = [\![\alpha]\!] + \dfrac{1}{\alpha_1} =< [\![\alpha]\!], \alpha_1 >$ olur. Şimdi $\alpha_1 > 1$ ve irrasyonel olduğundan ilk halde olduğu gibi öyle bir $\alpha_2 > 1$ irrasyonel sayısı vardır ki; $\alpha_1 = [\![\alpha_1]\!] + \dfrac{1}{\alpha_2} =< [\![\alpha_1]\!], \alpha_2 >$ dir. Bu değerler sürekli kesirde yerine konulursa $\alpha = [\![\alpha]\!] + \cfrac{1}{[\![\alpha_1]\!] + \cfrac{1}{\alpha_2}} =< [\![\alpha]\!], [\![\alpha_1]\!], \alpha_2 >$ elde edilir. Bu şekilde devam edilirse her $i \geq 1$ için $\alpha_i > 1$ bir irrasyonel sayıdır ve $\alpha = \alpha_0, \alpha_1, \alpha_2, \cdots$ sonsuz dizisi ile $< [\![\alpha_0]\!], [\![\alpha_1]\!], [\![\alpha_2]\!], \cdots >$ sonsuz basit sürekli kesri elde edilir.

Örnek 1.5.2 $\alpha = \sqrt{2}$'ye karşılık gelen sonsuz basit sürekli kesir açılımını belirleyelim. $[\![\sqrt{2}\,]\!] = 1$ dir. $\alpha_1 = \dfrac{1}{\sqrt{2} - 1}$ olsun. O halde α_1 irrasyonel ve $\dfrac{1}{\sqrt{2} - 1} = \sqrt{2} + 1$ dir. Buradan $\sqrt{2} = 1 + \dfrac{1}{\sqrt{2} + 1} =< 1, \sqrt{2} + 1 >$ elde edilir. Şimdi $[\![\sqrt{2} + 1]\!] = 2$ ve $\alpha_2 = \dfrac{1}{\sqrt{2} - 1} = \alpha_1$ olduğundan $[\![\alpha_2]\!] = 2$ dir. Buradan görüldüğü gibi her $i \geq 1$ için

$\alpha_i = \alpha_{i-1}$ dir. Böylece $\sqrt{2}$'ye karşılık olarak

$$< 1, 2, 2, 2, \cdots >$$

sonsuz basit sürekli kesri elde edilir (Asar ve Arıkan 2012).

1.5.1 Sonsuz Sürekli Kesirler

Tanım 1.5.3 $< q_0, q_1, \cdots >$ bir sonsuz sürekli kesir olsun. Eğer $< q_0 >, < q_0, q_1 >,$ $< q_0, q_1, q_2 >, \cdots$ sonsuz sürekli basit kesirlerin dizisinin limiti varsa, o halde $< q_0, q_1, q_2, \cdots >$ sonsuz sürekli kesri yakınsaktır denir (Asar ve Arıkan 2012).

Şimdi $< q_0, q_1, q_2, \cdots >$ bir sonlu ya da sonsuz basit sürekli kesir olsun. Her $n \geq 0$ için a_n ve b_n tamsayıları şöyle tanımlansın:

$$a_0 = q_0,\ a_1 = q_0 \cdot q_1 + 1,\ a_{n+2} = a_{n+1} \cdot q_{n+2} + a_n$$

$$b_0 = 1,\ b_1 = q_1,\ b_{n+2} = b_{n+1} \cdot q_{n+2} + b_n. \tag{1.5.1}$$

Teorem 1.5.4 $< q_0, q_1, \cdots >$ bir sonsuz sürekli kesir ve her $n \geq 0$ için a_n ve b_n, (1.5.1)'deki bağıntılarla tanımlansın. Ayrıca α bir pozitif reel sayı olsun. O halde aşağıdakiler sağlanır.

i. $< q_0, q_1, \cdots, q_n, \alpha >= \dfrac{\alpha a_n + a_{n-1}}{\alpha b_n + b_{n-1}},\ n > 0;$

ii. $< q_0, q_1, \cdots, q_n >= \dfrac{a_n}{b_n}$

dir (Asar ve Arıkan 2012).

Yardımcı Teorem 1.5.5 Her $n \geq 0$ için aşağıdakiler sağlanır.

i. $a_n \cdot b_{n+1} - a_{n+1} \cdot b_n = (-1)^{n+1}$ dir.

ii. $\dfrac{a_n}{b_n} - \dfrac{a_{n+1}}{b_{n+1}} = \dfrac{(-1)^{n+1}}{b_n \cdot b_{n+1}}$ dir.

iii. $\frac{a_{n+2}}{b_{n+2}}$ sayısı $\frac{a_n}{b_n}$ ile $\frac{a_{n+1}}{b_{n+1}}$ arasındadır.

iv. Her sonsuz basit sürekli kesir yakınsaktır (Asar ve Arıkan 2012).

Teorem 1.5.6 $< q_0, q_1, \cdots >$ bir sonsuz basit sürekli kesir olsun. O halde aşağıdakiler sağlanır.

i. $\lim_{n\to\infty} \frac{a_n}{b_n} = \alpha$ olacak şekilde bir α reel sayısı vardır. Bu $\frac{a_n}{b_n}$ kesrine de α'ya n. *yakınsayan değer* denir.

ii. Her $n \geq 0$ için

$$\left|\alpha - \frac{a_n}{b_n}\right| < \frac{1}{b_n \cdot b_{n+1}} < \frac{1}{b_n^2} \tag{1.5.2}$$

dir (Asar ve Arıkan 2012).

Teorem 1.5.7 Bir sonsuz basit sürekli kesrin değeri bir irrasyonel sayıdır (Asar ve Arıkan 2012).

Teorem 1.5.8 $\frac{a_n}{b_n}$, α'nın n. yakınsaması ise, $(a_n, b_n) = 1$ dir. (Khinchin 1963).

Teorem 1.5.9 Her $n \geq 0$ için

$$\left|\alpha - \frac{a_n}{b_n}\right| > \frac{1}{b_n(b_{n+1} + b_n)} \tag{1.5.3}$$

dir (Khinchin 1963).

Teorem 1.5.10 Eğer $\frac{a_n}{b_n}$ bir α sayısının $n > 0$ mertebeli bir yakınsaması ise,

$$\left|\alpha - \frac{a_n}{b_n}\right| < \frac{1}{2b_n^2}, \quad \left|\alpha - \frac{a_{n-1}}{b_{n-1}}\right| < \frac{1}{2b_{n-1}^2}$$

eşitsizliklerinden en az birini sağlamalıdır (Khinchin 1963).

Teorem 1.5.11 $\left|\alpha - \frac{a}{b}\right| < \frac{1}{2b^2}$ eşitsizliğini sağlayan her $\frac{a}{b}$ basit rasyonel kesri bir α sayısına yakınsar (Khinchin 1963).

Şimdi en genel durumda, (1.5.2) and (1.5.3) eşitsizliklerinden

$$\frac{1}{b_n(b_n + b_{n+1})} < \left|\alpha - \frac{a_n}{b_n}\right| \leq \frac{1}{b_n \cdot b_{n+1}}$$

elde edilir. Bu eşitsizliğe denk olarak

$$\frac{1}{b_n^2(1 + q_{n+1} + \dfrac{b_{n-1}}{b_n})} < \left|\alpha - \frac{a_n}{b_n}\right| \leq \frac{1}{b_n^2 \cdot q_{n+1} + \dfrac{b_{n-1}}{b_n}}$$

eşitsizliği ifade edilebilir. Buradan da

$$\frac{1}{b_n(q_{n+1} + 2)} < \left|\alpha - \frac{a_n}{b_n}\right| \leq \frac{1}{b_n^2 \cdot q_{n+1}}$$

eşitsizliğinin sağlandığı açıktır. Burada $q_0, q_1, \cdots, q_n$ değerlerinden daha büyük olan q_{n+1} elemanı $\dfrac{a_n}{b_n}$ kesrinin α sayısına yakınsayacağı en yakın değerdir.

1.6 İkinci Dereceden İki Değişkenli Formlar

Tanım 1.6.1 a, b, c sabit tamsayılar olmak üzere

$$F = F(x, y) = ax^2 + bxy + cy^2$$

tipindeki homojen ikinci dereceden iki değişkenli bir polinom, *ikinci dereceden iki değişkenli bir form* veya *basit form* olarak adlandırılır ve bu form $\{a, b, c\}$ şeklinde gösterilir.

$$d = b^2 - 4ac$$

tamsayısı bu formun *diskriminantı* olarak adlandırılır (Hua 1982).

$d \equiv 0, 1 \pmod 4$ olduğu kongrüanslar yardımıyla kolaylıkla görülebilir.

Teorem 1.6.2 F'nin tamsayı katsayılı iki lineer formun çarpımı şeklinde yazılabilmesi için gerek ve yeter şart d'nin bir tam kare olmasıdır (Hua 1982).

İspat. ($\Rightarrow$) $a \neq 0$ olmak üzere d bir tam kare olsun.

$$ax^2 + bx + c = a\left\{\left(x + \frac{b}{2a}\right)^2 - \frac{d}{4a^2}\right\} = 0$$

denkleminin rasyonel kökleri vardır ve bu yüzden bu form tamsayı katsayılı iki lineer formun çarpımı şeklinde ifade edilebilir. Eğer $a = 0$ ise $F(x, y) = (bx + cy)y$ dir.
($\Leftarrow$) Eğer

$$ax^2 + bxy + cy^2 = (rx + sy)(tx + uy)$$

ise

$$d = b^2 - 4ac = (st + ru)^2 - 4rtsu = (st - ru)^2$$

dir. Böylece ispat tamamlanır. ■

Şimdi d'nin bir tam kare olmadığını varsayalım.

Eğer $d < 0, a > 0$ ise

$$4aF = (2ax + by)^2 + (4ac - b^2)y^2 = (2ax + by)^2 - dy^2$$

ve her x, y için $F(x, y) \geq 0$ dır. $F(x, y) = 0$ olması için gerek ve yeter şart $x = y = 0$ olmasıdır. Bu tip formlar *pozitif belirli form* olarak adlandırılır. Eğer $d < 0, a < 0$ ise her x, y için $F(x, y) \leq 0$ dır ve bu da *negatif belirli form* olarak adlandırılır. Negatif form bir pozitif formun -1 ile çarpımı olduğundan sadece pozitif belirli formlar ile ilgilenmek yeterlidir. Bu da kısaca *belirli form* olarak adlandırılır. Eğer $d > 0$ ise

$$F(1, a) = a, \quad F(b, -2a) = ab^2 - b \cdot b \cdot 2a + c \cdot 4a^2 = -da$$

dır. Eğer $a \neq 0$ ise buradaki iki değer farklı işaretlidir. Eğer $c \neq 0$ ise benzer şekilde iki farklı işaretli değer seçilebilir. Eğer $a = c = 0$ ise,

$$F(1, 1) = b, \;\; F(1, -1) = -b$$

olacağından farklı işaretlere sahiptir. Yani $d > 0$ iken $F(x, y)$ hem pozitif hem negatif değerler alacağından bir *belirsiz form* olarak adlandırılır.

Tanım 1.6.3 $x = rX + sY,\ y = tX + uY,\ (ru - st) = 1$ tamsayı katsayılarının değişken değiştirmeleri kullanılarak $\begin{pmatrix} r & s \\ t & u \end{pmatrix}$ matrisi yardımıyla $F(x, y)$ formu $G(X, Y)$ formuna dönüştürülebilir. F ve G formlarına *denk formlar* denir ve bu $F \sim G$ ile gösterilir (Hua 1982).

Daha özel olarak, $F = \{a, b, c\}$ ve $G = \{a_1, b_1, c_1\}$ olsun. Bu durumda

$$\begin{aligned} a_1 &= ar^2 + brt + ct^2, \\ b_1 &= 2ars + b(ru + st) + 2ctu \\ &= 2ars + b(1 + 2st) + 2ctu, \\ c_1 &= as^2 + bsu + cu^2 \end{aligned}$$

bağıntıları elde edilir. Buradan da

$$\begin{aligned} b_1^2 - 4a_1c_1 &= (2ars + b(ru + st) + 2ctu)^2 \\ &\quad -4(ar^2 + brt + ct^2)(as^2 + bsu + cu^2) \\ &= (b^2 - 4ac)(ru - st)^2 = b^2 - 4ac = d \end{aligned}$$

olur. Yani denk formların diskriminantlarının aynı olduğu görülür.

Ayrıca pozitif belirli formlara denk olan formlar da pozitif belirli formlardır.

Teorem 1.6.4

i. $F \sim F$ dir. (Yansıma)

ii. $F \sim G$ ise $G \sim F$ dir. (Simetri)

iii. $F \sim G, G \sim H$ ise $F \sim H$ dır (Geçişme) (Hua 1982).

Denk olma bağıntısı d diskriminantlı formların kümesini denklik sınıflarına ayırır. Böylece bir sınıftaki tüm formlar kendi aralarında denktirler ve farklı iki sınıftaki iki form denk olamazlar.

1.6.1 İkinci Dereceden İki Değişkenli Formların Sınıf Sayısı

Teorem 1.6.5 Formların her sınıfında daima

$$|b| \leq |a| \leq |c|$$

şartını sağlayan bir form vardır (Hua 1982).

Teorem 1.6.6 Denklik sınıflarının sayısı sonludur (Hua 1982).

İspat. (i) $d > 0$ (belirsiz form). Teorem 1.6.5'ten

$$|ac| \geq b^2 = d + 4ac > 4ac$$

dir. Böylece $ac < 0$ dır. Ayrıca

$$4a^2 \leq 4|ac| = -4ac = d - b^2 \leq d$$

olur ki bu da

$$|a| \leq \frac{\sqrt{d}}{2}$$

dir. O halde Teorem 1.6.5'ten

$$|b| \leq \frac{\sqrt{d}}{2}$$

olur. Bu durumda a ve b için sonlu çoklukta değerler vardır. $c = \dfrac{b^2 - d}{4a}$ olduğundan, gerekli sonuç elde edilir.

(ii) $d < 0$ (belirli form). $a > 0$ olduğunu varsayarak Teorem 1.6.5'ten

$$-d = 4ac - b^2 \geq 4a^2 - b^2 \geq 3a^2$$

dir. Yani,

$$0 < a < \sqrt{\frac{|d|}{3}}$$

tür. Bu sonuç da Teorem 1.6.5'ten gelir. ■

Teorem 1.6.7 Diskriminantı d ile verilen pozitif belirli formların sınıflarının sayısı

$$b^2 - 4ac = d, \qquad \begin{cases} -a < b \leq a < c\,, \\ \text{veya } \ 0 \leq b \leq a = c \end{cases}$$

şartlarını sağlayan a, b, c tamsayılarının kümelerinin sayısına eşittir (Hua 1982).

1.6.2 $ax^2 + bxy + cy^2 = k$ Denkleminin Çözümleri

a, b, c ve k tamsayılar olmak üzere

$$ax^2 + bxy + cy^2 = k \tag{1.6.1}$$

denkleminin çözümlerini göz önüne alalım. $d = b^2 - 4ac$ dir. d'nin bir tam kare olmadığını varsayalım ve $(a, b, c) = 1$ olsun. (1.6.1) denkleminde $(x, y) = 1$ olacak şekildeki tüm çözümler *has çözümler* olarak adlandırılır.

Teorem 1.6.8 $d < 0$ olduğunu varsayalım.

$$w = \begin{cases} 2, & d < -4 \text{ ise}, \\ 4, & d = -4 \text{ ise}, \\ 6, & d = -3 \text{ ise} \end{cases}$$

olsun. O halde (1.6.1) denklemine karşılık gelen w tane çözüm vardır (Hua 1982).

Teorem 1.6.9 $d > 0$ olsun. O halde $x^2 - dy^2 = 4$ Diophant denkleminin tüm çözümleri şu şekilde bulunur: $x_0 + y_0\sqrt{d}\ (x_0 > 0,\ y_0 > 0)$ minimal olacak şekilde x_0, y_0 bir çözüm olsun. O halde tüm çözümler

$$\frac{x + y\sqrt{d}}{2} = \pm\Big(\frac{x_0 + y_0\sqrt{d}}{2}\Big)^n, \quad n = 0, \pm1, \pm2, \cdots$$

ile verilir (Hua 1982).

Şimdi

$$\varepsilon = \frac{x_0 + y_0\sqrt{d}}{2}, \quad \overline{\varepsilon} = \frac{x_0 - y_0\sqrt{d}}{2}$$

olsun. $\left(\frac{d}{n}\right)$ Kronecker sembolü olmak üzere

$$K(d) = \sum_{n=1}^{\infty} \Big(\frac{d}{n}\Big)\frac{1}{n}$$

önemli bir seridir. $\left(\frac{d}{n}\right),\ (\mathrm{mod}\ |d|)$'de reel karakter olduğundan (yani sadece ±1 ve 0 değerlerini alır), (Hua 1982, Teorem 7.2.3)'ten

$$\left| \sum_{a \le n \le b} \Big(\frac{d}{n}\Big) \right| < |d|$$

dir. Ayrıca (Hua 1982, Teorem 6.8.2)'den $K(d)$ yakınsak bir seridir.

Şimdi ikinci dereceden iki değişkenli formlar için sınıf sayısı formülünü verelim.

Teorem 1.6.10

$$h(d) = \begin{cases} \dfrac{w\sqrt{|d|}}{2\pi}K(d) & , \quad d < 0 \text{ ise,} \\ \dfrac{\sqrt{d}}{\log\varepsilon}K(d) & , \quad d > 0 \text{ ise} \end{cases}$$

dir (Hua 1982).

İkinci dereceden iki değişkenli formlar ile ilgili temel kavramları verdikten sonra, şimdi $4.$ bölümde ihtiyacımız olacak iki değişkenli formlar ile ilgili literatürden bilinen bazı önemli teorem ve önermeleri verelim.

a, b ve c sabit tamsayılar olmak üzere

$$F = F(x, y) = ax^2 + 2bxy + cy^2$$

ikinci dereceden ikili formu verilsin. $D = b^2 - ac$ iken bu formun diskriminantı $4D$ ile ifade edilsin. Bu durumda D_1 ve D_2 pozitif tamsayılar ve $D = D_1 D_2$ olmak üzere $D_1x^2 + D_2y^2$'nin diskriminantı $-4D$ dir. $-4D$ diskriminantlı pozitif ikinci dereceden ikili formların kümesi sonlu sayıda denklik sınıfına ayrılır. Bu denklik sınıflarının sayısı $h(-4D)$ ile gösterilir. Şimdi, bununla ilgili olarak, önemli iki sonucu ifade edelim.

Önerme 1.6.11 D yukarıda tanımlandığı gibi pozitif bir tamsayı olsun. Bu durumda

$$h(-4D) < \frac{4\sqrt{D}}{\pi} \log(2e\sqrt{D})$$

dir (Cohen 1993).

Yardımcı Teorem 1.6.12 D_1 ve D_2 aralarında asal pozitif tamsayılar ve $k \geq 2$, $D_1 D_2$ ile arasında asal bir tamsayı olsun.

(i) $D_1 D_2 \notin \{1, 3\}$ olsun. $w(k)$, k'nın farklı asal bölenlerinin sayısı iken,

$$D_1X^2 + D_2Y^2 = \lambda^2 k^Z, \;\; X, Y, Z \in \mathbb{Z}, \;\; (X, Y) = 1, \;\; Z > 0 \qquad (1.6.2)$$

denkleminin çözümleri en fazla $2^{w(k)-1}$ tane sınıfa ayrılabilir. Ayrıca her bir S sınıfında $X_1 > 0, Y_1 > 0$ olacak şekilde bir tek (X_1, Y_1, Z_1) çözüm vardır ve Z_1, S'nin çözümlerinin içinde minimaldir. Bu minimal çözüm için $D_1 = 1$ veya $D_2 = 1$ ise $Z_1 \mid h(-4D)$, aksi takdirde $2Z_1 \mid h(-4D)$ dir. Ayrıca, S'ye ait olan (1.6.2) denkleminin her (X, Y, Z) çözümü, $t \geq 1$ tamsayı, $\lambda_1 \in \{1, -1, i, -i\}$ ve $\lambda_2 \in \{1, -1\}$ olmak üzere

$$Z = Z_1 t, \quad \left(\frac{X\sqrt{D_1} + Y\sqrt{-D_2}}{\lambda}\right) = \lambda_1 \left(\frac{X_1\sqrt{D_1} + \lambda_2 Y_1\sqrt{-D_2}}{\lambda}\right)^t \qquad (1.6.3)$$

ile ifade edilebilir. $\lambda = \sqrt{2}$ ise t tektir. Ayrıca, $D_2 \neq 1$ veya t tek ise $\lambda_1 \in \{1, -1\}$ dir.

$D_2 = 1$ ve t çift ise $\lambda_1 \in \{i, -i\}$ dir.

(ii) $D_1 D_2 \in \{1, 3\}$ olsun. Bu durumda (1.6.2) denkleminin çözümleri en çok $2^{w(k)-1}$ tane sınıfa ayrılabilir. Ayrıca, her S sınıfında $X_1 > 0, Y_1 > 0$ olmak üzere tek bir $(X_1, Y_1, 1)$ çözümü vardır ki S'ye ait olan (1.6.2) denkleminin her (X, Y, Z) çözümü için $D_1 D_2 = 1$ ise $Z_1 = 1, \lambda_1 \in \{-1, 1, i, -i\}$ dir. Eğer $D_1 D_2 = 3$ ise

$$\lambda_1 \in \{-1, 1, i, -i, \frac{1+i\sqrt{3}}{2}, \frac{1-i\sqrt{3}}{2}, \frac{-1+i\sqrt{3}}{2}, \frac{-1-i\sqrt{3}}{2}\},$$

$\lambda_2 \in \{-1, 1\}$ dir (Bugeaud ve Shorey 2001).

1.7 Cisim Genişlemeleri

Tanım 1.7.1 E bir cisim, $\mathbb{F}$, E'nin bir altcismi olsun. O halde E'ye $\mathbb{F}$'nin bir *cisim genişlemesi* denir. $\mathbb{F} \leq E$ cisim genişlemesi

$$\begin{array}{c} E \\ | \\ \mathbb{F} \end{array}$$

şeklinde bir diyagramla gösterilir (Asar ve ark. 2012).

Tanım 1.7.2 $\mathbb{F}$ bir cisim ve E, $\mathbb{F}$'nin bir cisim genişlemesi olsun. $u \in E$ olsun. Eğer $\mathbb{F}[x]$'in sıfırdan farklı $f(x)$ polinomu için $f(\alpha) = 0$ ise α'ya F üzerinde bir *cebirsel eleman* denir. Eğer her $0 \neq f(x) \in \mathbb{F}[x]$ için $f(\alpha) \neq 0_{\mathbb{F}}$ ise α'ya $\mathbb{F}$ üzerinde bir *transandant eleman* denir (Asar ve ark. 2012).

Tanım 1.7.3 $\mathbb{Q}$ üzerinde cebirsel eleman olan bir kompleks sayıya *cebirsel sayı* ve transandant eleman olan bir kompleks sayıya da *transandant sayı* denir (Asar ve ark. 2012).

Örnek 1.7.4 $\mathbb{C}, \mathbb{Q}$ nun bir cisim genişlemesidir. $\sqrt{2},\ x^2 - 2$'nin bir kökü olduğundan $\mathbb{Q}$ üzerinde bir cebirsel elemandır. Aynı zamanda $\sqrt{-1} = i$ de x^2+1'in bir kökü olduğundan $\mathbb{Q}$ üzerinde cebirsel bir elemandır.

Örnek 1.7.5 π ve e, $\mathbb{Q}$ üzerinde transandanttır. e doğal logaritmanın tabanıdır (Asar ve ark. 2012).

Tanım 1.7.6 $u \in \mathbb{C}$ olsun. Eğer bir monik $0 \neq f(x) \in \mathbb{Z}[x]$ için $f(u) = 0$ ise u'ya bir *cebirsel tamsayı* denir (Asar ve Arıkan 2012).

Teorem 1.7.7 $\mathbb{F}$ bir cisim ve E, $\mathbb{F}$'nin bir cisim genişlemesi olsun. Ayrıca $u \in E$, $\mathbb{F}$ üzerinde cebirsel olsun. O zaman öyle bir monik ve indirgenmez $p(x) \in \mathbb{F}[x]$ vardır ki $p(u) = 0_{\mathbb{F}}$ dir. Ayrıca $p(x)$ tektir ve $g(u) = 0_{\mathbb{F}}$ olan her $g(x) \in \mathbb{F}[x]$'in bir bölenidir (Asar ve ark. 2012).

Bir *monik polinom*, en yüksek dereceye sahip olan x'in katsayısının 1 olduğu polinomdur.

Tanım 1.7.8 α bir cebirsel sayı olsun. $\mathbb{Q}$ üzerindeki α'nın *minimal polinomu*, $\mathbb{Q}$ üzerinde α'yı kök kabul eden en küçük dereceli monik polinomdur (Jarvis 2014).

Tanım 1.7.9 $\mathbb{F}$ bir cisim ve E, $\mathbb{F}$'nin bir cisim genişlemesi olsun. Ayrıca $\alpha \in E$, $\mathbb{F}$ üzerinde cebirsel olsun. O halde tek bir şekilde tanımlanan monik ve indirgenmez polinoma *α'nın $\mathbb{F}$ üzerindeki indirgenmez polinomu*, $der(p(x))$'e de *α'nın $\mathbb{F}$ üzerindeki derecesi* denir ve $p(x) = ind(\alpha, \mathbb{F}),\ der(p(x)) = der(\alpha, \mathbb{F})$ ile gösterilir (Asar ve ark. 2012).

Örnek 1.7.10 $ind(\sqrt{2}, \mathbb{Q}) = x^2 - 2$ olduğunu biliyoruz. $\mathbb{R}$'de bir $\alpha = \sqrt{1+\sqrt{3}},\ x^4 - 2x^2 - 2$'nin bir köküdür. Aynı zamanda $\mathbb{Q}[x]$'te de bir köktür. $x^4 - 2x^2 - 2$, $\mathbb{Q}$ üzerinde indirgenmez olduğundan (Eisenstein indirgenmezlik kriterinden $p = 2$ alınırsa $p \mid 2, p \nmid 1$ olduğundan indirgenmezdir),

$$ind(\sqrt{1+\sqrt{3}}, \mathbb{Q}) = x^4 - 2x^2 - 2$$

dir. $\mathbb{Q}$ üzerinde $\sqrt{1+\sqrt{3}}$'ün derecesi 4 tür (Fraleigh 2003).

Tanım 1.7.11 $\mathbb{F}$ bir cisim ve E, $\mathbb{F}$'nin bir cisim genişlemesi olsun. Ayrıca $S \subseteq E$ olsun. $\mathbb{F} \cup S$ tarafından üretilen altcisme $\mathbb{F}$'ye S'nin *katılmasıyla elde edilen altcisim*

denir ve $\mathbb{F}(S)$ ile gösterilir. Eğer $S = \{s_1, s_2, \cdots, s_n\}$ n elemanlı bir sonlu küme ise $\mathbb{F}(\{s_1, s_2 \cdots, s_n\}) = \mathbb{F}(s_1, s_2, \cdots, s_n)$ ile gösterilir. Eğer $n = 1$ ve $s_1 = s$ ise $\mathbb{F}(s)$'ye $\mathbb{F}$'ye s'nin *katılmasıyla elde edilen altcisim* denir. Ayrıca $\mathbb{F}(s)$'ye $\mathbb{F}$'nin bir *basit cisim genişlemesi* denir (Asar ve ark. 2012).

Tanım 1.7.12 $\mathbb{F}$ bir cisim ve E, $\mathbb{F}$'nin bir cisim genişlemesi olsun. O halde E'nin $\mathbb{F}$-uzayı olarak boyutuna *E'nin F üzerindeki derecesi* denir ve $[E : \mathbb{F}]$ ile gösterilir. $[E : \mathbb{F}]$'nin sonlu ya da sonsuz olmasına göre E'ye $\mathbb{F}$'nin bir *sonlu cisim genişlemesi* ya da *sonsuz cisim genişlemesi* denir (Asar ve ark. 2012).

Örnek 1.7.13 $\mathbb{R}$, $\mathbb{Q}$'nun bir sonsuz cisim genişlemesi, $\mathbb{C}$, $\mathbb{R}$'nin sonlu bir cisim genişlemesidir. $\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}\}$ ve $\{1, i\}$, $\mathbb{C}$ üzerinde lineer bağımsız olduğundan $[\mathbb{C} : \mathbb{R}] = 2$ dir. Öte yandan e sayısı hiçbir $g(x) \in \mathbb{Q}[x]$ polinomunun kökü değildir. Dolayısıyla $\{e^i \mid i \geq 0\}$ sonsuz kümesi $\mathbb{Q}$ üzerinde lineer bağımsızdır ve $[\mathbb{R} : \mathbb{Q}]$ sonsuzdur (Asar ve ark. 2012).

1.7.1 Cebirsel Genişleme

Tanım 1.7.14 E, $\mathbb{F}$'nin bir cisim genişlemesi olsun. Eğer E'nin her elemanı $\mathbb{F}$ üzerinde cebirsel ise E'ye $\mathbb{F}$'nin bir *cebirsel genişlemesi* denir (Asar ve ark. 2012).

Örnek 1.7.15 $\mathbb{C}$, $\mathbb{R}$'nin bir cebirsel genişlemesidir. $a, b \in \mathbb{R}$ olmak üzere $z = a + ib$ olsun.

$$g(x) = (x - z)(x - \bar{z}) = x^2 - 2ax + (a^2 + b^2) \in \mathbb{R}[x]$$

ve $g(z) = 0$ olduğundan $z, \mathbb{R}$ üzerinde cebirseldir (Asar ve ark. 2012).

Teorem 1.7.16 Her sonlu cisim genişlemesi bir cebirsel genişlemedir (Asar ve ark. 2012).

Teorem 1.7.17 $\mathbb{F} \leq E \leq K$ cisim kulesi verilsin. Eğer E, $\mathbb{F}$'nin ve K, E'nin sonlu genişlemeleri ise o zaman K, $\mathbb{F}$'nin sonlu bir cisim genişlemesidir ve

$$[K : \mathbb{F}] = [K : E] \cdot [E : \mathbb{F}]$$

dir (Asar ve ark. 2012).

Sonuç 1.7.18 $E,\ \mathbb{F}$ cisminin bir cisim genişlemesi ve $u \in E,\ \mathbb{F}$ üzerinde cebirsel olsun. Eğer $v \in \mathbb{F}(u)$ ise $v,\ \mathbb{F}$ üzerinde cebirseldir ve $der(v, \mathbb{F}) \mid der(u, \mathbb{F})$ dir (Asar ve ark. 2012).

Örnek 1.7.19 $\mathbb{F} = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ cisminin bir $\mathbb{Q}$ bazını ve $[\mathbb{F} : \mathbb{Q}]$ derecesini belirleyelim. Ayrıca $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ olduğunu gösterelim. $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3})$ olduğundan $\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}) \leq \mathbb{Q}(\sqrt{2})(\sqrt{3})$ cisim kulesi elde edilir. $ind(\sqrt{2}, \mathbb{Q}) = x^2 - 2$ olduğundan $\mathbb{Q}(\sqrt{2})$'nin bir $\mathbb{Q}$-bazı $\{1, \sqrt{2}\}$ dir. Şimdi $\sqrt{3}$'ün $\mathbb{Q}(\sqrt{2})$ üzerindeki indirgenmez polinomu $q(x)$ olsun. $\sqrt{3}$'ün $\mathbb{Q}$ üzerindeki indirgenmez polinomu $x^2 - 3$ olduğundan $q(x),\ x^2 - 3$'ü böler. Dolayısıyla ya $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$ ya da $q(x) = x^2 - 3$ tür. $3 \in \mathbb{Q}(\sqrt{2})$ olsun. O zaman $\sqrt{3} = a + b\sqrt{2}$ yazılabilir. Buradan $3 = a^2 + 2ab\sqrt{2} + 2b^2$ olduğundan $2ab\sqrt{2} = 3 - a^2 - 2b^2 \in \mathbb{Q}$ olur. Bunun için $2ab = 0$ olmalıdır. Eğer $a = 0$ ise $\dfrac{\sqrt{3}}{\sqrt{2}} = b \in \mathbb{Q}$ olur ki bu çelişkidir. Eğer $b = 0$ ise $\sqrt{3} = a \in \mathbb{Q}$ olur ki bu da çelişkidir. Dolayısıyla $\sqrt{3} = a \notin \mathbb{Q}(\sqrt{2})$ ve böylece $q(x) = x^2 - 3$ tür. O halde $\mathbb{F}$'nin bir $\mathbb{Q}(\sqrt{2})$ bazı $\{1, \sqrt{3}\}$ olduğundan Teorem 1.7.17'den dolayı, $\mathbb{F}$'nin bir $\mathbb{Q}$ bazı $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ dır. Dolayısıyla $[\mathbb{F} : \mathbb{Q}] = 4$ tür. $u = \sqrt{2} + \sqrt{3}$ olsun. O halde $4 = [\mathbb{F} : \mathbb{Q}] = [\mathbb{F} : \mathbb{Q}(u)][\mathbb{Q}(u) : \mathbb{Q}]$ dur. $der(u, \mathbb{Q}) = 4$ olduğundan $[\mathbb{Q}(u) : \mathbb{Q}] = 4$ tür. Bu değer yerine konulursa $[\mathbb{F} : \mathbb{Q}(u)] = 1$ ve buradan $\mathbb{F} = \mathbb{Q}(u)$ bulunur (Asar ve ark. 2012).

Teorem 1.7.20 $\mathbb{F}$ bir cisim, $E,\ \mathbb{F}$'nin bir cisim genişlemesi olsun. Aşağıdakiler denktir.

(i) $E,\ \mathbb{F}$'nin sonlu bir genişlemesidir.

(ii) $E = \mathbb{F}(u_1, u_2, \cdots, u_n)$ olacak şekilde $\mathbb{F}$ üzerinde cebirsel olan $u_1, u_2, \cdots, u_n$ elemanları vardır (Asar ve ark. 2012).

1.8 İkinci Mertebeden Tekrarlama Bağıntılı Diziler

Tanım 1.8.1 $k \geq 1$ bir tamsayı olsun. Bir $(u_n)_{n\geq 0} \subseteq \mathbb{C}$ dizisi, sabit $a_1, a_2, \cdots, a_k \in \mathbb{C}$ katsayıları ile her $n \geq 0$ için

$$u_{n+k} = a_1 u_{n+k-1} + a_2 u_{n+k-2} + \cdots + a_k u_k \tag{1.8.1}$$

şeklindeki bir tekrarlama bağıntısına sahipse bu diziye k. *mertebeden lineer tekrarlamalı dizi* denir (Luca 2009).

$a_k \neq 0$ olduğunu varsayalım. (Eğer $a_k = 0$ olursa $(u_n)_{n\geq 0}$ dizisi k'dan daha küçük lineer tekrarlamalı diziye karşılık gelir.) Eğer $a_1, a_2, \cdots, a_k \in \mathbb{Z}$ ve $u_0, u_1, \cdots, u_{k-1} \in \mathbb{Z}$ ise her $n \geq 0$ için tümevarım kullanılarak u_n nin bir tamsayı olduğu elde edilir.

$$f(X) = X^k - a_1 X^{k-1} - \cdots - a_k \in \mathbb{C}[X]$$

polinomu, $(u_n)_{n\geq 0}$ dizisinin *karakteristik polinomu* olarak adlandırılır. $\alpha_1, \alpha_2, \cdots, \alpha_s$ $f(X)$'in sırasıyla $\sigma_1, \sigma_2, \cdots, \sigma_s$ katlılıklarına sahip farklı kökleri olmak üzere

$$f(X) = \prod_{i=1}^{s} (X - \alpha_i)^{\sigma_i}$$

şeklinde yazılsın. Bu durumda aşağıdaki önerme verilebilir.

Önerme 1.8.2 Varsayalım ki $f(x) \in \mathbb{Z}[X]$ farklı köklere sahip olsun. O halde, $\forall n \geq 0$ için

$$u_n = \sum_{i=1}^{k} c_i \alpha_i^n \tag{1.8.2}$$

olacak şekilde $c_1, c_2, \cdots, c_k \in \mathbb{K} = \mathbb{Q}(\alpha_1, \alpha_2, \cdots, \alpha_k)$ sabitleri vardır (Luca 2009).

Eğer $k = 2$ ise, yani $(u_n)_{n\geq 0}$ ikinci dereceden bir tekrarlama bağıntısına sahip bir dizi ise

$$u_{n+2} = a_1 \cdot u_{n+1} + a_2 \cdot u_n \tag{1.8.3}$$

bağıntısı ile verilir. Bu durumda karakteristik polinom

$$f(X) = X^2 - a_1X - a_2 = (X - \alpha_1)(X - \alpha_2)$$

formundadır. $\alpha_1 \neq \alpha_2$ olsun. Önerme 1.8.2'den, $\forall n \geq 0$ için (1.8.3)'teki tekrarlama bağıntısı ile verilen $(u_n)_{n\geq 0}$ dizisinin Binet formülü

$$u_n = c_1\alpha_1^n + c_2\alpha_2^n \tag{1.8.4}$$

şeklindedir.

1.9 İkinci Mertebeden Tekrarlama Bağıntılı Dizi Örnekleri

1.9.1 Fibonacci ve Lucas Dizileri

Örnek 1.9.1 $\alpha_1 = \dfrac{1+\sqrt{5}}{2},\ \alpha_2 = \dfrac{1-\sqrt{5}}{2}$ olmak üzere $(F_n)_{n\geq 0}$ Fibonacci dizisi $F_0 = 0,\ F_1 = 1$ iken $F_{n+2} = F_{n+1} + F_n$ ($\forall n \geq 0$ için) formülü ile verilir.

Fibonacci dizisine karşılık gelen karakteristik polinom

$$f(x) = X^2 - X - 1 = (X - \alpha)(X - \beta)$$

ile, bu dizinin terimlerini üretecek bağıntı, yani Binet formülü

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$

ile verilir.

Örnek 1.9.2 $\alpha_1 = \dfrac{1+\sqrt{5}}{2},\ \alpha_2 = \dfrac{1-\sqrt{5}}{2}$ olmak üzere$(L_n)_{n\geq 0}$ Lucas dizisi, $L_0 = 2,\ L_1 = 1$ iken $L_{n+2} = L_{n+1} + L_n$ ($\forall n \geq 0$ için) formülü ile verilir.

Fibonacci dizisi ile aynı karakteristik polinoma sahiptir. Bu dizi için Binet formülü

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

ile verilir.

1.9.2 Lucas Dizileri

Tanım 1.9.3 α_1, α_2 aralarında asal olsun. $u_0 = 0, u_1 = 1$ olmak üzere (1.8.3)'teki tekrarlama bağıntısı ve (1.8.4)'teki Binet formülü ile ifade edilen ikinci mertebeden tekrarlama bağıntılı dizi bir Lucas dizisi olarak adlandırılır (Luca 2009).

α_1, α_2 karakteristik polinomun kökleri iken Tanım 1.9.3'de ifade edilen şartlar altında (1.8.4)'teki formüle sahip olan bir Lucas dizisi her $n \geq 0$ için,

$$u_n = \frac{\alpha_1^n - \alpha_2^n}{\alpha_1 - \alpha_2} \tag{1.9.1}$$

formunda yazılabilir. ((1.9.1)'de ifade edilen dizi *genelleştirilmiş Fibonacci dizisi* olarak da adlandırılmaktadır.)

Şimdi genel terimi (1.9.1)'deki bağıntı ile ifade edilen bir $(u_n)_{n\geq 0}$ Lucas dizisine benzer bir dizi tanımlayalım. $v_0 = 2, v_1 = a_1$ başlangıç değerleri ile aynı karakteristik polinoma ve (1.8.4)'teki formüle sahip bir $(v_n)_{n\geq 0}$ dizisi

$$v_n = \alpha_1^n + \alpha_2^n \quad (\forall n \geq 0 \text{ için}) \tag{1.9.2}$$

genel terimi ile verilir. ((1.9.2)'de ifade edilen dizi *genelleştirilmiş Lucas dizisi* olarak da adlandırılmaktadır.)

1.9.3 Lucas Dizisinin Terimlerinin Asal Çarpanları

Bu bölümde $(u_n)_{n\geq 0}$, (1.9.1)'deki bağıntı ile ifade edilen bir Lucas dizisidir. Şimdi verilecek teorem Lucas dizilerinin en önemli bölünebilme özelliklerini ifade eder.

Teorem 1.9.4 p bir asal sayı ve $\Delta = (\alpha_1 - \alpha_2)^2$ olsun. $(u_n)_{n\geq 0}$ Lucas dizisi için aşağıdaki özellikler gerçeklenir:

(i) $\forall n \geq 1$ için $p \mid a_2$ ise $p \nmid u_n$,

(ii) $p \mid \Delta$ ise $p \mid u_p$,

(iii) $p \mid \Delta a_2$ ve $\left(\frac{\Delta}{p}\right) = 1$ ise $p \mid u_{p-1}$,

(iv) p, (i)-(iii) şartlarını sağlamayan tek asal ise $p \mid u_{p+1}$ dir (Luca 2009).

Örnek 1.9.5 $(F_n)_{n\geq 0}$ için $\Delta = (\alpha - \beta)^2 = 5$ tir. $p = 13$ ise $\left(\frac{5}{13}\right) = -1$ olduğundan $13 \mid F_{14}$ tür. Yani $F_{14} = 377 = 13.29$ dur.

α_1, α_2 cebirsel tamsayılar olsun. $\alpha_1 + \alpha_2$ ve $\alpha_1 \cdot \alpha_2$ sıfırdan farklı aralarında asal tamsayılar ve $\frac{\alpha_1}{\alpha_2}$ birimin kökü değilse, (α_1, α_2) bir Lucas çifti olarak adlandırılır. Bir (α_1, α_2) Lucas çifti verilirse, (1.9.1)'deki bağıntıyla $u_n = u_n(\alpha_1, \alpha_2)$ Lucas sayı dizisi tanımlanır. Şimdi Lucas dizilerinin asal çarpanları ile ilgili önemli bir tanımı ifade edelim.

Tanım 1.9.6 (α_1, α_2) bir Lucas çifti olsun. Bir p asal sayısı için $p \mid u_n$ ancak $p \nmid (\alpha_1 - \alpha_2)^2 u_1 u_2 \cdots u_{n-1}$ ise p'ye $u_n(\alpha_1, \alpha_2)$ Lucas sayısının bir *ilkel böleni* denir. Eğer u_n'nin ilkel böleni yoksa bu diziye *n-kusurlu (defective)* veya *ilkel bölensiz Lucas dizisi* denir (Luca 2009).

Örnek 1.9.7 Fibonacci dizisinin ilk 20 terimi $1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584, 4181, 6765$ tir. $F_1 = F_2 = 1$, $F_5 = 5$ (ve $(\alpha - \beta)^2 = 5$), $F_6 = 2^3$ (ve $2 \mid F_3$), $F_{12} = 144 = 2^4 3^2$ (ve $2 \mid F_3,\ 3 \mid F_4$) ve yukarıdaki listede kalan diğer tüm terimler ilkel bölene sahiptirler.

Teorem 1.9.8 (İlkel Bölen Teoremi) $n \notin \{1, 2, 3, 4, 6\}$ olsun. $((\alpha_1, \alpha_2), n)$ ikilisi $(\pm((a_1 + \sqrt{\Delta})/2, (a_1 - \sqrt{\Delta})/2), n)$ formunda iken Çizelge 2.1'de (a_1, a_2, n) üçlüleri için verilmiş olan listedeki değerler haricinde u_n dizisi daima bir ilkel bölene sahiptir (Voutier 1995).

n	(a_1, Δ)
5	$(1,5),(1,-7),(2,-40),(1,-11),(1,-15),(12,-76),(12,-1364)$
7	$(1,-7),(1,-19)$
8	$(2,-24),(1,-7)$
10	$(2,-8),(5,-3)$
12	$(1,5),(1,-7),(1,-11),(2,-56),(1,-15),(1,-19)$
13	$(1,-7)$
18	$(1,-7)$
30	$(1,-7)$

Çizelge 2.1 İlkel Bölensiz (n-kusurlu) Lucas çiftleri

İlkel bölenlerle ilgili diğer önemli bir sonuç da aşağıda verilir:

Yardımcı Teorem 1.9.9 Herhangi $n > 30$ tamsayısı için n-kusurlu Lucas çifti yoktur. Başka bir ifade ile $n > 30$ için bir Lucas dizisinin $n.$ elemanının daima bir ilkel böleni vardır (Bilu ve ark. 2001).

1844'te E. Catalan

$$x^m - y^n = 1, \quad m \geq 2,\ n \geq 2 \tag{1.9.3}$$

denkleminin pozitif tamsayılardaki tek çözümünün $3^2 - 2^3 = 1$ olduğunu iddia etmişti (Catalan 1844). Bu sanı 2002'de Mihăilescu tarafından ispatlandı (Mihăilescu 2004). İlk olarak m ve n'nin asal olduğunu varsaymalıyız. Çünkü (x, y, m, n) bir çözüm ve p, q, $p \mid m$ ve $q \mid n$ olacak şekilde asallar ise $(x^{m/p}, y^{n/q}, p, q)$ da bir çözümdür. Dahası m ve n farklı asallardır. Çünkü $m = n$ ise

$$1 = x^m - y^m = (x-y)(x^{m-1} + \cdots + y^{m-1}) > x - y > 0,$$

olur ki bu da imkansızdır.

Şimdi 1850'de Lebesgue tarafından çözülen bir denklemi ele alalım ve bu denkleme Lucas dizilerinin ilkel bölen teoreminin nasıl uygulandığını görelim.

Önerme 1.9.10 (1.9.3) denkleminin $n = 2$ iken çözümü yoktur (Lebesgue 1850).

İspat. Varsayalım ki

$$x^m = y^2 + 1 \tag{1.9.4}$$

Diophant denkleminin bir çözümü olsun. y tek olsaydı $y^2 + 1 \equiv 2 \pmod 4$ olur. Bu $x^m \equiv 2 \pmod 4$ olmasını gerektirir. $m \geq 2$ olduğundan bu olamaz. O halde y çifttir. $\mathbb{Z}[i]$ tek türlü çarpanlara ayırma bölgesidir ve eşitliğin sağ tarafı $\mathbb{Z}[i]$'de çarpanlara ayrıldığında $(y+i)(y-i) = x^m$ şeklinde olur. $(y+i)$ ve $(y-i)$, $\mathbb{Z}[i]$'de aralarında asaldır. Öyle ki q, $(y+i)$ ve $(y-i)$ çarpanlarının ikisini de bölen bir asal olsun. O halde $q \mid (y+i)-(y-i)$ yani $q \mid 2i$ ve böylece $q \mid 2$ ve $q \mid x^m$ dir. x tek olduğundan bu bir çelişkidir. Böylece $(y + i)$ ve $(y - i)$ aralarında asal ve onların çarpımları x^m dir. ζ, $\mathbb{Z}[i]$'de birimsel eleman iken $y + i = \zeta\alpha_1^m,\ y - i = \zeta\alpha_2^m$ olacak şekilde $\alpha_1 = a + bi,\ \alpha_2 = a - bi \in \mathbb{Z}[i]$ vardır. Üstelik $x = a^2 + b^2$ dir. $\mathbb{Z}[i]$'nin birimselleri sadece 4'ü bölen sonlu mertebeli ± 1 ve $\pm i$ dir. m tek olduğundan α_1 bağdaşık olduğu sayılardan biri ile değiştirilebilir (örneğin; $\zeta^m\alpha_1$ ile) ve böylece $\zeta\alpha_1^m = \zeta^{m^2}\alpha_1^m = (\zeta^m\alpha_1)^m$ elde edilir. Buradan

$$y + i = \alpha_1^m$$

çıkarımının elde edilebilmesi için $\zeta = 1$ alınır. Yukarıdaki eşitlikten eşleniği çıkarılırsa

$$\alpha_2 = \overline{\alpha_1} \text{ iken}, \quad 2i = \alpha_1^m - \alpha_2^m$$

bulunur. $\alpha_1 - \alpha_2 = 2bi$, $2i$'yi böldüğünden $b = \pm 1$ ve

$$\pm 1 = \frac{\alpha_1^m - \alpha_2^m}{\alpha_1 - \alpha_2} \tag{1.9.5}$$

dir. α_1 ve α_2 yer değiştirebildiğinden $b = 1$ varsayabiliriz. Yukarıdaki eşitliğin sağ tarafı bir Lucas dizisinin $m.$ terimidir. Ayrıca $a_1 = \alpha_1 + \alpha_2 = 2a$ ve $a_2 = -(\alpha_1\alpha_2) = -(a^2 + 1) = -x$ olur ki burada a_2 tektir. Böylece a_1, a_2 aralarında asaldır. Şimdi α_1/α_2'nin

birimin kökü olmadığını gösterelim. Eğer α_1/α_2 birimin kökü ise $\alpha_1/\alpha_2 = \pm 1$ veya $\pm i \in \mathbb{Q}[i]$ dir. $\alpha_1/\alpha_2 = \pm 1$ ise ya $a+i = a-i$ dir ki bu yanlıştır, ya da $a+i = -a+i$ dir. Buradan $a = 0$ dır. Bu durumda $x = 1$ elde edilir ki bu da yanlıştır. $\alpha_1/\alpha_2 = \pm i$ ise, ya $a+i = ai+1$ ya da $a+i = -ai-1$ dir. Buradan sırasıyla $a = 1$ ya da $a = -1$ bulunur. İki durumda da $x = 2$ dir, bu da x'in tekliği ile çelişir. O halde (1.9.5) denkleminin sağ tarafının bir Lucas dizisinin $m.$ terimi olduğunu doğruladık. Ayrıca Tanım 1.9.6'ya göre bu dizinin ilkel böleni yoktur. Teorem 1.9.8'deki tabloya göre ya $m \in \{2, 3, 4, 6\}$ dır ya da $((\alpha_1, \alpha_2), m)$ üçlülerini göz önüne alalım. Tablodaki $((\alpha_1, \alpha_2), m)$ ikililerinden hiçbirisi (1.9.5)'e çözüm getirmez. O halde $m = 3$ olmalıdır. Buradan

$$\pm 1 = \frac{(a+i)^3 - (a-i)^3}{2i} = (a+i)^2 + (a+i)(a-i) + (a-i)^2 = 3a^2 - 1$$

elde edilir. Böylece $3a^2 \in \{0, 2\}$ dir. Bu da (1.9.4) denklemine herhangi bir çözüm vermez. ■

1.10 Baker'in Teorisi

1.10.1 Bir Cebirsel Sayının Büyüklüğü ve Mutlak Logaritmik Büyüklüğü

α bir cebirsel sayı ve α'nın minimal polinomu $a_0, a_1, \cdots, a_d \in \mathbb{Z}$, $a_0 > 0$ ve $(a_0, a_1, \cdots, a_d) = 1$ olmak üzere

$$P(x) = a_0 x^d + a_1 x^{d-1} + \cdots + a_1$$

ile verilsin.

$$H(\alpha) = \text{maks}(|a_0|, |a_1|, \cdots, |a_d|)$$

ve

$$der(\alpha) = d$$

şeklinde yazılsın. $H(\alpha)$'ya *α'nın büyüklüğü (height)* ve $der(\alpha)$'ya da *α'nın derecesi* denir. $\alpha \neq 0$ ve

$$H(\alpha) \leq m^d H(m\alpha) \quad (0 < m \in \mathbb{Z})$$

ise $H(\alpha) = H(1/\alpha)$, $der(\alpha) = der(1/\alpha)$ dır.

Teorem 1.10.1 α cebirsel sayı olsun. $v\alpha$ bir cebirsel tamsayı olacak şekilde en küçük $v = v(\alpha)$ pozitif tamsayı vardır (Alaca ve Williams 2004).

Yukarıdaki teoremde ifade edilen v tamsayısına α'nın *paydası* denir. $a_0\alpha$'nın bir cebirsel tamsayı olduğu da açıktır. O halde α'nın paydası için aşağıdaki eşitsizlik gerçeklenir:

$$v(\alpha) \leq a_0 \leq H(\alpha).$$

α'nın tüm eşlenikleri $\alpha = \alpha_1, \cdots \alpha_d$ ile gösterilsin.

$$|\overline{\alpha}| = \text{maks}_{1 \leq i \leq d} |\alpha_i|$$

olsun. α, β cebirsel sayıları için

$$|\overline{\alpha + \beta}| \leq |\overline{\alpha}| + |\overline{\beta}|, \quad |\overline{\alpha\beta}| \leq |\overline{\alpha}||\overline{\beta}|$$

eşitsizlikleri sağlanır. Eğer $\alpha \neq 0$ ise,

$$|v\alpha_1 \cdots v\alpha_d| \geq 1 \tag{1.10.1}$$

dir. Ayrıca

$$|v\alpha_1 \cdots v\alpha_d| \leq v^d |\alpha| |\overline{\alpha}|^{d-1} \tag{1.10.2}$$

dir. (1.10.1) ve (1.10.2) birleştirilerek

$$|\alpha| \geq v^{-d} |\overline{\alpha}|^{-d+1} \tag{1.10.3}$$

elde edilir.

(1.10.3) eşitsizliğini elde etmek için bu argüman Liouville tarafından, rasyonel sayılarla cebirsel sayıların yaklaşımları üzerine iyi bilinen bir eşitsizliği ispatlamak için kullanılmıştır (Liouville 1844). Bu argüman *Liouville tipi argüman* olarak bilinir.

Şimdi de α'nın büyüklüğü ve derecesi ile ilgili bazı önemli teorem ve sonuçlar verelim:

Yardımcı Teorem 1.10.2 α bir cebirsel sayı olsun. O halde

$$|\overline{\alpha}| \leq der(\alpha)H(\alpha)$$

dır (Shorey ve Tijdeman 1986).

Sonuç 1.10.3 α, sıfırdan farklı bir cebirsel sayı olsun. O halde

$$|\alpha| \geq (der(\alpha)H(\alpha))^{-1}$$

dir (Shorey ve Tijdeman 1986).

Yardımcı Teorem 1.10.4 δ sıfırdan farklı bir cebirsel sayı olsun.

$$H(\delta) \leq (2|\bar{\delta}|)^{der(\delta)}$$

dır (Shorey ve Tijdeman 1986).

Sonuç 1.10.5 $v \geq 0$ ve $d \geq 1$ olarak verilsin. $|\bar{\delta}| \leq v$ ve $der(\delta) \leq d$ olacak şekilde bir δ cebirsel sayısı, hesaplanabilir bir sonlu kümeye aittir (Shorey ve Tijdeman 1986).

Eğer β ve γ sabit derecelere sahip cebirsel sayılar ise, maks$(H(\beta), H(\gamma))$'ya göre $H(\beta+\gamma)$ ve $H(\beta\gamma)$ için sınırlar aşağıdaki lemmalar ile verilir.

Yardımcı Teorem 1.10.6 β ve γ, dereceleri en fazla d olan ve büyüklükleri $H(\geq 2)$ yi aşmayan cebirsel sayılar olsun. O halde

$$(a)\ \frac{\log H(\beta+\gamma)}{\log H} \leq C_1, \quad (b)\ \frac{\log H(\beta\gamma)}{\log H} \leq C_2$$

dir (Shorey ve Tijdeman 1986).

Yardımcı Teorem 1.10.7 $H \geq 2$ iken $der(\beta) \leq d$ ve $H(\beta) \leq H$ olacak şekilde β bir cebirsel sayı olsun. $\gamma^2 = \beta$ olacak şekilde bir $\gamma \in \mathbb{C}$ alınsın. Bu durumda sadece d'ye bağlı hesaplanabilir bir C_3 sayısı için

$$\log H(\gamma) \leq C_3 \log H$$

eşitsizliği sağlanır (Shorey ve Tijdeman 1986).

Tanım 1.10.8 (Mutlak Logaritmik Büyüklük) $\beta, \mathbb{Q}$ üzerinde derecesi n ve $\mathbb{Z}$ üzerinde $a_0\Sigma_{i=1}^{n}(X-\beta^i)$ minimal polinomuna sahip sıfırdan farklı herhangi bir cebirsel sayı olsun. $(\beta)_{1\leq i\leq n}^{(i)}$, β'nın eşlenikleri iken, β cebirsel sayısının *mutlak logaritmik büyüklüğü*

$$h(\beta) = \frac{1}{n}(\log|a_0| + \Sigma_{i=1}^{n} \log \text{maks}\{1, |\beta^{(i)}|\})$$

ile tanımlanır.

Örnek 1.10.9 (1) $h(p/q) = \log \text{maks}(|p|, |q|)$ $(p, q \in \mathbb{Q})$ dir.
(2) $x > 0$ için $\log^+ x = \text{maks}\{0, \log x\}$ iken $h(\sqrt{2}) = \frac{1}{2}\log^+|\sqrt{2}| + \log^+|-\sqrt{2}| = \frac{1}{2}$ dir.
(3) (2)'dekinin daha genelini düşünürsek $h(2^{1/n}) = (\log 2)/n$ dir.
(4) ζ birimin bir kökü iken $h(\zeta) = 0$ dır.
(5) $p = \frac{\pm\sqrt{14} \pm i\sqrt{2}}{4}, 2x^4 - 3x^2 + 2$ polinomunun bir kökü olsun. $|p| = 1$ olduğundan, $h(p) = \frac{\log 2}{4} = 0,173...$ tür.

1.10.2 Logaritmalarda Lineer Formlar ve Baker'in Teorisi

Tanım 1.10.10 $\alpha_1, \alpha_2, \cdots, \alpha_n$ sıfırdan farklı cebirsel sayılar ve $\log \alpha_1, \log \alpha_2, \cdots, \log \alpha_n$ de bu cebirsel sayıların logaritmaları ve $b_1, b_2, \cdots, b_n$ rasyonel tamsayılar olsun.

$$\lambda = b_1 \log \alpha_1 + b_2 \log \alpha_2 + \cdots + b_n \log \alpha_n \tag{1.10.4}$$

ifadesine bir λ *lineer formu* denir.

Eğer $\log \alpha_1$ ve $\log \alpha_2$, $\mathbb{Q}$'da lineer bağımsız ise cebirsel sayılar üzerinde de lineer bağımsızdır. Bu problem Hilbert'in 7. problemidir ve birbirinden bağımsız olarak yaptıkları çalışmalar ile 1934'te Gel'fond ve Schneider tarafından çözülmüştür (Gel'fond 1934, Schneider 1934). Ayrıca Baker tarafından da $\mathbb{Q}$ üzerinde lineer bağımsız olan $\log \alpha_1$, $\log \alpha_2, \cdots, \log \alpha_n$ sayılarının cebirsel sayılar üzerinde de lineer bağımsız olduğu ispatlanmıştır (Baker 1966). Sonrasında bu teoremin önemli genellemeleri de elde edilmiştir. Baker, (1.10.4)'teki logaritmaların lineer formları için kesin alt sınırlar bulmaya olanak sağlayacak önemli bir teorinin kurucusu olmuştur (Baker 1967a, b). Diophant denklemlerin modern teorisine ciddi katkı sağlayan bu teoriyle Baker, örneğin $f(x) \in \mathbb{Z}[x]$ en az üç farklı köke sahip bir polinom olmak üzere $f(x) = y^q$ $(q \geq 2)$ tipindeki bir Diophant denklemindeki bilinmeyenler için verimli üst sınırlar bulunmasına ve dolayısıyla bu denklemin çözülmesine olanak sağlamıştır.

Baker, logaritmalarda lineer formlar teorisi ile ilgili yaptığı çalışmaların bir derlemesini alan inceleme çalışması (survey) olarak 1977 yılında yayınlamıştır (Baker 1977).

Şimdi Baker'in teorisinin en temel sonuçlarından birini vermek için gerekli hazırlıkları yapalım.

Tanım 1.10.11 $n \geq 1$ ve $z_1, z_2, \cdots, z_n \in \mathbb{C}^*$ olsun. Eğer

$$z_1^{k_1} z_2^{k_2} \cdots z_n^{k_n} = 1$$

olacak şekilde sıfırdan farklı tamsayı bileşenli n-boyutlu $(k_1, k_2, \cdots, k_n) \in \mathbb{Z}^n$ varsa

$z_1, z_2, \cdots, z_n$ sayıları *çarpımsal bağımlı* olarak adlandırılır. Aksi takdirde (yani böyle bir sıfırdan farklı $(k_1, k_2, \cdots, k_n) \in \mathbb{Z}^n$ yoksa) $z_1, z_2, \cdots, z_n$ sayıları *çarpımsal bağımsız* olarak adlandırılır.

$C_1, C_2, \cdots, C_n$ pozitif reel sayılar olarak göz önüne alınsın. $\alpha_1, \alpha_2, \cdots, \alpha_n$, büyüklükleri $A_1, A_2, \cdots, A_n$ sayılarından küçük sıfırdan farklı cebirsel tamsayılar olsun. $1 \leq j \leq n$ için $A_j \geq 3$ olduğunu varsayalım.

$$A' = \text{maks}_{1 \leq j < n} A_j, \quad A = A_n,$$

$$\Omega = \Pi_{j=1}^{n} \log A_j, \quad \Omega' = \Pi_{j=1}^{n-1} \log A_j,$$

$$K = \mathbb{Q}(\alpha_1, \cdots, \alpha_n), \quad [K : \mathbb{Q}] = d$$

olsun. Bu durumda Baker'in önemli bir teoremini ifade edebiliriz.

Teorem 1.10.12 $b_1, b_2, \cdots, b_n$ rasyonel tamsayılarının mutlak değerleri $B(\geq 2)$ sayısından büyük olmasın.

$$0 < |b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n| < exp(-(C_1 nd)^{C_2 n}) \Omega \log \Omega' \log B$$

eşitsizliğinin rasyonel tamsayılarda çözümü olmayacak şekilde hesaplanabilir C_1 ve C_2 mutlak sabitleri bulunabilir (Baker 1977).

Tezin 2. bölümünde göz önüne alınacak başlık denklemin çözümü için Baker'in teoreminin (Teorem 1.10.12) faydalı bir versiyonu 2008'de Laurent tarafından verilmiştir. Şimdi bu teoremi ifade edelim:

Teorem 1.10.13 $\rho > 1$ ve $1/3 \leq \mu \leq 1$ olacak şekilde a_1, a_2, h, ρ ve μ reel sayılar olsun.

$$\sigma = \frac{1 + 2\mu - \mu^2}{2}, \quad \lambda = \sigma \log \rho, \quad H = \frac{h}{\lambda} + \frac{1}{\sigma},$$

$$w = 2\Big(1 + \sqrt{1 + \frac{1}{4H^2}}\Big), \quad \theta = \sqrt{1 + \frac{1}{4H^2}} + \frac{1}{2H}$$

alınsın. b_1 ve b_2 pozitif tamsayılar iken $\lambda = b_2 \log \alpha_2 - b_1 \log \alpha_1$ lineer formunu göz önüne alalım. α_1 ve α_2'nin çarpımsal olarak bağımsız olduğunu varsayalım. $D = [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}]/[\mathbb{R}(\alpha_1, \alpha_2) : \mathbb{R}]$ ve

$$h \geq \text{maks}\{D\Big(\log\Big(\frac{b_1}{a_2} + \frac{b_2}{a_1}\Big) + \log\lambda + 1.75\Big) + 0.06, \lambda, \frac{D\log 2}{2}\},$$

$$a_i \geq \text{maks}\{1, \rho|\log\alpha_i| - \log|\alpha_i| + 2Dh(\alpha_i)\} \quad (i = 1, 2),$$

$$a_1 a_2 \geq \lambda^2$$

olduğunu varsayalım. O halde

$$C = \frac{\mu}{\lambda^3\sigma}\Big(\frac{w}{6} + \frac{1}{2}\sqrt{\frac{w^2}{9} + \frac{8\lambda w^{5/4}\theta^{1/4}}{3\sqrt{a_1 a_2}H^{1/2}} + \frac{4}{3}\Big(\frac{1}{a_1} + \frac{1}{a_2}\Big)\frac{\lambda w}{H}}\Big)^2,$$

$$C' = \sqrt{\frac{C\sigma w\theta}{\lambda^3\mu}}$$

ile birlikte

$$\log|\lambda| \geq -C\Big(h + \frac{\lambda}{\sigma}\Big)^2 a_1 a_2 - \sqrt{w\theta}\Big(h + \frac{\lambda}{\sigma}\Big) - \log\Big(C'\Big(h + \frac{\lambda}{\sigma}\Big)^2 a_1 a_2\Big)$$

dir (Laurent 2008).

Varsayalım ki $A_1 \geq 1$ ve $A_2 \geq 1$ reel sayıları, $\mathbb{Q}(\alpha_1, \alpha_2)$ sayı cisminin derecesi D iken

$$\log A_i \geq \text{maks}\{h(\alpha_i), \frac{|\log\alpha_i|}{D}, \frac{1}{D}\} \quad (i = 1, 2)$$

şeklinde tanımlansın ve

$$b' = \frac{b_1}{D\log A_2} + \frac{b_2}{D\log A_1} \tag{1.10.5}$$

olsun.

$m = 10, 12, \cdots, 30$ için aşağıdaki çizelge ile $C_1 = C_1(m)$ ve $C_2 = C_2(m)$ katsayıları

tanımlanır.

m	10	12	14	16	18	20	22	24	26	28	30
C_1	32.3	29.9	28.2	26.9	26.0	25.2	24.5	24.0	23.5	23.1	22.8
C_2	25.2	23.4	22.1	21.1	20.3	19.7	19.2	18.8	18.4	18.1	17.9

Çizelge 2.2 ($m, C_1(m)$) ve ($m, C_2(m)$) Çiftleri

Sonuç 1.10.14 $\alpha_1, \alpha_2, \log \alpha_1, \log \alpha_2$ reel ve pozitif tamsayılar olsun. Bu durumda tablodaki her bir $(m, C_2(m))$ çifti için

$$\log |\lambda| \geq -C_2 D^4 (\text{maks}\{\log b' + 0.38, m/D, 1\})^2 \log A_1 \log A_2$$

dir (Laurent 2008).

Bu tezdeki 2. ve 3. bölümde Sonuç 1.10.14 kullanılırken $m = 10$ ve $C_2 = 25.2$ seçilmiştir.

2. TERAI SANISI HAKKINDA BİR DIOPHANT DENKLEM

2.1 $((\mathbf{c}+\mathbf{1})\mathbf{m^2}+\mathbf{1})^{\mathbf{x}}+(\mathbf{cm^2}-\mathbf{1})^{\mathbf{y}}=(\mathbf{am})^{\mathbf{z}}$ Diophant Denklemi

Bu bölüm, başlık denklemi hakkında orijinal sonuçlar içermektedir. Burada

$$((c+1)m^2+1)^x+(cm^2-1)^y=(am)^z$$

Diophant denkleminin pozitif tamsayı çözümleri ile ilgileneceğiz.

2.1.1 Giriş

a, b ve c aralarında asal ve 1'den büyük tamsayılar olsun. x, y ve z pozitif tamsayılar olmak üzere

$$a^x+b^y=c^z \tag{2.1.1}$$

üstel Diophant denkleminin sonlu çoklukta tamsayı çözümüne sahip olduğu 1933'te Mahler tarafından gösterildi. Mahler ispatında Thue-Siegel metodunun farklı bir versiyonunu kullandı (Mahler 1933). Ancak Mahler'in metodu denklemin mümkün olan çözümlerinin sayısı için bir üst sınır vermediğinden kullanışlı değildi. 7 yıl sonra (2.1.1) denkleminin çözümleri için faydalı sonuçlar Gel'fond tarafından verildi (Gelfond 1940). Gel'fond cebirsel sayıların logaritmalarında lineer formlar için alt sınır bulmaya dayalı olan Baker'in teorisinin ilkel bir halini kullanarak Mahler'in sonucunu ispatladı.

Sayılar teorisindeki "kongrüanslar ve Jacobi sembolü" gibi metotlar, cebirsel sayılar teorisinde "ikinci ve üçüncü dereceden sayı cisimlerindeki idealleri içeren bölünebilme argümanları" kullanılarak $a,b,c\leq 17$ farklı sabit asallar iken (2.1.1) denkleminin tüm çözümleri bazı yazarlar tarafından bulundu (Nagell 1958, Hadano 1976, Uchiyama 1976).

Yaklaşık 15 yıl sonra Jeśmanowicz bu denklem hakkında şu iddiada bulundu:

Sanı 2.1.1 a,b ve c pozitif tamsayıları $a^2+b^2=c^2$ bağıntısını sağlamak şartıyla (2.1.1) denklemi sadece $(x,y,z)=(2,2,2)$ çözümüne sahiptir (Jeśmanowicz 1956).

Sanının doğru olduğu birçok durumda ispatlandı. Ancak henüz tamamen ispatlanmadı. Yaklaşık 60 yıllık "Jeśmanowicz sanısı" ile ilgili 100'e yakın çalışmayı özetleyen bir "survey" çalışması Soydan, Demirci, Cangül ve Togbé tarafından yayınlandı (Soydan ve ark. 2017).

Jeśmanowicz sanısının daha geneli bir sanı 1994'te Terai tarafından şu şekilde verildi:

Sanı 2.1.2 (I. Terai Sanısı) a, b, c, p, q, r pozitif sabit tamsayıları $p, q, r \geq 2$ iken $a^p + b^q = c^r$ şartını sağlayacak şekilde ise (2.1.1) denkleminin tek pozitif tamsayı çözümü $(x, y, z) = (p, q, r)$ dir (Terai 1994).

1999'da Cao, Terai'nin I. Sanısının yanlış olduğunu farketti ve şu örneği verdi: Örneğin, 1958'de Nagel $3^x + 2^y = 5^z$ denkleminin $(x, y, z) = (1, 1, 1), (2, 4, 2)$ olacak şekilde iki çözümü olduğunu ve $7^x + 2^y = 3^z$ denkleminin de $(x, y, z) = (1, 1, 2), (2, 5, 4)$ olacak şekilde iki çözümü olduğunu ispatlamıştır. Dolayısıyla Terai'nin I. sanısı yanlıştır. Ayrıca $a = 1$ veya $b = 1$ ise de sanı yanlıştır (örneğin $1^1 + 1^1 = 2^1$, $p = q = r = 1$). Cao, (2.1.1) denklemi hakkında aşağıdaki sonucu verdi.

Teorem 2.1.3 Eğer maks$\{a, b, c\} > 13$ ise, (2.1.1) denkleminin $z > 1$ iken en fazla bir (x, y, z) tamsayı çözümü vardır (Cao 1999).

Terai 1994'teki sanısını destekleyici iki çalışma yaptı. 1999'da ise, 1994'teki sanısını şöyle uyarladı:

Sanı 2.1.4 (II. Terai Sanısı) $(a, b) = 1$ ve a, b, c, p, q, r pozitif sabit tamsayıları $p, q, r \geq 2$ iken $a^p + b^q = c^r$ şartını sağlayacak şekilde ise (2.1.1) denkleminin $a < b$ olmak üzere $(a, b, c) = (2, 3, 5)$ ve $(x, y, z) = (1, 1, 1)$,$(4, 2, 2)$; (a, b, c)= $(2, 7, 3)$ ve $(x, y, z) = (1, 1, 2)$,$(5, 2, 4)$; $(a, b, c) = (1, 2, 3)$ ve (x, y, z) =$(m, 1, 1)$, $(n, 3, 2)$ (m ve n keyfi sabit) istisnai durumları dışındaki tek tamsayı çözümü $(x, y, z) = (p, q, r)$ dir (Terai 1999).

2002'de Cao ve Dong (2.1.1) denklemini $p = q = 2$ ve $r \geq 3$ tek, $2 \parallel a$ ve $b \geq a \cdot 25.1$ iken göz önüne aldılar. Bu yazarlar tarafından $(2^n - 1)^x + 2^y = (2^n + 1)^z$ denkleminin $1 < n \in \mathbb{Z}^+$ iken sadece $(x, y, z) = (1, 1, 1)$ ve $(2, n + 2, 2)$ çözümlerine sahip olduğu gösterildi. Ayrıca II. Terai Sanısını şu şekilde modifiye ettiler:

Sanı 2.1.5 (Terai-Jeśmanowicz Sanısı) $a, b, c, p, q, r \in \mathbb{N}$, $r \geq 2$ ve $(a, b) = 1$ olmak üzere (2.1.1) denkleminin tek çözümü EBOB$(x, y, z) > 1$ iken $(x, y, z) = (p, q, r)$ dir (Cao ve Dong 2002).

1 yıl sonra Le, "Terai-Jeśmanowicz sanısının"da yanlış olduğunu gösterdi. Örneğin $n \in \mathbb{Z},\ n > 2$ iken $a = 2,\ b = 2^n - 1,\ c = 2^n + 1$ ise bu a, b, c değerleri maks$\{a, b, c\} > 7$ ve $a^{n+2} + b^2 = c^2$ denklemini sağlar, ancak a, b, c sabit aralarında asal pozitif tamsayılar ve $\min\{a, b, c\} > 1,\ x, y, z \in \mathbb{Z}$ iken (2.1.1) denkleminin çözümleri $(x, y, z) = (1, 1, 2)$ ve $(n + 2, 2, 2)$ dir. Bu da Terai-Jeśmanowicz sanısı için sonsuz çoklukta ters örnek bulunması demektir. Le bu makalesinde aşağıdaki sanıyı önerdi:

Sanı 2.1.6 (2.1.1) denklemi $\min(x, y, z) > 1$ iken en çok tek bir (x, y, z) çözümüne sahiptir (Le 2003).

Ayrıca Le bu çalışmasında

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

denklemini $(a, b) = 1,\ 2 \nmid a,\ 2 \mid b,\ r > 1,\ 2 \nmid r$ iken göz önüne aldı ve bu denklem hakkında bazı sonuçlar da verdi.

2009'da Cipu ve Mignotte tarafından Sanı 2.1.6'nın yanlış olduğu aşağıdaki teorem ile ifade edildi:

Teorem 2.1.7 $a \equiv 2 \pmod 4$, $b \equiv 3 \pmod 4$, $(a, b) = 1$, $r > 1$ tek olsun. $a^2 + b^2 = c^r$ eşitliğini sağlayacak sadece sonlu çoklukta (a, b, c, r) dörtlüsü vardır ve (2.1.1) denklemi $x, y, z > 1$ tamsayıları için birden fazla çözüme sahiptir. Bu dörtlülerin tümü için, $r < 770$ dir (Cipu ve Mignotte 2009).

2010 yılında Miyazaki, (Cao 1999), (Cao ve Dong 2002) ve (Le 2003) isimli çalışmaları göz önüne alarak II. Terai sanısını aşağıdaki şekliyle modifiye etti:

Sanı 2.1.8 $p, q, r \geq 2$ sabit tamsayıları ve a, b, c aralarında asal pozitif tamsayılar $a^p + b^q = c^r$ eşitliğini sağlayacak şekilde olsun. (2.1.1) denkleminin ($a < b$ iken) aşağıdaki

istisnai durumlar haricinde tek çözümü $(x, y, z) = (p, q, r)$ dir:

$$(a, b, c) = (1, 2, 3),\ (x, y, z) = (i, 1, 1), (j, 3, 2),\ i \geq 1,\ j \geq 1;$$

$$(a, b, c) = (2, 7, 3),\ (x, y, z) = (1, 1, 2), (5, 2, 4);$$

$$(a, b, c) = (2, 2^{k-2} - 1, 2^{k-2} + 1),\ (x, y, z) = (1, 1, 1), (k, 2, 2), k \geq 4$$

(Miyazaki 2010).

Miyazaki bu çalışmasında $q = r = 2$ durumunu (yani $a^p + b^2 = c^2$ eşitliğini) sağlayacak $a, b, c,$ ve p tamsayılarını göz önüne alarak Terai sanısının istisnai durumları hakkında bazı sonuçlar da vermiştir.

2011 yılındaki çalışmasında ise Miyazaki $p = q = 2$ ve $r > 2$ çift durumunu (yani $a^2 + b^2 = c^r$ eşitliğini sağlayacak a, b, c ve r tamsayılarını) göz önüne alarak Terai sanısını kısmen doğrulayan sonuçlar vermiştir (Miyazaki 2011).

Şimdi a, b, c, m sabit pozitif tamsayılar ve $a + b = c^2$ iken

$$(am^2 + 1)^x + (bm^2 - 1)^y = (cm)^z \tag{2.1.2}$$

Diophant denklemini göz önüne alalım. Bu denklem için de beklenen tek çözüm Terai sanısına göre $(x, y, z) = (1, 1, 2)$ dir. O halde bu denklem ile ilgili literatür bilgisini verelim.

2012'de (2.1.2) denkleminin $(a, b, c) = (3, 4, 5)$ iken tek çözümünün $(x, y, z) = (1, 1, 2)$ olduğu bazı koşullar altında Terai tarafından gösterildi (Terai 2012). 2014'te Su ve Li; 2016'da da Bertók aynı denklem üzerinde Terai tarafından çözülememiş durumları çözerek (2.1.2) denkleminin $(a, b, c) = (3, 4, 5)$ durumunun çözümünü tamamladılar (Su ve Li 2014, Bertók 2016).

2015'te Terai ve Hibino (2.1.2) denkleminin $(a, b, c) = (5, 12, 13)$ iken $m \not\equiv 17, 33 \pmod{40}$ koşulu altında tek çözümünün $(x, y, z) = (1, 1, 2)$ olduğunu gösterdi (Terai ve Hibino 2015).

2014'te Miyazaki ve Terai tarafından (2.1.2) denklemi $b = 1$, $a \equiv 3, 5 \pmod 8$, $c + 1 = a^2$ iken göz önüne alındı. Bu denklemin $(m, a, c) = (1, 3, 8)$ durumu dışında tek çözümünün $(x, y, z) = (1, 1, 2)$ ve istisnai durumlardaki çözümlerinin de $(x, y, z) = (1, 1, 2), (5, 2, 4)$ olduğu ispatlandı (Miyazaki ve Terai 2014).

2017'de Terai ve Hibino (2.1.2) denkleminin farklı bir versiyonu olan $(3pm^2 - 1)^x + (p(p - 3)m^2 + 1)^y = (pm)^z$ denklemini bazı koşullar altında göz önüne aldılar ve bu denklemin tek çözümünün $(x, y, z) = (1, 1, 2)$ olduğunu gösterdiler (Terai ve Hibino 2017).

Fu ve Yang, $2 \mid a$, $2 \nmid c$ ve $m > 1$ olduğunda (2.1.2) denkleminin $c \mid m$ ve $m > 36c^3 \log c$ koşulları altında tek pozitif çözümünün $(x, y, z) = (1, 1, 2)$ olduğunu ispatladılar (Fu ve Yang 2017).

Pan da, $a+b = c^2$, $2 \nmid c$, $m > 1$ ve $m \equiv \pm 1 \pmod c$ iken (2.1.2) denklemini ele aldı. $a \equiv 4, 5 \pmod 8$, $(*/*)$ Jacobi sembolü olmak üzere $((a+1)/c) = -1$ ve $m > 6c^2 \log c$ koşulları altında (2.1.2) denkleminin tek pozitif tamsayı çözümünün $(x, y, z) = (1, 1, 2)$ olduğunu gösterdi (Pan 2017).

2.2 Ana Sonuç

Tezin bu bölümünde (2.1.2) denklemini göz önüne alıyoruz. Bu çalışma 2012-2016 yılları arasında (Terai 2012), (Su ve Li 2014), (Bertók 2016) ve (Miyazaki ve Terai 2014) isimli çalışmaların kısmen bir genellemesi niteliğindedir.

Teorem 2.2.1 $a, c \in \mathbb{N}$, $a \equiv 11, 13 \pmod{24}$ ve $2c + 1 = a^2$ olsun. Bu durumda $m \equiv \pm 1 \pmod a$ ve $m > a^2$ iken

$$((c + 1)m^2 + 1)^x + (cm^2 - 1)^y = (am)^z \tag{2.2.1}$$

denkleminin tek pozitif tamsayı çözümü $(x, y, z) = (1, 1, 2)$ dir (Kızıldere ve ark. 2018).

2.3 Ana Sonucun İspatı

2.3.1 $m = 1$ Durumu

Yardımcı Teorem 2.3.1 $a, c \in \mathbb{N}$, $a \equiv 11, 13 \pmod{24}$ olsun. $2c + 1 = a^2$ iken

$$(c+2)^x + (c-1)^y = a^z \tag{2.3.1}$$

denkleminin tek pozitif tamsayı çözümü $(x, y, z) = (1, 1, 2)$ dir (Kızıldere ve ark. 2018).

İspat. $m = 1$ iken (2.2.1) denklemini göz önüne alalım. $2c + 1 = a^2$ olduğundan (2.2.1) denklemi

$$[(a^2+3)/2]^x + [(a^2-3)/2]^y = a^z \tag{2.3.2}$$

olur. Bu denklem $(a-1)/2$ ve $(a+1)/2$ modlarında ele alınırsa, sırasıyla

$$2^x + (-1)^y \equiv 1 \pmod{(a-1)/2},$$

$$2^x + (-1)^y \equiv (-1)^z \pmod{(a+1)/2}$$

kongrüansları elde edilir. Özellikle $a > 5$ ve $a \equiv 3, 5 \pmod{8}$ iken, yukarıdaki kongürüanslardan z'nin çift ve y'nin tek olduğu elde edilir. $z = 2Z$ ($Z \in \mathbb{Z}$) olsun. $2c+1 = a^2$ eşitliği kullanılarak, (2.3.2)'den

$$(c+2)^x + (c-1)^y = (2c+1)^Z$$

denklemi elde edilir. $4 \mid c$ olduğundan, yukarıdaki denklem 4 modunda ele alınırsa, $x = 1$ bulunur. Buradan da

$$c + 2 + (c-1)^y = (2c+1)^Z \tag{2.3.3}$$

denklemi elde edilir. $Z \leq y < 2Z$ olduğu açıktır. Şimdi $y > 1$ iken bir çelişki elde edeceğiz. O halde $y \geq 3$ ve $y < 2Z$ dir. Eğer $1 + y = 2Z$ ise (2.3.3)'ten $(2c+1)^{\frac{1+y}{2}} - (c-1)^y = c + 2 > 0$ bulunur ve buradan $\frac{3}{2} < \frac{2y}{1+y} < \frac{\log(2c+1)}{\log(c-1)} \leq \frac{\log 17}{\log 7}$ elde edilir ki bu

da imkansızdır. O halde $1 + y < 2Z$ dir. Diğer yandan, (2.3.3) denklemi c^2 modunda ele alınırsa,

$$c + 2 + (-1 + cy) \equiv 1 + 2cZ \pmod{c^2}$$

elde edilir ki bu da

$$1 + y \equiv 2Z \pmod{c}$$

demektir. $1 + y < 2Z$ olduğundan, bu kongrüans

$$c \leq 2Z - (1 + y) \tag{2.3.4}$$

eşitsizliğini verir. Diğer taraftan, Sonuç 1.10.14'ten,

$$y < 2521 \log(2c + 1)$$

olduğunu göstereceğiz. Bunu göstermek için, ilk olarak (2.3.3)'ten elde edilen, aşağıdaki iki logaritmalarda lineer formunu ele alacağız:

$$\Omega = Z \log(2c + 1) - y \log(c - 1) \ \ (> 0).$$

$k > 0$ iken $\log(1 + k) < k$ olduğundan,

$$0 < \Omega = \log\left(\frac{(2c+1)^Z}{(c-1)^y}\right) = \log\left(1 + \frac{c+2}{(c-1)^2}\right) < \frac{c+2}{(c-1)^y}$$

dir. Böylece,

$$\log \Omega < \log(c + 2) - y \log(c - 1) \tag{2.3.5}$$

elde edilir.

Diğer yandan, Sonuç 1.10.14'ü uygulayarak, Ω için bir alt sınır bulmak istiyoruz.

Sonuç 1.10.14'ten, $d' = \frac{y}{\log(2c+1)} + \frac{z}{\log(c-1)}$ iken, aşağıdaki eşitsizlik elde edilir:

$$\log \Omega \geq -25.2(\text{maks}\{\log d' + 0.38, 10\})^2 \log(c-1)\log(2c+1). \tag{2.3.6}$$

Şimdi $(c+1)^{y+1} > (2c+1)^Z$ olduğunu göstereceğiz. $c \equiv 12 \pmod{24}$ iken,

$$\begin{aligned}(c-1)^{y+1} - (2c+1)^Z &= (c-1)((2c+1)^Z - (c+2)) - (2c+1)^Z \\ &= (c-2)(2c+1)^Z - (c-1)(c+2) \\ &\geq c^2 - 4c > 0\end{aligned}$$

dır. Böylece $d' < \frac{2y+1}{\log(2c+1)}$ dir.

$T = \frac{y}{\log(2c+1)}$ alalım. (2.3.5) ve (2.3.6) eşitsizlikleri kullanılarak,

$$\begin{aligned}y\log(c-1) < \log(c+2) + 25.2(\text{maks}\{\log\left(2T + \frac{1}{\log(2c+1)}\right) + 0.38, 10\})^2 \\ \times \log(c-1)\log(2c+1)\end{aligned}$$

elde edilir. Böylece $\log(2c+1) \geq \log(25) > 3$ olduğundan,

$$T < 1 + 25.2(\text{maks}\{\log(2T+1) + 0.38, 10\})^2 \tag{2.3.7}$$

bulunur. Bu $T < 2521$ olduğunu gösterir. $Z \leq y$ ile birlikte (2.3.4) ve (2.3.7) eşitsizliklerinden

$$c \leq 2Z - (1+y) < y < 2521\log(2c+1)$$

eşitsizliği elde edilir. Buradan da $c \leq 27518$ bulunur. Son olarak PARI/GP programı kullanılarak (2.3.3) denkleminin $c \leq 27518$ iken çözüme sahip olmadığı görülür. Böylece ispat tamamlanır. ■

2.3.2 $m \geq 2$ Durumu

(x, y, z), (2.2.1) denkleminin bir çözümü olsun. Önceki bölümün sonucundan, $m \geq 2$ varsayarak, x, y, z ler için pariteleri belirlemek istiyoruz. $m > a^2$ ile $m \equiv \pm 1 \pmod{a}$ ve $a \equiv 11, 13 \pmod{24}$ kongrüansları kullanılarak, aşağıdaki sonucu ispatlayacağız.

Yardımcı Teorem 2.3.2 Varsayalım ki $(x, y, z) = (1, 1, 2)$, (2.2.1) denkleminin bir çözümü olsun. Bu durumda z çift, x ve y tektir (Kızıldere ve ark. 2018).

İspat. (x, y, z), (2.2.1) denklemi için bir çözüm olsun. $cm^2 - 1 = \left(\left(\frac{a^2-1}{2}\right)m^2 - 1\right) > am$ olduğu $1 + 2c = a^2$ eşitliğinden görülür. Böylece (2.2.1)'den dolayı $z \geq 2$ dir. (2.2.1) denklemini m^2 modunda ele alırsak $1 + (-1)^y \equiv 0 \pmod{m^2}$ bulunur. Böylece $m \geq 2$ iken y tektir. $1 + 2c = a^2$ ve $m \equiv \pm 1 \pmod{a}$ kongrüansları kullanılırsa, (2.2.1) denklemi

$$(-c)^x \equiv -c^y \pmod{a}$$

kongrüansına dönüşür ki bu da $\left(\frac{-c}{a}\right)^x = \left(\frac{-c}{a}\right)^y$ olmasını gerektirir. Buradan da x ve y'nin aynı paritede olduğunu görürüz. Böylece y tek olduğundan x de tektir.

Şimdi $\left(\frac{m}{cm^2-1}\right) = 1$ ve $\left(\frac{a}{cm^2-1}\right) = -1$ olduğunu göstereceğiz. $cm^2 - 1 \equiv 3 \pmod{8}$ ve $c \equiv 12 \pmod{24}$ olduğunu biliyoruz. $\gamma \geq 0$ ve r tek tamsayı olmak üzere $m = 2^\gamma r$ yazalım. Böylece

$$\left(\frac{m}{cm^2-1}\right) = \left(\frac{2}{cm^2-1}\right)^\gamma \left(\frac{r}{cm^2-1}\right) = \left(\frac{r}{cm^2-1}\right) = 1$$

elde edilir.

$a \equiv 11 \pmod{24}$ ise, $\left(\frac{3}{a}\right) = 1, \left(\frac{2}{a}\right) = -1$ ve $\left(\frac{2c+2}{a}\right) = \left(\frac{a^2+1}{a}\right) = 1$ olduğundan,

$$\left(\frac{a}{cm^2-1}\right) = -\left(\frac{cm^2-1}{a}\right) = -\left(\frac{c-1}{a}\right) = \left(\frac{c+2}{a}\right) = \left(\frac{2}{a}\right)\left(\frac{c-1}{a}\right)$$

$$= \left(\frac{2c-2}{a}\right) = \left(\frac{a^2-3}{a}\right) = \left(\frac{-3}{a}\right) = \left(\frac{-1}{a}\right)\left(\frac{3}{a}\right) = -1$$

dir.

$a \equiv 13 \pmod{24}$ ise, $\left(\frac{3}{a}\right) = 1, \left(\frac{2}{a}\right) = -1$ ve $\left(\frac{2c+2}{a}\right) = \left(\frac{a^2+1}{a}\right) = 1$ olduğundan da,

$$\left(\frac{a}{cm^2-1}\right) = \left(\frac{cm^2-1}{a}\right) = \left(\frac{c-1}{a}\right) = \left(\frac{\frac{a^2-1}{2}-1}{a}\right) = \left(\frac{\frac{a^2-3}{2}}{a}\right) = \left(\frac{4(\frac{a^2-3}{2})}{a}\right)$$

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

olur.

Böylece

$$\left(\frac{am}{cm^2-1}\right) = \left(\frac{a}{cm^2-1}\right)\left(\frac{m}{cm^2-1}\right) = (-1).1 = -1$$

bulunur.

$1 + 2c = a^2$ olduğu kullanılırsa,

$$\left(\frac{(c+1)m^2+1}{cm^2-1}\right) = \left(\frac{(c+1)m^2+cm^2}{cm^2-1}\right) = \left(\frac{a^2m^2}{cm^2-1}\right) = 1$$

elde edilir. Bu sonuçlar yardımıyla, (2.2.1) denkleminden z'nin çift olduğu elde edilir. ■

Şimdi m çift olduğunda, (2.2.1) denklemini m^3 modunda ele alarak bu denklemin tek pozitif tamsayı çözümünün $(x, y, z) = (1, 1, 2)$ olduğunu gösterelim.

Yardımcı Teorem 2.3.3 m çift iken, (2.2.1) denkleminin tek pozitif tamsayı çözümü $(x, y, z) = (1, 1, 2)$ dir (Kızıldere ve ark. 2018).

İspat. $z \leq 2$ olduğunda (2.2.1)'den $(x, y, z) = (1, 1, 2)$ olduğu açıktır. Bu durumda $z \geq 3$ olduğunu kabul edebiliriz. Yardımcı Teorem 2.3.2'den y ve x'in tek olduğunu biliyoruz.

(2.2.1) denklemi m^3 modunda göz önüne alınırsa,

$$(c+1)m^2x + 1 + cm^2 - 1 \equiv 0 \pmod{m^3}$$

bulunur ki bu da,

$$(c+1)x + cy \equiv 0 \pmod{m}$$

olmasını gerektirir. Ancak bu kongrüans m'nin çift, c'nin çift ve x'in tekliği ile çelişir. Bu durumda ispat biter. ■

Yardımcı Teorem 2.3.4 m tek iken $x = 1$ dir (Kızıldere ve ark. 2018).

İspat. Yardımcı Teorem 2.3.2'den y tek olduğunda z'nin çift olduğu görülür. Şimdi $x \geq 2$ olduğunu varsayalım. (2.2.1) denklemi 4 modunda ele alınırsa,

$$(-1)^y \equiv 1 \pmod{4}$$

bulunur. Böylece y çifttir. Bu da Yardımcı Teorem 2.3.2 ile çelişir. O halde $x = 1$ dir. ■

2.3.3 $W^z - V^y = U$ Pillai Denklemi

1930-1940 yılları arasında U sabit ve sıfırdan farklı bir tamsayı; W, V, z ve y pozitif tamsayılar, $z \geq 2, y \geq 2$ olmak üzere

$$W^z - V^y = U \tag{2.3.8}$$

Diophant denklemi Pillai tarafından çalışıldı ve Pillai 1936'da şu iddiada bulundu:

Sanı 2.3.5 $z \geq 2,\ y \geq 2$ ve $U \geq 1$ olmak üzere (2.3.8) denklemi sonlu çoklukta (W, V, z, y) tamsayı çözümüne sahiptir (Pillai 1936).

Bu sanı henüz ispatlanamadı. Ancak bu denklem ve sanı hakkında birçok faydalı sonuçlar elde edildi. Pillai sanısı ile ilgili en önemli sonuçlardan birisi şöyle ifade edilir:

Teorem 2.3.6 $W \geq 2,\ V \geq 2,\ (W, V) = 1$ ve U sabit sıfırdan farklı pozitif tamsayılar olmak üzere (2.3.8) denklemi en çok iki tane (z, y) çözüme sahiptir (Bennett 2001).

Şimdi (2.2.1) denklemine dönelim. Yardımcı Teoremler 2.3.2 ve 2.3.4'te (2.2.1) denklemi için y'nin tek ve $x = 1$ olduğu gösterildi. $y = 1$ olduğunda (2.2.1) den $z = 2$ elde edilir. Böylece $y \geq 3$ varsayabiliriz. Bu durumda (2.2.1) denklemi $U = (c+1)m^2 + 1, V = cm^2 - 1$ ve $W = am$ iken (2.3.8) Pillai denkleminin çözümlerini bulmaya indirgenir.

İlk olarak y için bir alt sınır elde edelim.

Yardımcı Teorem 2.3.7 (2.3.8) denklemi için $y \geq (m^2-1)/c - 1$ dir (Kızıldere ve ark. 2018).

İspat. $y \geq 3$ ise (2.3.8)'den

$$(am)^z = (c+1)m^2 + 1 + (cm^2-1)^y \geq (c+1)m^2 + 1 + (cm^2-1)^3 > (am)^3$$

elde edilir. Bu durumda $z \geq 4$ tür. (2.3.8) denklemi m^4 modunda ele alınırsa,

$$(c+1)m^2 + 1 + cm^2 y - 1 \equiv 0 \pmod{m^4}$$

bulunur ve buradan da $c + 1 + cy \equiv 0 \pmod{m^2}$ elde edilir. Bu ise $y \geq (m^2-1)/c - 1$ olduğunu gösterir. ■

Yardımcı Teorem 2.3.8 (2.3.8) denklemi için $y < 2521 \log W$ dur (Kızıldere ve ark. 2018).

İspat. (2.3.8) denkleminden elde edilen

$$\Gamma = z \log W - y \log V \ \ (> 0)$$

lineer formunu göz önüne alalım.

$l > 0$ için $\log(1+l) < l$ olduğundan,

$$0 < \Gamma = \log\left(\frac{W^z}{V^y}\right) = \log\left(1 + \frac{U}{V^y}\right) < \frac{U}{V^y} \tag{2.3.9}$$

elde edilir. Böylece

$$\log \Gamma < \log U - y \log V \tag{2.3.10}$$

bulunur. Diğer taraftan, Sonuç 1.10.14'ü uygulayarak, Γ için bir alt sınır bulmak istiyoruz. Sonuç 1.10.14'ten, $d' = \frac{y}{\log W} + \frac{z}{\log V}$ iken

$$\log \Gamma \geq -25.2(\text{maks}\{\log d' + 0.38, 10\})^2 \log V \log W \tag{2.3.11}$$

eşitsizliği elde edilir. Şimdi $V^{y+1} > W^z$ olduğunu gösterelim.

$$V^{y+1} - W^z = V(W^z - U) - W^z = (V-1)W^z - UV$$

$$\geq (cm^2 - 2)(2c+1)m^2 - ((c+1)m^2)(cm^2 - 1) > 0$$

dır. Böylece $d' < \frac{2y+1}{\log W}$ olduğu görülür.

$R = \frac{y}{\log W}$ olsun. (2.3.10) ve (2.3.11) eşitsizlikleri kullanılarak,

$$y \log V < \log U + 25.2(\text{maks}\{\log \left(2R + \frac{1}{\log W}\right) + 0.38, 10\})^2 \log V \log W$$

elde edilir. Ayrıca $\log W \geq \log 33 > 3$ ve $U < V$ olduğundan,

$$R < 1 + 25.2(\text{maks}\{\log \left(2R + \frac{1}{3}\right) + 0.38, 10\})^2$$

dir. Buradan $R < 2521$ bulunur. Böylece ispat tamamlanır. ■

Şimdi Teorem 2.2.1'i ispatlayabiliriz. Lemma 2.3.7 ve 2.3.8'den,

$$2\Big(\frac{m^2-1}{a^2-1}\Big) - 1 < 2521 \log(am)$$

elde edilir. Eğer $m > a^2$ ise,

$$2m + 1 < 2521 \log(am)$$

dir. Buradan $m < 18586$ bulunur. Böylece $a \leq 136$ dır. (2.3.9)'dan,

$$\left|\frac{\log V}{\log W} - \frac{z}{y}\right| < \frac{U}{yV^y \log W}$$

eşitsizliği elde edilir ve böylece $y \geq 3$ olduğunda $\left|\frac{\log V}{\log W} - \frac{z}{y}\right| < \frac{1}{2y^2}$ bulunur. Teorem 1.5.11 gereği bu eşitsizlikte $\frac{z}{y}$, $\frac{\log V}{\log W}$'nun $n.$ yakınsamadır.

Aksi takdirde, eğer $\frac{a_r}{b_r}$, $\frac{\log V}{\log W}$'nun $r.$ kısmi yakınsaması ise, $\frac{\log V}{\log W}$'nun $(r+1).$ kısmi kesri u_{r+1} iken

$$\left|\frac{\log V}{\log W} - \frac{a_r}{b_r}\right| > \frac{1}{(u_{r+1}+2)e_r^2}$$

elde edilir. $\frac{z}{y} = \frac{a_r}{b_r}$ alalım. $b_r \leq y$ dir. Buradan

$$u_{r+1} > \frac{V^y \log W}{Uy} - 2 \geq \frac{V^{b_r} \log W}{Ub_r} - 2 \tag{2.3.12}$$

bulunur. Son olarak PARI/GP programı kullanılarak, $a \equiv 11, 13 \pmod{24}$ ile her bir $a \leq 136$ ve $3 \leq m \leq 18585$ için $b_r < 2521 \log(am)$ ile her bir r için (2.3.12) eşitsizliğinin sağlanmadığı görülür. Böylece Teorem 2.2.1'in ispatı tamamlanır. ■

3. $(\mathbf{n-1})^{\mathbf{x}}+(\mathbf{n+2})^{\mathbf{y}}=\mathbf{n}^{\mathbf{z}}$ DIOPHANT DENKLEMİ

Bu bölüm, başlık denklemi hakkında orijinal sonuçlar içermektedir. Burada $n \geq 2$ olmak üzere

$$(n-1)^x+(n+2)^y=n^z \tag{3.0.1}$$

Diophant denkleminin tüm pozitif tamsayı çözümleri ile ilgileneceğiz.

3.1 Giriş

Bölüm 2.1.1'de $a^x+b^y=c^z$ denkleminin tarihçesi ve literatürü hakkında bazı bilgiler verildi.

Bu tezde (3.0.1) denkleminin çalışılmasındaki ilk motivasyon kaynağı, bu denklemin özel hallerinin yani $2^x+5^y=3^z$ ve $4^x+7^y=5^z$ denkleminin Nagell tarafından göz önüne alınmış olmasıdır (Nagell 1958, Teorem 3 ve Teorem 9). Dolayısıyla (3.0.1) denkleminin çalışılması Nagell'in çalışmasının bir genellemesi olacaktır.

Bu denklemin çalışılmasındaki ikinci motivasyon kaynağı da Yardımcı Teorem 2.3.1'deki (2.3.1) denkleminin bir versiyonunun herhangi bir koşul olmaksızın çözülmesi isteğidir.

Şimdi de (3.0.1) denkleminin farklı literatür bilgisine göz atalım. İlk olarak $t \geq 1$ iken

$$(tb-1)^x+b^y=(tb+1)^z \tag{3.1.1}$$

denklemini göz önüne alalım. Burada b'nin çift olduğu açıktır. Bu denklem için aşikar çözümler aşağıdaki gibi verilir:

$$(x,y,z)=\begin{cases}(i,1,1):i\geq 1,\ (j,3,2):j\geq 1, & b=2 \text{ ve } t=1 \text{ ise,}\\ (2,k+1,2), & k\geq 1 \text{ iken } t=b^k/4 \text{ ise,}\\ (1,1,1), & b=2 \text{ ise,}\\ (1,13,2), & b=2 \text{ ve } t=45 \text{ ise.}\end{cases}$$

(3.1.1) denklemi $t = 1$ durumunda He ve Togbé tarafından çözülmüştür (He ve Togbé 2009). Bu çalışmanın ardından Miyazaki ve Togbé, $t > 1$ ve tek iken (3.1.1) denklemini ele almış ve aşikar olmayan çözümlerinin olmadığını göstermişlerdir (Miyazaki ve Togbé 2012). Son olarak da Miyazaki, Togbé ve Yuan (3.1.1) denklemini t çift iken ele alarak bu denklemin çözümünü tamamlamışlardır (Miyazaki ve ark. 2016).

2019'da Fu, He, Yang ve Zhu tarafından (3.1.1) denkleminin farklı bir varyasyonu ele alınarak $n, x, y, z \in \mathbb{Z}^+$ iken, $(n+2)^x + (n+1)^y = n^z$ denkleminin tek pozitif tamsayı çözümünün $(n, x, y, z) = (3, 1, 1, 2)$ olduğu gösterilmiştir (Fu ve ark. 2019).

3.2 Ana Sonuç

Teorem 3.2.1 n bir pozitif tamsayı olsun. (3.0.1) denkleminin pozitif tamsayılardaki tek çözümü $(n, x, y, z) = (3, 2, 1, 2), (3, 1, 2, 3)$ tür (Bai ve ark. 2019).

3.3 Ana Sonucun İspatı

$n = 2$ iken, (3.0.1) denklemi $2^x - 4^y = 1$ denklemine karşılık gelir. Bu denklemin pozitif tamsayılarda çözümü yoktur. O halde $n > 2$ varsayalım. Bu başlık altında ispatı dört alt durumda ele alacağız:

- $n > 64$,
- $n \geq 7$ ve $z \geq 2n$,
- $y \leq n \leq 64$ ve $z < 2n$,
- $2 < n < 7$.

3.3.1 $n \geq 64$ Durumu.

$n > 64$ olduğunu varsayalım. Eğer $(n-1)^x \geq \frac{1}{2}n^z$ ise, $x \geq z$ dir. O halde ilk olarak $x > z$ durumunu göz önüne alalım. $(1 - \frac{1}{n})^z > e^{-z/n}$ iken,

$$1 > \left(1 - \frac{1}{n}\right)^z \cdot (n-1)^{x-z} > \frac{(n-1)^{x-z}}{e^{z/n}}$$

eşitsizliği elde edilir. Buradan $e^{z/n} > (n-1)^{x-z} > 63$ bulunur ki bu da $z > 4n$ demektir.

Şimdi $x = z$ durumunu ele alalım. Bu durumda $(n+2)^y > \frac{1}{n} \cdot n^z$ dir. $y < z$ olduğundan,

$$e^{2y/n} > \left(1 + \frac{2}{n}\right)^{n/2 \times 2y/n} > \frac{1}{n} \cdot n^{z-y} \tag{3.3.1}$$

elde edilir. $z - y > 1$ ise (3.3.1) eşitsizliğinden $e^{2y/n} > n \geq 64$ bulunur. Böylece $y > 2n$ dir. $(n-1)^x < \frac{1}{2} \cdot n^z$ ise, $(n+2)^y > \frac{1}{2} n^z$ dir. O halde

$$e^{2y/n} > \left(1 + \frac{2}{n}\right)^{n/2 \times 2y/n} > \frac{1}{2} \cdot n^{z-y} \tag{3.3.2}$$

olur. $z - y > 1$ iken, (3.3.2) eşitsizliğinden $e^{2y/n} > n^2/2 \geq 64$ elde edilir. Böylece $y > 2n$ dir. $z - y = 1$ ise, benzer şekilde $e^{2y/n} > n/2 \geq 32$ olur. Buradan da $z > y > n$ bulunur. Dolayısıyla

$$x > z > 4n \text{ veya } z > y > n \text{ veya } x = z = y + 1$$

elde edilir.

$(n-1)^{y+1} + (n+2)^y = n^{y+1}$ ve $n > 64$ olduğundan, $y \leq 3$ veya $y > n$ dir. Eğer $(n-1)^{y+1} + (n+2)^y = n^{y+1}$ ve $y \leq 3$ ise, basit bir hesaplama ile $y = 1$ ve $n = 3$ olduğu görülür. Sonuç olarak $n > 64$ iken,

$$x > z > 4n \text{ veya } z > y > n$$

dir.

(i) y **çift durumu**

y'nin çift olduğunu varsayalım. $z > n$ ve $n > 64$ iken, Önerme 1.6.11'den $z > n > h(\mathbb{Q}(\sqrt{-d}))$ elde edilir. Burada $h(\mathbb{Q}(\sqrt{-d}))$, $\mathbb{Q}(\sqrt{-d})$ kuadratik cisminin sınıf sayısıdır. Yardımcı Teorem 1.6.12'ye göre

$$(n-1)x_0^2 + y_0^2 = n^{z_0},\ 2 \nmid x$$

veya

$$x_0^2 + y_0^2 = n^{z_0},\ 2 \mid x$$

ve $z_0 \mid h(\mathbb{Q}(\sqrt{-4(n-1)}))$ olacak şekilde x_0, y_0, z_0 tamsayıları vardır. Böylece $z/z_0 \geq 5$ iken,

$$(n-1)^{\frac{x-1}{2}}\sqrt{-(n-1)} + (n+2)^{\frac{y}{2}} = \pm(x_0\sqrt{-(n-1)} + y_0)^{z/z_0} \tag{3.3.3}$$

veya

$$(n-1)^{\frac{x}{2}}\sqrt{-1} + (n+2)^{\frac{y}{2}} = \pm(x_0\sqrt{-1} + y_0)^{z/z_0} \tag{3.3.4}$$

dır. Ancak bu durum Teorem 1.9.8 ve Teorem 1.9.9'dan dolayı imkansızdır. $z/z_0 = 2, 3, 4$ olduğu durumların da imkansız olduğunu görmek kolaydır.

$z/z_0 = 4$ iken ispatta izlenecek yol $z/z_0 = 2$ durumu ile benzer olacağından $z/z_0 = 4$ durumunun ispatını vermeye gerek görmedik. İlk olarak $z/z_0 = 2$ için (3.3.3) denklemi ele alınsın. O halde $(n-1)^{\frac{x-1}{2}}\sqrt{-(n-1)} + (n+2)^{\frac{y}{2}} = \pm(x_0\sqrt{-(n-1)} + y_0)^2$ dir ve böylece

$$2x_0y_0 = \pm(n-1)^{\frac{x-1}{2}}$$

elde edilir. $x_0^2(n-1) + y_0^2 = n^{z_0}$ olduğundan $y_0 = \pm 1$ ve $2x_0 = (n-1)^{\frac{x-1}{2}}$ dir. Böylece $(n-1)^x + 4 = 4n^{z_0}$ bulunur. x'in tek oluşu ile birlikte bu denklem 4 modunda ele alınırsa $n = 3$ elde edilir. O halde $2 \nmid x$ ve $2 \mid y$ olduğunda $2^x + 5^y = 3^z$ denkleminin tek pozitif tamsayı çözümü $(x, y, z) = (1, 1, 2)$ dir (Nagell 1958, Teorem 3). Ancak, bu istenen çözüm değildir.

Şimdi $z/z_0 = 3$ için (3.3.3) denklemi ele alınsın. O zaman $(n-1)^{\frac{x-1}{2}}\sqrt{-(n-1)} + (n+2)^{\frac{y}{2}} = \pm(x_0\sqrt{-(n-1)} + y_0)^3$ tür ve böylece

$$x_0(3y_0^2 - x_0^2(n-1)) = \pm(n-1)^{\frac{x-1}{2}}, \quad y_0(y_0^2 - 3x_0^2(n-1)) = \pm(n+2)^{\frac{y}{2}}$$

dir. $(3, n-1) = 1$ olduğundan $x_0 = \pm(n-1)^{\frac{x-1}{2}}$ ve $y_0 = \pm(n+2)^{\frac{y}{2}}$ olduğu çıkarılabilir

ve $x_0^2(n-1)+y_0^2=n^{z_0}$ dır ki bu da imkansızdır.

Şimdi de ilk olarak $z/z_0=2$ için (3.3.4) denklemi ele alınsın. Bu durumda $(n-1)^{\frac{x}{2}}\sqrt{-1}+(n+2)^{\frac{y}{2}}=\pm(x_0\sqrt{-1}+y_0)^2$ elde edilir ve buradan

$$2x_0y_0=\pm(n-1)^{\frac{x-1}{2}}$$

bulunur. $x_0^2(n-1)+y_0^2=n^{z_0}$ olduğundan $y_0=\pm1$ ve $2x_0=(n-1)^{\frac{x}{2}}$ dir. Böylece $(n-1)^x+4=4n^{z_0}$ bulunur. x çift iken bu denklem 4 modunda ele alınırsa $n=5$ elde edilir. Bu durumda $2\nmid x$ ve $2\mid y$ iken $4^x+7^y=5^z$ denkleminin (x,y,z) tamsayı çözümü yoktur (Nagell 1958, Teorem 9).

Son olarak da $z/z_0=3$ için (3.3.4) denklemi ele alınsın. Bu durumda $(n-1)^{\frac{x}{2}}\sqrt{-1}+(n+2)^{\frac{y}{2}}=\pm(x_0\sqrt{-1}+y_0)^3$ tür. Böylece

$$x_0(3y_0^2-x_0^2(n-1))=\pm(n-1)^{\frac{x}{2}},\quad y_0(y_0^2-3x_0^2(n-1))=\pm(n+2)^{\frac{y}{2}}$$

elde edilir. $(3,n-1)=1$ olduğundan $x_0=\pm(n-1)^{\frac{x}{2}}$ ve $y_0=\pm(n+2)^{\frac{y}{2}}$ olduğu çıkarılabilir ki bu da imkansızdır. Böylelikle y'nin çift olduğu durum tamamlanmış olur.

(ii) y **tek ve** x **çift durumu**

y'nin tek x'in çift olduğunu varsayalım. $z>n$ ve $n>64$ olduğundan, Önerme 1.6.11 gereğince $z>n>h(\mathbb{Q}(\sqrt{-4(n+2)}))$ dir. Böylece Yardımcı Teorem 1.6.12'den

$$x_0^2+(n+2)y_0^2=n^{z_0}$$

ve $z_0\mid h(\mathbb{Q}(\sqrt{-4(n+2)}))$ olacak şekide x_0,y_0,z_0 tamsayıları vardır. Bu durumda $z/z_0\geq5$ iken,

$$(n-1)^{\frac{x}{2}}+(n+2)^{\frac{y-1}{2}}\sqrt{-(n+2)}=\pm(x_0+y_0\sqrt{-(n+2)})^{z/z_0}$$

dır. Bu da Teorem 1.9.8 ve Teorem 1.9.9'dan imkansızdır. Burada da $z/z_0=2,3,4$

olamayacağı (i) durumundaki gibi gösterilebilir.

(iii) x **ve** y **tek durumu**

Varsayalım ki x ve y'nin ikiside tek olsun. Eğer z çift ise, (3.0.1) denklemini $n+1$ modunda ele alarak $(-2)^x \equiv 0 \pmod{n+1}$ olduğu bulunur ki bu da $t \leq x$ iken $n+1 = 2^t$ olduğunu gösterir. Bu durumda (3.0.1) denklemi

$$(2^t - 2)^x + (2^t + 1)^y = (2^t - 1)^z, \ 2 \mid z \tag{3.3.5}$$

denklemine dönüşür. (3.3.5) denklemini 3 modunda ele alalım. Eğer t çift ise $(-1)^x + (-1)^y \equiv 0 \pmod{3}$ olur. Bu kongrüans daha sade bir şekilde $-2 \equiv 0 \pmod{3}$ olur ki bu imkansızdır. t tek olduğunda ise $0 \equiv 1 \pmod{3}$ olur ki bu da imkansızdır. O halde (iii) durumunun ispatı tamamlanır.

(iv) x, y **ve** z **tek durumu**

x, y ve z'nin tek olduğunu varsayalım. (3.0.1) denklemi n modunda ele alınırsa,

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

bulunur. Bu da $n \equiv 1, 7 \pmod{8}$ oluşunu gerektirir. Eğer $n \equiv 1 \pmod{8}$ ise, (3.0.1) denklemi 8 modunda ele alınırsa

$$3^y \equiv 1 \pmod{8}$$

kongrüansı elde edilir. Böylece $2 \mid y$ dir. Bu ise çelişkidir. $n \equiv 7 \pmod{8}$ olduğunda ise ispat iki durumda incelenir.

a. $x \geq 3$ durumu:

$n \equiv 7 \pmod{8}$ iken (3.0.1) denklemi 8 modunda göz önüne alınırsa

$$6^x + 1^y \equiv (-1)^z \pmod{8}$$

elde edilir. Buradan $2 \mid z$ dir. Bu durum $x \geq 3$ iken z'nin tekliği ile çelişir.

O halde (3.0.1) denklemini $n \equiv 7 \pmod 8$, y ve z tek ve $x = 1$ iken göz önüne almalıyız.

b. $x = 1$ durumu:

(3.0.1) denklemi $x = 1$ iken

$$n - 1 + (n+2)^y = n^z \tag{3.3.6}$$

denklemine dönüşür. $z > y > n$ ve $n \equiv 7 \pmod 8$ olduğunda $y \geq 73$ ve $n \geq 71$ dir. Eğer $z \geq 2y$ ise,

$$n - 1 = n^z - (n+2)^y \geq n^{2y} - (n+2)^y > n^2 - (n+2) = n^2 - n - 2$$

bulunur. Bu ise imkansızdır. O halde $2y > z$ dir.

$$\Omega = z \log n - y \log(n+2)$$

olsun. (3.3.6)'dan, $e^{\Omega} - 1 = \frac{n-1}{(n+2)^y}$ bulunur. $n \geq 71$ ve $t > 0$ iken $\log(1+t) < t$ olduğundan,

$$0 < \Omega < \frac{1}{1.04(n+2)^{y-1}} \tag{3.3.7}$$

eşitsizliği elde edilir. Ω'nın tanımı ve $2y > z$ olduğu kullanılırsa

$$\frac{2y-1}{y} \geq \frac{z}{y} > \frac{\log(n+2)}{\log n}$$

bulunur. Böylece

$$y > \frac{\log n}{\log(\frac{n^2}{n+2})} > (n - 70.99) \log n \tag{3.3.8}$$

dir. (1.10.5) eşitliğinde

$$D = 1,\ \ b_1 = y,\ \ b_2 = z,\ \ A_1 = n+2,\ \ A_2 = n$$

alınsın. Bu eşitlikler (3.3.7) eşitsizliğinde kullanıldığında

$$\frac{z}{\log(n+2)} - \frac{y}{\log n} < \frac{1}{1.04(n+2)^{y-1}\log n \log(n+2)} < 0.36 \cdot 10^{-135}$$

eşitsizliği elde edilir. Yukarıdaki eşitsizlik $d' = \frac{z}{\log(n+2)} + \frac{y}{\log n}$ iken

$$d' < \frac{2y}{\log n} + 0.36 \cdot 10^{-135}$$

eşitsizliğine dönüşür.

Eğer $\log d' + 0.38 > 10$ ise,

$$\log|\Omega| \geq -25.2(\log(\frac{2y}{\log n} + 0.36 \cdot 10^{-135}) + 0.38)^2 \log n \log(n+2) \qquad (3.3.9)$$

olur. (3.3.7) eşitsizliği kullanılarak

$$\log|\Omega| < -(y-1)\log(n+2) - 0.039 \qquad (3.3.10)$$

elde edilir. (3.3.9) ve (3.3.10) eşitsizlikleri birleştirildiğinde

$$\frac{y}{\log n} < \frac{-0.039 + \log(n+2)}{\log n \cdot \log(n+2)} + 25.2(\log(\frac{2y}{\log n} + 0.36 \cdot 10^{-135}) + 0.38)^2 \qquad (3.3.11)$$

bulunur. Bu eşitsizlik daha sade bir hale getirilirse

$$\frac{y}{\log n} < 0.24 + 25.2(\log(\frac{y}{\log n} + 0.18 \cdot 10^{-135}) + 1.08)^2 \qquad (3.3.12)$$

elde edilir. (3.3.12) eşitsizliğinden $y < 1870 \log n$ bulunur. Bu durumda

$d' < 2y/\log n + 0.36 \cdot 10^{-135} < 3741$ yani $\log d' < 8.23$ olur. Ancak bu durum $\log d' + 0.38 > 10$ varsayımı ile çelişir.

Şimdi $\log d' + 0.38 \leq 10$ durumunu göz önüne alalım. Sonuç 1.10.14'ten dolayı

$$\log |\Omega| \geq -25.2 \cdot 10^2 \log n \log(n+2) \tag{3.3.13}$$

dir. (3.3.10) ve (3.3.13) kullanılarak

$$y - 1 < 25.2 \cdot 10^2 \log n \tag{3.3.14}$$

bulunur. (3.3.8) ve (3.3.14) birleştirilerek

$$n < 70.99 + \frac{1}{\log n} + 25.2 \cdot 10^2 < 2591$$

elde edilir. Böylece y ve n için

$$n < 2591, \quad y < 19808 \tag{3.3.15}$$

üst sınırları elde edilmiş olur. Son olarak PARI-GP programı yardımıyla $71 \leq n < 2591$, $73 \leq y < 19808$, $73 < z < 39616$ ve $n \equiv 7 \pmod 8$ koşulları altında (3.3.6) denkleminin (n, y, z) pozitif tamsayı çözümünün olmadığı görülür. Böylece bu durumun ispatı tamamlanır.

3.3.2 $n \geq 7$ ve $z \geq 2n$ Durumu.

$n \geq 7$ ve $z \geq 2n$ iken, $z \geq 2n > h(\mathbb{Q}(\sqrt{-4(n+2)}))$ elde edilir. Burada da 3.3.1'deki yöntem kullanılarak ispat tamamlanır.

3.3.3 $2 < n < 7$ Durumu.

$2 < n < 7$ için, (3.0.1) denklemi sırasıyla $n = 3, 4, 5, 6$ iken,

$$2^x + 5^y = 3^z \tag{3.3.16}$$

$$3^x + 6^y = 4^z \tag{3.3.17}$$

$$4^x + 7^y = 5^z \tag{3.3.18}$$

$$5^x + 8^y = 6^z \tag{3.3.19}$$

denklemlerine dönüşür. İlk olarak (3.3.16) denklemini ele alalım. Bu denklemin $x \geq 2$ iken tek pozitif tamsayı çözümü $(x, y, z) = (1, 2, 3), (2, 1, 2)$ dir ki bu çözümler istenilen çözümdür (Nagell 1958, Teorem 3). Ardından (3.3.17) denklemi ele alınırsa bu denklemin çözümünün olmadığı görülür. (3.3.18) denklemi ele alındığında ise bu denklemin pozitif tamsayılarda çözümü yoktur (Nagell 1958, Teorem 9). Son olarak (3.3.19) denkleminin de çözümü yoktur.

3.3.4 $7 \leq n \leq 64$ Durumu.

Burada, (3.0.1) denklemi için $7 \leq n \leq 64$ durumu ele alınır. PARI/GP programı kullanılarak, $7 \leq n \leq 64$, $x > 1$ ve $z < 2n$ iken (3.0.1) denkleminin (n, x, y, z) tamsayı çözümü olmadığı görülür. Böylece teoremin ispatı tamamlanır.

KAYNAKLAR

Alaca, S, Williams K.S. 2004. Introductory Algebraic Number Theory. Cambridge University Press, New York, 448 s.

Asar, A. O., Arıkan, A., Arıkan, A. 2012. Cebir. Gazi Kitabevi, Ankara, 381 s.

Asar, A. O., Arıkan, A. 2012. Sayılar Teorisi. Gazi Kitabevi, Ankara, 269 s.

Bai, H., Kızıldere, E., Soydan, G., Yuan, P. 2019. On the Diophantine equation $(n-1)^x + (n+2)^y = n^z$, *Colloq. Math.*, yayına kabul edildi.

Baker, A. 1966 Lineer forms in the logarithms of algebraic numbers. I. *Mathematica*, **13**: 204-216.

Baker, A. 1967a Lineer forms in the logarithms of algebraic numbers. II. *Mathematica*, **14**: 102-107.

Baker, A. 1967b Lineer forms in the logarithms of algebraic numbers. III. *Mathematica*, **14**: 220-228.

Baker, A. 1977 The theory of linear forms in logarithms. *Proc. Conf.*, Cambridge 1976: 1-27.

Bennett, M. A. 2001. On Some Exponential Equations of S. S. Pillai. *Canad. J. Math.*, **53**: 897-922.

Bertók, Cs. 2016. The complete solution of the Diophantine equation $(4m^2+1)^x + (5m^2-1)^y = (3m)^z$. *Period. Math. Hung.*, **72**: 37-42.

Bilu, Y., Hanrot, G., Voutier, P.M. 2001. Existence of primitive divisors of Lucas and Lehmer numbers. *With an appendix by M. Mignotte. J. Reine Angew. Math.*, **539**: 75-122.

Bugeaud, Y., Shorey, T. N. 2001. On the number of solutions of the generalized Ramanujan-Nagell equation. *J. Reine Angew. Math.*, **539**: 55-74.

Cao, Z. 1999. A note on the Diophantine equation $a^x + b^y = c^z$. *Acta Arith.*, **91**: 85-93.

Cao, Z., Dong, X.L. 2002. On the Terai-Jeśmanowicz conjecture. *Publ. Math. Debrecen*, **61**: 253-265.

Catalan, E. 1844. Note extraite d'une lettre adressée à l' éditeur. *Acta Arith.*, **140**: 251–270.

Cipu, M., Mignotte, M. 2009. On a conjecture on exponential Diophantine equations. *J. Reine Angew. Math.*, **27**: 192.

Cohen, H. 1993. A Course in Computational Algebraic Number Theory. Graduate Texts in Mathematics 138, Springer Verlag, Berlin, Heidelberg, 563 s.

Fraleigh, J.B. 2003. A First Course In Abstract Algebra. Addision-Wesley Publishing Company, 520 s.

Fu, R., Yang, H., 2017. On the exponential Diophantine equation $(am^2+1)^x + (bm^2 -$

$1)^y = (cm)^z$ with $c \mid m$. *Period. Math. Hung.*, **75**: 143-149.

Fu, R., He, B., Yang, H., Zhu, H. 2019. On some ternary pure exponential Diophantine equations with three consecutive positive integers bases. *Proc. Indian Acad. Sci. (Math. Sci.)*, **129**: 1-12.

Gel'fond, A. O. 1934. Sur le septième problème de Hilbert. *Bull. Acad. Sci.*, **4**: 623-630.

Gel'fond, A. O. 1940. Sur la divisibilite de la difference des puissances de deux nombres entiers par une puissance d'un ideal premier. *Math. Sb.*, **7**: 7-25.

Hadano, T. 1976. On the Diophantine equation $a^x = b^y + c^z$. *Math. J. Okayama University*, **19**: 1-5.

He, B., Togbé, A. 2009. The exponential Diophantine equation $n^x + (n+1)^y = (n+2)^z$ revisited. *Glasgow Math. J.*, **51**: 659-667.

Hua, L. K. 1982. Introduction to Number Theory. Springer Verlag, Berlin, 572 s.

Jarvis, F. 2014. Algebraic Number Theory. Springer International Publishing, Switzerland, 292 s.

Jeśmanowicz, L. 1955-1956. Some remarks on Pythagorean numbers. *Wiadom Math.*, **1**: 196-202.

Khinchin, A. Y. 1963. Continued Fractions 3rd edition. P. Noordhoff Ltd, Graningen.

Kızıldere, E., Miyazaki, T., Soydan, G. 2018. On the Diophantine equation $((c+1)m^2+1)^x + (cm^2-1)^y = (am)^z$. *Turkish J. of Math.*, **42**: 2690-2698.

Laurent, M. 2008. Linear forms in two logarithms and interpolation determinants II. *Acta Arith.*, **133**: 325-348.

Le, M. 2003. A conjecture concerning the exponential Diophantine equation $a^x + b^y = c^z$. *Acta Arith.*, **106**: 345-353.

Lebesgue, V. A. 1850. Sur l'impossibilité en nombres entiers de l'quation $x^m = y^2 + 1$. *Nouv. Ann. Math.*, **9**: 178-181.

Liouville, J. 1844 Sur des classes très étendues de quantités dont la valeur n'est ni algebrique, ni même réductible à des irrationelles algébriques. *C.r. hebd. Séanc. Acad. Sci.*, **18**: 883-5, 910-11, *J. Math. Pures Appl.*, **16**: 133-42 (1851).

Luca, F. 2009. Diophantine Equation. Effective methods for Diophantine Equation, 26-30 January, 2009, Debrecen, Hungary.

Mahler, K. 1933. Zur approximation algebraischer Zahlen I: Über den grössten Primteiler binarer formen. *Math. Ann.*, **107**: 691-730.

Matiyasevich, Y. V. 1970. Solution of the tenth problem of Hilbert. *Mat. Lapok*, **21**: 83-87.

Menezes, A. J., Oorschot, P. C., Vanstone, S. A. 1996. Handbook of Applied Cryptography. CRC Press, USA, 780 s.

Mihăilescu, P. 2004. Primary Cyclotomic Units and a Proof of Catalan's Conjecture. *J.*

Reine angew. Math., **572**: 167-195.

Miyazaki, T. 2010. Exceptional cases of Terai's conjecture on Diophantine equations. *Arch. Math. (Basel)*, **95**: 519-527.

Miyazaki, T. 2011. Terai's conjecture on exponential Diophantine equations. *Int. J. Number Theory*, **7**: 981-999.

Miyazaki, T., Terai, N. 2014. On the exponential Diophantine equation $(m^2+1)^x + (cm^2-1)^y = (am)^z$. *Bull. Aust. Math. Soc.*, **90**: 9-19.

Miyazaki, T., Togbé, A. 2012. The Diophantine equation $(2am-1)^x + (2m)^y = (2am+1)^z$. *International Journal of Number Theory*, **8**: 2035-2044.

Miyazaki, T., Togbé, A., Yuan, P. 2016. On the Diophant equation $a^x + b^y = (a+2)^z$. *Acta Math. Hung.*, **149**: 1-9.

Nagell, T. 1958. Sur une classe d équations exponentielles. *Ark. Math.*, **3**: 569-582.

Pan, X. 2017. A note on the exponential Diophantine equation $(am^2+1)^x+(bm^2-1)^y = (cm)^z$. *Colloq. Math.*, **149**: 265-273.

PARI 2017. The PARI Group PARI/GP. version 2.9.4, Universite de Bordeaux. http://pari.math.u-bordeaux.fr.

Pillai, S. S. 1936. On $a^x - b^y = c$. *J. Indian Math. Soc. (N. S.)*, **2**: 119-122.

Schneider, T. H. 1934. Transzendenzuntersuchungen periodischer Funktionen I. Transzendenz von Potenzen. *J. Reine Angew. Math.*, **172**: 65-69.

Shorey, T. N., Tijdeman, R. 1986. Exponential Diophantine Equations. Cambridge University Press, Cambridge, 240 s.

Soydan, G., Demirci, M., Cangül, I. N., Togbé, A. 2017. On the conjecture of Jeśmanowicz. *Int. J. of App. Math. and Stat.*, **56**: 46-72.

Su, J., Li, X. 2014. The exponential Diophantine equation $(4m^2+1)^x + (5m^2-1)^y = (3m)^z$. *Abstr. Appl. Anal.*, **2014**: 1-5.

Terai, N. 1994. The Diophantine equation $a^x + b^y = c^z$. *Proc. Japan. Ser. A Math. Sci.*, **70**: 22-26.

Terai, N. 1999. Applications of a lower bound for linear forms in two logarithms to exponential Diophantine equations. *Acta. Arith.*, **90**: 17-35.

Terai, N. 2012. On the exponential Diophantine equation $(4m^2+1)^x + (5m^2-1)^y = (3m)^z$. *Int. J. Algebra*, **6**: 1135-1146.

Terai, N., Hibino, T. 2015. On the exponential Diophantine equation $(12m^2+1)^x + (13m^2-1)^y = (5m)^z$. *Int. J. Algebra*, **9**: 261-272.

Terai, N., Hibino, T. 2017. On the exponential Diophantine equation $(3pm^2-1)^x + (p(p-3)m^2+1)^y = (pm)^z$. *Period. Math. Hung.*, **74**: 227-234.

Uchiyama, S. 1976. On the Diophantine equation $2^x = 3^y + 13^z$. *Math. J. Okayama Univ.*, **19**: 31-38.

Voutier, P.M. 1995. Primitive divisors of Lucas and Lehmer sequences. *Math. Comp.*, **64**: 869-888.

ÖZGEÇMİŞ

Adı Soyadı	:	ELİF KIZILDERE
Doğum Yeri ve Tarihi	:	BURSA 1992
Yabancı Dil	:	İNGİLİZCE
Eğitim Durumu (Kurum ve Yıl)	:	
Lise	:	BURSA CUMHURİYET LİSESİ, 2006-2010
Lisans	:	BURSA ULUDAĞ ÜNİVERSİTESİ, 2012-2016
Yüksek Lisans	:	BURSA ULUDAĞ ÜNİVERSİTESİ, 2016-2019
İletişim(e-posta)	:	elfkzldre@gmail.com

Yayınlar

Kızıldere, E., Soydan, G. 2019. On the exponential Diophantine equation $(5pm^2 - 1)^x + (p(p-5)m^2 + 1)^y = (pm)^z$, yayına sunuldu.

Kızıldere, E., Miyazaki, T., Soydan, G. 2018. On the Diophantine equation $((c+1)m^2 + 1)^x + (cm^2 - 1)^y = (am)^z$. *Turkish J. of Math.*, **42**; 2690-2698.

Bai, H., Kızıldere, E., Soydan, G., Yuan, P. 2019. On the Diophantine equation $(n-1)^x + (n+2)^y = n^z$. *Colloq. Math.*, yayına kabul edildi.

Kızıldere, E., Le, M., Soydan, G. 2019. A note on the ternary purely exponential Diophantine equation $A^x + B^y = C^z$ with $A + B = C^2$, yayına sunuldu.

Kızıldere, E., Soydan, G., Han, Q., Yuan, P. 2019. The shuffle variant of a Diophantine equation of Miyazaki and Togbé, yayına sunuldu.