4235

P_{-2} CÜMLELER AİLESİNİN KARAKTERİZASYONU

İlhan ÖZTÜRK

Erciyes Üniversitesi
Fen Bilimleri Enstitüsü'ne
Matematik Anabilim Dalında
Doktora Tezi Olarak Sunulmuştur.

Haziran — 1988

T. C.
Yükseköğretim Kurulu
Dokümantasyon Merkezi

Erciyes Üniversitesi

Fen Bilimleri Enstitüsü Müdürlüğüne

Bu çalışma, jürimiz tarafından Matematik Anabilim Dalında Doktora tezi olarak kabul edilmiştir.

6/7/1988

Başkan : Prof. Dr. Mehmet Palamutoğlu

Üye : Prof. Dr. Ekrem Çelikel

Üye : Doç. Dr. Cihan Orhan

ONAY

Yukarıdaki imzaların, adı geçen öğretim üyelerine ait olduğunu onaylarım.

7/7/1988

Enstitü Müdürü

ÖZGEÇMİŞ

Adı ve Soyadı : İlhan Öztürk
Baba Adı : Ahmet
Anne Adı : Zikirhan
Doğum yeri ve yılı : Pınarbaşı-1953

İlkokulu Kaynar İlkokulunda, Ortaokulu Pınarbaşı kazasında bitirdi. Daha sonra Kırşehir Öğretmen Okuluna yatılı olarak girdi. Oradan Ankara Yüksek Öğretmen Okulu hazırlık lisesine seçildi. Daha sonra İstanbul Yüksek Öğretmen Okulu adına İstanbul Üniversitesi Fen Fakültesi Matematik-Astronomi Bölümünü bitirdi. Pınarbaşı Lisesinde 4 yıl Matematik öğretmenliği yaptı. Kısa dönem askerliğini bitirdikten sonra 1982 yılında Erciyes Üniversitesi Kayseri Meslek Yüksek Okulu'na öğretim görevlisi olarak atandı. Ocak-1985 tarihinde, Erciyes Üniversitesi Fen Bilimleri Enstitüsünde Yüksek Lisans çalışmasını tamamladı. Halen Kayseri Meslek Yüksek Okulunda öğretim görevlisi olarak çalışmaktadır.

Bu çalışma konusunu bana veren ve çalışmalarım boyunca ilgi ve yardımlarını esirgemeyen hocam sayın Prof. Dr. Ekrem ÖZTÜRK'e , ayrıca doktora yeterlilik imtihanına kadar olan süre içinde, bana yakın ilgi ve alaka gösteren, fikirlerinden faydalanma imkanı veren sayın Doç. Dr. Hasan ŞENAY'a teşekkürlerimi arz ederim.

İlhan ÖZTÜRK

ÖZET

$\{a,b,c\}$ cümlesinin herhangi iki elemanının çarpımını iki eksilttiğimizde bir tam kare elde ediliyorsa, bu cümleye P_{-2} özelliğine sahip cümle denir.

Bu çalışmada, $a,b,c \in Z^+$, $a<b<c$ olmak üzere aşağıdaki eşitlikleri sağlayan $\{a,b,c\}$ üçlüleri üzerinde duruldu.

$$a.b-2 = x^2$$
$$a.c-2 = y^2$$
$$b.c-2 = z^2$$

Burada $x, y, z \in Z$ dir. P_{-2} özelliğini sağlayan bu üçlülerin sonsuz tane olduğu ispatlandı. Ve $\{1,b,c\}$, $\{2,b,c\}$ üçlüleri aşağıdaki formda karakterize edildi.

$$\{1,b,c\} = \{1, n^2+2, n^2+2n+3\}, \ (n \in N_0)$$

$$\{2,b,c\} = \{2, 2n^2+1, 2n^2+4n+3\}, \ (n \in N)$$

Daha sonra genel olarak $\{a,b,c\}$ üçlülerinin istenilen özelliğe sahip olacak şekildeki a ların ne olabileceği araştırıldı. $\{a,b,c\}$ üçlüleri de aşağıdaki formda bulundu.

$$\{a, b, c\} = \{a, n(an \pm 2\mu) + (\mu^2+2)/a, (n+1)(an+a \pm 2\mu) + (\mu^2+2)/a\}$$

Burada $n \geq 2$, $n \in N$, $0 < \mu < a/2$, $\mu^2 \equiv -2 \pmod a$ dır. Bunlara ilave olarak, $\{1,b,c\}$, $\{2,b,c\}$ ve genel olarak $\{a, b, c\}$ üçlülerinin dörtlülere genişletilemediği gösterildi.

ABSTRACT

It is called that the set {a, b, c} has the property P_{-2}, if the product of any two elements of {a, b, c} decreased by 2 is a perfect square.

In this study we consider triples of positive integers $a < b < c$ satisfying the following equalities

$$a.b - 2 = x^2$$
$$a.c - 2 = y^2$$
$$b.c - 2 = z^2$$

for some $x, y, z \in Z$. We prowed that there are infinitely many triples with the property P_{-2}.

We charactrized {1, b, c}, {2 b, c} triples in the following form:

$$\{1, b, c\} = \{1,\ n^2+2,\ n^2+2n+3\},\ (n \in N_0),$$

$$\{2, b, c\} = \{2,\ 2n^2+1,\ 2n^2+4n+3\},\ (n \in N),$$

After then generally we have investigated a's such that {a, b, c} triples have the required property and we found {a, b, c} triples in the following form:

$$\{a, b, c\} = \{a,\ n(an \pm 2\mu) + (\mu^2+2)/a,\ (n+1)(an+a \pm 2\mu) + (\mu^2+2)/a\}$$

where $n \geq 2$, $n \in N$, $0 < \mu < a/2$, $\mu^2 \equiv -2 \pmod a$. In addition to these we showed the sets {1, b, c}, {2, b, c} and {a, b, c} cannot be extended4 - tuples.

SEMBOLLER

N	: Doğal sayılar cümlesi
N_0	: $N \cup \{0\}$
Z	: Tam sayılar cümlesi
Z^+	: Pozitif Tam sayılar cümlesi
$n \mid a$	: n, a'yı kalansız olarak böler.
$n \nmid a$	: n, a'yı bölmez.
(m,n)	: m ile n'nin en büyük ortak böleni
$(m,n)=d$	: m ile n'nin en büyük ortak böleni d dir.
$(m,n)=1$	: m ile n, aralarında asaldır.
$(a_1, a_2, \ldots, a_k)=1$	: a_i $(i=1, 2, \ldots, k)$ ler aralarında asaldır.
KR	: Kuadratik rezidü
KN	: Kuadratik olmayan rezidü
$\left(\frac{a}{p}\right)$	: Legendre sembolü (p üzerinde a)

İÇİNDEKİLER

GİRİŞ

a.b+k=tam kare şartını sağlayan a,b tam sayılarının oluşturduğu cümleler üzerindeki çalışmalar çok eskilere dayanır. L. E. Dickson [1], konu ile ilgili çalışmaların Diophantus'a dayandığını ifade etmektedir. Ünlü matematikçi Fermat; 1, 3, 8, 120 sayılarının P_1 özelliğini sağladığını göstermiştir [12]. Daha sonra A.Baker ve H.Davenport [8], {1, 3, 8, 120} cümlesinin P_1 özelliğini sağlayacak şekilde beş elemanlı bir cümle olamayacağını ispat etmişlerdir. P. Kanagasabapathy ve T. Ponnudurai [9] { 1, 3, 8, 120 } cümlesinin genişletilemediğini, Baker'den farklı metotlar uygulayarak ispat etmişlerdir. V.E.Hoggatt Jr. ve G.E.Bergum[10] ise Fibonacci dizilerini kullanarak {1,3,8,120} cümlesinden başka P_1 özelliğini sağlayan dörtlülerin olabileceğini, fakat bu dörtlülerin beşliler olarak ifade edilemeyeceğini göstermişlerdir. P. Herchelheim [11], P_1 cümlelerini ikililer, üçlüler ve dörtlüler olarak ele almış, dörtlülerin beşlilere genişletilemediğini ispatlamıştır.

Yakın zamanda N.Thamotherampillai[13] ise {1,2,7} cümlesini ele aldı.Bu cümlenin bir P_2 cümlesi olduğunu ve aynı özelliği sağlayan dördüncü bir elemanın bulunamayacağını gösterdi. {1,5,10} cümlesi üzerinde çalışmalar yapan S.P.Mohanty ve A.M.S.Ramasamy[14] bu cümlenin P_{-1} cümlesi olduğunu ve dörtlü olarak ifade edilemeyeceğini ispat ettiler.Genel olarak P_k cümlelerinin üçlülerden dörtlülere genişletilip genişletilemediğini

T. C.
Yükseköğretim Kurulu
Dokümantasyon Merkezi

araştıran E.Brown[15] ,özel olarak P_{-1} cümlesi olan {1,2,5} cümlesinin genişletilemediğini gösterdi. Eşzamanlı Diophantine denklemlerini ve Pell denklemini kullanarak {1,5,12} ile verilen P_4 cümlesini {1,5,12,96} gibi dörtlü olarak ifade edenler S.P.Mohanty ve A.M.S.Ramasamy[16] dır. M.Nutt[17], Thamotherampıllaı'nın { 1, 2, 7 } cümlesinden hareket ederek P_2 cümlelerinin genişletilemediğini genel olarak ıspat etti.

Biz bu çalışmada P_{-2} özelliğini sağlayan üçlüler üzerinde durduk.Şimdiye kadar yapılan çalışmalar, bir P_k cümlesinin genişletilip genişletilemediği problemi üzerinde yoğunlaşmıştır. Biz ise çalışmamızda diğerlerinden farklı olarak P_{-2} özelliğinde olan cümlelerin ayrıntılı bir karakterizasyonunu yaptık. Şöyleki: P_{-2} özelliğini sağlayan üçlülerin teşkili, bunların oluşturduğu cümle aileleri ve eleman sayıları hakkında bir takım sonuçlar elde ettik.İlave olarak üçlüler şeklinde ele aldığımız P_{-2} cümlelerinin genişletilemediğini de ıspat ettik.

Bu çalışma üç bölümden oluşmuştur.Birinci bölüm , ihtiyaç duyacağımız temel tanım ve teoremleri kapsamaktadır. İkinci bölümde, P_{-2} özelliğinde olan {1,b,c}, {2,b,c} ve genel olarak {a,b,c} üçlülerinin teşkili ve bunların oluşturdukları aileleri karakterize eden beş tane teoremin ifade ve ıspatını verdik. Bu ıspatlarda Pell denkleminin geniş bir uygulamasını da yaptık. Çalışmamızın son bölümü olan üçüncü bölüm ise, üç tane teoremin ifade ve ıspatını kapsamaktadır. Bu teoremlerde, kongrüans teorisini kullanarak ve eşzamanlı Diophantine denklemleri oluşturarak P_{-2} özelliğinde olan {1,b,c}, {2,b,c} ve en genel halde {a,b,c} üçlülerinin dörtlülere genişletilemediğini göstermiş olduk.

BİRİNCİ BÖLÜM

1.TEMEL TANIM VE TEOREMLER

Bu bölümde daha sonraki bölümlerde kullanacağımız temel tanım ve teoremleri vereceğiz.

Tanım 1.1. $n \neq 0$, $n \in Z$ olsun. Şayet $n \mid (x-y)$ ise x, y ile n modülüne göre kongrüenttir denir ve $x \equiv y \pmod{n}$ yazılır. n modülüne göre x tamsayısına kongrüent olan bütün tam sayıların cümlesine (mod n) ye göre bir kongrüans sınıfı denir [2].

Kongrüans bağıntıları aşağıdaki özellikleri sahiptirler [3]. $x, y, z, t \in Z$ olmak üzere

i) $x \equiv y \pmod{n}$ ve $y \equiv z \pmod{n}$ ise $x \equiv z \pmod{n}$

ii) $x \equiv y \pmod{n}$ ve $t \equiv z \pmod{n}$ ise $x \pm t \equiv y \pm z \pmod{n}$

iii) $x \equiv y \pmod{n}$ ve $t \equiv z \pmod{n}$ ise $x.t \equiv y.z \pmod{n}$

iv) $x \equiv y \pmod{n}$ ise $x.t \equiv y.t \pmod{n}$

v) $x \equiv y \pmod{n}$ ve $h \in Z^+$ ise $x^h \equiv y^h \pmod{n}$

vi) $f(x)$, katsayıları tam olan bir polinom olsun. Eğer $x_0 \equiv y_0 \pmod{n}$ ise

$f(x_0) \equiv f(y_0) \pmod{n}$

vii) $m \in Z$ ve $m.x \equiv m.y \pmod{n}$, $(m,n)=d$ ise $x \equiv y \pmod{n/d}$

viii) $(m,n)=1$, $m.x \equiv m.y \pmod n$ ise $x \equiv y \pmod n$

Tanım 1.2 a ve b tamsayıları (mod n) ye göre aynı kalana sahip iseler, bu tamsayılara n modülüne göre aynı kalan sınıfındandır denir. a ve b tamsayılarının aynı kalan sınıfında olması için gerek ve yeter şart $a \equiv b \pmod n$ olmasıdır [3].

Tanım 1.3. $0,1,2,\ldots,n-1$ elemanlarının oluşturduğu cümleye n modülüne göre bir komple kalan sistemi (sınıfı), bu elemanlardan n ile aralarında asal olanların oluşturduğu cümleye de n modülüne göre indirgenmiş kalan sistemi (sınıfı) adı verilir [4].

Tanım 1.4. $n \nmid a$ olmak üzere $ax + b \equiv 0 \pmod n$ şeklinde tanımlanan kongrüansa lineer kongrüans denir. Eğer $(a,n) = d$ ve $d \mid b$ ise bu kongrüansın d tane çözümü vardır. Özel olarak $d = 1$ ise bu kongrüansın bir tane çözümü vardır [3].

Tanım 1.5. $a_0, a_1, \ldots, a_k$ tam sayılar olmak üzere $f(x) = a_0x^k + a_1x^{k-1} + \ldots + a_k$ şeklinde tanımlanan polinoma tam katsayılı polinom yada kısaca tam polinom adı verilir. Eğer $(a_0, a_1, \ldots, a_k) = 1$, yani katsayılar aralarında asal ise böyle bir polinoma ilkel polinom denir [3].

Tanım 1.6. $f(x)$ bir tam polinom, $n \in \mathbb{N}$ olsun. c bir tamsayı olmak üzere şayet $n \mid f(c)$ ise c tamsayısına $f(x) \equiv 0 \pmod n$ kongrüansının bir kökü yada bir çözümü denir [4].

Tanım 1.7. $b_0, b_1, \ldots, b_m, \ldots, b_r \in \mathbb{Z}$ olmak üzere $b_0 + b_1x + b_2x^2 + \ldots + b_mx^m + \ldots + b_rx^r \equiv 0 \pmod n$ cebirsel kongrüansı verilsin. Eğer n ile bölünemeyen ilk katsayı b_m ise bu kongrüansın derecesi m dir denir [3].

Şimdi $f(x) \equiv 0 (\mathrm{mod}\ n)$ şeklindeki kongrüansların çözümlerini karakterize eden üç tane teoremin ifadesini verelim.

Teorem 1.1. p asal ve $f(x) \equiv 0 (\mathrm{mod}\ p)$ kongrüansı m. inci mertebeden bir kongrüans olsun. Bu takdirde bu kongrüansın $(\mathrm{mod}\ p)$ ye göre birbirine kongrüent olmayan en fazla m tane çözümü vardır [5].

Teorem 1.2. $f(x)$, tam bir polinom, $m_1, m_2, \ldots, m_r$ ikişer ikişer aralarında asal olan pozitif tamsayılar ve $m = m_1 . m_2 \ldots m_r$ olsun. Bu takdirde $f(x) \equiv 0 (\mathrm{mod}\ m)$ kongrüansının çözülebilir olması için gerek ve yeter şart her bir $i (i=1, 2, \ldots, r)$ için $f(x) \equiv 0 (\mathrm{mod}\ m_i)$ kongrüanslarının çözülebilir olmasıdır [5].

Teorem 1.3. $f(x)$ bir tam polinom, p asal, $\alpha \geq 2$, $\alpha \in Z$ olsun. $f(x) \equiv 0 (\mathrm{mod}\ p^{\alpha})$ kongrüansının bir çözümünün x_0 olması için gerek ve yeter şart $x_0 = a + y_0 p^{\alpha-1}$ olmasıdır. Burada a, $f(x) \equiv 0 (\mathrm{mod}\ p^{\alpha-1})$ kongrüansının bir çözümü, y_0 ise $(f(a)/p^{\alpha-1}) + yf'(a) \equiv 0 (\mathrm{mod}\ p)$ kongrüansının bir çözümüdür. Ayrıca $0 \leq a < p^{\alpha-1}$ ve $0 \leq y_0 < p$ dir [6].

İlerleyen bölümlerde ifade ve ispat edeceğimiz teoremlerde sık sık kuadratik kongrüanslarla karşılaşacağız. Bu sebeble kuadratik kongrüanslar ve kuadratik rezidülerle ilgili tanım ve teoremleri aşağıda vereceğiz.

Tanım 1.8. $n \neq 0$ ve $n \in Z$, $(a, n) = 1$ olacak şekilde a ve n tamsayıları verilsin. $q \geq 2$ şartını sağlayan q doğal sayısı için $x^q \equiv a (\mathrm{mod}\ n)$ kongrüansı çözülebiliyor ise a ya n modülüne göre q. inci kuvvetten rezidü denir. Özel olarak $q=2$ ise a ya kuadratik rezidü, $q=3$ ise kübik, $q=4$ ise bikuadratik rezidü adı verilir[3].

Tanım 1.9. $n \neq 0$, $(a, n)=1$ olmak üzere $x^2 \equiv a(\mathrm{mod}\ n)$ şeklinde verilen kongrüans çözülebilir ise a ya n nin kuadratik rezidüsü, bu kongrüans çözülemez ise a ya n nin kuadratik olmayan rezidüsü denir. Kısalık için kuadratik rezidü KR ile, kuadratik olmayan rezidü KN ile gösterilir[3].

Teorem 1.4. $h \in Z^+$ olmak üzere $p=2h+1$ şeklinde verilen bir tek asal olsun. a tamsayısı p nin bir kuadratik rezidüsü veya kuadratik olmayan rezidüsü ise sırasıyla $a^{1/2.(p-1)} \equiv +1(\mathrm{mod}\ p)$ veya $a^{1/2.(p-1)} \equiv -1(\mathrm{mod}\ p)$ dir[3].

Teorem 1.5. p tek asal sayısının kuadratik ve kuadratik olmayan rezidülerinin sayısı eşittir ve her ikiside $(p-1)/2$ tanedir[4].

Teorem 1.6. -2 sayısı verilsin. Bu takdirde $8n+1$ ve $8n+3$ sayıları asal olacak şekilde herhangi iki sayı ise, -2 sayısı bu asallar için bir KR dür. Ayrıca $8n+5$ ve $8n+7$ sayıları asal olacak şekilde herhangi iki sayı ise -2 sayısı bu asallar için bir KN dür[3].

Tanım 1.10. (Legendre Sembolü): p tek asal, $n \not\equiv 0(\mathrm{mod}\ p)$ olsun. Bu takdirde $\left(\frac{n}{p}\right)$ ile gösterilen ve " p üzerinde n" diye okunan legendre sembolü

$$\left(\frac{n}{p}\right)=\begin{cases} +1, & \text{eğer } n, p \text{ asalının bir KR sü ise} \\ -1, & \text{eğer } n, p \text{ asalının bir KN sü ise} \end{cases}$$

şeklinde tanımlanır. Şayet $n \equiv 0(\mathrm{mod}\ p)$ ise $\left(\frac{n}{p}\right)=0$ dır[5].

Legendre sembolünün aşağıdaki özellikleri vardır[7].

i) $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

ii) $a \equiv b(\mathrm{mod}\ p)$ ise $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$

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

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

Şimdi de Legendre sembolünün daha genel bir ifadesi olan Jakobi sembolünü tanımlayalım.

Tanım 1.11. (Jakobi Sembolü): P tek pozitif tamsayısı her bir $i(i=1,2,\ldots,r)$ için p_i ler asal olmak üzere $P=\prod_{i=1}^{r} p_i^{\alpha_i}$ şeklinde verilsin. Bu taktirde $\left(\frac{n}{P}\right)$ Jakobi sembolü, $\left(\frac{n}{p_i}\right)$ Legendre sembolü olmak üzere

$$\left(\frac{n}{P}\right)=\prod_{i=1}^{r}\left(\frac{n}{p_i}\right)^{\alpha_i}$$

eşitliği ile verilir. Buna göre $\left(\frac{n}{P}\right)=1,-1,0$ olabilir.

Ayrıca $\left(\frac{n}{P}\right)=0$ olması için gerek ve yeter şart $(n,P)>1$ olmasıdır[5].

Şimdi Jakobi sembolü ile $x^2 \equiv a(\mathrm{mod}\ P)$ kongrüansının çözülebilir olması arasındaki ilişkiyi belirtelim. Eğer $x^2 \equiv a(\mathrm{mod}\ P)$ kongrüansının bir çözümü varsa P' nin bir çarpanı olan her p_i asalı için $\left(\frac{a}{p_i}\right)=1$ olacağından $\left(\frac{a}{P}\right)=1$ dir. Yani verilen kongrüans çözülebilir ise $\left(\frac{a}{P}\right)=1$ dir. Ancak bunun tersi doğru değildir. Başka bir ifade ile $\left(\frac{a}{P}\right)=1$ olması $x^2 \equiv a(\mathrm{mod}\ P)$ kongrüansının çözülebilir olmasını gerektirmez. Zira P nin herhangi iki çarpanı olan p_i, p_j asalları için $\left(\frac{a}{p_i}\right)=-1$, $\left(\frac{a}{p_j}\right)=-1$, olduğu halde $\left(\frac{a}{P}\right)=+1$ dir. Halbuki $\left(\frac{a}{p_i}\right)=-1$ ise $x^2 \equiv a\ (\mathrm{mod}\ P)$ kongrüansı çözülemezdir.

Teorem 1.7. (Karşılıklı Kuadratik Rezidü Teoremi): Eğer p ve q tek asallar ise bu taktirde

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

dir[4].

Teorem 1.8. Eğer p ve q tek asallarının her ikiside 4n+3 şeklinde ise $\left(\frac{p}{q}\right)=-\left(\frac{q}{p}\right)$, diğer durumlarda $\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)$ dir [4].

Aşağıda ifadelerini vereceğimiz üç teorem de özellikle, kuadratik kongrüansların çözülebilmesi için gerek ve yeter şartları ortaya koydukları gibi, bu tür kongrüansların kaç tane çözümlerinin olduğu hakkında da bize bilgi verirler.

Teorem 1.9. $x^2 \equiv a \pmod n$ kongrüansı verilsin. $(a,n)=d$, $d=e^2f$, $a=da_1$, $n=dn_1$, e, f, a_1, n_1 tamsayılar ve f karesel olmayan bir tamsayı olsun. Bu taktirde verilen kongrüansın çözülebilir olması için gerek ve yeter şart $(f,n_1)=1$ ve fa_1 değerinin n_1 in bir KR sü olmasıdır [3].

Teorem 1.10. p bir tek asal, a ; p ile bölünemeyen bir tamsayı, $q \geq 2$, ve $p\nmid q$ olacak şekilde q doğal sayısı verilsin. Eğer $x^q \equiv a \pmod{p^\alpha}$ kongrüansı $\alpha=1$ için çözülebilir ise $\alpha > 1$ olan bütün α tamsayıları için de çözülebilirdir [3].

Teorem 1.11.

i) q, a tek sayılar olsun. Bu taktirde $x^q \equiv a \pmod{2^\alpha}$ kongrüansının tam bir tane çözümü vardır.

ii) a tek, $q=2m$, m tek tamsayı olsun. $\alpha \geq 3$ olmak üzere $x^q \equiv a \pmod{2^\alpha}$ kongrüansı, şayet $a \equiv 1 \pmod 8$ ise dört tane birbirine kongrüent olmayan çözüme sahiptir. Diğer durumlarda çözüm yoktur.

iii) a tek sayı, $q=2m$, m tek tamsayı ve $\alpha=2$ olsun. Bu taktirde $x^q \equiv a \pmod{2^\alpha}$

kongrüansı , şayet $a \equiv 1 \pmod 4$ ise iki tane birbirine kongrüent olmayan çözüme sahiptir. Diğer durumlarda çözüm yoktur [3].

Buraya kadar verdiğimiz tanım ve teoremler genel olarak kongrüanslar teorisi üzerine olan tanım ve teoremlerdir.Çalışmamızın ilerleyen bölümlerinde bunları sık sık kullanma ve uygulama imkanı bulacağız. Bu çalışmamızda çok sık olarak kullanmaya ihtiyaç duyacağımız bir kavram da Diophantine Denklem kavramıdır. Özellikle Sayılar Teorisi literatüründe Pell Denklemi olarak geçen ve D karesel olmayan bir tamsayı olmak üzere

$$x^2-Dy^2=1 \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots(1.1)$$

şeklinde tanımlanan Diophantine denklemi, ıspatını ileriki bölümlerde yapacağımız teoremlerde sık sık kullanacağımız bir çok özelliklere sahiptir.
O halde (1.1) Diophantine denklemini karakterize eden temel teoremlerin ifadelerini ve bu denklemle ilgili tanımları aşağıda verelim.

Teorem 1.12. (1.1) Diophantine denklemini sağlayan en az bir tane x,y doğal sayı çifti vardır [3].

Tanım 1.12. (1.1) Diophantine denkleminin bütün çözümleri (x,y) olarak verilsin. Eğer (x_1,y_1) verilen bütün çözümlerin en küçüğü ise (x_1,y_1) çözümüne (1.1) Pell denkleminin minimal veya temel çözümü denir [3].

Tanım 1.13. (1.1) denkleminin bir (x_0,y_0) çözümü eğer $x_0.y_0=0$ şartını sağlıyorsa bu (x_0,y_0) çözümüne (1.1) Pell denkleminin triviyal (aşikar) çözümü denir [3].

Tanım 1.14. (1.1) denkleminin herhangi iki çözümü (x_1,y_1) ve (x_2,y_2) olarak verilsin. Eğer $x_1=x_2$ ve $y_1=y_2$ ise bu iki çözüm birbirine eşittir denir. Şayet bu çözümler için $x_1+y_1\sqrt{D} > x_2+y_2\sqrt{D}$ şartı sağlanıyorsa (x_1,y_1) çözümü diğerinden büyüktür denir [3].

Teorem 1.13. (1.1) Diophantine denkleminin sonsuz tane çözümü vardır. (x_n, y_n) şeklindeki bütün çözümler ; (x_1, y_1) temel çözümler olmak üzere

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

eşitliğinden elde edilir.Burada $n \in \mathbb{N}$ dir [3].

(1.1) Diophatine denkleminin minimal çözümü genel olarak deneme yoluyla bulunabilir. Ancak bazı durumlarda bu yolla minimal çözüm bulmak pek kolay olmaz. Bu taktirde (1.1) denkleminin çözümlerini bulmak için

$$u^2-Dv^2=-1 \quad \ldots\ldots\ldots\ldots\ldots\ldots(1.2)$$

denkleminden faydalanabiliriz.Şimdi ilgili teoremi verelim.

Teorem 1.14 (1.2) Diophantine denklemi çözülebilir ve temel çözümü (u_1, v_1) olsun. Bu taktirde, (x_1, y_1) (1.1) denkleminin temel çözümü ise

$$(x_1+y_1\sqrt{D}) = (u_1+v_1\sqrt{D})^2$$

dir. Ayrıca

$$(u_n+v_n\sqrt{D})= (u_1+v_1\sqrt{D})^n$$

eşitliğinde

i)n ; bütün pozitif tek tamsayıları taradığında u_n ve v_n ler (1.2) denkleminin bütün çözümlerini verirler.

ii)n ; bütün pozitif çift tamsayıları taradığında $x = u_n$, $y=v_n$ de (1.1) denkleminin bütün çözümlerini verirler [3].

D karesel olmayan bir doğal sayı , C sıfırdan farklı bir tamsayı olmak üzere

$$u^2-Dv^2= C \quad \ldots\ldots\ldots\ldots\ldots\ldots(1.3)$$
$$u^2-Dv^2=-C \quad \ldots\ldots\ldots\ldots\ldots\ldots(1.4)$$

şeklinde verilen Diophantine denklemlerini göz önüne alalım.

Tanım 1.15. (1.3) Denkleminin bir çözümü; (u,v), (1.1) denkleminin bir çözümü (x,y) olsun. Bu takdirde;

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

olduğundan (u',v') de (1.3) denkleminin bir çözümüdür. Bu çözüme (u,v) ile birleştirilmiş çözüm denir. Birleştirilmiş bütün çözümlerin cümlesi de (1.3) ün çözüm sınıfını oluştururlar [3].

(1.3) denkleminin herhangi iki çözümü (u,v) ve (x,y) olsun. Bu iki çözümün aynı sınıftan olması için gerek ve yeter şart

$$\frac{ux - vyD}{C} \quad \text{ve} \quad \frac{vx - uy}{C} \quad \ldots\ldots (1.5)$$

değerlerinin tamsayı olmalarıdır [3].

Bir K sınıfının (u_i,v_i),(i=1,2,3,...) çözümlerini kapsadığını düşünelim. $(u_i,-v_i)$, (i=1,2,3,...) çözümlerinin oluşturduğu sınıfı da $\overline{K}$ ile gösterelim. K ve $\overline{K}$ sınıflarına biribirinin Konjugesi denir. K ve $\overline{K}$ sınıfları genellikle farklıdırlar. Eğer aynı iseler K sınıfına belirsiz (muğlak) sınıf denir. K dan bir(u^*, v^*) çözümünü seçelim. v^* , K daki v lerin negatif olmayan en küçük değeri olsun. Eğer K belirsiz değilse, u^* da v^* gibi tek türlü seçilir. Eğer K belirsiz ise $u^* \geq 0$ olacak şekilde tek türlü seçilebilir. Bu şekilde seçilen (u^*, v^*) çözümüne K nın temel çözümü adı verilir. Eğer $C=\pm 1$ ise (1.3) denkleminin çözüm sınıfı bir tanedir ve oda belirsizdir. [3].

Teorem 1.15. (1.3) denkleminin bir K sınıfının temel çözümü (u,v), (1.1) denkleminin temel çözümü de (x_1, y_1) ise

$$0 \leq v \leq \frac{y_1}{\sqrt{2(x_1+1)}} \sqrt{C} \qquad \ldots\ldots.(1.6)$$

$$0 < |u| \leq \sqrt{\tfrac{1}{2}(x_1+1)C}$$

eşitsizlikleri sağlanır [3].

Teorem 1.16. (1.4) Diophantine denkleminin bir K sınıfının temel çözümü (u,v) ve (1.1) in temel çözümü (x_1, y_1) ise

$$0 \leq v \leq \frac{y_1}{\sqrt{2(x_1-1)}} \sqrt{C} \qquad \ldots\ldots.(1.7)$$

$$0 \leq |u| \leq \sqrt{\tfrac{1}{2}(x_1-1)C}$$

eşitsizlikleri sağlanır[3].

Şimdi de (1.3) ve (1.4) Diophantine denklemlerinin bütün çözümlerinin nasıl bulunacağını gösteren bir teoremin ifadesini verelim.

Teorem 1.17. (1.3) ve (1.4) Diophantine denklemlerinin bütün çözüm sınıflarının sayısı sonlu ve bütün sınıfların temel çözümleri bulunabilsin. Ayrıca bu temel çözümler (1.6) ve (1.7) şartlarını sağlasınlar. Eğer (u^*, v^*), K sınıfının bir temel çözümü ise K sınıfının (u,v) şeklindeki bütün çözümleri

$$u+v\sqrt{D} = (u^* + v^*\sqrt{D})\ (x+y\sqrt{D})$$

şeklinde verilir. Burada (x,y), (1.1) denkleminin bütün çözümlerini taramaktadır[3].

İKİNCİ BÖLÜM

2. P_{-2} CÜMLELERİNİN TEŞKİLİ VE ÖZELLİKLERİ.

Bu bölümde P_{-2} cümlelerini göz önüne alacağız.Önce genel olarak $k \in Z$ olmak üzere P_k özelliğini tanımlayacağız.Daha sonra k=-2 için özel olarak P_{-2} özelliğini sağlayan elemanların oluşturduğu cümleleri inceleyeceğiz.

Tanım.2.1. $i \neq j$ $(i, j = 1, 2,...,n)$ olmak üzere $x_i x_j + k$=tam kare şartını sağlayan $x_1, x_2,...x_n$ pozitif tamsayılarına n.inci tipten P_k özelliğine sahip elemanlar, bunların oluşturduğu cümleye de P_k özelliğine sahip cümle adı verilir[15].

Buna göre k=-2 alındığında elde edilecek cümleye P_{-2} özelliğini sağlayan cümle denir.

Eğer a, b, c üçlüsü P_{-2} özelliğini sağlayan bir üçlü ise, bu takdirde $x, y, z \in Z$ olmak üzere,

$$
\begin{aligned}
&a.b-2=x^2 \\
&a.c-2=y^2 \quad \text{.......................................}(2.1) \\
&b.c-2=z^2
\end{aligned}
$$

eşitliklerini sağlarlar.Burada bizim problemimiz (2.1) sistemini sağlayan a,b,c doğal sayılarının nasıl bulunacağıdır.Bu problemi düşünürken $a < b < c$

sıralamasını yaparsak hem genelliği bozmamış olur, hem de bulabileceğimiz a,b,c üclülerinde sıralama problemini ortadan kaldırmış oluruz. a,b,c doğal sayılarını bulma problemi simdi (2.1) sistemini oluşturan Diophantine denklemlerinin çözümlerini bulma problemi olarak alınabilir.

(2.1) sisteminde a=1 alalım.Bu taktirde aradığımız üçlüler {1,b,c} üçlüleridir. Bu üçlülerin belirlenmesini sağlayan aşağıdaki teoremi verelim:

Teorem 2.1. $a=1$, $1<b<c$, $b, c \in \mathbb{N}$ olmak üzere (2.1) sistemini sağlayan sonsuz tane $\{1,b,c\}$ üçlüleri vardır.

Ispat : (2.1) Sisteminin birinci ve ikinci denklemlerinden $b=x^2+2$, $c=y^2+2$ elde ederiz.Üçüncü denklemde bu değerleri yerine koyarsak,

$$(x^2+2)(y^2+2)-2=z^2 \qquad \text{.......................................} (2.2)$$

denklemini buluruz. (2.2) eşitliğinin sol tarafı

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

şeklinde yazılabilir.Bu ifade de $y-x=\pm 1$ şartını sağlayan her $x,y \in \mathbb{Z}$ için bir

tamkare olacağından $0 \le x < y$ alarak,(2.1) sistemini sağlayan $\{1, b, c\}$ üçlülerini bulmak daima mümkündür. Mesela hemen aklımıza gelen $\{1,b,c\}$ üçlüleri $\{1,2,3\}$, $\{1,3,6\}$, $\{1, 6, 11\}$, $\{1,11,18\}$, ... şeklinde olur. Bunlara (2.1) sisteminin temel çözümleri adını verelim.Bu taktirde $b=x^2+2$, $c=y^2+2$ ve $y-x=\pm 1$ olduğu dikkate

alınırsa (2.1) sisteminin temel çözümlerini $n \in \mathbb{N}_0$ olmak üzere

$$\{1, b, c\}=\{1, n^2+2, n^2+2n+3\} \qquad \text{..............................} (2.3)$$

şeklinde ifade edebiliriz. Herbir $n \ge 0$ tamsayısı için bir üçlü elde edilebileceğinden, bu üçlülerin sayısı sonsuz tanedir. Bu da teoremin ıspatını tamamlar.

Teorem 2.2. $x_0 \ge 0$ eşitsizliğini sağlayan her bir x_0 tamsayısına karşılık P_{-2} özelliğini sağlayan sonsuz tane elemanların oluşturduğu bir

$A_{x_0}=\{\{1,\ b(x_0),\ c_i\}\}_{i\in I}$ cümleler ailesi vardır, burada $I \subset N$ dir. $x_0 \neq y_0$ için $A_{x_0} \cap A_{y_0} = \emptyset$ dir.

Ispat : Teorem 2.1. de P_{-2} özelliğini sağlayan $\{1,b,c\}$ üçlülerinin varlığını ıspat ettik.(2.1) sisteminin düzenlenmesi ile elde edilen (2.2) eşitliğini gözönüne alalım.(2.2) eşitliği düzenlenirse

$$z^2-(x^2+2)y^2 = 2(x^2+1) \qquad \text{.........(2.4)}$$

denklemi elde edilir.Eğer $x=x_0$ ise (2.4) denklemi

$$z^2-(x_0^2+2)y^2 = 2(x_0^2+1) \qquad \text{.........(2.5)}$$

şeklinde ifade edilebilir. (2.5) denklemi bir Diophantine denklemidir. Ve biz bunun bütün çözümlerini arıyoruz.Teorem 2.1 den her $y = x+1$ için (2.1) sistemini sağlayan uygun üçlüler bulabileceğimize göre (2.5) denkleminde $y=x_0 \pm 1$ yazar ve düzenlersek $z = x_0^2 \pm x_0+2$ elde ederiz.Böylece (2.5) Diophantine denklemi için,

$$(x_0\ ,\ x_0 \pm 1\ ,\ x_0^2 \pm x_0+2)\ ,\ (x_0 \geq 0) \qquad \text{.........(2.6)}$$

çözümünü elde ederiz. (2.6) ile bulduğumuz çözümlere (2.5) Diophantine denkleminin temel çözümleri diyelim.

Şimdi (2.5) Diophantine denklemine yeniden dönelim. Her $x_0 \geq 0$ şartını sağlayan x_0 tamsayısı için $x_0^2+2=D$ sayısı karesel bir sayı değildir. Aksinin doğru olduğunu kabul edelim. Yani $p \in N$ olmak üzere $x_0^2+2=p^2$ olduğunu kabul edelim.Bu taktirde

$$x_0^2+2 = p^2$$

$$p^2 - x_0^2 = 2$$

$$(p-x_0)\,(p+x_0) = 2$$

Ve burada $p-x_0=1$, $p+x_0=2$ ve buradan da $2p=3$, $p=3/2 \notin N$ elde edilir.Bu da bir çelişkidir. Böylece (2.5) denklemi $D= x_0{}^2+2$ karesel olmayan tamsayı olmak üzere

$$z^2-Dy^2=2(D-1) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2.7)$$

şekline dönüşür.

şimdi $x_0 \geq 0$ için (2.7) denkleminin çözümlerini inceleyelim. $x_0=0$ ise (2.7) denklemi

$$z^2-2y^2=2 \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2.8)$$

denklemini verir. (2.8) in bütün çözümlerini bulmak için

$$z^2-2y^2=1 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2.9)$$

Pell Denklemine ihtiyaç duyarız. Tanım 1.12. den (2.9) denkleminin temel çözümü $(\mathcal{Z},\mathcal{Y})=(3,2)$ ve Teorem 1.13. den (2.9) denkleminin bütün çözümleri $(\mathcal{Z}_n,\mathcal{Y}_n)$ ise

$$(\mathcal{Z}_n+\mathcal{Y}_n\sqrt{2})=(3+2\sqrt{2})^n \quad (n=0,1,2,3,\ldots)$$

şeklinde verilir.Diğer taraftan (2.8) denkleminin (2.6) ile verilen temel çözümleri $(z,y)=(2,1), (2,-1)$ dir.Halbuki Tanım 1.15 ve (1.5) ifadelerine göre (2,1) ve (2,-1) çözümleri aynı sınıftandır. (2.8) denkleminin (1.6) ile elde edilecek çözümleri ile (2.6) ile elde edilecek çözümleri aynıdır ve bir tanedir.O halde (2.8) denkleminin çözüm sınıf numarası 1 dir. Teorem .1.17 uyarınca (2.8) denkleminin bütün çözümleri (z_n,y_n) şeklinde ise,

$$(z_n+y_n\sqrt{2})=(2+\sqrt{2})(3+2\sqrt{2})^n \quad (n=0,1,2,3,\ldots)$$

şeklinde verilir.Bu çözümlerle ilgili kısa bir tablo verelim

n	z_n	y_n
0	2	1
1	10	7
2	58	41

3	338	239
4	1970	1393
5	11482	8119
6	66922	41321
7	390050	27587
8	2273378	1607521

TABLO -1-

Tablo-1.den hareketle (2.8) Diophantine denkleminin $x_0=0$ için elde ettiğimiz çözümleri ve buna karşılık gelen $\{1,b,c_i\}$ üçlülerinden bir kaç tanesini aşağıda verelim. (2.1) den $b=x_0^2+2$, $c=y^2+2$ olduğundan

$(x,y,z)=(0,1,2)$	üçlüsüne	karşılık	$\{1,b,c_1\}=\{1,2,3\}$
" $=(0,7,10)$	"	"	$\{1,b,c_2\}=\{1,2,51\}$
" $=(0,41,58)$	"	"	$\{1,b,c_3\}=\{1,2,1683\}$
" $=(0,239,338)$	"	"	$\{1,b,c_4\}=\{1,2,57123\}$

....

üçlülerini elde ederiz. Böylece $x_0=0$ için

$$A_0=\Big\{\{1,2,3\}, \{1,2,51\}, \{1,2,1683\}, \{1,2,57123\}, \ldots\Big\}$$

cümleler ailesini elde etmiş olduk.

Şimdi $x_0=1$ alalım. Bu taktirde (2.7) denklemi

$$z^2-3y^2=4 \qquad \text{.......................................} (2.10)$$

şeklinde olur. (2.10) Diophantine denkleminin bütün çözümlerini bulmak için

$$z^2-3y^2=1 \qquad \text{.......................................} (2.11)$$

Pell Denklemini kullanacağız. (2.11) Pell Denkleminin temel çözümü

$(x,y) = (2,1)$ dir. (2.10) denkleminin temel çözümleri ise (2.6) dan $(z,y)=(4,2),(2,0)$ dır. Halbuki (1.5) şartları uyarınca bunlar aynı sınıftandır ve (2.10) denkleminin çözüm sınıf numarası 1 dir. O halde (2.10) denkleminin bütün çözümleri (z_n,y_n) şeklinde ise Teorem .1.17 gereğince

$$(z_n+\sqrt{3}\,y_n)=(4+2\sqrt{3})\,(2+\sqrt{3})^n \qquad (n=0,1,2,3,\ldots)$$

şeklinde verilir.Elde edilecek çözümlerle ilgili kısa bilgi Tablo-2 ile aşağıda verilmiştir.

n	z_n	y_n
0	4	2
1	14	8
2	52	30
3	194	112
4	724	418
5	2702	1560
6	10084	5822
7	37634	21728
8	140452	81090

<u>TABLO-2</u>

Tablo-2.yi gözönünde bulundurursak $x_0=1$ alındığında elde edeceğimiz $\{1,b,c_i\}$ üçlüleri

$(x,y,z)=(1,2,4)$	üçlüsüne	karşılık	$\{1,b,c_1\}=\{1,3,6\}$
" $=(1,8,14)$	"	"	$\{1,b,c_2\}=\{1,3,66\}$
" $=(1,30,52)$	"	"	$\{1,b,c_3\}=\{1,3,902\}$
" $=(1,112,192)$	"	"	$\{1,b,c_4\}=\{1,3,12546\}$

şeklinde olur. Yani $x_0=1$ için (2.1) sistemini sağlayan $\{1,b,c_i\}$ üçlülerinin cümlesi olarak

$$A_1=\Big\{\{1,3,6\},\{1,3,66\},\{1,3,902\},\{1,3,12546\},\ldots\Big\}$$

cümleler ailesini bulmuş oluruz.

$x_0=2$ aldığımızda (2.7) Diophantine Denklemi

$$z^2-6y^2=10 \quad \ldots\ldots\ldots\ldots\ldots (2.12)$$

ve Pell Denklemi de

$$z^2-6y^2=1 \quad \ldots\ldots\ldots\ldots\ldots (2.13)$$

şeklinde elde edilir. (2.12) nin temel çözümleri (2.6) dan $(z,y)=(8,3)$, $(4,1)$ dir. Ve (1.5) şartları uyarınca bunlar ayrı sınıftandır. O halde (2.12) denkleminin çözüm sınıf numarası 2 dir. Dolayısı ile Teorem 1.17 dikkate alınırsa (2.13) ün minimal çözümü $(\bar{z},\bar{y}) = (5,2)$ olduğundan ,(2.12) nin bütün çözümleri

$$(z_n+\sqrt{6}\,y_n) = (8+3\sqrt{6})(5+2\sqrt{6})^n \quad (n=0,1,2,3,\ldots)$$

$$(z_n^*+\sqrt{6}y_n^*) = (4+\sqrt{6})(5+2\sqrt{6})^n \quad (n=0,1,2,3,\ldots)$$

eşitlikleri ile verilir. Bu eşitliklerle elde edilen (2.12) nin çözümlerinin bir kaçı aşağıda Tablo.3 ve Tablo.4 ile verilmiştir.

n	z_n	y_n
0	8	3
1	76	31
2	752	307
3	7444	3039
4	73688	30083
5	729436	297791
6	7220672	2947827

7	71477284	29180479
8	707552168	288856963

TABLO-3

n	z_n^*	y_n^*
0	4	1
1	32	13
2	316	129
3	3128	1277
4	30964	12641
5	306512	125133
6	3034156	1238689
7	30035048	12261757
8	297316324	121378881

TABLO-4

Tablo.3, Tablo.4 gözönünde bulundurulursa $x_0=2$, ve (2.12) denkleminin çözümlerine karşılık gelen $\{1,b,c_i\}$ üçlüleri

$(x,y,z)=(2,3,8)$	üçlüsüne karşılık		$\{1,b,c_1\}=\{1,6,11\}$
" $=(2,13,32)$	"	"	$\{1,b,c_2\}=\{1,6,171\}$
" $=(2,31,76)$	"	"	$\{1,b,c_3\}=\{1,6,963\}$
" $=(2,129,316)$	"	"	$\{1,b,c_4\}=\{1,6,16643\}$

....

ve böylece $x_0=2$ için

$$A_2=\{\{1,6,11\},\{1,6,171\},\{1,6,963\},\{1,6,16643\},\ldots\}$$

cümleler ailesini elde ederiz.

Benzer bir düşünce ile hareket ederek $x_0=3,4,5,\ldots$ için de sırasıyla A_3, A_4, A_5...

aileleri elde edilir. O halde her bir $x_0 \geq 0$ tamsayısı için bir A_{x_0} cümleler ailesi bulunmuş olur. Ayrıca (2.7) Diophantine Denkleminin her bir x_0 için sonsuz tane çözümü olacağından A_{x_0} ailesi sonsuz elemanlı olacaktır. Diğer taraftan $A_{x_0}=\{\{1, b(x_0), c_i\}\}_{i \in I}$ ailesinin teşkil tarzından $b=x_0^2+2$ dir. $x_0 \neq y_0$ için $b(x_0) \neq b(y_0)$ olacağından $A_{x_0} \cap A_{y_0} = \emptyset$ sonucunu elde etmiş oluruz. Bu da teoremin ıspatını tamamlar.

Şimdi (2.1) denklem sisteminde a=2 alalım. Bu taktirde

$$\begin{aligned} &2b-2=u^2 \\ &2c-2=v^2 \qquad \text{..............................(2.14)} \\ &bc-2=t^2 \end{aligned}$$

denklem sistemi elde ederiz. Burada $u,v,t \in Z$ dir. (2.14) denklem sistemini sağlayan $\{2,b,c\}$ üçlülerini bulmak demek P_{-2} özelliğini sağlayan üçlüler bulmak demektir. Şimdi $\{2,b,c\}$ üçlüleriyle ilgili bir teoremin ifade ve ispatını verelim.

Teorem 2.3. $u,v,t \in Z$ olmak üzere (2.14) sistemini sağlayan sonsuz tane $\{2,b,c\}$ doğal sayı üçlüleri vardır.

Ispat: (2.14) sisteminin birinci ve ikinci denklemlerinden $2|u^2$ ve $2|v^2$ elde ederiz. O halde $u=2U$, $v=2V$ yazılırsa $b=2U^2+1$, $c=2V^2+1$ elde edilir. $2<b<c$ ve $b,c \in N$ olduğundan $1 \leq U < V$ olmalıdır. Bulunan bu b ve c değerleri (2.14) sisteminin üçüncü denkleminde yerlerine yazılırsa

$$(2U^2+1)(2V^2+1)-2=t^2 \quad \text{........................ (2.15)}$$

eşitliğini elde ederiz. Halbuki (2.15) eşitliğinin sol tarafı

$$(2UV+1)^2+2[(U-V)^2-1]$$

formunda yazılabileceğinden $U-V=\pm1$ şartını sağlayan her U,V tamsayıları için (2.14) sistemini sağlayan uygun $\{2,b,c\}$ üçlüleri vardır. Mesela $\{2,3,9\}$, $\{2,9,19\}$, $\{2,19,33\}$, ... bu üçlülerden bir kaçıdır. Bu şekilde bulacağımız üçlülere (2.14) sisteminin temel çözümleri adını verelim. $b=2U^2+1$, $c=2V^2+1$ olduğundan her $n\in N$ için

$$\{2,b,c\}=\{2,\ 2n^2+1,\ 2n^2+4n+3\} \quad \text{.............................}(2.16)$$

şeklinde elde edilecek üçlüler, (2.14) sisteminin temel çözümleridir. Ayrıca (2.16) ile her n doğal sayısına karşılık bir $\{2,b,c\}$ üçlüsü elde edilebileceğinden $\{2,b,c\}$ üçlüleri sonsuz tanedir. Böylece teoremin ıspatı tamamlanmış olur.

Teorem 2.4. $u_0 \geq 1$ eşitliğini sağlayan her bir u_0 pozitif tamsayısına karşılık P_{-2} özelliğinde olan sonsuz sayıda elemanların oluşturduğu bir $A_{u_0}=\{\{2,b(u_0),c_i\}\}_{i\in I}$ cümleler ailesi vardır. Burada $I\subset N$ dir. Üstelik her $u_0\neq v_0$ için $A_{u_0}\cap A_{v_0}=\emptyset$ dır.

Ispat: Teorem 2.2.gibi yapılır.

Teorem 2.1, Teorem 2.2, Teorem 2.3 ve Teorem 2.4 ile P_{-2} özelliğini sağlayan $\{1,b,c\}$, $\{2,b,c\}$ üçlülerinin varlığını, sonsuz tane olduklarını ve bunların oluşturdukları cümlelerin hangi yapıda olduklarını vermiş olduk. Aslında yaptığımız şey (2.1) sisteminde $a=1$, $a=2$ alarak, bu sistemi çözüp, cümleler oluşturmak oldu. (2.1) sistemini sağlayan çözümler için daima $a < b < c$ sıralamasını koruduk. Bunun nedeni bir $\{a,b,c\}$ cümlesinde elemanların yerlerinin değişmesi ile cümlenin yapısı değişmeyeceğinden $a < b < c$ sıralaması, bize oluşturduğumuz ailenin herbir elemanının farklı olmasını garantilemesindendir. O halde, eğer a elemanını seçebilirsek, b ve c'yi bulmak pek zor olmayacaktır. Aklımıza şöyle bir soru gelebilir. Acaba, her a doğal sayısı için, P_{-2} özelliğinde olan $\{a,b,c\}$ doğal sayı üçlüleri varmıdır?

Bu soruya olumlu cevap vermek maalesef mümkün olmadı. Bunun için bir karşıt örnek vermek yeter. Mesela, $a=4$ alınırsa, b ve c tam sayı olarak bulunamaz. Gerçekten (2.1) sisteminin birinci denkleminden

$$4b-2=x^2$$
$$b=(x^2+2)/4$$

elde edilir. Eğer x, tek tamsayı ise $x^2 \equiv 1 \pmod 4$, x çift tamsayı ise $x^2 \equiv 0 \pmod 4$ dür. Yukarıdaki eşitliklerden $x^2 \equiv -2 \pmod 4$ elde edilir. Halbuki x'in her durumu için bu kongrüansın çözümü yoktur. O halde yukarıdaki eşitliği sağlayan uygun x tamsayısı yok, dolayısı ile uygun b tamsayısı bulunamaz. Böylece iddiamız doğrulanmış olur. O zaman şu soruyu sorabiliriz: Acaba, P_{-2} özelliğini sağlayan {a,b,c} üçlülerini teşkil etmek için a nasıl seçilmelidir?

Şimdi bu soruya cevap arayalım. (2.1)sisteminin birinci ve ikinci denklemlerinden

$$b=(x^2+2)/a\,,\ c=(y^2+2)/a \quad \text{.............................}(2.17)$$

eşitliklerini elde ederiz. $a\,.\,b=x^2+2$ olduğundan

$$x^2 \equiv -2 \pmod a \quad \text{.......................................}(2.18)$$

kongrüansını bulmuş oluruz. Böylece, a'yı belirleme problemimiz (2.18) kongrüansının çözülebilmesi problemine dönüşmüş olur.(2.18) kongrüansını sağlayan bütün a 'lar P_{-2} özelliğini sağlayan üçlülerinin teşkili için uygun a'lardır.

i) Eğer a asal olarak seçilecekse (2.18) kongrüansını sağlayan a 'lar -2 sayısını KR kabul eden a 'lardır. Yani $\left(\frac{-2}{a}\right)=1$ olan a'lar istenen a 'lardır. O halde Teorem 1.6 ya göre a sayısı, $a=8k+1$, $a=8k+3$ şeklindeki asal sayılardan seçilmelidir.

ii) a sayısı bileşik sayı olsun. Bu takdirde Teorem 1.10 dan dolayı $(8k+1)$ ve $(8k+3)$ şeklindeki asalların bütün kuvvetleri a olarak seçilebilir. Ayrıca, $(8k+1)$ ve $(8k+3)$ şeklindeki asalların 2 ile çarpımları da uygun a sayıları olabilirler. Böylece,

$$M_1=\{a: a=(8k+1)^{\alpha}\ ;\ \alpha=1,2,3,\ldots,\ (8k+1)\ \text{asal}\ ,\ k\in Z\}$$

$$M_2=\{a: a=(8k+3)^{\beta}\ ;\ \beta=1,2,3,\ldots,\ (8k+3)\ \text{asal}\ ,\ k\in Z\}$$

$$M_3=\{a: a=(8k+1)^{\alpha}.(8k+3)^{\beta};\ \alpha,\beta=1,2,3,\ldots,\ (8k+1),(8k+3)\ \text{asal}\ ,\ k\in Z\}$$

$$M_4=\{a: a=2(8k+1)^{\alpha}\ ;\ \alpha=1,2,3,\ldots,\ (8k+1)\ \text{asal}\ ,\ k\in Z\}$$

$$M_5=\{a: a=2(8k+3)^{\beta}\ ;\ \beta=1,2,3,\ldots,\ (8k+3)\ \text{asal}\ ,\ k\in Z\}$$

cümlelerinin birleşimi olan,

$$\mathfrak{M} = \{1,2\} \cup M_1 \cup M_2 \cup M_3 \cup M_4 \cup M_5$$

cümlesi a'nın seçilebileceği muhtemel değerler cümlesidir. Bu cümleyi bazı elemanları ile açık yazarsak,

$$\mathfrak{M} = \{1,2,3,6,9,11,17,18,19,22,27,34,38,41,43,51, \ldots\}$$

şeklinde olur.

Şimdi $a \in \mathfrak{M}$, $a \neq 1,2$ alarak (2.1) sistemini yeniden göz önüne alalım.(2.17) ifadelerini (2.1) sisteminin üçüncü denkleminde değerlendirirsek,

$$(x^2+2)(y^2+2) - 2a^2 = (az)^2 \qquad \text{.......................................(2.19)}$$

eşitliğini elde ederiz. (2.19) eşitliğinin sol tarafı,

$$(xy+2)^2 + 2[(x-y)^2 - a^2]$$

formunda olduğundan (2.19) eşitliğinin sol tarafı $y-x = \pm a$ şartını sağlayan her x,y için, bir karedir. O halde $y-x = \pm a$ şartını sağlayan her x,y tamsayıları için (2.1) sistemini sağlayan uygun a, b, c üçlüleri daima mevcuttur. $a < b < c$ sıralaması $x < y$ sıralamasını gerektireceğinden, $y-x = \pm a$ şartını $y-x = a$ şeklinde değerlendirebiliriz. Diğer taraftan, $a \neq 1,2$, $a \in \mathfrak{M}$ olan her a için

$0 < \mu < a/2$ ve $\mu^2 \equiv -2 \pmod a$ şartını sağlayan bir μ değeri vardır. O halde

$x = an \pm \mu$ ve $y = x+a$ alınırsa, (2.1) sistemini sağlayan ve sonsuz tane olan

$\{a, b, c\}$ üçlülerini elde etmiş oluruz. Böylece aşağıdaki teoremi ispat etmiş olduk.

Teorem 2.5. $\forall a \in \mathfrak{M}$, $(a \neq 1,2)$ için (2.1) sistemini sağlayan $\{a, b, c\}$ üçlülerinin sonsuz bir koleksiyonu vardır, öyleki bu üçlüler,

$$\{a, b, c\} = \{a,\ n(an \pm 2\mu) + (\mu^2+2)/a,\ (n+1)(an+a \pm 2\mu) + (\mu^2+2)/a\},\ (n \geq 2) \text{....(2.20)}$$

şeklindedir. Burada, $0 < \mu < a/2$ ve $\mu^2 \equiv -2 \pmod a$ dır.

ÜÇÜNCÜ BÖLÜM

3. TEŞKİL EDİLEN P_{-2} CÜMLELERİNİN GENİŞLETİLEMEZLİĞİ

İkinci bölümde ifade ve ıspatlarını verdiğimiz teoremlerle P_{-2} özelliğini sağlayan $\{1,b,c\}$, $\{2,b,c\}$ ve genel olarak $\{a,b,c\}$ üçlülerinin nasıl teşkil edilebileceğini, bu üçlülerin oluşturduğu cümlelerin nasıl cümleler olduğunu gösterdik. Ayrıca söz konusu üçlülerin genel ifadelerini (2.3), (2.16) ve (2.20) ifadeleri ile verdik. Şimdi üzerinde duracağımız problem, bu üçlülerin P_{-2} özelliğini sağlayan 4-lüler şeklinde ifade edilip edilemeyeceğini araştırmak olacaktır. Bu bölümde vereceğimiz üç teorem sırasıyla $\{1,b,c\}$, $\{2,b,c\}$ ve $\{a,b,c\}$ üçlülerinin dört elemanlı cümleler halinde genişletilip genişletilemediği problemine cevap vermiş olacaktır.

Teorem 3.1. $n \in N_0$ olmak üzere $\{1,\ n^2+2,\ n^2+2n+3\}$ cümlesinin elemanları olan üçlüler, P_{-2} özelliğini sağlayacak şekilde dörtlülere genişletilemezler.

Ispat : İddiamızın aksine, $\{1,\ n^2+2,\ n^2+2n+3\}$ cümlesi, P_{-2} özelliğini sağlayacak şekilde dördüncü bir d elemanı ile genişletilebilsin. Yani $\{1, n^2+2, n^2+2n+3, d\}$ cümlesi P_{-2} özelliğini sağlayan bir cümle olsun. Bu takdirde $u,v,t \in Z$ olmak üzere

$$\begin{aligned} 1.d-2&=u^2 \\ (n^2+2).d-2&=v^2 \qquad \text{..} \quad (3.1) \\ (n^2+2n+3).d-2&=t^2 \end{aligned}$$

Diophantine Denklem sistemini elde ederiz. Eğer (3.1) sistemini oluşturan Diophantine Denklemlerinin eşzamanlı olmadığını gösterirsek ıspat tamamlanmış olur. (3.1) sisteminin birinci denkleminden $d = u^2+2$ buluruz. Bunu ikinci ve üçüncü denklemlerde değerlendirirsek

$$(n^2+2).u^2 = v^2-2(n^2+1) \text{ .... } (3.2)$$
$$(n^2+2n+3).u^2 = t^2-2(n^2+2n+2) \text{ .... } (3.3)$$

Diophantine Denklemlerini elde ederiz. Şimdi (3.2) ve (3.3) denklemlerinin eş zamanlı olup olmadığını, her $n \in N_0$ için inceleyelim.

i) n tek olsun.

Bu takdirde $n^2 \equiv 1 \pmod 4$ olduğundan (3.2) Diophantine Denklemi

$$3u^2 \equiv v^2 \pmod 4$$

kongrüansını verir. Diğer taraftan her v tam sayısı için $v^2 \equiv 0$ veya $1 \pmod 4$ olacağından bu son kongrüans

$$3u^2 \equiv 0 \pmod 4 \text{ .... } (3.4)$$
$$3u^2 \equiv 1 \pmod 4 \text{ .... } (3.5)$$

kongrüanslarını verir. (3.5) kongrüansı çözülemezdir. (3.4) kongrüansının çözülebilmesi için de u çift olmalıdır.

(3.3) Diophantine Denklemi ise bu durumda

$$2u^2 \equiv t^2-2 \pmod 4$$

kongrüansını verir. $t^2 \equiv 0$ veya $1 \pmod 4$ olacağından bu son kongrüans

$$2u^2 \equiv 2 \pmod 4 \text{ .... } (3.6)$$
$$2u^2 \equiv -1 \pmod 4 \text{ .... } (3.7)$$

şeklinde ifade edilebilir. (3.7) kongrüansının çözümü yoktur. (3.6) kongrüansı

$$u^2 \equiv 1 \pmod 2$$

kongrüansını verir. Bunun çözülebilmesi için de u tek olmalıdır. Bu da bir çelişkidir. O halde n tek ise (3.2) ve (3.3) Diophantine denklemleri eş zamanlı değildir. Yani aynı zamanda ortak çözümleri yoktur.

ii) n çift olsun.

Bu durumda $n^2 \equiv 0 \pmod 4$ olduğundan (3.2) Diophantine denklemi

$$2u^2 \equiv v^2 - 2 \pmod 4$$

kongrüansı şeklinde karşımıza çıkar. Bu da bize

$$2u^2 \equiv -2 \pmod 4 \quad \text{.................................(3.8)}$$

$$2u^2 \equiv -1 \pmod 4 \quad \text{.................................(3.9)}$$

kongrüanslarını verir. (3.9) kongrüansı çözülemezdir. (3.8) kongrüansının çözülebilmesi için de u tek olmalıdır.

(3.3) Diophantine denklemi ise

$$3u^2 \equiv t^2 \pmod 4$$

kongrüansını verir. Buradan

$$3u^2 \equiv 0 \pmod 4 \quad \text{.................................(3.10)}$$

$$3u^2 \equiv 1 \pmod 4 \quad \text{.................................(3.11)}$$

kongrüanslarını buluruz. (3.11) kongrüansının çözümü yoktur. (3.10) kongrüansının çözülebilmesi için u çift olmalıdır. Daha önce u tek olmalıdır sonucunu bulmuştuk. O halde (3.2) ve (3.3) Diophantine denklemlerinin her $n \in N_0$ için ortak çözümleri yoktur. Öyleyse (3.1) sistemini sağlayan bir d tam sayısı yoktur. Bu da ispatı tamamlar.

Teorem 3.2: $n \in N$ olmak üzere $\{2,\ 2n^2+1,\ 2n^2+4n+3\}$ cümlesinin elemanları olan üçlüler, P_{-2} özelliğini sağlayacak şekilde dörtlülere genişletilemezler.

İspat: İddiamızın aksine $\{2,\ 2n^2+1,\ 2n^2+4n+3\}$ üçlülerinin dörtlülere genişletilebildiğini kabul edelim. B u takdirde $A,B,C \in Z$ olmak üzere

$$
\begin{aligned}
2.e-2 &= A^2 \\
(2n^2+1).e-2 &= B^2 \qquad \text{.................................(3.12)} \\
(2n^2+4n+3).e-2 &= C^2
\end{aligned}
$$

sistemini sağlayan bir e doğal sayısı vardır. Bu durumda (3.12) sisteminin birinci denkleminden $2|A^2$ ve buradan $A=2D$ yazabiliriz. Böylece, $e=2D^2+1$ bulunur. Bu değeri (3.12) nin ikinci ve üçüncü denklemlerinde değerlendirir ve gerekli düzenlemeler yapılırsa

$$2(2n^2+1)D^2 = B^2-2n^2+1 \qquad \text{.....................(3.13)}$$
$$2(2n^2+4n+3)D^2 = C^2-2n^2-4n-1 \qquad \text{................(3.14)}$$

Diophantine denklemleri bulunmuş olur.

i) n tek olsun.

Bu takdirde $n^2 \equiv 1 \pmod 4$ olacağından (3.13) denkleminden

$$2D^2 \equiv B^2-1 \pmod 4 \qquad \text{.................................(3.15)}$$

kongrüansı elde edilir. Buda

$$2D^2 \equiv -1 \pmod 4 \qquad \text{.......................................(3.16)}$$
$$2D^2 \equiv 0 \pmod 4 \qquad \text{...(3.17)}$$

kongrüanslarını verir. (3.16) kongrüansının hiçbir çözümü yoktur. (3.17) kongrüansı da eğer D çift ise çözülebilirdir.

(3.14) Diophantine denklemi ise

$$2D^2 \equiv C^2-3 \pmod 4 \quad \text{.......................(3.18)}$$

kongrüansını verir. Buradan

$$2D^2 \equiv -3 \pmod 4 \quad \text{...........................(3.19)}$$
$$2D^2 \equiv -2 \pmod 4 \quad \text{...........................(3.20)}$$

elde ederiz. (3.19) kongrüansı çözülemezdir. (3.20) kongrüansının çözelebilmesi için D tek olmalıdır. Önce D çift bulmuştuk. Bu bir çelişkidir. O halde (3.13) ve (3.14) Diophantine denklemleri tek n doğal sayıları için eşzamanlı değildir.

ii) n çift olsun.
Bu durumda $n^2 \equiv 0 \pmod 4$ olduğundan (3.13) denklemi

$$2D^2 \equiv B^2+1 \pmod 4 \quad \text{.........................(3.21)}$$

kongrüansını verir. Bu da

$$2D^2 \equiv 1 \pmod 4 \quad \text{.................................(3.22)}$$
$$2D^2 \equiv 2 \pmod 4 \quad \text{.................................(3.23)}$$

kongrüanslarına denktir. (3.22) kongrüansı çözülemezdir. (3.23) kongrüansının çözelebilmesi için D tek olmalıdır.

(3.14) denklemi de çift n ler için

$$2D^2 \equiv C^2-1 \pmod 4 \quad \text{.............................(3.24)}$$

kongrüansını verir. Bu (3.15) kongrüansı ile aynıdır. Ve çözümlü olabilmesi için D ler çift olmalıdır. Halbuki biraz önce D tek olmalıdır demiştik. Bu da bir çelişkidir. O halde her $n \in \mathbb{N}$ için (3.13) ve (3.14) Diophantine denklemleri eşzamanlı değildir. Yani (3.12) sistemini sağlayan bir e doğal sayısı yoktur. Böylece teoremin ispatı tamamlanmıştır.

Şimdi çalışmamızın son teoreminin ifade ve ispatını vereceğiz. Bu teoremde, Teorem 2.5 ile verdiğimiz $\{a,b,c\}$ üçlülerinin dörtlülere genişletilemediğini ifade ve ispat ettik

Teorem 3.3: a, Teorem 2.5 de belirlendiği gibi seçilmek üzere

$$\{a,\ n(an \pm 2\mu) + (\mu^2+2)/a,\ \ (n+1)(an+a \pm 2\mu) + (\mu^2+2)/a\}$$

şeklinde verilen üçlüler cümlesi, P_{-2} özelliğini sağlayacak şekilde dörtlülere genişletilemezdir. Burada $n \geq 2$, $n \in N$, $0 < \mu < a/2$, $\mu^2 \equiv -2 \pmod a$ dır.

İspat : Teoremin ispatını a ve n nin mümkün olan durumlarını ayrı ayrı gözönüne alarak yapacağız. İddiamızın aksine verilen üçlülerin dörtlülere genişletilebildiğini kabul edelim. Bu takdirde $x,y,z \in Z$ olmak üzere

$$a.f - 2 = x^2$$

$$[n(an \pm 2\mu) + (\mu^2+2)/a].f - 2 = y^2 \quad \ldots\ldots\ldots\ldots(3.25)$$

$$[(n+1)(an+a \pm 2\mu) + (\mu^2+2)/a].f - 2 = z^2$$

denklem sistemini sağlayan bir f doğal sayısı vardır. (3.25) sisteminin birinci denkleminden elde edilen $f = (x^2+2)/a$ değeri ikinci ve üçüncü denklemlerde yerine yazılır ve düzenlenirse

$$(a^2n^2 \pm 2an\mu + \mu^2+2)x^2 = Y^2 + 2a^2 - 2a^2n^2 \mp 4an\mu - 2\mu^2 - 4 \quad \ldots\ldots\ldots(3.26)$$

$$(a^2n^2 + 2a^2n \pm 2an\mu \pm 2a\mu + a^2 + \mu^2 + 2)x^2 = Z^2 - 2a^2n^2 - 4a^2n \mp 4an\mu \mp 4a\mu - 2\mu^2 - 4 \quad \ldots\ldots\ldots(3.27)$$

Diophantine denklemlerini elde ederiz. Burada $ay = Y$, $az = Z$ alınmıştır. Teoremin ispatı için, (3.26) ile (3.27) Diophantine denklemlerinin eşzamanlı olmadığını göstermek yeter.

1) n tek olsun.

Bu takdirde $n^2 \equiv 1 \pmod 4$ dür.

i) a tek olsun

Bu durumda a nın alabileceği değerler ya $\{(8k+1)^{\alpha},\ \alpha = 1,2,3,...,(8k+1)$ asal$\}$ ya $\{(8k+3)^{\beta},\ \beta = 1,2,3,...,(8k+3)$ asal$\}$ yada $\{(8k+1)^{\alpha}.(8k+3)^{\beta},\ (8k+1), (8k+3)$ asal $\}$ şeklinde olmalıdır. Bütün bu durumlarda a tek olduğundan $a^2 \equiv 1 \pmod 4$, $a^2 n^2 \equiv 1 \pmod 4$, $2a^2 n \equiv 2 \pmod 4$ elde edilir.

i_1) μ çift olsun. Dolayısı ile $\mu^2 \equiv 0 \pmod 4$, $2an\mu \equiv 0 \pmod 4$, $2a\mu \equiv 0 \pmod 4$ olduğundan (3.26) denklemi

$$3x^2 \equiv Y^2 \pmod 4 \quad\text{..................................}(3.28)$$

Kongrüansını verir. Bu kongrüans ise

$$3x^2 \equiv 1 \pmod 4 \quad\text{..............................}(3.29)$$

$$3x^2 \equiv 0 \pmod 4 \quad\text{..............................}(3.30)$$

kongrüanslarına denktir. (3.29) Kongrüansı çözülemezdir. (3.30) Kongrüansının çözülebilir olması için x çift olmalıdır.

Aynı şartlarda (3.27) denklemi

$$2x^2 \equiv Z^2 - 2 \pmod 4 \quad\text{..........................}(3.31)$$

Kongrüansını verir. Buradan da

$$2x^2 \equiv -1 \pmod 4 \quad\text{..............................}(3.32)$$

$$2x^2 \equiv -2 \pmod 4 \quad\text{..............................}(3.33)$$

Kongrüanslarını elde ederiz. (3.32) Kongrüansı çözülemezdir. (3.33) Kongrüansı ise, ancak tek x tam sayıları için çözülebilirdir. Bu da bir çelişkidir. O halde bu şartlarda (3.26) ve (3.27) denklemleri eşzamanlı değildir.

i_2) μ tek olsun. Bu takdirde $\mu^2 \equiv 1 \pmod 4$, $2an\mu \equiv 2 \pmod 4$, $2a\mu \equiv 2 \pmod 4$ olur. Bu durumda (3.26) denklemi

$$2x^2 \equiv Y^2 - 2 \pmod 4$$

kongrüansını verir. Halbuki bu son kongrüans, (3.31) kongrüansı gibidir ve tek x tamsayıları için çözülebilir. (3.27) Denklemi ise

$$3x^2 \equiv Z^2 \pmod 4$$

kongrüansını verir. Bu son kongrüans (3.28) kongrüansı gibidir. Bunu sağlayan x tam sayıları da çift x lerdir. Böylece yine bir çelişki elde ettik.

Sonuç olarak n tek ve a tek olduğunda (3.26) ve (3.27) Diophantine denklemleri eşzamanlı değildir.

ii) a çift olsun.

Bu durumda $a = \{2(8k+1)^{\alpha}, (8k+1)$ asal, $\alpha = 1,2,3,\ldots\}$ veya $a = \{2(8k+3)^{\beta}, (8k+3)$ asal, $\beta = 1,2,3,\ldots\}$ şeklinde değerler alabilir. Her iki durumda $a^2 \equiv 4 \pmod{16}$ dır. Diğer taraftan $0 < \mu < a/2$ ve $\mu^2 \equiv -2 \pmod a$ olduğundan a çift olduğunda μ de çift olmak zorundadır. O halde ya $\mu = 4h$ yada $\mu = 4h+2$ $(h \in Z^+)$ olabilir.

ii_1) $\mu = 4h$ $(h \in Z^+)$ olsun. Bu takdirde $\mu^2 \equiv 0 \pmod{16}$, $n^2 \equiv 1$ veya $9 \pmod{16}$, $a^2n^2 \equiv 4 \pmod{16}$, $2an\mu \equiv 0 \pmod{16}$, $2a^2n \equiv 8 \pmod{16}$, $2a\mu \equiv 0 \pmod{16}$ olduğundan (3.26) denklemi

$$6x^2 \equiv Y^2 - 4 \pmod{16} \qquad \ldots\ldots (3.34)$$

kongrüansını verir. Halbuki her bir Y tamsayısı için $Y^2 \equiv 0,1,4,9 \pmod{16}$

olacağından (3.34) kongrüansı aşağıdaki dört kongrüansa denktir.

$$6x^2 \equiv -4 \pmod{16} \quad ....(3.35)$$

$$6x^2 \equiv -3 \pmod{16} \quad ....(3.36)$$

$$6x^2 \equiv 0 \pmod{16} \quad ....(3.37)$$

$$6x^2 \equiv 5 \pmod{16} \quad ....(3.38)$$

(3.35), (3.36), (3.38) kongrüanslarının çözümleri yoktur. (3.37) Kongrüansı

$$x^2 \equiv 0 \pmod{16}$$

kongrüansına denktir. Bu son kongrüansın çözülebilmesi için x çift ve x=4k ($k \in Z$) formunda olmalıdır.

Şimdi aynı şartlarda (3.27) denklemine bakalım. Bu durumda (3.27) denklemi

$$2x^2 \equiv Z^2 - 12 \pmod{16} ....(3.39)$$

kongrüanzını verir. $Z^2 \equiv 0,1,4,9 \pmod{16}$ olacağından (3.39) kongrüansı

$$2x^2 \equiv -12 \pmod{16} \quad ....(3.40)$$

$$2x^2 \equiv -11 \pmod{16} \quad ....(3.41)$$

$$2x^2 \equiv -8 \pmod{16} \quad ....(3.42)$$

$$2x^2 \equiv -3 \pmod{16} \quad ....(3.43)$$

kongrüanslarına denktir. (3.40), (3.41), (3.43) kongrüanslarının çözümü yoktur. (3.42) kongrüansı ise

$$x^2 \equiv 4 \pmod{8}$$

kongrüansına denktir. Bu son kongrüansın çözümlü olabilmesi için x çift ancak $x=4k+2 (k \in Z)$ formunda olmalıdır. (3.26) denklemi için $x=4k (k \in Z)$ elde edilmişti. Bu bir çelişkidir. Yani eğer $\mu=4h (h \in Z^+)$ şeklinde ise (3.26) ve (3.27) Diophantine denklemleri eş zamanlı değildir.

ii_2) $\mu=4h+2$ $(h \in Z^+)$ olsun. Bu taktirde $\mu^2 \equiv 4 (\bmod 16)$, $2an\mu \equiv 8 (\bmod 16)$, $2a\mu \equiv 8 (\bmod 16)$, $2a^2n \equiv 8 (\bmod 16)$, $a^2n^2 \equiv 4 (\bmod 16)$ olduğundan (3.26) Diophantine denklemi

$$2x^2 \equiv Y^2 - 12 (\bmod 16)$$

kongrüansını verir. Bu kongrüans ise (3.39) kongrüansına benzerdir ve çözülebilir olması için x çift ve $x=4k+2$ $(k \in Z)$ olmalıdır.

(3.27) denklemine bakalım. Bu durumda (3.27) denklemi

$$6x^2 \equiv Z^2 - 4 (\bmod 16)$$

kongrüansını verir. Bu son kongrüans ise (3.34) kongrüansına benzerdir. Bu da ancak çift ve $x=4k$ $(k \in Z)$ şeklinde olan x ler için çözülebilirdir. Bu bir çelişkidir. Yani (3.26), (3.27) denklemlerini sağlayan aynı x yoktur.

Sonuç olarak n doğal sayısı tek ise (3.26) ve (3.27) Diophantine Denklemleri eşzamanlı değildirler.

2) n çift olsun

Bu durumda $n^2 \equiv 0 (\bmod 4)$ dir.

iii) a tek olsun. Bu taktirde $a^2 \equiv 1 (\bmod 4)$ olur.

iii_1) μ çift olduğunda $\mu^2 \equiv 0 (\bmod 4)$, $a^2n^2 \equiv 0 (\bmod 4)$, $2a\mu \equiv 0 (\bmod 4)$, $2a^2n \equiv 0 (\bmod 4)$,

$2an\mu \equiv 0 (mod\ 4)$, olacağından (3.26) Diophantine denklemi

$$2x^2 \equiv Y^2 - 2 (mod\ 4)$$

kongrüansını verir.Bu kongrüans da daha önce incelediğimiz (3.31) kongrüansına denktir.Bu son kongrüansın çözülebilmesi için x tek olmalıdır. (3.27) Diophantine denklemi ise bu durumda

$$3x^2 \equiv Z^2 (mod\ 4)$$

kongrüansına denktir. Halbuki bu kongrüans (3.28) ile daha önce verilen kongrüansa denktir. Ve bu kongrüansın çözülebilmesi için x çift olmalıdır. Bu bir çelişkidir.

iii_2) μ tek olduğunda $\mu^2 \equiv 1 (mod\ 4)$, $2an\mu \equiv 0 (mod\ 4)$, $2a\mu \equiv 2\ (mod\ 4)$,

$2a^2n \equiv 0\ (mod\ 4)$ olacağından (3.26) denklemi

$$3x^2 \equiv Y^2\ (mod\ 4)$$

kongrüansını verir. Bu da (3.28) kongrüansına denk ve ancak x çift ise çözülebilir. (3.27) denklemi ise bu şartlarda

$$2x^2 \equiv Z^2 - 2\ (mod\ 4)$$

kongrüansına denktir. Bu da (3.31) kongrüansı gibidir ve bunun çözülebilmesi için x tek olmalıdır. Bu da bir çelişkidir. O halde n çift, a tek ise (3.26) ve (3.27) Diophantine denklemleri eşzamanlı değildir.

iv) a çift olsun. $a = \{2(8k+1)^{\alpha}$; $(8k+1)$ asal$\}$ veya $a = \{2(8k+3)^{\beta}$, $(8k+3)$ asal$\}$ dır.Her iki durumda $a^2 \equiv 4 (mod\ 16)$ dır. a çift olduğunda μ de cift olmalıdır. Zira $\mu^2 \equiv -2 (mod\ a)$ dır. O halde μ ya $\mu = 4h$ $(h \in Z^+)$ yada $\mu = 4h+2 (h \in Z^+)$ formunda yazılabilir.

iv_1) $\mu=4h(h\in Z^+)$ şeklinde olsun. Bu taktirde $\mu^2\equiv 0 \pmod{16}$, $2an\mu\equiv 0 \pmod{16}$, $2a\mu\equiv 0 \pmod{16}$, $2a^2n\equiv 0 \pmod{16}$, $n^2\equiv 0$ veya $4 \pmod{16}$, $a^2n^2\equiv 0 \pmod{16}$ olacağından (3.26) denklemi

$$2x^2\equiv Y^2+4 \pmod{16} \quad \ldots\ldots\ldots\ldots (3.44)$$

kongrüansını verir. Halbuki $Y^2\equiv 0,1,4,9 \pmod{16}$ olacağından (3.44) kongrüansı

$$2x^2\equiv 4 \pmod{16} \quad \ldots\ldots\ldots\ldots (3.45)$$

$$2x^2\equiv 5 \pmod{16} \quad \ldots\ldots\ldots\ldots (3.46)$$

$$2x^2\equiv 8 \pmod{16} \quad \ldots\ldots\ldots\ldots (3.47)$$

$$2x^2\equiv 13 \pmod{16} \quad \ldots\ldots\ldots\ldots (3.48)$$

kongrüanslarına denktir. (3.45), (3.46), (3.48) kongrüansları çözülemezdir. (3.47) kongrüansı ise

$$x^2\equiv 4 \pmod{8}$$

Şeklinde ifade edilebilir ve bunun çözülebilmesi için x çift, $x=4k+2$ $(k\in Z)$ olmalıdır.

Aynı şartlarda (3.27) denklemi

$$6x^2\equiv Z^2-4 \pmod{16} \quad \ldots\ldots\ldots\ldots (3.49)$$

kongrüansını verir. Bu kongrüans da daha önce incelediğimiz (3.34) kongrüansının benzeridir. Bunun çözülebilmesi için de x çift, $x=4k$ $(k\in Z)$ olmalıdır. Bu da yukarıda bulduğumuz sonuçla çelişir.

iv_2) $\mu=4h+2$ ($h\in Z^+$) olduğunda $\mu^2\equiv 4$ (mod 16), $2an\mu\equiv 0$ (mod 16), $2a\mu\equiv 8$(mod 16), $2a^2n\equiv 0$ (mod 16) olduğundan (3.26) denklemi

$$6x^2\equiv Y^2-4 \pmod{16}$$

kongrüansını verir. Bu da (3.49) kongrüansı ile aynıdır. Bunun çözülebilmesi için x cift, $x=4k$ ($k\in Z$) formunda olmalıdır. Aynı şartlarda (3.27) denklemi

$$2x^2\equiv Z^2-12 \pmod{16}$$

kongrüansını verir. Bu kongrüansda (3.39) kongrüansı ile aynıdır. Bunun çözülebilmesi için x çift, $x=4k+2$ ($k\in Z$) formunda olmalıdır. Bu da bir çelişkidir. O halde n doğal sayısı çift ise (3.26) ve (3.27) Diophantine denklemleri eşzamanlı değildir.

Böylece $n\geq 2$ bir tamsayı olmak kaydıyla ve her $a\in\Pi$ için (3.26) ve (3.27) Diophantine denklemlerinin eşzamanlı olmadığını görmüş olduk. O halde (3.25) denklem sistemini sağlayan bir f doğal sayısı yoktur. Bu da teoremin ıspatını tamamlar.

KAYNAKLAR

[1] L.E.DICKSON,"History of the Theory of numbers" vol.II, Carnegie İnstitute, Washington, 1920; reptind, Chelsea, New York ,1966.

[2] H.COHN, "Advanced Number Theory", Dover Publications, Inc. New York,1962

[3] T.NAGELL, "Introduction to Number Theory", Chelsea Publishing Company, New york, 1964

[4] G.H.HARDY and E.M.WRIGHT, "An Introduction to the Theory of Numbers " OXFORD, at the Clarendon Press, 1960.

[5] T.M.APOSTOL, "Introduction to Analytic Number Theory" Springer-Verlag, New York,1976

[6] C.T.LONG, "Elementary Introduction to Number Theory" D.C.Heath and Company,1967

[7] W.J.LEVEQUE, "Topics In Number Theory", Vol.1. Addison-Wesley Publishing Company, 1965

[8] A.BAKER and H.DAVENPORT, "The Equations $3x^2-2=y^2$ and $8x^2-7=z^2$" Quart. J.Math. Oxford. ser(2) v.20. (1969). p.129-137

[9] P.KANAGASABAPATHY and T.PONNUDURAI, " The Simultaneous Diophantine Equations $y^2-3x^2=-2$ and $z^2-8x^2=-7$ ". Quart. J. Math. Oxford (3), 26(1975), 275 - 278 .

[10] V.E.HOGGATT , JR. and G.E. BERGUM, " A Problem of Fermat and The Fibonacci Sequence " The Fibonacci Quart. 15(1977), 323-330 .

[11] P.HEICHELHEIM, "The Study of Positive Integers (a,b) Such That a.b+1 is a Square" Fibonacci Quart. V.17 (1979), 269-274

[12] J.ARKIN, V.E.HOGGATT, JR. and E.G.STRAUS, "On Euler's Solution of a Problem of Diophantus" Fibonacci Quart. 17 (1979), 333-339.

[13] N.THAMOTHERAMPILLAI, "The Set of Number's{1,2,7}", Bull.Cal.Math.Soc., 72, 195-197(1980)

[14] S.P.MOHANTY and A.M.RAMASAMY, "The Simultaneous Diophantine Equations $5y^2-20=x^2$ and $2y^2+1=z^2$", Journal Number of Theory 18.356-359(1984)

[15] E.BROWN," Sets in Which xy+k is Always a Square" Mathematics of Computation,Vol.45. Number,172 p.613-620(1985)

[16] S.P.MOHANTY and A.M. S. RAMASAMY, "The Characteristic Number of two Simultaneous Pell's Equations and Its Application" Simon Stevin, A Quart J. of Pure and Applied Math. Vol.59. Number 2(1985).

[17] M.NUTT, "Generalizations of Thamotherampillui's {1,2,7}" Bul. Cal. Math. 78. 7-9. (1986).

T. C.
Yükseköğretim Kurulu
Dokümantasyon Merkezi