T.C

SELÇUK ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

BAZI ÖZEL TİP

DIOPHANTINE DENKLEMLERİNİN ÇÖZÜMLERİ

ESRA DEMİRPOLAT

YÜKSEK LİSANS TEZİ

MATEMATİK ANABİLİM DALI

KONYA, 2008

T.C

SELÇUK ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

BAZI ÖZEL TİP

DIOPHANTINE DENKLEMLERİNİN ÇÖZÜMLERİ

ESRA DEMİRPOLAT

YÜKSEK LİSANS TEZİ

MATEMATİK ANABİLİM DALI

Bu tez …./…./…… tarihinde aşağıdaki jüri tarafından oybirliği / oyçokluğu ile kabul edilmiştir.

Prof. Dr. Hasan ŞENAY	**Prof. Dr. Halil ARDAHAN**	**Doç. Dr. Cengiz ÇINAR**
(Danışman)	**(Üye)**	**(Üye)**

ÖZET

YÜKSEK LİSANS TEZİ

BAZI ÖZEL TİP

DIOPHANTINE DENKLEMLERİNİN ÇÖZÜMLERİ

ESRA DEMİRPOLAT

SELÇUK ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

MATEMATİK ANABİLİM DALI

2008, 22 sayfa

Danışman : Prof. Dr. Hasan ŞENAY

Jüri:

Prof. Dr. Hasan ŞENAY   Prof. Dr. Halil ARDAHAN   Doç. Dr. Cengiz ÇINAR

Bu çalışma, sayılar teorisinde önemli bir yeri olan Diophantine denklemleri üzerine hazırlanmıştır. Çalışmanın birinci bölümü Giriş'e ayrılmış, burada kaynak araştırması sonucunda elde edilen bilgilerin ve çözülen denklemlerin özeti verilmiştir.

İkinci bölümde temel tanım ve teoremler verilmiştir. Üçüncü bölümde bazı özel tip diophantine denklemlerinin çözümleri ve kullanılan lemmalar ve teoremler verilmiştir. Dördüncü bölümde araştırma sonucunda elde edilen diophantine denklemleri verilmiştir. Beşinci bölümde ise kaynaklar verilmiştir.

Biz bu çalışmada $x^2+11=y^n$, $x^2+67=y^n$ denklemlerinin x,y,n tamsayıları için çözümlerini $n\geq 3$ olmak üzere bulduk ve $x^2+11^{2k+1}=y^n$ denkleminin tamsayılarda çözümünün olmadığını $n\geq 3$ için gösterdik.

ANAHTAR KELİMELER: Diophantine denklemleri, Cebirsel sayılar, Cebirsel tamsayılar

ABSTRACT

MASTER THESIS

SOULUTIONS OF CERTAIN SPECIFIC TYPE DIOPHANTINE EQUATIONS

ESRA DEMİRPOLAT

SELÇUK ÜNİVERSİTY

GRADUATE SCHOOL OF NATURAL AND APPLİED SCİENCES

DEPARMENT OF MATHEMATİCS

Supervisor: Prof. Dr. Hasan ŞENAY

2008, 22 Page

Jury:

Prof. Dr. Hasan ŞENAY Prof. Dr. Halil ARDAHAN Doç. Dr. Cengiz ÇINAR

This study has been done over Diophantine equations which has a prominent position in number theory. First chapter of the study has been allocated to “Introduction”, here information obtained from the result of resource research and summary of solved equations have been provided.

In the second chapter basic definitions and theorems have been provided. In the third chapter solutions of certain specific type Diophantine equations and lemmas, theorems used have been provided. In the forth chapter Diophantine equations obtained at the result of the research have been provided. The fifth chapter includes resources.

In this study we provided x,y,n solutions of equations $x^2+11=y^n$, $x^2+67=y^n$ for $n\geq3$ in integers and there is no solution for equation $x^2+11^{2k+1}=y^n$ for $n\geq3$ in integers.

Key Words: Diophantine equations, algebraic numbers, algebraic integers

ÖNSÖZ

Bu tez çalışması, Selçuk Üniversitesi Eğitim Fakültesi Orta Öğretim Fen ve Matematik Anabilim Dalı Başkanı Prof. Dr. Hasan ŞENAY danışmanlığında yapılarak, Selçuk Üniversitesi Fen Bilimleri Enstitüsüne Yüksek Lisans tezi olarak sunulmuştur.

Bu çalışma konusunu bana veren ve çalışmam süresince her türlü yardımlarını esirgemeyen değerli hocam Prof. Dr. Hasan ŞENAY'a teşekkür ederim.

İÇİNDEKİLER

1. BÖLÜM

LİTERATÜR ÖZETİ

$X^2+C=Y^n$ Diophantine denkleminin Fermat tarafından bulunan $C=2$ ve $n=3$ oluğunda tek sonucu $X=5$ ve $Y=3$'tür. (COHN 1993)

Genel n için ilk sonuç $C=1$ olduğunda çözümün olmadığını kanıtlayan V.A.Lebesgue'dan gelmektedir.

$C=3$ ve 5 için hiç sonuç olmadığını kanıtlamıştır. (NAGELL 1923)

$C=4$ olduğunda $X=2$ ve $X=11$ olduğunu göstermiştir (NAGELL 1955)

$X^2+3^m=y^n$ denkleminin çözümünün x,y,m pozitif tamsayılar, m tek ve $n\geq 3$ için $m=5+6M$, $x=10.3^{3M}$ $y=7.3^{2M}$ ve $n=3$ değerleri ile yapıldığını gösterdiler (ARIF ve MURIEFAH 1998).

$x^2+5^{2k+1}=y^n$ denkleminin $k\geq 0$ ve x,y tamsayıları için çözümün olmadığını göstermişlerdir (ARIF ve MRIEFAH 1999).

$x^2+q^{2k+1}=y^n$ denkleminin q tek asal, $q\not\equiv 7 (mod\ 8)$, $n\geq 5$ şartını sağlayan tek tamsayı ve n 3'ün katı olmamak üzere, $(n,h)=1$ olduğunda, h: $Q(\sqrt{-q})$cisminde bir sınır sayısı olduğunda , çözüm ikililerinin;

$q=19$, $n=5$, $k=5M$, $x=22434.19^{5M}$, $y=55.19^{2M}$ ve

$$q=341\ ,\ \ n=5\ ,\ k=5M\ ,\ x=275964.341^{5M}\ ,\ \ y=377.19^{2M}$$

olduğunu gösterdiler (ARIF ve MURIEFAH 2002).

$x^2+2^k=y^n$ denkleminin k tek sayı, x ve y pozitif tamsayılar ve $n\geq 3$ için çözümünü yapmışlardır (ARIF ve MURIEFAH 1997).

Biz bu çalışmada $x^2+11=y^n$, $x^2+67=y^n$ denklemlerinin x,y,n tamsayıları için çözümlerini $n\geq 3$ olmak üzere bulduk ve $x^2+11^{2k+1}=y^n$ denkleminin tamsayılarda çözümünün olmadığını $n\geq 3$ için gösterdik.

2. BÖLÜM

CEBİRSEL SAYILAR, CEBİRSEL TAMSAYILAR, DIOPHANTINE DENKLEMLERİ

2.1.Cebirsel Sayılar

Tanım 2.1.1. Katsayılarının hepsi sıfırdan farklı rasyonel sayılar olan

$$P(x)=a_0.x^n+a_1.x^{n-1}+\ldots+a_n$$

biçimindeki polinomu sağlayan gerçek yada karmaşık sayıya cebirsel sayı denir (ŞENAY 2007).

Tanım 2.1.2. Katsayıları Q'da olan ,bir sabitten(yani derecesi 0 olan polinom) farklı $P(x)$ polinomuna , eğer $P(x)$' in $Q[x]$' de kapsanan daha küçük dereceli bölenleri yalnızca sabitler ise indirgenemez denir (ŞENAY 2007).

Tanım 2.1.3. En yüksek dereceli terimin katsayısı bir olan polinoma monik polinom denir (ŞENAY 2007).

Tanım 2.1.4. Bir α cebirsel sayısının sağladığı en küçük dereceli $P(x)$ polinomuna α'nın minimal polinomu denir (ŞENAY 2007).

Lemma2.1.1. Eğer monik $P(x)$ polinomu α cebirsel sayısının minimal polinomu ise , Q rasyonel sayılar cismi üzerinde indirgenemez bir polinomdur.

İspat: İddianın aksine $P(x)$ polinomunun indirgenebilir olduğunu varsayalım. Bu durumda $f(x)$ ve $g(x)$ polinomları $Q[x]$'in pozitif dereceli iki polinomu olmak üzere, $P(x)$ polinomunu $P(x)=f(x).g(x)$ şeklinde yazabiliriz. O zaman bu kabulle $f(\alpha),g(\alpha)\in Q$ olmak üzere $0=P(\alpha)=f(\alpha).g(\alpha)$ ve Q' nun cisim olduğunu göz önüne alırsak, $f(\alpha)=0$ veya $g(\alpha)=0$ elde ederiz. Ancak bu vardığımız her iki sonuç da $f(x)$ ve $g(x)$ polinomlarının derecelerinin $P(x)$'in derecesinden küçük olmaları nedeniyle mümkün değildir (ŞENAY 2007).

2.2. Cebirsel tamsayılar

Tanım 2.2.1. Bir α cebirsel sayısına, katsayıları tamsayı olan

$$P(x)=x^n+a_{n-1}.x^{n-1}+\ldots+a_0$$

monik polinomunun kökü olması durumunda cebirsel tamsayı denir.Yani $P(\alpha)=0$ olacak şekilde tam katsayılı bir $P(x)$ monik polinomu varsa α cebirsel sayısı bir cebirsel tamsayıdır (ŞENAY 2007).

Tüm cebirsel tamsayıların cümlesi, k cebirsel sayı cümlesinin bir alt halkasını oluşturur. Bu halkayı R_k ile belirteceğiz.

Tanım 2.2.2. Bir $\varepsilon\in R_k$ tamsayısı için $1/\varepsilon$ da cebirsel tamsayı ise ε'ya tersinir eleman denir (ŞENAY 2007).

Tanım 2.2.3. $\alpha\in R_k$ elemanına eğer α'nın $R_k$daki her böleni ya kendisinin bir ilgilisi veya tersinir eleman ise indirgenemez denir (ŞENAY 2007).

Tanım 2.2.4. R_k da tersinir olmayan sıfırdan farklı bir π tam sayısına herhangi $\alpha, \beta \in R_k$ tamsayıları için $\pi | \alpha\beta$ olması ya $\pi | \alpha$ yada $\pi | \beta$ olmasını gerektiriyorsa asaldır denir (ŞENAY 2007).

Tanım 2.2.5. Bir R_k halkasına, her $\alpha \in R_k$ tamsayısının sonlu sayıda indirgenemez elemanların çarpımı olarak temsili, çarpanların sırasının ve indirgenemez elemanlarının ilgilileri ile değişimi dışında tek türlü ise, tek çarpanlanma bölgesi denir (ŞENAY 2007).

Teorem 2.2.1. Bir bölgede çarpanlara ayrılışın tek olmasının gerek ve yeter koşulu her indirgenemez elemanın asal olmasıdır (ŞENAY 2007).

Teorem 2.2.2. Herhangi bir α cebirsel sayısı için $c\alpha$ bir cebirsel tamsayı olacak biçimde bir $c \in N$ vardır (ŞENAY 2007).

İspat. α cebirsel sayısının Q üzerinde minimal polinomu,

$P(x)= x^n+a_{n-1}.x^{n-1}+\ldots+a_0$ olsun.

Şimdi $a_i \in Q$ olduğunu göz önüne alırsak,

$c.a_0 = b_0$, $c.a_1 = b_1$, ... , $c.a_{n-1}=b_{n-1} \in Z$ olacak biçimde bir $c \in N$ vardır. (Bunu $P(x)$ polinomunun katsayılarının paydalarının en küçük ortak katı ile bulabiliriz.)

Böylece , $(c\alpha)^n + ,b_{n-1} (c\alpha)^{n-1} +c. b_{n-2}. (c\alpha)^{n-2} + \ldots + c^{n-1} . b_0 = 0$ olmak üzere

$c^n. \alpha^n + c^{n-1}. b_{n-1} \alpha^{n-1} +\ldots.+ c^{n-1} . b_0 = 0$ elde ederiz ki , bu $\beta = c\alpha$ sayısının cebirsel tamsayı olduğunu gösterir.

Tanım 2.2.5. α, β cebirsel tamsayılar olmak üzere $\alpha = \beta . \gamma$ olacak biçimde bir γ cebirsel tamsayısı varsa β cebirsel tamsayısına α cebirsel tamsayısını böler denir ve bu durum $\beta | \alpha$ şeklinde gösterilir. Buna göre $\gamma | \alpha$ ve $\gamma | \beta$ ise λ , μ cebirsel tamsayıları için $\gamma | \lambda \alpha + \mu \beta$ dır (ŞENAY 2007).

2.3. Diophantine Denklemleri

Tanım 2.3.1.

m bir doğal sayı, $a_0, a_1, \ldots a_{m-1}, a_m$ tamsayılar ve $a_0 \neq 0$, $a_m \neq 0$ olmak üzere ,

$a_0 x^m + a_1 x^{m-1} + \ldots + a_{m-1} x + a_m = 0$ (1) şeklinde tamsayı katsayılı denklemleri inceleyelim. Eğer bu (1) denklemini sağlayan bir x tamsayısı varsa; o zaman $\left(a_0 x^{m-1} + a_1 x^{m-2} + \ldots + a_{m-1}\right) x = -a_m$ bulunur. Bu durumda; x tamsayısı a_m tamsayısının bir böleni olmalıdır. Böylece a_m tamsayısı sıfırdan farklı olacağından; a_m tamsayısının sonlu sayıda böleni mevcut olur. Bu durumda (1) denkleminin bütün tamsayı çözümleri sonlu sayıda deneme ile bulunabilir. a_m in bütün bölenlerini (pozitif ve negatif) sırasıyla (1) denkleminde yerine yazarak; bunlardan

(1) denklemini sağlayanları alırız. Eğer $a_m = 0$ ise o zaman, açık olarak $x = 0$ denklemin bir çözümü olur. Bu durumda diğer çözümler;

$$a_0 x^{m-1} + a_1 x^{m-2} + \ldots + a_{m-2} x + a_{m-1} = 0$$

denklemi çözülerek bulunur. Bu denklemin $a_{m-1} \neq 0$ olması durumundaki çözümleri yukarıdaki gibi bulunacağı açıktır.Eğer $a_{m-1} = 0$ ise o zaman denklemimiz $m-2$ dereceden bir denkleme dönüşecektir. Bu şekilde devam edilerek bütün çözümler bulunur (SIRPENSKI 1988).

Tanım 2.3.2 . x , y , z tamsayılar olmak üzere $x^2+y^2=z^2$ denklemine 2 . dereceden üç bilinmeyenli diophantine denklemi denir. Bu denklem Pisagor denklemi olarakta bilinir.

Bu denklemin sonsuz sayıda çözümünün bulunduğunu ilk defa Pisagor verdiği bir formülle ispatlamıştır.

Bu denklem trigonometri ve analitik geometride özel öneme sahiptir. Ayrıca $x=y$ durumu irrasyonel sayıların varlığının en basit ispatıdır (ŞENAY 2007).

Teorem 2.3.1. $x^2+y^2=z^2$ denkleminin, y çift sayı olmak üzere bütün ilkel çözümleri m ve n aralarında asal tamsayılar, $m>n$ ve biri tek diğeri çift olmak üzere,

$$x= m^2- n^2 \ , \ y= 2.m.n \ , \ z= m^2+ n^2 \quad \text{ile verilir.}$$

İspat. $x^2 + y^2 = z^2$ (2) denkleminin bütün primitif çözümleri m, n sayıları ile bulunur(Bazen bu m, n tamsayılarına çözüm üreteçleri de denir). Elbette bunun için $\frac{x+z}{y}$ rasyonel sayısının $\frac{m}{n}$ indirgenemez kesri biçiminde olması yeterlidir.

Şimdi (2) denkleminin bütün primitif çözümlerinin sistematik olarak bir listesini vermek için; m'nin ardışık 2, 3, 4, . . . değerlerine karşılık, m den küçük ve m ile n aralarında asal olmak üzere biri tek iken diğeri çift olacak şekilde n sayılarını seçelim.

m	n	x	y	z	Alan	m	n	x	y	z	Alan	m	n	x	y	z	Alan
2	1	3	4	5	6	7	6	13	84	85	546	10	7	51	140	149	3570
3	2	5	12	13	30	8	1	63	16	65	504	10	9	19	180	181	1710
4	1	15	8	17	60	8	3	55	48	73	1320	11	2	117	44	125	2574
4	3	7	24	25	84	8	5	39	80	89	1560	11	4	105	88	137	4620
5	2	21	20	29	210	8	7	15	112	113	840	11	6	157	132	157	10362
5	4	9	40	41	180	9	2	77	36	85	1386	11	8	57	176	185	5016
6	1	35	12	37	210	9	4	65	72	97	2340	11	10	21	220	221	2310
6	5	11	60	61	330	9	8	17	144	145	1224	12	1	143	24	145	1716
7	2	45	28	53	630	10	1	99	20	101	990	12	5	119	120	169	7140
7	4	33	56	65	924	10	3	91	60	109	2730	12	7	95	168	193	7980

Bildiğimiz gibi $x^2 + y^2 = z^2$ denkleminin bütün doğal sayılardaki çözümlerini elde etmek için, primitif çözümlerin her biri sırasıyla 1, 2, 3, . . . doğal sayılarıyla çarpılmalıdır ve sonra her bir çözümde x ile y nin yerleri değiştirilir. Üstelik $x^2+y^2=z^2$ denkleminin doğal sayılardaki her bir çözümü bu yolla tam olarak bulunur.

$(m^2 - n^2)^2 + (2mn)^2 = (m^2 + n^2)^2$ özdeşliğinden dolayı $x = m^2 - n^2$, $y = 2mn$, $z = m^2 + n^2$ formüllerini $m > n$ şartını sağlayan m, n doğal sayıları için kullanarak $x^2+y^2=z^2$ denkleminin doğal sayılardaki çözümlerini buluruz. Fakat bununla beraber yukarıdaki biçimde x ile y nin yer değiştirmesiyle elde edilen bütün çözümler; $x^2 + y^2 = z^2$ denkleminin doğal sayılardaki bütün çözümlerini vermez. Yani 9, 12, 15 çözümü

$x = m^2 - n^2$, $y = 2mn$, $z = m^2 + n^2$ denklemlerinden elde edilemez.

Çünkü $n < m$ ve m ile n doğal sayı olacak şekilde m ve n bulunamaz. Zira $15 - 1^2 = 14$, $15 - 2^2 = 11$, $15 - 3^2 = 6$ sayılarının hiçbiri bir doğal sayının karesi değildir.

$x^2 + y^2 = z^2$ denkleminin bütün çözümleri; m,n,k doğal sayılar ve $n < m$ olmak üzere;

$$x = (m^2 - n^2)k,\ \ y = 2mnk,\ \ z = (m^2 + n^2)k$$

ifadelerinden ve x ile y ler yer değiştirilerek elde edilir. Bununla beraber verilen bu formüllerde bazen farklı m, n,k doğal sayı değerleri için aynı sayılar elde edilebilir.

Örneğin; yukarıda verilen formüllerde hem $m = 2$, $n = 1$, $k = 4$ değerleri, hem de $m = 4$, $n = 2$, $k = 1$ değerleri için aynı 12, 16, 20 üçgenini elde ederiz. Yine yukarıda verilen formüllerde hem $m = 8$, $n = 4$, $k = 1$; hem $m = 4$, $n = 2$, $k = 4$; hem de $m = 2$, $n = 1$, $k = 16$ değerleri için aynı 48, 64, 80 üçgeni elde edilir. Yukarıdaki tabloda verilen çözümlerden ilki (2) denkleminin x, y, z doğal sayılarında mümkün olan en küçük çözümüdür. Üstelik bu çözümdeki x, y, z sayıları doğal sayılardır. Bu değerlerin; üzere $x^2+y^2=z^2$ denkleminin ardışık doğal sayılardan ibaret tek çözümü olduğunu ispatlamak zor değildir. Gerçekten eğer ardışık n-1, n, n+1 doğal sayıları

$(n-1)^2 + n^2 = (n+1)^2$ denklemini sağlıyor ise o zaman $n^2 = 4n$ elde edilir ki buradan $n = 4$ elde edilir ki o zaman 3, 4, 5 üçgenine ulaşılır ki bu da aranandır.

Kolayca ispat edilebilir ki $3^n + 4^n = 5^n$ denkleminin $n = 2$ değeri dışında doğal sayılarda çözümü yoktur. Doğru olduğunu gösterelim; $n = 1$ için; $3+4 > 5 \Rightarrow 3^1+4^1 > 5^1 \Rightarrow 3^1+4^1 \neq 5^1$ olur ki $n = 1$ için sağlanmaz. $n = 2$ için; $3^2+4^2 = 5^2$ olduğunu biliyoruz.

$n > 2$ *için* $5^n = 5^2\, 5^{n-2} = 3^2.5^{n-2} + 4^2.5^{n-2} > 3^2.3^{n-2} + 4^2.4^{n-2} = 3^n + 4^n$ olur ki böylece $n > 2$ için $5^n \neq 3^n + 4^n$ dir.

Fermat'ın ikinciden daha yüksek dereceden 3 bilinmiyenli denklemlerin çözümünde kullandığı ' sonsuz iniş metodu' nun bir uygulaması aşağıdaki teoremde verilmiştir. Bu metod; bir tek $(x,y,z)\in Z^3$ pozitif çözüm üçlüsünün varlığından hareketle z bileşeni durmadan azalan sonsuz sayıda $(x,y,z)\in Z^3$ çözümlerinin bir dizisini elde etmeye dayanır. Sonunda bu çözümler dizisinin üçüncü $z_0,z_1,z_2,\ldots , z_n,\ldots$ bileşenlerinin $z_0>z_1>z_2>\ldots > z_n>\ldots$ şeklinde pozitif tamsayıların azalan bir sonsuz dizisi elde edilir ki bu, İyi Sıralama Prensibi ile çeliştiğinden, istediğimiz sonuç kurulmuş olur (SIRPENSKI 1988).

Teorem 2.3.2. $x^4+y^4=z^2$ Fermat denkleminin $x,y,z\neq 0$ olan hiçbir tamsayı (x,y,z) çözümü yoktur.

İspat. Bu denklemin $(x_0,y_0,z_0)\neq(0,0,0)$ olan bir çözümünün bulunduğunu varsayalım. Böyle bir $(x,y,z)\in Z^3$ çözümünde x,y veya z nin işaretinin değişimi yeni bir çözüm üreteceğinden x,y,z bileşenlerinin pozitif olduğunu varsayabiliriz. Şimdi z_0 bileşenini denklemin diğer (x,y,z) çözümlerinin z'leri arasında en küçük olacak şekilde seçelim. Ayrıca bu sayıların karşılıklı olarak aralarında asal olduğunu da kabul edebiliriz. Gerçekten bir (x,y,z) pozitif çözümünde $(x,y)>1$ olsaydı, Aritmetiğin Temel Teoremi gereği *x ve y* nin ikisini de bölen p gibi bir asal sayı bulunacaktı. Bu durumda

$p^4|x^4+y^4$ *den,* $p^4|\, z^2$ ve sonuçta $p^2|z$ olduğundan,

$$(x/p)^4+(y/p)^4=(z/p^2)^2$$

bulunur. Şimdi bu elde edilen yeni (x/p, y/p, z/p^2) çözüm üçlüsünün üçüncü bileşeni için $z/p^2<z$ olduğundan, bu sonuç (x, y, z) çözümünde z'nin en küçük seçilmesiyle çelişir ki, bu da $(x,y)=1$ olmasını gerektirir. Böylece $(x_0^2)^2+(y_0^2)^2=z_0^2$ eşitliğinden (x_0^2, y_0^2, z_0) ilkel Pisagor üçlüsünün **:** $x^4+y^4=z^2$ denkleminin bir çözümü olduğunu söyleyebiliriz. O halde x_0^2 ve y_0^2 aynı anda tek ve aynı anda çift olamazlar. Buna göre x_0^2 nin tek ve y_0^2 nin çift olduğunu kabul edelim. Bu durumda Teorem 2.3.1 e göre $x_0^2=a^2-b^2$, $y_0^2=2ab$, $z_0= a^2+b^2$ olacak biçimde a ve b gibi aralarında asal $(a>b)$ ve her ikisi tek veya çift olmayan tamsayılar vardır. Böylece $x_0^2=a^2-b^2$ den (x_0 , b,a) nın x_0 tek olmak üzere bir ilkel pisagor üçlüsü olduğu sonucuna varılır.O zaman yine aynı sebeple

$$x_0^2= r^2-s^2 , b=2rs , a= r^2+s^2$$

olacak şekilde $(r,s)=1$ olan r,s tamsayıları vardır. Şimdi r,s ve a karşılıklı aralarında asal olduğundan $y^2=2ab=4ars$ eşitliği ancak ve ancak r,s ve a nın kendilerinin bir tamkare olmaları durumunda mümkündür. O halde $r=m^2$, $s=n^2$ ve $a=t^2$ olacak biçimde m,n ve t tamsayıları vardır.Öte yandan $a= r^2+s^2$ eşitliğinden , $m^4+n^4=t^2$ bulunur.

$$z_0=a^2+b^2> a^2=t^4 \text{ olup buradan da}$$

$$0<t=\sqrt{a}<\sqrt[4]{z}<z_0$$

elde edilir. Öte yandan $m^4+n^4=t^2$ eşitliği (m,n,t) üçlüsünün **:** $x^4+y^4=z^2$ nin $t< z_0$ olan bir çözümü olduğunu gösterir.

Oysa biz (x,y,z) çözümünde $z_0\in \mathbb{Z}^+$ ı en küçük seçtiğimizden bu çelişkidir.bu çelişki teoremi ispatlar (ŞENAY 2007).

3. BÖLÜM

BAZI ÖZEL TİP DIOPHANTİNE DENKLEMLERİNİN ÇÖZÜMÜ

$x^2+c=y^n$ Denklemi

Ön Hazırlıklar. Bu denklemi $Q(\sqrt{-c})$ cisminde tek çarpanlanmanın geçerli olması durumunda çözmek mümkün olacaktır.n=p'lerin tek asal olması genelliği etkilemez.

Gerçekten bu denklem , $(x+\sqrt{-c}, x-\sqrt{-c})=1$ olmak üzere idealler yardımıyla,

$$(x+\sqrt{-c}).(x-\sqrt{-c})= y^p$$

şeklinde çarpanlarına ayrılabilecektir. Buradan a ve b tamsayıları için

(3.1) $\pm x+\sqrt{-c} = (a+b\sqrt{-c})^p$ olur. Bu durumda x, $y=a^2+b^2c$ ile bir çözüm olacaktır. Burada (3.1)'in bir çözüm için gerekli olmadığına ilgi çekilmelidir. Bu yalnızca aşağıdaki durumlarda oluşur.

1. $c \not\equiv 3 (mod\ 4)$
2. Tersinir elemenlardan bir problem ortaya çıkmamalı
3. Çalıştığımız $Q(\sqrt{-c})$ cismi tek çarpanlanma bölgesi olmalı
4. c kare çarpansız pozitif tamsayı olmalı
5. $\pm x+\sqrt{-c}$ terimlerinin ortak bir çarpanı yoktur.

İlk olarak, eğer $c \equiv 3$ (mod4) ise (3.1)'e ilavaten,

(3.2) $\pm x+\sqrt{-c} = (1/2.(A+B\sqrt{-c}))^p$ ile birlikte $y=1/4.(A^2+B^2.c)$ elde ederiz. Bu sadece $p=3$ durumunda oluşur. Gerçekten (3.2)'deki sanal kısımları eşitlersek

$$2^p=B.\sum_{r=0}^{p-1/2} C(p,2r+1).A^{p-2r-1}.(-B^2.c)^r$$

elde edilir ve böylece B tek , B=± 1 dir. Şu halde,

$$\pm 2 \equiv \pm 2^p \equiv (-c)^{p-1/2} \equiv (-c/p) \equiv 0, \pm 1 (\mathrm{modp})$$

ise sonuçta $\pm 8 = 3A^2 - c$'yi gerektirir ki bu bize aşağıdaki lemmanın ispatını verir.

Lemma3.1.1. (3.2) durumu sadece ve sadece $c=3A^2 \pm 8$ durumunda oluşur ve sadece $p=3$ ve $x=A^2-3A$ sonucunu verir.

Daha sonra tersinir elemanlarla ilgili soruyu göz önüne alabiliriz. .Eğer $p \neq 3$ ise cisimdeki tersinir elemanlar c'nin değeri ne olursa olsun (3.1)'deki kuvvetler içinde kaybolur. Hatta $p=3$ bile bu olsa hala bu her zaman söz konusudur. Yeter ki $c=3d^2$ olmasın ve tersinir elemanlar yalnızca ± 1veya $\pm i$ dir. Bununla birlikte $c=3d^2$ ise altı tane tersinir eleman vardır. Bunlar ± 1, $\pm w$, $\pm w^2$ dir.(3.1) ve (3.2)'den ayrı olarak ,bu durum bizi

(3.3) $\pm x+d\sqrt{-3} = w.(1/2.(A+Bd(\sqrt{-3})))^3$, $A \equiv B(mod\ 2)$'ye götürür.

Lemma 3.1.2. (3.3) durumu için gerek ve yeter koşul $c=48.D^6$, $X=4D^3$ $p=3$ olmasıdır (COHN 1993).

Teorem 3.2.1.$C>0$ olsun.$C=cd^2$,$c \not\equiv 7(mod 8)$ .Eğer p bir tek asal ve $x^2+C=y^P$ için x ve y'nin ikisi de pozitif tamsayılar,

1. a ve b tamsayıları ile b/d mevcut olsun. $y=a^2 + b^2c$ *ve* $\pm x+\sqrt{-c} =(a+b\sqrt{-c})^p$, veya

2. $c\equiv 3(mod\ 8)$, $p=3$ ve A ve B tek tamsayıları ile B/d mevcut olsun. $y=1/4.(A^2+B^2c)$,

$\pm x+d\sqrt{-c} =1/8. (A+B\sqrt{-c})^3$ veya

3. p/h ,$Q(\sqrt{-c})$cisminde bir sınır sayısı veya

4. $C=3A^2 \pm 8$,$p=3$,$x=A^3 \pm 3A$ veya

5. $C=48 D^6$,$p=3$,$x=4 D^3$ tür (COHN 1993).

(3.1)için işlem. (3.1) dan sanal kısımları eşitlersek ,

$$1= b. \sum_{r=0}^{p-1/2} C(p,2r+1).a^{p-2r-1}.(-b^2.c)^r$$

ve böylece $b=\pm 1$ dir.

(3.4) $\pm 1=. \sum_{r=0}^{p-1/2} C(p,2r+1).\ a^{p-2r-1}.(-c)^r$ ve buradan şu sonuçlar ortaya çıkar.

(3.4) den a ve c zıt işaretli olmalıdır. Eğer a ve c den her ikisi de çift ise o zaman (3.4) denkleminin sağ tarafı çift olmalıydı, oysa eğer a ve c nin her ikisi de tek ise o zaman sağlar.

$$\pm 1= \sum_{r=0}^{p-1/2} C(p,2r+1) =2^{p-1} \equiv 0\ (mod\ 2)$$ ’ yi elde ederiz.

4. BÖLÜM

4.1. $x^2+11=y^n$ DIOPHANTINE DENKLEMİNİN ÇÖZÜMÜ

Bu bölümde $x^2+11=y^n$ denklemini x,y,n tamsayıları için, n≥3 olmak üzere çözdük. Denklemin çözümü $(11,x)=1$ ve $11|x$ gibi iki ana duruma ayrılmıştır.

Durum 1. $(11,x)=1$ olsun. $n=p$ ler tek asal sayı olduğunda genelliği bozmamış oluruz. Böylece $x^2+11=y^p$ denklemi elde edilir.

COHN'un 1993'deki makalesinde verdiği teorem 1'e göre iki durum vardır. Bunlar;

$y= a^2+11b^2$ olduğunda,

$$x+\sqrt{-11}=(a+b\sqrt{-11})^p \qquad (4.1.1)$$

$y= a^2+11b^2/4$, a ve b tamsayılar olduğunda,

$$x+\sqrt{-11}=\left(\frac{a+b\sqrt{-11}}{2}\right)^3 \quad (a\equiv b\equiv 1 \ (mod\ 2)) \qquad (4.1.2)$$

(4.1.1) denkleminde $y= a^2+11b^2$ ve y tek olduğunda, a ve b den biri tek diğeri çifttir. Sanal kısımları eşitleyerek ;

$$1 = b.\sum_{r=0}^{p-1/2} C(p,2r+1).a^{p-2r-1}.(-11b^2)^r$$

olur.

Buradan b tek ise $b=\pm 1$ dir. Böylece,

$$\pm 1= \sum_{r=0}^{p-1/2} C(p,2r+1).a^{p-2r-1}.(-11)^{r} \text{ olur.}$$

Bu COHN'un 1993'deki makalesinde verdiği lemma 4 ve lemma 5'e göre imkansızdır.

Şimdi denklem (4.1.2)' yi göz önüne alalım. Sanal kısımları eşitleyerek;

$$8=b.(3a^2-11b^2) \text{ elde ederiz..} \qquad (4.1.3)$$

$b=\pm 1$ olması durumunda $\pm 8=3a^2-11$ elde edilir.

Buradan elde edilen tek çözüm $a=\pm 1$ ve böylece $y=\dfrac{a^2+11b^2}{4}$ olduğundan $y=3$ olur ki buradan,

$$x=\left|\frac{a^3-33ab^2}{8}\right|=\left|\frac{-1-33.(-1).1}{8}\right|=4$$

bulunur.

Durum 2. $11|\ x$ olsun. Dolayısıyla $11|\ y$ olur. $u>0$, $v>0$ ve $(11,X)=(11,Y)=1$ olduğunda,

$x=11^{u}.X$ ve $y=11^{v}.Y$ olduğunu varsayalım. Bu durumda denklemimiz,

$$11^{2u}.X^{2}+11=11^{nv}.Y^{n} \text{ şekline dönüşür.}$$

$min\ (2u,1,nv)=1$ olduğundan 11'i denklemde sadeleştirirsek $11^{2u-1}X^{2}+1=11^{nv-1}.Y^{n}$ elde edilir. Bu denklemi mod 11'de düşünecek olursak, $nv-1=0$ elde edilir ki böylece n tek ve $n=1$ olur bu $n\geq 3$ kabulümüzle çelişir ki bu da ispatı tamamlar.

4.2. $x^2+11^{2k+1}=y^n$ DIOPHANTİNE DENKLEMİNİN ÇÖZÜMÜ

$x^2+11^{2k+1}=y^n$ denkleminin çözümü k=0 için bölüm (4.1)'de verilmiştir. Bütün k>0 değerleri için x,y,n tamsayılar ve $n\geq 3$ olmak üzere denklemin çözümünün olmadığını göstereceğiz.

$(11,x)=1$ ve $11|\,x$ gibi iki ana durumu göz önüne almamız gerekir.

Durum 1. $(11,x)=1$ olsun.$n=p$'ler tek asal sayı olduğunda genelliği bozmamış oluruz. COHN'un 1993'deki makalesinde verdiği teorem 1'e göre iki durum vardır.

Bunlar;

$y=a^2+11b^2$ olduğunda,

$$x+11^k\sqrt{-11}=(a+b\sqrt{-11})^p \qquad (4.2.1)$$

$y=a^2+11b^2/4$, a ve b tamsayılar olduğunda ,

$$x+11^k\sqrt{-11}=\left(\frac{a+b\sqrt{-11}}{2}\right)^3 \quad (a\equiv b\equiv 1\ (mod\ 2)) \qquad (4.2.2)$$

(4.2.1) denkleminde $y=a^2+11b^2$ ve y tek tamsayı olduğunda a ve b den biri tek diğeri çifttir. Sanal kısımları eşitleyerek ;

$$11^k = \quad b.\sum_{r=0}^{p-1/2} C(\,p,2r+1\,).a^{\,p-2r-1}.(-11b^2)^r \text{ böylece } b \text{ tektir.}$$

11, x'i bölmediğinden $\sum$ daki ifadeyi de bölemez. Buradan $b=\pm\ 11^k$ elde ederiz.

Böylece,

$$\pm 1= \sum_{r=0}^{p-1/2} C(p,2r+1)\,.a^{p-2r-1}.(-11^{2k+1})^{r}$$

denklemini elde ederiz. COHN'un 1993'deki makalesinde verdiği Lemma 4 ve 5'den her iki işaretin varlığı imkansızdır. Böylece çözümlerin olmadığı iddiamız güçlenmiştir.

Denklem (4.2.2)'yi düşünelim.Sanal kısımları eşitlersek ,

$$8.11^{k}=b.(3a^{2}-11b^{2}) \qquad (4.2.3)$$

elde edilir. (4.2.3)'de $b=\pm 1$ ise $\pm 8.11^{k}=3a^{2}-11$ olur.Buradan,

$$11.(\pm 8.11^{k-1}+1)= 3a^{2}$$

olur ki bu imkansızdır.

Durum 2. $11| x$ olsun. Buradan $11| y$ dir. $u>0$, $v>0$ ve $(11,X)=(11,Y)=1$ olduğunda $x=11^{u}.X$ *ve* $y=11^{v}.Y$ olsun. Buradan, $11^{2u}.X^{2}+11^{2k+1}=11^{nv}.Y^{n}$ de üç olasılık vardır.

1. $2u=min(2u,2k+1,nv)$ olsun. 11^{2u}' yu denklemde sadeleştirirsek,

$X^{2}+11^{2k-2u+1}= 11^{nv-2u}.Y^{n}$ elde edilir.Buradan mod 11'e göre $nv-2u=0$ sonucunu çıkarırız. $X^{2}+11^{2.(k-u)+1}=Y^{n}$ olur ki durum 1'e göre bu imkansızdır.

2. $2k+1=min(2u,2k+1,nv)$ olsun. 11^{2k+1}'i denklemde sadeleştirirsek,

$11^{2u-2k-1}.X^{2}+1= 11^{nv-2k-1}.Y^{n}$ olur.Buradan $11.(11^{u-k-1}.X)^{2}+1= 11^{nv-2k-1}.Y^{n}$ elde edilir.*Mod* 11'den $nv-2k-1=0$ olur.Böylece $11.(11^{u-k-1}.X)^{2}+1= Y^{n}$ olur ki $n\geq 3$ için bu imkansızdır. (NAGELL 1955)

3. $nv=min(2u,2k+1,nv)$ olsun. 11^{nv}'yi denklemde sadeleştirirsek,

$11^{2u\text{-}nv}.X^2+11^{2k+1-nv} = Y^n$ olur. Bu durumda $(11,Y)=1$ olduğundan $2u\text{-}nv=0$ veya $2k+1\text{-}nv=0$ olmalıdır ki 1 ve 2'de bunun imkansız olduğu açıklanmıştır.Bu da ispatı bitirir.

4.3. $x^2+67=y^n$ DIOPHANTINE DENKLEMİNİN ÇÖZÜMÜ

Bu bölümde $x^2+67=y^n$ denklemini x,y,n tamsayılar için, $n\geq 3$ olmak üzere çözdük. Denklemin çözümü $(67,x)=1$ ve $67| x$ gibi iki ana duruma ayrılmıştır.

Durum 1. $(67,x)=1$ olsun.$n=p$ ler tek asal sayı olduğunda genelliği bozmamış oluruz.Böylece $x^2+67=y^p$ denklemi elde edilir.

COHN'un 1993'deki makelesinde verdiği Teorem1'e göre iki durum vardır.Bunlar,

y= a^2+67b^2 olduğunda,

$$x+\sqrt{-67}=(a+b\sqrt{-67})^p \qquad (4.4.1)$$

$y=a^2+67b^2/4$,a ve b tamsayılar olduğunda,

$$x+\sqrt{-67}=\left(\frac{a+b\sqrt{-67}}{2}\right)^3 \quad (a\equiv b\equiv 1 \ (mod\ 2)) \qquad (4.4.2)$$

Durum 1 de y= a^2+67b^2 olduğunda; y tek olduğundan, a ve b den biri tek diğeri çifttir. (4.4.1) denklemindeki sanal kısımları eşitleyerek,

$$1 = \quad b.\sum_{r=0}^{p-1/2} C(\,p,2r+1\,).a^{\,p\text{-}2r\text{-}1}.(\text{-}67b^2)^r$$

olur. Buradan b tek olduğundan $b=\pm 1$ dir.Böylece,

$$\pm 1= \quad \sum_{r=0}^{p-1/2} C(\,p,2r+1\,).a^{p\text{-}2r\text{-}1}.(\text{-}67)^{r} \text{ olur.}$$

Bu, COHN,1993'deki Lemma 4 ve 5'den imkansızır. Şimdi (4.3.2)'yi düşünelim.

Sanal kısımları eşitleyerek,

$$8=b.(3a^2\text{-}67b^2) \text{ olur.}$$

$b=\pm 1$ olması durumunda $\pm\ 8=3a^2\text{-}67$ elde edilir.

Buradan elde edilen tek çözüm $a=\pm 5$ ve böylece $y=\dfrac{a^2+67b^2}{4}$ olduğundan y=23

olur ki buradan,

$$x=\left|\frac{a^3-201ab^2}{8}\right|=\left|\frac{5^3-201.5.1}{8}\right|=110$$

bulunur.

Durum 2. 67| x olsun.Dolayısıyla 67| y olur. $u>0,\ v>0$ ve $(67,X)=(67,Y)=1$

olduğunda $x=67^u.X$ ve $y=67^v.Y$ olduğunu varsayalım. Bu durumda denklemimiz,

$$67^{2u}.X^2+67=67^{nv}.Y^n$$

şekline dönüşür.

$min(2u,1,nv)=1$ olduğundan 67'yi denklemde sadeleştirirsek,

$$67^{2u\text{-}1}\,X^2+1=67^{nv\text{-}1}.Y^n$$

elde edilir.Bu denklemi *mod* 67'de düşünecek olursak, nv-1=0 elde edilir ki böylece n tek ve n=1 olur ki bu $n \geq 3$ kabulümüzle çelişir bu da ispatı tamamlar.

5.KAYNAKLAR

S.A. ARIF AND F.S.A MURIEFAH, 1998 J.Math, Scı Vol.21 No 3.619-620 On The Dıophantıne Equatıon $X^2+3^m=Y^n$

S.A. ARIF AND F.S.A MURIEFAH, 1997 J.Math, Scı Vol.20, No 2 ,299-304 On The Dıophantıne Equatıon $x^2+2^k= y^n$

S.A. ARIF AND F.S.A MURIEFAH,1999 Indıan J. Pure Appl. Math.30(3) 229-231, On The Dıophantıne Equatıon $x^2+5^{2k+1} = =y^n$

S.A. ARIF AND F.S.A MURIEFAH, 2002 Journel Of Number Theory 95.95-100, On The Dıophantıne Equatıon $x^2+q^{2k+1} =y^n$

YANN BUGEEAUD, 1997 On The Diophantine Equation $X^2-P^m=Y^n$

J.H.E COHN, 1993 Acta Arıthmetıca Lxv.4 ,$x^2+C=y^n$ Dıophantıne Equatıon

J.H.E COHN, 1993 Glasgow Math J.35.203-206 The Dıophantıne Equatıon $x^2+3=y^n$

K. CHAO, 1964 Scı.Sınıca (Notes) 14 ,474-460 The Diophantine Eqution $x^2=y^n+1, xy\neq 0$

L.EULER Algebra ,Vol 2. The Dıophantıne Equatıon $x^2+C= y^n$ (C=1)

W. LJUNGGREN, 1963 On The Dıophantıne Equatıon $Cx^2+D= y^n$

MAOHUA LE ,1995 On The Dıophantıne Equatıon $x^2 +7= y^n$

NAGELL, 1955 Contrıbutıons To The Theory Of A Category Of Dıophantıne Equatıons Of The Second Degree Wıth Two Unknows, Nova Acta Reg. Soc. Upsal. Iv. Ser, 16, Uppsala, P.1-38

B. POONEN (BERKELEY,CALIF), 1998 Acta Arıthmetıca LXXXVI , On The Dıophantıne Equatıon $x^n + y^n = z^m$

N. TERAI, 1993 The Diophantine Eqution $X^2 + Q^M = P^N$

W. SIRPENSKI, 1988 Elementary Theory Of Numbers, Pwn – Polish Scıentıfıc Publıshers

H. ŞENAY, 2007 Sayılar Teorisi Dersleri,241-287,435-498