BAZI DİOPHANTİNE DENKLEMLERİ ÇÖZMEK İÇİN ELEMENTER METOTLAR VE BUNLARIN UYGULAMALARI

Caner AĞAOĞLU

T.C
ULUDAĞ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BAZI DİOPHANTİNE DENKLEMLERİ ÇÖZMEK İÇİN ELEMENTER METOTLAR VE BUNLARIN UYGULAMALARI

Caner AĞAOĞLU

Yrd. Doç. Dr. Musa DEMİRCİ
(Danışman**)**

YÜKSEK LİSANS TEZİ
MATEMATİK ANABİLİM DALI

BURSA – 2015

TEZ ONAYI

Caner AĞAOĞLU tarafından hazırlanan ‘‘Bazı Diophantine Denklemleri Çözmek için Elementer Metotlar ve Bunların Uygulamaları’’ adlı tez çalışması aşağıdaki jüri tarafından oy birliği/oy çokluğu ile Fen Bilimleri Enstitüsü Matematik Anabilim Dalı’nda **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Danışman **:**Yrd. Doç. Dr. Musa DEMİRCİ

Üye **:**Prof. Dr. İsmail Naci CANGÜL İmza
Uludağ Üniversitesi Fen Edebiyat Fakültesi
Matematik Anabilim Dalı

Üye **:**Yrd. Doç. Dr. Musa DEMİRCİ İmza
Uludağ Üniversitesi Fen Edebiyat Fakültesi
Matematik Anabilim Dalı

Üye **:**Doç. Dr. Sebahattin İKİKARDEŞ İmza
Balıkesir Üniversitesi Fen Edebiyat Fakültesi
Matematik Anabilim Dalı

Yukarıdaki sonucu onaylarım

Prof. Dr. Ali Osman DEMİR

Enstitü Müdürü

../../….(Tarih)

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 yapmadığıma,
- ve bu tezin herhangi bir bölümünü bu üniversite veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı,

beyan ederim.

../../….

İmza

Caner AĞAOĞLU

ÖZET

Yüksek Lisans Tezi

BAZI DİOPHANTİNE DENKLEMLERİ ÇÖZMEK İÇİN ELEMENTER METOTLAR VE BUNLARIN UYGULAMALARI

Caner AĞAOĞLU

Uludağ Üniversitesi
Fen Bilimleri Enstitüsü
Matematik Anabilim Dalı

Danışman: Yrd. Doç. Dr. Musa DEMİRCİ

Diophantine denklemleri katsayıları tamsayılar olan iki yada daha fazla değişkenli denklemlerdir. Genel olarak bu denklemleri Lineer ve Üstel Diophantine Denklemleri olarak iki farklı şekilde sınıflandırabiliriz.

Literatürde Üstel Diophantine denklemleriyle ilgili birçok makale bulunmaktadır. Bu çalışmada Fermat'nın son teoremi olarak bilinen $x^n + y^n = z^n$ Diophantine denkleminden yola çıkılarak

$$x^n + py^n = p^2 z^n$$

Diophantine denkleminin p sayısının asal, x, y ve z lerin pozitif tamsayılar $(n \geq 3)$ olduğu durumda aşikâr olan çözümler dışında başka çözümlerinin olmadığı literatürdeki sonuçlar ve Fermat'nın sonsuz indirgeme metodu yardımıyla yeniden gösterilmeye çalışıldı. Bu metotda pozitif tamsayılar kümesinin özellikleri ve bölünebilme kurallarından faydalanılarak mümkün olan en kısa yoldan çözüme ulaşılmaya çalışıldı.

ANAHTAR KELİMELER: Diophantine denklemleri, çözüm metotları,

2015, vi + 35 sayfa

ABSTRACT

MScThesis

Elementary Methods for Solving Some Diophantine Equations and Their Applications

Caner AĞAOĞLU

Uludağ University
Graduate School of Natural and Applied Sciences
Department of Mathematic

Supervisor: Asst. Prof. Dr. Musa DEMİRCİ

Diophantine equations are a kind of equation with two or more variables the coefficients of which are integers. In general they are classified into two groups: linear and exponential Diophantine equations.

In the literature there are many papers about exponential Diophantine equations. One of the most popular problem is known as Fermat's Last Theorem which states that whether the equation $x^n + y^n = z^n$ where $n \geq 3$ and x, y, z and n are integers has got any nontrivial integer solutions or not. In this work, we considered a special form of the exponential Diophantine equation which is

$$x^n + py^n = p^2 z^n$$

where p is prime and x, y, z are non-negative integers. In general form of we used Fermat's Method of Infinite Descent (FMID) to determine the existence of solutions.

Key words: Diophantine equations, solution methods,

2015, vi+ 35 pages

TEŞEKKÜR

Eğitim hayatım boyunca gerek maddi gerekse manevi hiçbir desteğini benden esirgemeyen başta aileme ve üzerimde büyük emeği bulunan rahmetli enişteme; ayrıca tezimi tamamlamam konusunda yardımları ve psikolojik desteğiyle sürekli yanımda olan kız kardeşime sonsuz teşekkür ve şükranlarımı iletirken, yüksek lisans eğitimim sırasında çalışmalarımın her aşamasında öneri, bilgi ve yardımlarını benden esirgemeyerek daha iyiye yöneltmeye çalışan ve tüm bu süreç boyunca her anlamda bana ışık tutan başta danışman hocam Sayın Yrd. Doç. Dr. Musa DEMİRCİ' ye ve diğer tüm hocalarıma saygı ve sevgilerimle teşekkür ederim.

Caner AĞAOĞLU

../../….

İÇİNDEKİLER

Sayfa

SİMGELER ve KISALTMALAR DİZİNİ

Simgeler	Açıklama
$\mathbb{Z}$	Tamsayılar
$\mathbb{Z}^+$	Pozitif Tamsayılar
$\mathbb{Z}^{\boldsymbol{n}}$	Tamsayıların n. Kuvveti
$\mathbb{Q}$	Rasyonel Sayılar
$\mathbb{Q}(t)$	Genişletilmiş Rasyonel sayılar cismi

Kısaltmalar	Açıklama
FMID	Fermat'nın sonsuz indirgeme metodu

ÇİZELGELER DİZİNİ

Sayfa

1.GİRİŞ

1.0. Ön Bilgiler

İskenderiye'li Diophantus cebirin babası olarak tanımlanır. Ayrıca cebir denklemleri ve sayılar teorisi üzerine olan Arithmatica kitabının da yazarıdır. Değişkenleri sadece tamsayılar olan ve kendi adını taşıyan denklemlere de Diophantine denklemleri (Diophantine polinom denklemleri) denir. Diophantus'un hayatı ile ilgili çok az bilgiye sahip olmakla birlikte hangi dönemde yaşadığıyla ilgili yapılan çalışmalar sadece 500 yıllık bir döneme indirgenebilmiştir.

M.Ö. 2000'li yıllarda bile $x^2 + y^2 = z^2$ denklemini gerçekleyen (x, y, z) sıralı tamsayı üçlülerinden bazıları Babil'li matematikçiler tarafından bilinmekteydi. Bu denklemler üzerindeki ilk sistematik çalışmaların Diophantus ile başladığı düşünülmektedir. Bu yüzden bu denklemlere İskenderiye'li matematikçi Diophantus'un ismi verilmiştir.

Diophantus'un Mezopotamya matematiğinden geniş ölçüde etkilenmiş olduğunu söyleyebiliriz. Bu denklemin sonsuz tane çözümünün olduğu ilk olarak Pisagor tarafından ispatlanmıştır. 1636 yılında Fermat, Fermat'nın son teoremi olarak bilinen ünlü teorisini ortaya koymuş ve bu teorinin ispatlanması için oldukça fazla sayıda matematikçi çalışmış, son olarak 1995 yılında A. Wiles tarafından 109 sayfalık bir makale halinde tam olarak çözüme kavuşturulmuştur.

$$a_0x^n + a_1x^{n-1}y + a_2x^{n-2}y^2 + \cdots + a_ny^n = \mathrm{c}$$

denklemi üzerinde değişik yöntemler kullanılarak tamsayılarda çözümlerin bulunması üzerindeki çalışmalar 1800'lü yıllarda A. Thue ile başlamış, E. Landau ile devam etmiş ve literatürden görüleceği gibi günümüze kadar gelmiştir (Çenberci 2009). Ele aldığımız problemle ilgili son yıllarda yayınlanmış ve denklemlerin çözümünün olup olmadığını, eğer varsa da bu çözümlerin neler olduğunu ele alan bir kaç makaleye örnek olarak, “The Diophantine Equation $x^2 + 11^m = y^n$ (Soydan ve ark. 2009)”, “On The Diophantine Equation $x^2 + 5^a 11^b = y^n$ (Cangül ve ark. 2010)”, “On The Diophantine Equation $x^2 + 2^a 3^b 11^c = y^n$ (Cangül ve ark. 2013)” ve “On a Diophantine Equation (Luca 2000)” verilebilir.

1.1. Diophantine Denklemleri

n bir doğal sayı, a_0, a_1, a_2 ... a_{n-1}, a_n tamsayılar ve $a_0 \neq 0$, $a_n \neq 0$ olmak üzere,

$$a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_{n-1}x + a_n = 0 \tag{1.1.1}$$

şeklinde tamsayı katsayılı denklemleri inceleyelim. Eğer bu (1.1.1) denklemini sağlayan bir x tamsayısı varsa; o zaman

$$(a_0x^{n-1} + a_1x^{n-2} + \ldots + a_{n-1})x = -a_n$$

bulunur. Bu durumda; x tamsayısı a_n tamsayısının bir böleni olmalıdır. Böylece a_n tamsayısı sıfırdan farklı olacağından; a_n tamsayısının sonlu sayıda böleni mevcut olur. Bu durumda (1.1.1) denkleminin bütün tamsayı çözümleri sonlu sayıda deneme ile bulunabilir. a_n'in bütün bölenleri (pozitif ve negatif) sırasıyla (1.1.1) denkleminde yerine yazarak; bunlarda (1.1.1) denklemini sağlayanları alırız. Eğer $a_n = 0$ ise o zaman, açık olarak $x = 0$ denklemin bir çözümü olur. Bu durumda diğer çözümler;

$$a_0x^{n-1} + a_1x^{n-2} + \ldots + a_{n-1} = 0$$

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

Tanım 1. 1. 1 : x, y, z tamsayılar olmak üzere $x^2 + y^2 = z^2$ denklemine 2. dereceden üç bilinmeyenli Diophantine denklemi denir. Bu denklem Pisagor denklemi olarak da bilinir (Şenay 2007).

Teorem 1. 1. 2 : $x^2 + y^2 = z^2$ denkleminin, y çift sayı olmak üzere bütün ilkel çözümleri m ve n aralarında asal tamsayılar $m > n$ ve biri tek diğeri çift olmak üzere,

$x = m^2 - n^2$, $y = 2mn$, $z = m^2 + n^2$ ile verilir (Sierpinski 1988).

İspat : $x^2 + y^2 = z^2$ (1.1.2)

denkleminin bütün temel çözümleri m, n sayıları yardımı 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 (1.1.2) denkleminin bütün primitif (aralarında asal) 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.

Tablo 1.1.3 : m ve n değerlerine karşılık gelen x, y, z değerleri için üçgenin alanı

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	8	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, temel çözümlerin her biri sırasıyla $1, 2, 3$ ... doğal sayılarıyla çarpılmalıdır ve sonra her bir çözümde x ile y değişkenlerinin 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 değişkenlerinin 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. Dolayısıyla $15 - 1^2 = 14,\ 15 - 2^2 = 11,\ 15 - 3^2 = 6$ 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;

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

ifadelerinden ve x ile y değişkenleri 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 (1.1.2) denkleminin $x,\ y,\ z$ doğal sayılarında mümkün olan en küçük çözümüdür. Üstelik bu çözümdeki $x,\ y,\ z$ sayıları doğal sayılardır. Bu değerlerin; $x^2 + y^2 = z^2$ 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 ve o zaman $3, 4, 5$ üçgenine ulaşılır. Dolayısıyla bu da aranandır.

Kolayca ispat edilebilir ki $3^n + 4^n = 5^n$ denkleminin $n = 2$ değeri dışında doğal sayılarda çözümü yoktur. Bu ifadenin 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 $5^n \neq 3^n + 4^n$olduğu görülür.

Fermat'nın derecesi ikiden daha büyük olan üç bilinmeyenli denklemlerin çözümünde kullandığı 'Sonsuz İndirgeme Metodu'nun uygulanması ile ilgili yöntem aşağıdaki teoremde verilmiştir. Bu metot; bir tek $(x, y, z) \in \mathbb{Z}^3$ pozitif çözüm üçlüsünün varlığından hareketle z bileşeni durmadan azalan sonsuz sayıda $(x, y, z) \in \mathbb{Z}^3$ çözümlerinin bir dizisini elde etmeye dayanır. Sonunda bu çözümler dizisinin üçüncü $z_0, z_1, z_2, \dots, z_n, \dots$ bileşenlerinin $z_0 > z_1 > z_2 > \cdots > z_n > \cdots$ şeklinde pozitif tamsayıların azalan bir sonsuz dizisi elde edilir ki bu, İyi Sıralama Prensibi ile çeliştiğinden istediğimiz sonuç elde edilmiş olur (Sierpinski 1988).

Teorem 1. 1. 4 : $x^4 + y^4 = z^2$ Fermat denkleminin $x,\ y,\ z\ \neq 0$ olan hiçbir (x, y, z) tamsayı çözümü yoktur (Şenay 2007).

İspat : Bu denklemin $(x_0, y_0, z_0) \neq (0, 0, 0)$ olan bir çözümünün bulunduğunu varsayalım. Böyle bir $(x, y, z) \in \mathbb{Z}^3$ 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 $p^4 \mid x^4 + y^4$ ifadesinden, $p^4 \mid z^2$ ve sonuçta $p^2 \mid z$ olduğundan,

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

bulunur. Şimdi elde edilen $(\frac{x}{p}, \frac{y}{p}, \frac{z}{p^2})$ çözüm üçlüsünün üçüncü bileşeni için $\frac{z}{p^2} < z$ 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 1. 1. 2'ye 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 olan $(a > b)$ ve her ikisi tek veya çift olmayan tamsayılar vardır. Böylece $x_0^2 = a^2 - b^2$ eşitliğinden (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 tam kare olmaları durumunda mümkündür. O halde $r = m^2, s = n^2$ ve $a = t^2$ olacak biçimde m, n ve t tamsayıları vardır. Ayrıca $a = r^2 + s^2$ eşitliğinden $m^4 + n^4 = t^2$ bulunur. $z_0 = a^2 + b^2 > a^2 = t^4$ 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 $z_0 \in \mathbb{Z}^+$ sayısını en küçük seçtiğimizden bu çelişkilidir. Bu çelişki teoremi ispatlar (Şenay 2007).

Bu tezde üstel Diophantine denkleminin özel bir hali olan

$$x^n + py^n = p^2 z^n$$

denkleminin, p asal ve $x,\ y,\ z$ birer tamsayı iken aşikâr çözümlerinin dışında çözümlerinin olmadığı, Fermat'nın sonsuz indirgeme metodu yardımıyla gösterilmeye çalışıldı.

$$Ax^n + By^n = Cz^n$$

Diophantine denkleminin ispatını ünlü matematikçi A. Wiles 1995 yılında tamamlamış ve mümkün olan çözümlerin sadece aşikâr çözümler olduğunu göstermiştir. Bu teoremin ispatının bir kısmında da Fermat'nın sonsuz indirgeme metodundan faydalanılmıştır.

$$X^p + Y^p = Z^p$$

Fermat denkleminin hatta daha genel olarak

$$bx^n + cy^n = dz^n$$

denkleminin p'nin özel durumları için çözüme sahip olmadığı gösterilmiştir (Barry J. Powell 1984).

$n = 3$ ve $p = 2$ olduğu durumda

$$x^n + py^n = p^2 z^n$$

denkleminin tamsayılarda çözümünün olmadığı Fermat'nın sonsuz indirgeme metodu aracılığıyla gösterilmiştir (Andreescu ve ark. 2010).

$n = 4$ olduğu durumda

$$x^4 + py^4 = z^4$$

özel Diophantine denkleminin aşikâr olan çözümlerinden başka hiçbir tamsayı çözümlerinin olmadığı ispatlanmıştır (Manley 2006).

2. BÖLÜM

TEMEL KAVRAMLAR, KONGRÜANSLAR

2. 1 . Tamsayıların Bazı Özellikleri ve Bölünebilme

Tanım 2. 1. 1 : a sıfırdan farklı bir tamsayı olmak üzere $b = ac$ olacak şekilde bir c tamsayısı varsa, b, a ile bölünebilir denir ve $a \mid b$ şeklinde gösterilir. Eğer b, a ile bölünemiyorsa $a \nmid b$ şeklinde gösterilir.

$a \mid b$ gösterimi a böler b; a, b'nin bir böleni veya b, a'nın bir katıdır şeklinde söylenir. Bölünebilmenin bazı özellikleri aşağıdaki teoremle ifade edilebilir.

Teorem 2. 1. 2 : Her $a, b, c \in \mathbb{Z}$ için

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

ii) $a \mid b$ ve $b \mid c$ ise $a \mid c$

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

iv) $a \mid b$ ve $b \mid a$ ise $a = \pm b$

$a \mid b, a > 0,\ b > 0$ ise $a \leq b$ dir. (Niven 1972)

Tanım 2. 1. 3 : $a, b, c, d \in \mathbb{Z}$ olsun.

i) $d \mid a \wedge d \mid b$

ii) $c \mid a \wedge c \mid b \Rightarrow c \mid d$ koşulları sağlanıyorsa d 'ye a ile b 'nin en büyük ortak böleni denir ve $(a, b) = d$ ile gösterilir.

Teorem 2. 1. 4 : b ve c tamsayılarının en büyük ortak böleni d ise bu durumda d

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

ii) b ve c'nin bütün pozitif ortak bölenleriyle bölünebilen pozitif tamsayılardır (Niven 1972).

Teorem 2. 1. 5 : Pozitif tamsayıların boş olmayan her S alt cümlesinin bir en küçük elemanı vardır (Atasoy 1991).

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

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

kümesini göz önüne alalım. Hiçbir pozitif tamsayının ardışığı olmadığından $1 \in K$ dır. $x \in K$ ve $y \in S$ *ise* $x + 1 = x_1 \leq y$ yazabiliriz. $x_1 = y$ ise x_1, S kümesinin en küçük elemanı olur. Kabulümüzden dolayı bu olamayacağından $x_1 \in K$ bulunur. Yani $x_1 < y$ olur. Benzer düşünceler tekrar edilirse, sonlu adımdan sonra yine $a \in K$ olmak üzere,

$$x_1 < x_2 < \cdots < a$$

elde edilir. Bu ise K'nın bütün pozitif tamsayıları kapsadığını gösterir ki, bu da S cümlesinin boş olmasını gerektirir. Fakat $S \neq \emptyset$ alındığından $S = \emptyset$ olması bir çelişkidir. O halde S cümlesinin bir en küçük elemanı vardır (Atasoy 1991).

Bu teoreme pozitif tamsayılarda iyi sıralama prensibi adı verilir.

Teorem 2. 1. 6 (Bölme Algoritması): a, b iki tamsayı ve $b > 0$ olmak üzere

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

olacak şekilde bir tek q ve r tamsayı çifti vardır (Long 1967).

İspat : $C = \{a - sb : s \in \mathbb{Z}, a - sb \geq 0\}$ kümesini gözönüne alalım. $a \geq 0$ ise $a - 0b$ sayısı C kümesinin elemanıdır. $a < 0$ ise $b \geq 1$ $için$ $a - ab = a(1 - b) \geq 0$ olur ki, C'nin elemanıdır. Böylece a'nın her iki durumu için de C boş değildir.

Bu yüzden Teorem 2.1.4'e göre C'nin bir en küçük elemanı vardır. C'deki en küçük eleman r olacak şekilde s'ye verilecek değer q olsun. O zaman $r = a – bq$ olur ki bu $0 \leq r$ olmasıdır ve

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

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

Şimdi q ve r tamsayılarının tekliğini gösterelim. Kabul edelim ki

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

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

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

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

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

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

yazılır. Bu ise $r = r_1$ olmasıdır (Long 1967).

2. 2. Kongrüanslar

Tanım 2. 2. 1 : Sıfırdan farklı bir a tamsayısı $a-b$ farkını bölüyorsa a'ya m modülüne göre b 'ye denktir denir ve $a \equiv b\ (mod\ m)$ şeklinde gösterilir. $m,\ a-b$ farkını bölmüyorsa $a,\ m$ modülüne göre b'ye denk değildir denir ve $a \not\equiv b\ (mod\ m)$ şeklinde gösterilir. Böylece $a-b$ farkının m ile bölünebilmesi, $-m$ ile de bölünebilmesini gerektireceğinden genellikle modülü pozitif olarak sınırlayacağız.

Kongrüansların aşağıdaki temel özellikleri vardır.

Teorem 2. 2. 2 : a, b, c, d, x ve y tamsayılar olmak üzere;

i) $a \equiv b\ (mod\ m)$ ise $b \equiv a\ (mod\ m)$ ve $a-b \equiv 0\ (mod\ m)$

ii) $a \equiv b\ (mod\ m)$ ve $b \equiv c\ (mod\ m)$ ise $a \equiv c\ (mod\ m)$

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

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

v) $a \equiv b\ (mod\ m)$ ve $d \mid m,\ d > 0$ ise $a \equiv b\ (mod\ m)$ olur.

Teorem 2. 2. 3 : a, m, y, d ve x tamsayılar olmak üzere;

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

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

Teorem 2. 2. 4 : a, m, y, d ve x tamsayılar ve $(a, m) = d$ olmak üzere $ax \equiv b (mod\ m)$ kongrüansının çözümünün olması için gerek ve yeter şart $d \mid b$ olmasıdır (Atasoy 1991).

3. BÖLÜM

DİOPHANTİNE DENKLEMLERİNİN ÇÖZÜMLERİ İÇİN ELEMENTER METOTLAR

3.1. Çarpanlara Ayırma Metodu

$f(x_1, x_2 \dots x_n) \ = \ 0$ şeklinde bir denklem verildiğinde bu denklemi

$$f_1\ (x_1, x_2 \dots x_n)\ f_2(x_1, x_2 \dots x_n) \dots\ f_k(x_1, x_2 \dots x_n) \ = \ a$$

şeklinde parçalamalıyız. $f_1, f_2, \dots, f_k \in \mathbb{Z}[x_1, x_2 \dots x_n],\ \ a \in \mathbb{Z}$

$$\begin{gathered} f_1(x_1, x_2 \dots x_n) = a_1 \\ f_2(x_1, x_2 \dots x_n) = a_2 \\ . \\ . \\ . \\ f_k(x_1, x_2 \dots x_n) = a_k \end{gathered}$$

verilen denklemin çözümleridir.

Mesela $\frac{1}{x} + \frac{1}{y} = \frac{1}{n}$ denkleminde $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ ise denkleminin pozitif tamsayı çözümleri $(2\alpha_1 + 1) \dots\ (2\alpha_k + 1)$ tanedir. Gerçekten verilen denklem $(x - n).(y - n) = n^2$ şeklinde düzenlendiğinde ve $n^2 = p_1^{2\alpha_1} \dots p_k^{2\alpha_k}$ olduğunda $(2\alpha_1 + 1) \dots\ (2\alpha_k + 1)$ tane pozitif bölene sahiptir.

Örnek 3. 1. 1 : $(x^2 + 1)(y^2 + 1) + (x - y)(1 - xy)^2 = 4(1 + xy)$ denkleminin tüm tamsayı çözümlerini bulunuz.

Çözüm : $x^2y^2 + x^2 + y^2 + 1 + 2x - 2x^2y - 2y + 2xy^2 = 4 + 4xy$

$$x^2y^2 - 2xy + 1 + \ x^2 + y^2 - 2xy + 2(x - y)(1 - xy) = 4$$

$$(xy - 1)^2 + (x - y)^2 - 2(x - y)(xy - 1) = 4$$

$$[xy - 1 - (x - y)]^2 = 4$$

olup

$$(x+1)(y-1) = \pm 2$$

elde edilir. Burada iki durum söz konusudur.

Ya;

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

ya da

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

dir.

Önce $(x+1)(y-1) = 2$ durumunu ele alalım.

$$(x+1) = 2, (y-1) = 1$$
$$(x+1) = -2, (y-1) = -1$$
$$(x+1) = 1, (y-1) = 2$$
$$(x+1) = -1, (y-1) = -2$$

olup çözümler $(1, 2), (-3, 0), (0, 3), (-2, -1)$ olur.

İkinci olarak $(x+1)(y-1) = -2$ ise;

$$(x+1) = -2, (y-1) = 1$$
$$(x+1) = 2, (y-1) = -1$$
$$(x+1) = 1, (y-1) = -2$$
$$(x+1) = -1, (y-1) = 2$$

olup çözümler$(1,0)$, $(-3,2)$, $(0,-1)$, $(-2,3)$ olur ki verilen denklemin 8 adet çözümü vardır.

Eğer; $\frac{\boldsymbol{1}}{\boldsymbol{X}} + \frac{\boldsymbol{1}}{\boldsymbol{Y}} = \frac{\boldsymbol{1}}{\boldsymbol{n}}$denkleminde $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ ise denklemin pozitif tamsayı çözümleri $(2\alpha_1 + 1) \ldots (2\alpha_k + 1)$ tanedir.

Gerçektende verilen denklem $(x-n)(y-n)=n^2$ şeklinde düzenlendiğinde ve $n^2 = p_1^{2\alpha_1} \dots p_k^{2\alpha_k}$ olduğundan $(2\alpha_1+1) \dots (2\alpha_k+1)$ tane pozitif bölene sahiptir (Andreescu ve ark. 2010).

3.2. EşitsizlikMetodu

Bu yöntemin örnek üzerinde incelenmesi, yöntemin anlaşılmasını kolaylaştıracaktır.

Örnek 3. 2. 1: $x^3+y^3=(x+y)^2$ denkleminin tüm (x,y) tamsayı çözümlerini bulalım.

Çözüm : Eğer $x+y \neq 0$ ise;

$$x^2-xy+y^2=x+y \tag{3.2.1}$$

denklemiyle başlayabiliriz. Bu durumda (3.2.1) denkleminin eşiti

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

olur. $(x-1)^2 \leq 1$ ve $(y-1) \leq 1$ aralığına kısıtlayan x, y değişkenleri $[0,2]$ aralığına karşılık gelmektedir. O halde çözümler

$$(0,1),(1,0),(1,2),(2,1),(2,2)$$

şeklindedir(Andreescu ve ark. 2010).

3.3. Parametrik Metot

$f(x_1,x_2 \dots x_n)=0$ ve $x_1=g_1(k_1,k_2 \dots k_l)$, $x_2=g_2(k_1,k_2 \dots k_l)$, $x_n=g_n(k_1,k_2 \dots k_l)$ şeklinde olduğunda parametrik metot kullanılır. Burada $g_1,g_2,\dots,g_n$tamsayı değerleri, değişken fonksiyonlar ve $k_1,k_2,\dots,k_l \in \mathbb{Z}$ dir. Bazı Diophantine denklemlerinin çözümleri oluşturulurken çoğul parametrik metotlar kullanılabilir.

Birçok Diophantine denklemi için tüm çözümleri açık bir şekilde bulmak mümkün olmayabilir .Böyle birçok durumda parametrik metot sonlu birçok çözümün varlığının ispatını sağlar.

Örnek 3. 3. 1 : $\frac{1}{x}+\frac{1}{y}=\frac{1}{z}$ denklemini sağlayan tüm pozitif tamsayı çözümleri bulunuz.

Çözüm : Denklemi $z=\frac{xy}{x+y}$ şeklinde yeniden düzenleyelim. $ebob(x,y)=d$ olsun. Öyleyse $x=dm, y=dn$ ve $ebob(m,n)=1$ olur ki bu durumda $ebob(mn,m+n)=1$ olması demektir. Bu yüzden

$$z=\frac{dmn}{m+n},\ (m+n)\,\big|\,d,\ \text{yani } d=k(m+n), k\in\mathbb{Z}^{+}$$

denkleminin çözümleri $x=km(m+n),\ y=kn(m+n),\ z=kmn$ şeklinde olup burada $k,m,n\ \in\mathbb{Z}^{+}$olur (Andreescu ve ark. 2010).

3.4. Modüler Aritmetik Metodu

Bu metodu bir uygulama üzerinde inceleyelim.

Örnek 3. 4. 1 :$(x+1)^2+(x+2)^2+\cdots+(x+2001)^2=y^2$ denkleminin çözümü - nün olmadığını gösterelim.

Çözüm. $x = z-1001$ olsun. Bu $(x+1)^2+(x+2)^2+\cdots+(x+2001)^2=y^2$ denkleminde yerine yazılırsa

$(z-1000)^2+(z-999)^2+\cdots+(z-1)^2+z^2+(z+1)^2+\cdots+(z+1000)^2=y^2$

ya da

$$2001z^2+2(1^2+2^2+\cdots+1000^2)=y^2$$

olup bu da

$$2001z^2+2\frac{1000.1001.2001}{6}=y^2$$

$$2001z^2+1000.1001.667=y^2$$

olup

$$2001z^2+1000.1001.667\equiv 2\ (mod 3)$$

olduğundan böyle bir ifade tam kare olamaz (Andreescu ve ark. 2010).

3.5. Matematiksel Tümevarım Metodu

Matematiksel tümevarım metodu negatif olmayan tamsayılara dayanan durumları ispatlamak için kullanılan zarif ve güçlü bir metottur.

$(P(n))_{n\geq 0}$önermesi verilsin.

1. Matematiksel tümevarım (Zayıf Form): Kabul edelim ki
   - $P(n_0)$ doğru olsun.
   - Tüm $k \geq n_0$'lar için $P(k)$ doğruise $P(k+1)$'de doğrudur. Öyleyse $P(n)$ tüm $n \geq n_0$'lar için doğrudur.
2. Matematiksel tümevarım (s adım ile): s uygun bir pozitif tam sayı olsun.
   - $P(n_0), P(n_0+1), \dots, P(n_0+s-1)$ doğru olsun.
   - Tüm $k \geq n_0$ için $P(k)$ doğru ise $P(k+s)$ de doğrudur. Öyleyse $P(n)$ tüm $n \geq n_0$'lar için doğrudur.
3. Matematiksel tümevarım (Güçlü Form):
   - $P(n_0)$ doğru olsun.
   - Tüm $k \geq n_0$ 'lar için $P(m), n_0 \leq m \leq k$ aralığındaki m ler için doğrudur. Öyleyse $P(k+1)$'de doğrudur. Dolayısıyla $P(n)$ tüm $n \geq n_0$ lar için doğrudur.

Bu ispat metodu sayılar teorisi de dahil, matematiğin çeşitli alanlarında yaygın bir şekilde kullanılır.

Örnek 3. 5. 1 : $7x^2 + y^2 = 2^n$ denkleminin $n \geq 3$ için tüm pozitif tek tamsayı çözümlerini bulunuz.

Çözüm : $n \geq 3$ için x_n, y_n gibi tek tamsayı çözümlerinin varolduğunu gösterelim.

$$7x_n^2 + y_n^2 = 2^n, \qquad n \geq 3$$

$n = 3$ için $x_3 = y_3 = 1$ dir. Şimdi $n \geq 3$ için verilen bir sayının x_n, y_n gibi tek tamsayı çözümlerinin olup olmadığına bakalım. (x_{n+1}, y_{n+1}) çifti

$$7x_{n+1}^2 + y_{n+1}^2 = 2^{n+1}$$

gibi denklemin tek pozitif tamsayı çözümlerini verir. Aslında

$$7(\frac{x_n \pm y_n}{2})^2 + \left(\frac{7x_n \pm y_n}{2}\right)^2 = 2(7x_n^2 + y_n^2) = 2^{n+1}$$

ki açıkça

$$\left|\frac{x_n - y_n}{2}\right| \text{ve} \left(\frac{x_n + y_n}{2}\right)$$

sayılarından biri tektir.

Örneğin;

$$\left(\frac{x_n + y_n}{2}\right)$$

tek ise

$$\frac{7x_n - y_n}{2} = 3x_n + \left(\frac{x_n - y_n}{2}\right)$$

olup tektir. Bu yüzden;

$$x_{n+1} = \left(\frac{x_n + y_n}{2}\right), y_{n+1} = \frac{7x_n - y_n}{2}$$

seçilebilir. Eğer;

$$\left(\frac{x_n - y_n}{2}\right)$$

tek ise

$$\frac{7x_n + y_n}{2} = 3x_n + \left(\frac{x_n + y_n}{2}\right)$$

ve ayrıca

$$x_{n+1} = \left|\frac{x_n - y_n}{2}\right| \; ve \; y_{n+1} = \frac{7x_n + y_n}{2}$$

seçilebilir (Andreescu ve ark. 2010).

3.6. Fermat’nın Sonsuz İndirgeme Metodu (FMID)

Pierre de Fermat (1601-1665) sadece amatör bir matematikçi olarak düşünülmesine rağmen, matematiğe katkılarıyla ünlenmiştir. Fermat, Orleans Üniversitesinde 1631 yılından önce medeni kanun üzerine derece almış ve Toulouse kentinde konsey üyesi ve hukukçu olarak bulunmuştur.

Fermat, buluşları ve metotları sayesinde matematik dünyası üzerinde büyük etki bırakmıştır. Fermat ‘Sonsuz İndirgeme’ olarak adlandırdığı metodu ispatlayarak kullanan ilk matematikçidir.

P, negatif olmayan tamsayılarla ilgili olsun ve $(P(n))_{n\geq 1}$, bir önerme olsun.

$P(n)$: ‘ n P’yi doğrular.’

Aşağıdaki metot n’in çok büyük olduğu değerlerde $P(n)$’in yanlış olduğu durumdaki ispatında kullanılır.

k negatif olmayan bir tamsayı olsun. Kabul edelim ki aşağıdakiler sağlansın:

- $P(k)$ doğru değildir,
- her ne zaman $P(m)$, $m > k$ pozitif tamsayıları için doğruysa, $P(j)$’nin doğru olması için $m > j \geq k$ özelliğinde j’ler bulunur.

Öyleyse $P(n)$, tüm $n \geq k$ için yanlıştır.

Fermat’nın sonsuz indirgeme metodu (FMID) şu şekilde formülize edilebilir:

k, negatif olmayan bir tamsayı olsun. Kabul edelim ki;

- Her ne zaman $P(m)$, bir $m > k$ tamsayısı için doğruysa $P(j)$’nin doğru olması için, $m > j > k$ özelliğinde bir en küçük j tamsayısı olmalıdır.

Diophantine denklemleri için kullanılan 2 farklı İndirgeme metodu (FMID) vardır:

FMID 1: $n_1 > n_2 > \cdots$şeklinde negatif olmayan tamsayıların dizisi yoktur. Eğer n_0, $P(n)$’in doğru olması için n’nin en küçük tamsayı değeri ise; $P(n)$, $n < n_0$ için yanlıştır.

FMID 2: $(n_i)_{i\geq 1}$ negatif olmayan tamsayılar dizisi $n_1 \geq n_2 \geq \cdots$ eşitsizliğini sağlarsa; $n_{i_0} = n_{i_0+1} = \cdots$ gibi i_0 tamsayıları vardır.

Örnek 3. 6. 1 : $x^3 + 2y^3 = 4z^3$ denkleminin negatif olmayan tamsayılarda $(0, 0, 0)$ dışında başka çözümü yoktur. Gösteriniz.

Çözüm : Kabul edelim ki $x_1 > 0, y_1 > 0, z_1 > 0$ olacak şekilde (x_1, y_1, z_1) aşikâr olmayan bir çözüm olsun. Buradan hareketle

$$x_1^3 + 2y_1^3 = 4z_1^3$$

ise $2 \mid x_1$ olup $x_1 = 2x_2$ olacak şekilde $x_2 \in \mathbb{Z}^+$ vardır. Öyleyse

$$4x_2^3 + y_1^3 = 2z_1^3$$

olup $2 \mid y_1$'dir. Dolayısıyla $y_1 = 2y_2$olacak şekilde $y_2 \in \mathbb{Z}^+$vardır. Aynı şekilde devam edilirse

$$x_2^3 + 2y_2^3 = z_1^3$$

olup $2 \mid z_1$'dir. $z_1 = 2z_2$, $z_2 \in \mathbb{Z}^+$ olur. Buradan (x_2, y_2, z_2) gibi yeni çözümler elde edilir ki $x_1 > x_2, y_1 > y_2, z_1 > z_2$ şeklindedir. Bu işleme bu şekilde devam edilirse $x_1 > x_2 > x_3 > \cdots$ özelliğinde sonsuz bir dizi elde edilir. Pozitif tamsayılar 0 ile alttan sınırlı olduğundan dolayı böyle bir sonsuz dizi bulunamaz. Yani bir çelişki elde edilir ki bu da aşikâr çözümler dışında başka çözüm olmadığını gösterir (Andreescu ve ark. 2010).

Örnek 3. 6. 2 : p asal bir sayı olmak üzere $x^3 + py^3 = p^2z^3$ denkleminin aşikâr çözümü dışında çözümü yoktur.

Çözüm : $x_1 > 0, y_1 > 0, z_1 > 0$ olacak şekilde (x_1, y_1, z_1) aşikâr olmayan çözümler olsun.

$$x_1^3 + py_1^3 = p^2 z_1^3$$

$$x_1^3 = p(pz_1^3 - y_1^3)$$

olup $p \mid x_1^3$ olduğundan $p \mid x_1$'dir. $x_1 = px_2$ olacak şekilde $x_2 \in \mathbb{Z}^+$vardır.

$$p^3 x_2^3 + py_1^3 = p^2 z_1^3$$

olup eşitliğin her iki tarafı p ile bölünürse

$$y_1^3 = p(z_1^3 - p^2 x_2^3)$$

olup $p \mid y_1^3$ olduğundan $p \mid y_1$ 'dir. $y_1 = py_2$ olacak şekilde $y_2 \in \mathbb{Z}^+$ vardır. Benzer şekilde bu işlem devam edildiğinde

$$z_1^3 = p(x_2^3 + p^2 y_2^3)$$

olup $p \mid z_1^3$,$p \mid z_1$'dir. Dolayısıyla $z_1 = pz_2$olacak şekilde $z_2 \in \mathbb{Z}^+$ve bu işleme devam edildiği takdirde $x > x_1 > x_2 > \cdots$ $y > y_1 > y_2 > \cdots$ $z > z_1 > z_2 > \cdots$ olup sonsuz bir dizi elde edilir. Pozitif tamsayılar alttan sınırlı olduğundan böyle bir dizi mümkün değildir. Dolayısıyla aşikâr çözüm dışında çözüm yoktur.

Teorem 3. 6. 3 : n tek sayı, p asal iken $x^n + py^n = p^2 z^n$ denkleminin aşikâr çözümü dışında çözümü yoktur.

İspat : n tek sayı, p asal ve $p > 2$ için

$$x^n + py^n = p^2 z^n$$

olduğundan $p \mid py^n$ ve $p \mid p^2z^n$'dır.

$$x^n = p^2z^n - py^n = p(pz^n - y^n)$$

olduğundan $p \mid x^n$'dır. p asal olduğundan dolayı $p \mid x$ elde edilir. Dolayısıyla $x = px_1$ olacak şekilde $x_1 \in \mathbb{Z}^+$ vardır. Buradan

$$x^n = p^n x_1^n$$

elde edilip denklemde yerine yazılırsa

$$p^n x_1^n + py^n = p^2 z^n$$

denklemin her iki tarafı p ile bölünürse

$$y^n = p(pz^n - p^{n-2}x_1^n)$$

olup ve $n > 2$ olduğundan $p \mid y^n$ ve $p \mid y$'dir. $y = py_1$ olacak şekilde $y_1 \in \mathbb{Z}^+$ vardır.

$$p^n y^n = pz^n - p^{n-1}x_1^n$$

denkleminin her iki tarafı p ile bölünürse

$$p^{n-1}y^n = z^n - p^{n-2}x_1^n$$

$$z^n = p(p^{n-2}y_1^n + p^{n-3}x_1^n)$$

olup $p \mid z^n$ ve $p \mid z$dir. $z = pz_1$ olacak şekilde $z_1 \in \mathbb{Z}^+$ vardır.

$$p^n z_1^n = p^{n-1}y_1^n + p^{n-2}x_1^n$$

yazılır ve her iki taraf p^{n-2} ile sadeleştirilirse

$$p^2 z_1^n = p y_1^n + x_1^n$$

ve bu şekilde devam edersek $x > x_1 > x_2 > \cdots$, $y > y_1 > y_2 > \cdots$ ve $z > z_1 > z_2 > \cdots$ olup Fermat'nın sonsuz indirgeme metodu gereği tamsayılar alttan sınırlı olduğu için n tek sayı ve p asal olduğu durumda

$$x^n + p y^n = p^2 z^n$$

denkleminin aşikâr çözümü dışında çözümü yoktur.

Teorem 3. 6. 4 : $n = 4$, p asal ve x, y, z aralarında asal ise;

$$x^4 + p y^4 = p^2 z^4$$

denkleminin çözümü yoktur.

İspat : Bunu göstermek için kabul edelim ki (x_1, y_1, z_1) bir çözüm olsun. Buna göre

$$x_1^4 + p y_1^4 = p^2 z_1^4$$

$$x_1^4 = p(p z_1^4 - y_1^4)$$

ise $p \mid x_1^4$ olduğundan $p \mid x_1$ 'dir. $x_1 = p x_2$ olacak şekilde $x_2 \in \mathbb{Z}^+$ ve $x_1 \equiv 0 \ (mod p)$ vardır.

$$p^4 x_2^4 + p y_1^4 = p^2 z_1^4$$

her iki taraf p ile sadeleştirilirse

$$p^3 x_2^4 + y_1^4 = p z_1^4$$

$$y_1^4 = p(z_1^4 - p^2 x_2^4)$$

olup $p \mid y_1^4$ yani $p \mid y_1$ ’dir. $y_1 \equiv 0\ (mod p)$ olduğundan bu $(x_1, y_1) = 1$ olması ile çelişir. Dolayısıyla (x_1, y_1, z_1)’nin bir çözüm olması mümkün değildir.

4. BÖLÜM

4.1. $x^4 + py^4 = z^4$ DENKLEMİNİN KUADRATİK ÇÖZÜMLERİ

Teorem 4. 1. 1 : $p \equiv 3\ (mod8)$ için $x^4 + py^4 = z^4$ denkleminin tüm ikinci dereceden çözümleri (a, b, c) üçlüsü $x^4 + py^4 = z^4$ denkleminin bir rasyonel çözümü olmak üzere $(a, b, \sqrt{c})$ şeklindedir.

Sonuç 4. 1. 2 : $p \equiv 11\ (mod16)$ iken $x^4 + py^4 = z^4$ denkleminin tüm ikinci dereceden çözümleri $xyz = 0$ şartını sağlar.
$x^4 + 3y^4 = z^4$ denkleminin $(1, 1, \sqrt{2})$ çözümü $x^4 + 3y^4 = z^4$ denkleminin bir rasyonel çözümünden indirgenir.

Sonuç 4. 1. 3 : Eğer $(a, b, c) x^2 + Dy^4 = z^4$, $x^4 + Dy^2 = z^4$ ya da $x^4 + Dy^4 = z^2$ denklemlerinden biri için bir rasyonel çözümse sırasıyla $(\sqrt{a}, b, c)$, $(a, \sqrt{b}, c)$, $(a, b, \sqrt{c})$ üçlüsü $x^4 + Dy^4 = z^4$ denkleminin ikinci dereceden bir indirgenmiş çözümüdür.

Sonuç 4. 1. 4 : $p \equiv 3\ (mod8)$ iken $x^4 + py^4 = z^4$ denkleminin tüm ikinci dereceden çözümleri indirgenmiştir.

Sonuç 4. 1. 5 : $p \equiv 3\ (mod8)$ iken

$$x^4 + py^2 = 1 \tag{4.1.1}$$

denkleminin rasyonel çözümleri yoktur (Nagell 1964). Benzer şekilde $p \equiv 3\ (mod8)$ iken;

$$x^2 + py^4 = 1 \tag{4.1.2}$$

denkleminin rasyonel çözümü yoktur (Mordell 1969). Dikkat edilirse $x^2 + py^4 = 1$ denklemi $v^2 = u^3 + 4pu$ eliptik eğrisi ile ilişkilidir. Çünkü (u, v) , $v^2 = u^3 + 4pu$ denkleminin aşikâr olmayan bir çözümü ise;

$$(\frac{(8pu - v^2)}{v^2}, \frac{2u}{v})$$

$x^2 + py^4 = 1$ denkleminin çözümüdür. Bu yüzden $p \equiv 3\ (mod 8)$ iken

$$v^2 = u^3 + 4pu, \tag{4.1.3}$$

Denkleminin tüm rasyonel çözümleri $uv = 0$ şartını sağlar.
Şimdi $p \equiv 11\ (mod 16)$ için

$$x^4 + py^4 = z^2 \tag{4.1.4}$$

denkleminin tüm rasyonel çözümleri $xyz = 0$ şartını sağlar (Mordell 1969).
Şimdi (4.1.4) denklemini $p \equiv 3\ (mod 16)$ iken düşünelim. Bu denklem

$$v^2 = u(u^2 + p) \tag{4.1.5}$$

eliptik eğrileriyle ilgilidir (Bremner ve ark. 1984). Dolayısıyla her bir u ya da pu bir tam kare olmalıdır. pu tam kare ise,

$$(\frac{pv}{u^2})^2 = \left(\frac{p}{u}\right)^3 + p(\frac{p}{u})$$

olmalıdır. Bu yüzden u bir tam kare olmak üzere $v^2 = u(u^2 + p)$ denkleminin bir çözümünü elde etmiş oluruz. $ebob(x, y) = 1$ olmak üzere

$$u = \frac{x^2}{y^2}\ , \qquad v = \frac{xz}{y^3}$$

kabul ederek

$$x^4 + py^4 = z^2$$

denklemi için bir çözüme sahip oluruz.

Silverman (1986)'a göre

$$v = u(u^2 + p)^5, p \equiv 3 \ (mod16)$$

denklemi için $rank = 1$ 'dir. Bu durum $p \equiv 3 \ (mod16)$ iken $x^4 + py^4 = z^2$ denkleminin sonsuz çoklukta çözümünün olduğunu gösterir. Örneğin, $p = 3$ iken $(1,2)$, $v^2 = u(u^2 + p)$'nin çözümüdür. Dolayısıyla $(1, 1, 2)$ de

$$x^4 + py^4 = z^2$$

denkleminin bir çözümüdür. $p = 19 \ iken \ (19,30)$, $v^2 = u(u^2 + p)$'nin bir çözümüdür ve $(3, 1, 10)$ da

$$x^4 + py^4 = z^2$$

denkleminin bir çözümüdür. $p = 67$ iken $((2401/225), (148274/3375))$ (4.1.5)'in bir çözümü olup $(49, 15, 3026)$ da (4.1.4)'ün çözümüdür.

$$px^4 - 4y^4 = z^2, p \equiv 3 \ (mod8) \tag{4.1.6}$$

denkleminin tüm rasyonel çözümleri $xyz = 0$ şartını sağlar. Çünkü $-1, p$ modunda ikinci dereceden bir kalan değildir.

Teorem 4.1.1'nin ispatı (4.1.5) denklemine dayalıdır. $z \neq 0$ olduğunda

$$x^4 + py^4 = 1 \tag{4.1.7}$$

denkleminin çözümüne odaklanılır. $x, y \in K$ ve K ise $\mathbb{Q}$ 'nun ikinci dereceden bir genişlemesidir. $y \neq 0$ iken (4.1.7) denklemi için verilen herhangi bir çözüm mevcut ise

$$t = \frac{1 - x^2}{y^2}$$

olarak tanımlandığında x^2 için $x^2 = -ty^2 + 1$ ifadesi elde edilir. (4.1.7) denkleminde x^2'yi yerine koyarak y^2 için bir çözüm bulabiliriz. Öyleyse

$$x^2 = \frac{p-t}{p+t^2}^2 \;, \quad y^2 = \frac{2t}{p+t^2} \tag{4.1.8}$$

$x, y \in K$, $t \in K$'dır. Burada ele alınacak 2 durum vardır. Her bir t rasyoneldir ya da irrasyoneldir. En son durumda ikinci dereceden bir çözüm olmadığını ve sadece indirgenmiş ikinci dereceden çözüm olduğunu göstereceğiz. İlk olarak t'nin rasyonel olduğunu kabul edelim. (4.1.8)'deki x^2 ve y^2 rasyoneldir. x rasyonel fakat y irrasyonel ise $y^2 = y_1$ yazılarak $x^4 + py_1^2 = 1$ denklemi için bir rasyonel çözüm elde edilir. y rasyonel ancak x rasyonel değilse, $x^2 = x_1$ alınarak $x_1^2 + py^4 = 1$ denklemi için bir rasyonel çözüm elde edilir. x ve y'nin her ikisi de rasyonel değilse $x = x_1\sqrt{d}$ ve $y = y_1\sqrt{d}$ bakarak bazı $d \in Q$ için $x_1^4 + py_1^4 = (\frac{1}{d})^2$ denklemi için bir rasyonel çözüm buluruz. Tanım 4.1.3'e göre bu ikinci dereceden çözümlerden indirgenmiş olan (4.1.1) ve (4.1.2) ile hem $x^4 + py^2 = 1$ hem de $x^2 + py^4 = 1$ sıfırdan farklı rasyonel çözümlere sahiptir. Bu yüzden tüm kalan çözümler $x^4 + py^4 = z^2$den gelir.

Kabul edelim ki t irrasyonel olsun. Böylece bazı rasyonel B ve C sabitleri için $K = \mathbb{Q}(t)$ ve $F(t) = t^2 + Bt + C = 0$ elde edilir.(4.1.8) de verilen içinde t bulunduran x^2 ve y^2 rasyonel ifadeleri yerine t'ye bağlı $K = \mathbb{Q}(t)$ ve $F(t) = t^2 + Bt + C = 0$ polinomları tercih ederiz.

$X = (p + t^2)xy$ ve $Y = (p + t^2)y$ olsun. Böylece dikkat edilirse $X^2 = 2t(p - t^2)$ ve $Y^2 = 2t(p + t^2)$ olduğu görülür. $X, Y \in K$ olduğundan $X = a + bt$ ve $Y = a_1 + b_1 t$ olacak şekilde $a,\ b,\ a_1,\ b_1 \in \mathbb{Q}$ vardır. X, Y değerleri yerine konulduğunda t'nin

$$t\ (a+bz)^2-2z(p-z^2) \text{ve} (a_1+\ b_1z)^2-2z(p+z^2)$$

üçüncü dereceden polinomun bir kökü olduğu görülür. Böylece iki polinomda $F(z)$tarafından bölünebilir. Üçüncü dereceden bu iki polinomu bölen ikinci dereceden indirgenemeyen bir polinomun olmadığını göstereceğiz. Yani böyle t'nin var olmadığı ispatlanabilir. $M+Nz$ ve M_1+N_1z bu üçüncü dereceden polinomlar için iki bölüm olsun. Böylece M, N, M_1, N_1 rasyonel sabitler ve $N, N_1 \neq 0$ iken

$$(a+bz)^2-2z(p-z^2)=\ F(z)(M+Nz) \tag{4.1.9}$$

$$(a_1+\ b_1z)^2-2z(p+z^2)=F(z)(M_1+N_1z) \tag{4.1.10}$$

yazılabilir. Açıkça görülmektedir ki $-M/N$ ve $-\ M_1/N_1$ sabitleri (4.1.9) ve (4.1.10)'un sol tarafındaki polinomların birer köküdür. Dolayısıyla $(a+bz)^2=2z(p-z^2)$ ve $(a_1+\ b_1z)^2=2z(p+z^2)$ denklemleri için rasyonel çözümler vardır. Bunlar nelerdir?

$$v=2(a_1+\ b_1z) \text{ ve } u=2z$$

ele alınırsa tek çözümü

$$u=\ v=0 \text{ olan } v^2=u^3+4pu$$

olur. Bu yüzden $z=0$,

$$(a_1+\ b_1z)^2=2z(p+z^2)$$

için tek çözümdür. Bu yüzden $0=M_1/N_1$ olduğu görülür. $M_1=0$ dır ve (4.1.10) denklemine göre $a=0$ dır.

$$N_1F(z)=-2z^2+b_1^2z-2p,$$

$F(z)$'nin (4.1.9) denklemini sağlamadığı gösterilebilir. (4.1.9) denkleminde $F(z)$ yerine yazılır $(a+bz)^2-2z(p-z^2)=-2z^2+b_1^2z-2p$ elde edilir ve katsayıları karşılaştırılır. $F(z)$, (4.1.9) denklemini sağlamaz. Bununla birlikte eğer
$(a+bz)^2-2z(p-z^2)=(-2z^2+b_1^2z-2p)(M+Nz)/N_1$denklemi dikkate alınırsa Bu denklem genişletilir ve z^3'ün katsayısına bakılırsa $N_1=-N$ olduğu görülür. Sabit terimden – $M/N=-a^2/(2p)$ (4.1.9) eşitliğinin sağ taraf sabitindeki sıfır – M/N dir. Yani (4.1.9) daki sıfır; $u,v\in\mathbb{Z}$ ve $ebob(u,v)=1$ ile $a\in\mathbb{Q}$ ya da $-u^2/(2pv^2)$ ile $-a^2/(2p)$ formuna sahip olmalı. Bu yüzden (4.1.9)'un sol taraf sabitinden;

$$2(-u^2/(2pv^2)(p-(-u^2/(2pv^2))^2)$$

ifadesinin kare olduğunu görürüz. Bu yüzden,

$$((u^2)(u^4-4p^3v^4))/(4(v^6)(p^3))$$

karedir ki bu da $p(u^4-4p^3v^4)$ kare olması anlamına gelir. Böylece (4.1.6)'daki denklem için bir çözüm elde edilebilir ki bu istenilen özellikte hiçbir a'nın var olmadığı sonucunu verir. (4.1.7) denkleminin tüm ikinci dereceden çözümlerinin $x^4+py^4=z^2$ den indirgenmiş olan çözümler olduğu gösterilmişti. Dolayısıyla bu sonuçla Teorem 4.1.1'nin ispatı tamamlanır (Manley 2006).

5. SONUÇLAR VE TARTIŞMA

Bu çalışmada, Diophantine denklemlerinden $x^n + py^n = p^2z^n$ formundaki özel denklem ailesinin aşikar çözümler dışında bir çözüme sahip olup olmadığını inceledik. Bu incelemeyi yaparken konu üzerinde daha önce yapılmış olan çok sayıda makale ve kitap taraması yapıp onlarda kullanılmış olan metotları ve özellikle FMID'ı (Fermat'nın Sonsuz İndirgeme Metodu) kullandık.

Diophantine denklemlerinin çok sayıda özel formu literatürde mevcuttur. Bunlar, Lineer Diophantine denklemleri, Pell denklemleri, Fermat'nın son teoremi gibi denklemlerdir. Dolayısıyla bu tür denklemlerin çözüm yöntemleride kullanıldıkları denkleme bağlı olarak çeşitlilik göstermektedir. Bu da literatür taramasında karşımıza çıkan en büyük zorluktur.

Başlangıçta $x^n + py^n = p^2z^n$ denklemini tüm n doğal sayıları için incelemek istemiş olsak da bunu sadece n bir tek doğal sayı iken yapabildik. $n = 4$dışındaki diğer çift doğal sayılar için x, y, z aralarında asal değilken çözümün var olup olmadığına dair bir sonuca ulaşamadık. Sonuç olarak bu durumun tartışılması sonraki aşamada yapılabilecek bir çalışma olarak düşünülmektedir.

KAYNAKLAR

Bremner, A. Cassels, J.W.S. 1984. On the equation $Y^2 = X(X^2 + p)$, Math. Comp. 42: 257-264.

Mordell, L, J. 1969. Diophantine equations, Pure Appl. Math.,vol. 30, Academic Press, London.

Nagell, T. 1964. Introduction to number theory, 2nd ed., Chelsea Publishing Co., New York, 230.

Silverman, J. H. 1986. The arithmetic of elliptic curves, Grad. Texts in Math.,vol. 106, Springer-Verlag, New York.

Manley, E. D. 2006. On Quadratıc Solutions of $x^4 + py^4 = z^4$ Rocky Mountain Journal of Math. Vol. 36, 3: 1027-1031.

Sierpinski, W. 1988. Elementary Theory of Number Pwn-Polish Scientific Publishers

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

Çenberci, S. 2009. $\mathrm{A}x^2 + B^m = y^n$ Diophantine denklemi ve Terai Konjektürü Üzerine. Doktora Tezi, Selçuk Üniversitesi Fen Bilimleri Enstitüsü, Matematik Anabilim Dalı, Konya.

Niven, I. 1972. An Introduction to the Theory of Numbers John Wiley Sonsinc, New York.

Calvin, T. L. 1967 Elemantary Introduction to Number Theory D. C. Heathand Company Boston.

Atasoy, M. 1991. Diophantine Denklemleri. Yüksek Lisans Tezi, Erciyes Üniversitesi Fen Bilimleri Enstitüsü, Matematik Anabilim Dalı, Kayseri.

Andreescu, T. Andrica, D. Cucurezeanu, I. 2010. An Introduction to Diophantine Equtions. Springer New York Dordrecht Heidelberg London, 339 pp.

Powell B.J. 1984. Proof of the Impossibility of the Fermat Equation$x^n + y^n = z^n$for special Values of p and of More General Equation $bx^n + cy^n = dz^n$Journel of Number Theory 18: 34-40.

Soydan, G. Demirci, M. Cangül, İ. N. 2009. The Diophantine Equation $x^2 + 11^m = y^n$ Advanced Studies in ContemporaryMathematics, 19(2), 183-188.

Cangül, İ. N. Demirci, M. Soydan, G. Tzanakis, N. 2010. On TheDiophantineEquation $x^2 + 5^a 11^b = y^n$ Functiones et Approximatio Commentarii Mathematici, 43(2), 209-225.

Cangül, İ. N. Demirci, M. İnam, İ. Luca, F. Soydan, G. 2013. On The Diophantine Equation $x^2 + 2^a 3^b 11^c = y^n$ Mathematica Slovaca, 63(3), 647-659.

Florian, L. 2000 On a DiophantineEquation Bulletin of theAustralian Mathematical Society, 61 (2), 241-246.

ÖZGEÇMİŞ

Adı ve Soyadı	: Caner AĞAOĞLU
Doğum Yeri ve Tarihi	: Bursa, 28/05/1990
Yabancı Dili	: İngilizce

Eğitim Durumu (Kurumu ve Yıl)

Lise	: Çınar Lisesi, 2004-2007
Lisans	: Eskişehir Osmangazi Üniversitesi, 2007-2011

İletişim	: agaoglucaner@gmail.com