P_3 CÜMLELER AİLESİNİN KARAKTERİZASYONU

Hüseyin ALTINDİŞ

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

Haziran — 1988

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 Balcıoğlu

Üye : Prof. Dr. Ekrem Öztürk

Üye : Doç. Dr. Cihan Orhan

Yukarıdaki imzaların adı geçen öğretim üyelerine ait olduğunu onaylarım.

7/7/1988

Enstitü Müdürü

ÖZGEÇMİŞ

Adı Soyadı	: Hüseyin ALTINDİŞ
Baba Adı	: Ahmet
Ana Adı	: Hikmet
Dogum yeri ve yılı	: Kayseri 24.01.1955

İlk, Orta ve Lise öğrenimini Kayseri'de tamamladı. E.A. Üniversitesi Fen Fakültesi Matematik Bölümünden Matematik-Fizik Lisans diploması alarak 1977 yılında mezun oldu. Çalışma Bakanlığının bir ünitesinde İstatistik Raportörü olarak memuriyete başladı. Daha sonra askerlik hizmetini İzmir İstihkam Okulunda öğretmen olarak tamamladı. Erciyes Üniversitesi Mühendislik Fakültesinde Araştırma Görevlisi olarak 1,5 yıl çalıştıktan sonra aynı üniversitenin Fen-Edebiyat Fakültesi Matematik Bölüne Araştırma görevlisi olarak naklen geçti. E.Ü.Fen-Bilimleri Enstitüsünde Yüksek Lisansını Ocak 1985 de tamamladı. Halen Fen-Edebiyat Fakültesi Matematik Bölümünde Öğretim Görevlisi olarak çalışmaktadır.

Bu çalışma konusunu veren, çalışmalarım boyunca yakın ilgi ve yardımlarını esirgemeyen hocam Prof.Dr.Ekrem ÖZTÜRK'e minnet ve şükranlarımı arz ederim. Ayrıca S.Ü. Fen-Edebiyat Fakültesi Matematik Bölüm Başkanı Doç.Dr. Hasan ŞENAY'a yardımları için teşekkür ederim.

Hüseyin ALTINDİŞ

ÖZET

Sayıların $\{a,b,c\}$ cümlesinin herhangi iki elemanı çarpılıp 3 artırıldığında eğer bir tamkare ise $\{a,b,c\}$ cümlesi P_3 özelliğine sahiptir.

Bu çalışmada bazı pozitif x,y,z tamsayıları için

$$ab + 3 = x^2$$
$$ac + 3 = y^2$$
$$bc + 3 = z^2$$

eşitliklerini sağlayan $a<b<c$ pozitif tamsayılarının üçlülerini göz önüne aldık ve ıspat ettik ki P_3 özelliğini sağlayan sonsuz çoklukta bu üçlülerden vardır.

Buna ilaveten $n \equiv 1 \pmod 4$ ve d herhangi bir pozitif tamsayı olmak üzere

$$\{2,\ 2n^2 + 2n - 1,\ 2n^2 + 6n + 3,\ d\}$$

cümlesi bu özelliğe sahip değildir. Yani $n \equiv 1 \pmod 4$ kabulü altında

$$\{2,\ 2n^2 + 2n - 1,\ 2n^2 + 6n + 3\}$$

cümlesi 4 lülere genişletilemezler.

ABSTRACT

The set of numbers $\{a,b,c\}$ has the property P_3 such that the product of any two elements of the set increased by 3 is a perfect square.

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

$$ab + 3 = x^2$$
$$ac + 3 = y^2$$
$$bc + 3 = z^2$$

for some positive integers x, y, z and we proved that there are infinitely many triples with the property P_3 that the products in pairs increased by 3 are squares.

In addition to this, we showed that this property does not hold for the sets $\{2,\ 2n^2+2n-1,\ 2n^2+6n+3,\ d\}$ where $n \equiv 1 \pmod 4$ and d is any positive integer, that is the sets $\{2,\ 2n^2+2n-1,\ 2n^2+6n+3\}$ can not be extended to 4 tuples under the assumption $n \equiv 1 \pmod 4$.

SEMBOLLER

N	:	Doğal sayılar cümlesi
Z	:	Tamsayılar cümlesi
Z^+	:	Pozitif Tamsayılar cümlesi
I_o	:	İndis cümlesi
$a \mid b$	:	a b yi kalansız olarak böler
$a \nmid b$	:	a b yi bölmez
$(a,b)=d$	:	a ile b nin en büyük ortak böleni d dir.
$(a,b)=1$	:	a ile b aralarında asaldır.

İÇİNDEKİLER

ÖNSÖZ

Katsayıları tam olan ve birden fazla bilinmeyen ihtiva eden cebirsel denklemlerin tamsayılı çözümlerinin bulunması sayılar teorisinin en güç konularından birisidir. Bu türden problemler eski çağlardan beri bir çok matematikçinin araştırmalarına konu olmuştur. Özellikle Yunanlı matematikçi Pythagoras (M.Ö.VI.), İskenderiyeli Matematikçi Diophantus (M.S.II-III), Yeni Çağ matematikçilerinden Pierre Fermat (M.S.XVII), Leonhard Euler (M.S. XVIII) gibi matematikçiler bu konuda epey uğraşmışlardır [1].

Denklemlerin tamsayılı çözümlerinin bulunması sadece teorik olarak ilgi çekici değil, özellikle sayılar teorisinin birçok problemi ile yakından ilgilidir. Bu çalışmada çeşitli Diophantine denklemleri kurularak bunların çözümünden hareketle P_3 cümleleri oluşturulmuştur. Çalışma iki bölümdür. Birinci Bölümde ele aldığımız probleme benzer çalışmalar kronolojik bir sırada verilmiş olup, ayrıca problemimizin çözümünde faydalandığımız temel tanım ve teoremler üzerinde durulmuştur. İkinci Bölüm çalışmanın orijinal kısmını teşkil etmektedir. Yapılan benzeri çalışmalardan farklı olarak P_3 cümleleri nasıl teşkil edilebilir sorusu üzerinde durulmuş, P_3 cümlelerinin elemanları karekterize edilmiş, bunlardan birisinin bazı n ler için dörtlülere genişletilemeyeceği gösterilmiştir.

BİRİNCİ BÖLÜM

1.1. GİRİŞ

Bu çalışmanın amacı, genel olarak herhangi üç sayıdan ikisi birbiriyle çarpılıp verilen bir tamsayı ile toplandığında bir tamkare olacak şekilde pozitif tamsayıların bulunması problemidir. Daha açık ifade etmek gerekirse $x_i.x_j + k$ = tamkare olacak şekilde $(i,j = 1,2,3;\ i \neq j)$ oluşturulan $\{x_1,x_2,x_3\}$ cümlesine P_k özelliğine sahiptir denir. Problemimiz bu tip cümlelerin araştırılmasıdır.

Alışılagelmiş kaynak olan Dickson [2] nun "History of the Number Theory" isimli eserinde konu hakkında geniş bilgi bulunmamakla beraber, Diophantus'a kadar uzandığı belirtilmektedir.

Bugüne kadar yapılan çalışmaların çoğu Fermatın problemi olarak bilinen 1,3,8,120 sayıları üzerinde olmuştur. Fermat bu sayılardan herhangi ikisi birbiriyle çarpılıp 1 artırıldığında bir tamkare sayıya eşit olduğunu yani P_1 özelliğine sahip elemanlar olduğunu ifade etmiştir.

Baker ve Davenport [3], P_1 özelliği korunmak üzere 120 sayısının yerine 1,3,8,x gibi bir sayının getirilemeyeceğini ayrıca 1,3,8,x,y şeklinde aynı özelliği koruyan 5 elemanlı bir cümlenin olamayacağını göstermişlerdir.

P.Kanagsabapathy ve T. Ponnudurai [4], aynı sayılar üzerinde durmuşlar 120 sayısının yerine başka bir sayı getirilimeyeceğini Baker'in metodundan farklı bir metodla göstermişlerdir.

1977 yılında yapılan bir çalışmada [5] Fibonacci dizilerinden hareketle P_1 özelliğine sahip cümleler teşkil edilmiş $n > 1$ olmak üzere

$$F_{2n},\ F_{2n+2},\ F_{2n+4} \text{ ve } X = 4F_{2n+1}\ F_{2n+2}\ F_{2n+3}$$

sayılarının P_1 özelliğine sahip elemanlar olduğu gösterilmiştir. {3,8,21,2080} , {8,21,55,37128} v.s.

P.Heichelheim [6], {1,3,8,120} cümlesi genişletilebilirse 5. elemanın mutlaka bir tamsayı olamayacağını göstermiştir. Keza kaynak [7] benzer mahiyette bir çalışmadır.

1980 yılında yayınlanan N.Thamotherampillai [8] nin makalesi P_2 özelliğine sahip {1,2,7} cümlesinin genişletilemeyeceği hakkındadır.

Mohanty ve Ramasamy [9], P_{-1} özelliğini tanımlamışlar

$$5Y^2 - 20 = X^2 \text{ ve } 2Y^2 + 1 = Z^2$$

Diophantine denklemlerinden hareketle {1,5,10} , P_{-1} cümlesinin genişletilemeyeceğini göstermişlerdir.

Ezra Brown [10] daha kapsamlı bir çalışma ile 1985 yılında;

i) $\{n^2 + 1,\ (n+1)^2 + 1,\ (2n+1)^2 + 4\}$, $n \not\equiv 0 \pmod 4$
ii) {17, 26, 85}

iii) $\{2,\ 2n^2 + 2n + 1,\ 2n^2 + 6n + 5\}$, $n \equiv 1 \pmod 4$
iv) $\{1,\ 2,\ 5\}$

P_{-1} cümlelerinin genişletilemeyeceğini göstermiştir.

Yine Mohanty ve Ramasamy [11], P_4 cümlesini tanımlamışlar $\{1,5,12\}$ cümlesinden hareketle $\{1,5,12,96\}$ cümlesini teşkil etmişlerdir.

M.Nutt [12], 1986 yılında thamotherampıllai'nin P_2 özeliğine sahip $\{1,2,7\}$ cümlesini genelleştirmiş ve bu cümlelerin genişletilemeyecegini göstermiştir.

1.2. TEMEL TANIM VE TEOREMLER

Bu kesimde İkinci Bölümde kullanacağımız tanım ve teoremleri vereceğiz. Önce kongrüanslarla ilgili tanım ve teoremler daha sonra ise Pell denklemi ile ilgili tanım ve teoremler verilmiştir.

Tanım 1.1. n,d tamsayılar olmak üzere $n = c.d$ olacak şekilde bir c tamsayısı varsa d'n yi böler denir ve $d \mid n$ şeklinde gösterilir [13].

Tanım 1.2. $a_0, a_1, \ldots a_n$ tamsayılar olmak üzere $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$ şeklinde tanımlanan polinoma tam katsayılı polinom denir [13].

Tanım 1.3. $m \neq 0$, $m \in Z$ olsun. Şayet $m \mid a-b$ ise a ile b m modülüne göre kongrüenttir denir ve

$$a \equiv b \pmod m$$

şeklinde gösterilir [14].

Kongrüansların aşağıdaki özellikleri vardır.

i) $a \equiv b \pmod m$ ve $b \equiv c \pmod m$ ise $a \equiv c \pmod m$

ii) $a \equiv b \pmod m$ ve $c \equiv d \pmod m$ ise $a \mp c \equiv b \mp d \pmod m$

iii) $a \equiv b \pmod m$ ve $c \equiv d \pmod m$ ise $ac \equiv bd \pmod m$

iv) $a \equiv b \pmod m$ ise $ac \equiv bc \pmod m$

v) $a \equiv b \pmod m$ ise $a^k \equiv b^k \pmod m$, $k \in Z^+$

vi) $ka \equiv kb \pmod m$ ve $(k,m) = d$ ise

$$a \equiv b \left(\bmod \frac{m}{d}\right).$$

Özel olarak $d = 1$ ise $ka \equiv kb \pmod m$ olduğunda

$$a \equiv b \pmod m$$

Tanım 1.4. $0,1,2,\ldots m-1$, elemanlarının oluşturduğu cümleye (modm) ye göre komple kalan sistemi, bu elemanlardan m ile aralarında asal olanların oluşturduğu cümleye de (modm) ye göre indirgenmiş kalan sistemi denir [14].

Tanım 1.5. a ve b tamsayıları bir m modülüne göre aynı kalana sahip iseler bunlara m modülüne göre aynı kalan sınıfındadır denir [14].

Tanım 1.6. $f(x)$ bir tam katsayılı polinom, $m \in N$ olsun. c bir tamsayı olmak üzere $m \mid f(c)$ ise c ye

$$f(x) \equiv 0 \pmod m$$

cebirsel kongrüansının bir kökü ya da çözümü denir [15].

Tanım 1.7. $a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n + a_r x^r \equiv 0 \pmod m$ tam katsayılı cebirsel kongrüansı verilsin. m ile bölünemeyen ilk katsayı a_n ise bu kongrüansın derecesi n dir denir [15].

Tanım 1.8. $ax + b \equiv 0 \pmod m$, $m \nmid a$ şeklinde tanımlanan kongrüansa lineer kongrüans denir. $(m,a) = d$ ve $d \mid b$ ise bu kongrüansın d tane çözümü vardır [16].

Teorem 1.1 $f(x) \equiv 0 \pmod{p}$, n. dereceden bir kongrüans ve p asal olmak üzere bu kongrüansın en fazla n tane birbirine kongrüent olmayan çözümü vardır. Modül bileşik sayı olduğunda teorem dogru değildir [15].

Teorem 1.2. $m = \prod_{i=1}^{r} m_i$, $(m_i, m_j) = 1$, $i \neq j$, $1 \leq i \leq r$, $1 \leq j \leq r$

olmak üzere $f(x) \equiv 0 \pmod{m}$ kongrüansının çözülebilir olması için gerek ve yeter şart

$$
\begin{aligned}
f(x) &\equiv 0 \pmod{m_1} \\
f(x) &\equiv 0 \pmod{m_2} \\
&\cdots\cdots\cdots\cdots \\
&\cdots\cdots\cdots\cdots \\
&\cdots\cdots\cdots\cdots \\
f(x) &\equiv 0 \pmod{m_r}
\end{aligned}
$$

sistemin çözülebilmesidir. $m_i = p_i^{\alpha}$, p_i asal, $\alpha \in N$, $i=1,2..r$ için de teorem doğrudur [16].

Teorem 1.3. $f(x)$ bir tam polinom, p asal, $\alpha \geq 2$ $\alpha \in N$ olsun. x_o ın $f(x) \equiv 0 \pmod{p^{\alpha}}$ nın bir kökü olması için gerek ve yeter şart, a, $f(x) \equiv 0 \pmod{p^{\alpha-1}}$ in bir çözümü ve y_o,

$$\frac{f(a)}{p^{\alpha-1}} + y.f'(a) \equiv 0 \pmod{p}$$

nin bir çözümü olmak üzere $x_o = a + y_o p^{\alpha-1}$ olmasıdır. Burada $0 \leq a < p^{\alpha-1}$ ve $0 \leq y_o < p$ [16].

Tanım 1.9. $m \neq 0$, $m \in Z$, $(m,a) = 1$ olacak şekilde m ve a tamsayıları verilsin. $q \geq 2$, $q \in N$ olmak üzere

$$x^q \equiv a \pmod{m}$$

kongrüansı çözülebilir ise a ya (modm) ye göre q. kuvvetler rezidü denir. Özel olarak q=2 ise a ya kuadratik, q=3 ise kübik, q=4 ise bikuadratik rezidü denir [15].

Tanım 1.10. $m \neq 0$, $(m,a) = 1$ olmak üzere

$$x^2 \equiv a \pmod{m}$$

kongrüansı çözülebilir ise a ya m nin kuadratik rezidüsü denir ve KR ile gösterilir. Eğer kongrüans çözülemez ise a ya m nin kuadratik olmayan rezidüsü denir ve KN ile gösterilir [15].

Teorem 1.4. p tek asalın KR ve KN lerinin sayısı birbirine eşit olup herbirisi $\frac{1}{2}(p-1)$ tanedir [17].

Teorem 1.5. (Euler Kriteri) p tek asal ve a bir tamsayı olsun. a, p nin KR'sü veya KN'sü ise sırasıyla

$$a^{\frac{1}{2}(p-1)} \equiv 1 \pmod{p} \text{ veya } a^{\frac{1}{2}(p-1)} \equiv -1 \pmod{p}$$

dir [14].

Teorem 1.6. 3 sayısı $12k\mp1$ şeklindeki asalların KR'sü $12k\mp5$ şeklindeki asalların KN'südür [13].

Tanım 1.11. (Legendre Sembolü)

P tek asal $p \nmid a$ olsun. Bu taktirde $\left(\frac{a}{p}\right)$ ile gösterilen Legendre sembolü

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \; ; & \text{eğer a p nin KR'sü ise} \\ -1 \; ; & \text{eğer a p nin KN'sü ise} \end{cases}$$

olarak tanımlanır. Eğer $a \equiv 0 \pmod{p}$ ise $\left(\frac{a}{p}\right) = 0$ dır [13]. Aynı tanımı aşağıdaki şekilde de vermek mümkündür.

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

[15].

Teorem 1.7. Legendre sembolünün aşağıdaki özellikleri vardır [18].

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

Tanım 1.12. (Jakobi sembolü) Her bir i için p_i ler asal olmak üzere P,

$$P = \prod_{i=1}^{r} p_i^{\alpha_i}$$

şeklinde pozitif tek bir tamsayı olsun. $\left(\frac{a}{P}\right)$ ile gösterilen Jakobi sembolü

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

dir. Burada $\left(\frac{a}{p_i}\right)$ Legendre sembolüdür [13].

Teorem 1.8. (Karşılıklı kuadratik Rezidü Teoremi) p ve q farklı tek asallar olmak üzere

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

dir [17].

Teorem 1.9. $(m,a) = d$, $d = e^2f$, $a = da_1$, $m = dm_1$ e, f, a_1, m_1 tamsayılar, f karesel olmayan bir tamsayı olmak üzere

$$x^2 \equiv a \pmod{m}$$

kongrüansının çözülebilmesi için gerek ve yeter şart. $(f,m_1) = 1$ ve fa_1 KR m_1 olmasıdır [15].

Teorem 1.10. p tek asal a, p ile bölünemeyen bir tamsayı, q, p ile bölünemeyen bir doğal sayı ve $q \geqslant 2$ olsun.

$$x^q \equiv a \pmod{p^\alpha}$$

kongrüansı $\alpha = 1$ için çözülebiliyorsa $\alpha > 1$ şartını sağlayan bütün α tamsayıları için çözülebilirdir [15].

Teorem 1.11. i) q, a tek sayılar $\alpha \in N$ olmak üzere

$$x^q \equiv a \pmod{2^\alpha}$$

kongrüansının tam bir tane çözümü vardır.
ii) a tek, $q \equiv 2 \pmod{4}$, $\alpha \geqslant 3$ olmak üzere

$$x^q \equiv a \pmod{2^\alpha}$$

kongrüansının $a \equiv 1 \pmod{8}$ olduğunda dört tane birbirine kongrüent olmayan çözümü vardır. Diğer durumlarda çözüm yoktur.
iii) a tek, $q \equiv 2 \pmod{4}$ ve $\alpha = 2$ olsun. $a \equiv 1 \pmod{4}$ ise

$$x^q \equiv a \pmod{2^\alpha}$$

kongrüansının birbirine kongrüent olmayan iki çözümü vardır [15].

Tanım 1.13. Katsayıları tam olan 1. ve daha yüksek dereceden bilinmeyenler ihtiva eden denklemler genel olarak diophantine denklemleri olarak adlandırılır. C sıfırdan farklı bir tamsayı, D karesel olmayan bir doğal sayı olmak üzere

$$x^2 - Dy^2 = C$$

şeklindeki diophantine denklemi de Pell denklemi olarak bilinir [19].

Teorem 1.12. D karesel olmayan bir doğal sayı olmak üzere

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

diophantine denklemini sağlayan en az bir tane x,y doğal sayı çifti vardır [20].

Tanım 1.14. (1.1) Pell denkleminin x,y çözümleri $x+y\sqrt{D}$ olarak verilsin. Eger $x_o + y_o\sqrt{D}$ bunların en küçüğü ise $x_o + y_o\sqrt{D}$ çözümüne Pell denkleminin minimal çözümü ya da temel çözümü adı verilir [15],[20].

Tanım 1.15. $xy = 0$ şartını sağlayan $x + y\sqrt{D}$ çözümüne $x^2 - Dy^2 = 1$ denkleminin triviyal çözümü denir [15]]

Tanım 1.16. $x_1 + y_1\sqrt{D}$ ve $x_2 + y_2\sqrt{D}$, (1.1) denkleminin iki çözümü olsun. $x_1 = x_2$ ve $y_1 = y_2$ ise bu iki çözüme eşittir denir. Eğer $x_1 + y_1\sqrt{D} > x_2 + y_2\sqrt{D}$ ise $x_1 + y_1\sqrt{D}$ çözümü diğerinden daha büyüktür denir [15].

Teorem 1.13. D karesel olmayan bir doğal sayı olmak üzere (1.1) Pell denkleminin sonsuz sayıda tamsayılı çözümleri vardır. $x_o + y_o\sqrt{D}$ minimal çözümü olmak üzere pozitif x,y çözümleri

$$x_n + y_n\sqrt{D} = (x_o + y_o\sqrt{D})^n, \quad n \in N$$

eşitliği ile verilir. Burada

$$x_n = x_o^n + \sum_{k=1} \binom{n}{2k} x_o^{n-2k} y_o^{2k} D^k$$

$$y_n = \sum_{k=1} \binom{n}{2k-1} x_o^{n-2k+1} y_o^{2k-1} D^{k-1}$$

dir [15].

Teorem 1.14. D karesel olmayan bir doğal sayı ve

$$\xi^2 - D\eta^2 = -1 \qquad (1.2)$$

denkleminin minimal çözümü $\xi_o + \eta_o \sqrt{D}$ olsun. O zaman

$$x_o + y_o \sqrt{D} = (\xi_o + \eta_o \sqrt{D})^2 = \xi_o^2 + D\eta_o^2 + 2\xi_o\eta_o \sqrt{D}$$

ifadesi (1.1) denkleminin minimal çözümüdür. Şayet

$$\xi_n + \eta_n \sqrt{D} = (\xi_o + \eta_o \sqrt{D})^n \qquad (1.3)$$

dersek

$$\xi_n = \xi_o^n + \sum_{k=1} \binom{n}{2k} \xi_o^{n-2k} \eta_o^{2k} D^k$$

$$\eta_n = \sum_{k=1} \binom{n}{2k-1} \xi_o^{n-2k+1} \eta_o^{2k-1} D^{k-1}$$

dir. Şimdi (1.3) ifadesi

i) n bütün pozitif tek tamsayıları taradığında (1.2) denkleminin bütün pozitif ξ , η çözümlerini verir.

ii) n bütün pozitif çift tamsayıları taradığında (1.1) denkleminin bütün pozitif $x = \xi_n$, $y = \eta_n$ çözümlerini verir [15].

Tanım 1.17. D karesel olmayan bir doğal sayı $C \neq 0$ bir tamsayı olsun

$$u^2 - Dv^2 = C \qquad (1.4)$$

denkleminin bir çözümü $u + v\sqrt{D}$ olsun. $x + y\sqrt{D}$ de

$$x^2 - Dy^2 = 1$$

denkleminin herhangi bir çözümü ise

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

ifadesi (1.4) Pell denkleminin bir çözümüdür.

Bu çözüme $u + v\sqrt{D}$ ile birleştirilmiş çözüm denir. Birleştirilmiş bütün çözümlerin cümlesi (1.4) denkleminin çözümlerinin sınıfını oluşturur [15].

(1.4) Pell denkleminin herhangi iki çözümü $u + v\sqrt{D}$ ve $u' + v'\sqrt{D}$ olsun. Bu iki çözümün aynı sınıftan olması için gerek ve yeter şart

$$\frac{uu' - vv'D}{C} \quad \text{ve} \quad \frac{vu' - uv'}{C}$$

ifadelerinin birer tamsayı olmasıdır.

Bir K sınıfının $u_i + v_i\sqrt{D}$, $i = 1,2,\ldots$ çözümlerini kapsadığını düşünelim. $u_i - v_i\sqrt{D}$, $i = 1,2,\ldots$ çözümleri de bir sınıfta kapsanır. Bu sınıfıda $\overline{K}$ ile gösterirsek K ve $\overline{K}$ biri diğerinin konjugesi adını alır. Genellikle K ve $\overline{K}$ sınıfları farklıdırlar. Eğer aynı ise K ya belirsiz sınıf adı verilir.

K sınıfından bir (u^*, v^*) çözümü seçelim. v^*, K sınıfındaki v lerin negatif olmayan en küçük değeri olsun. Eğer K sınıfı belirsiz değilse u^* da v^* gibi seçilir. Eğer K sınıfı belirsiz ise $u^* \geq 0$ olacak şekilde tek türlü seçilir. Böyle seçilen (u^*, v^*) çözümüne K sınıfının temel çözümü adı verilir [15].

Teorem 1.15. $u^2 - Dv^2 = C$ denkleminin K sınıfının temel çözümü $u + v\sqrt{D}$, $x^2 - Dy^2 = 1$ denkleminin temel çözümüde $x_o + y_o\sqrt{D}$ ise

i) $$0 \leqslant v \leqslant \frac{y_o}{\sqrt{2(x_o + 1)}} \sqrt{C}$$

ii) $$0 < |u| \leqslant \sqrt{\frac{1}{2}(x_o + 1)C}$$

eşitsizlikleri vardır [15].

Teorem 1.16. $u^2 - Dv^2 = -C$ denkleminin bir K sınıfının temel çözümü $u + v\sqrt{D}$, $x^2 - Dy^2 = 1$ denkleminin temel çözümüde $xo + yo\sqrt{D}$ ise

i) $$0 < v \leqslant \frac{y_o}{\sqrt{2(x_o - 1)}} \sqrt{C}$$

ii) $$0 \leqslant |u| \leqslant \sqrt{\frac{1}{2}(x_o - 1)C}$$

eşitsizlikleri vardır [15].

Teorem 1.17. D ve C doğal sayılar ayrıca D karesel olmasın.

$$u^2 - Dv^2 = C$$
$$u^2 - Dv^2 = -C$$

denklemlerinin çözüm sınıflarının sayısı sonlu olsun. $u^* + v^*\sqrt{D}$, K sınıfının temel çözümü ise sınıfın, $u + v\sqrt{D}$ şeklindeki bütün çözümleri

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

eşitliği ile verilir. Burada $x + y\sqrt{D}$, $x^2 - Dy^2 = \mp 1$ denkleminin bütün çözümlerini tarar [15].

İKİNCİ BÖLÜM

2.1. P_3 CÜMLELER AİLESİNİN TEŞKİLİ

Çalışmamızın esasını teşkil eden bu bölümde ilk olarak P_3 cümlesini tanımlayarak bu cümlenin elemanlarının nasıl teşkil edilebileceğine ait teoremleri ifade ve ispat edeceğiz. Genel olarak üç elemanlı P_3 cümleleri üzerinde duracak, dört elemanlı P_3 cümlelerinin teşkil edilip edilemeyeceğini ayrıca inceleyeceğiz.

Tanım 2.1. $i \neq j$, $i,j = 1,2,\ldots n$ olmak üzere

$$x_i x_j + 3 = A^2$$

olacak şekilde bir A tamsayısı varsa $x_1, x_2, \ldots x_n$ pozitif tamsayılarının $\{x_1, x_2, \ldots x_n\}$ cümlesine n elemanlı P_3 cümlesi adı verilir.

Örnek olarak $\{1,2,5\}$ cümlesi üç elemanlı P_{-1} cümlesi, $\{1,3,8,120\}$ cümlesi ise dört elemanlı P_1 cümlesidir.

Kabul edelimki $\{a,b,c\}$ üç elemanlı bir P_3 cümlesi olsun. Böyle cümleler nasıl teşkil edebilir sorusuna cevap problemimizin temelini teşkil etmektedir. Tanımdan a,b,c tamsayıları pozitiftirler. $a < b < c$ olsun. Burada $a < b < c$ şartını koymamızın sebebi aynı elemanlardan oluşan cümleyi bir başka formda elde etmememizdir. Çünkü bilindiği gibi cümlenin yapısında elemanların sırası önemli değildir. Bizim için esas olan istenilen özellikteki elemanların bulunmasıdır. Böylece aynı elemanlardan oluşan cümlenin değişik permütasyonlarından kurtulmuş olacağız.

x,y,z ler tamsayılar olmak üzere tanıma denk olan

$$\begin{aligned} ab + 3 &= x^2 \\ ac + 3 &= y^2 \\ bc + 3 &= z^2 \end{aligned} \qquad (2.1)$$

eşitlikleri yazılabilir. Şimdi aşağıdaki teoremi ifade ve ispat edebiliriz.

Teorem 2.1. Bazı x,y,z tamsayıları ve $a = 1$ için (2.1) sistemini sağlayan sonsuz çoklukta $\{1,b,c\}$ şeklinde cümleler vardır.

Ispat. (2.1) sisteminde $a = 1$ alınmakla

$$\begin{aligned} b + 3 &= x^2 \\ c + 3 &= y^2 \\ bc + 3 &= z^2 \end{aligned} \qquad (2.2)$$

sistemi elde edilir. $b = x^2 - 3$, $c = y^2 - 3$ olur. $1 < b < c$ olacagından $3 \leqslant x < y$ olduğu görülür. b ve c nin bu değerleri (2.2) sisteminin 3. denkleminde kullanılırsa

$$(x^2 - 3)(y^2 - 3) + 3 = z^2 \qquad (2.3)$$

eşitliği elde edilir. Eşitliğin sol tarafının bir tam kare olması gerekir (2.3) ifadesi

$$(xy - 3)^2 - 3[(x - y)^2 - 1] = z^2 \qquad (2.4)$$

olarak yeniden düzenlenirse $y - x = \mp 1$ şartını sağlayan her x,y tamsayısı için sol taraf daima bir tamkaredir. böylece uygun (x, y, z) üçlüleri her zaman bulunabilir. $3 \leqslant x < y$ olduğu dikkate alınarak $(3,4,9)$, $(4,5,17)$, $(5,6,27)$, ... üçlüleri bulunabilir. Bu üçlülere karşılık olarakta sırasıyla $\{1,6,13\}$, $\{1,13,22\}$, $\{1,22,33\}$, ... şeklinde $\{1,b,c\}$ cümleleri teşkil edilebilir.

Bunlara (2.2) sisteminin temel çözümleri adı verilir. Bu çözümler $n \geqslant 3$, $n \in N$ olmak üzere, $b = x^2 - 3$, $c = y^2 - 3$ eşitlikleri gözönüne alınarak

$$\{1, n^2 - 3, n^2 + 2n - 2\}$$

olarak genelleştirilebilir. Her bir n, $n \geqslant 3$ doğal sayısına karşılık bir tane $\{1,b,c\}$ cümlesi bulunabileceğinden bu üçlülerin sayısının sonsuz olduğu görülmüş olur.

Şimdi (2.3) ifadesine tekrar dönelim. x,y,z arasında bir başka bağıntı

$$z^2 - (x^2 - 3)y^2 = -3(x^2 - 4) \qquad (2.5)$$

olarak kurulabilir. $x^2 - 3 = D$ denilirse D, $x \geqslant 3$ olmak üzere hiçbir x tamsayısı için tamkare değildir. Gerçekten

$$x^2 - 3 = c^2$$

gibi bir c tamsayısının varlığını kabul edersek

$$x^2 - c^2 = 3$$
$$(x - c)(x + c) = 3$$

olur.

$$(x - c) = 1$$
$$(x + c) = 3$$

olabilir ki buradan $x = 2$ bulunur. Bu da $3 \leq x < y$ eşitsizliğini sağlamaz.

D karesel olamayacağına göre (2.5) denklemi

$$z^2 - Dy^2 = -3(D - 1) \qquad (2.6)$$

şeklinde bir Pell denklemidir. Her bir D için sonsuz sayıda (z,y) çözümü vardır (Teorem 1.12 ve Teorem 1.17).

Şimdi, $x = x_j = 3$ için (2.5) dolayısıyla (2.6) denklemi

$$z^2 - 6y^2 = -15 \qquad (2.7)$$

şeklinde bir Pell denklemidir. Bu denklemin bütün tamsayılı çözümlerini bulmalıyız. Bunun içinde

$$z^2 - 6y^2 = 1 \qquad (2.8)$$

denkleminin bütün çözümlerinden faydalanmak zorundayız. (2.8) denkleminin minimal çözümü (Z_o, Y_o) olmak üzere bütün çözümleri

$$\bar{Z}_n + \bar{Y}_n \sqrt{D} = (Zo + Yo\sqrt{D})^n, \quad n = 0,1,2,\ldots$$

ile verilir (Teorem 1.13). Kolaylıkla $(Zo, Yo) = (5,2)$ olduğu görülür. Şimdi (2.8) denklemi için aşağıdaki tabloyu verebiliriz.

n	$\bar{Z}_n$	$\bar{Y}_n$
0	1	0
1	5	2
2	49	20
3	485	198
4	4801	1960

5	47525	19402
6	470449	192060
7	4656965	1901198
8	46099201	18819920

Tablo : I

Öte yandan (2.7) denkleminin çözüm sınıf numarası 2 dir. Gerçekten (2.7) nin bir çözümü (z,y) ise

$$0 < y \leqslant \frac{y_o}{\sqrt{2(z_o - 1)}} \sqrt{15}$$

$$0 \leqslant |z| \leqslant \sqrt{\frac{1}{2}(z_o - 1).15}$$

eşitsizlikleri sağlanmalıdır (Teorem 1.16). Buradan $0 < y \leqslant 2$ ve $-5 \leqslant z \leqslant 5$ bulunur. Dolayısıyla (z,y) çözümleri olarak $(z',y') = (3,2)$ ve $(z'',y'') = (-3,2)$ bulunur.

$$\frac{z'z'' - y'y''.6}{-15} \notin \mathbb{Z} \quad \text{ve} \quad \frac{y'z'' - z'y''}{-15} \notin \mathbb{Z}$$

olduğundan bu çözümler aynı sınıftan değildir. Yani (2.7) denkleminin çözüm sınıf numarası 2 dir. Bu sınıfların temel çözümleri (3,2) ve (-3,2) dir.

Şimdi (2,7) denkleminin bütün çözümlerini bulabiliriz. Bütün çözümler her bir n, (n = 0,1,2...) için

$$z_n + y_n \sqrt{6} = (3 + 2\sqrt{6})(5 + 2\sqrt{6})^n \qquad (2.9)$$

ve

$$z_n + y_n \sqrt{6} = (-3 + 2\sqrt{6})(5 + 2\sqrt{6})^n \qquad (2.10)$$

eşitlikleri ile verilir (Teorem 1.17). (2.9) ve (2.10) için tablo 2 ve tablo 3 düzenlenmiştir.

n	Z_n	Y_n
0	3	2
1	39	16
2	387	158
3	3831	1564
4	37923	15482
5	375399	153256
6	3716067	1517078
7	36785271	15017524
8	364136643	148658162

Tablo : 2

n	Z_n	Y_n
0	-3	2
1	9	4
2	93	38
3	921	376
4	9117	3722
5	90249	36844
6	893373	364718
7	8843481	3610336
8	87541437	35738642

Tablo : 3

Bu tablolar dikkate alınarak (2.5) denklemini sağlayan (3,y,z) üçlüleri olarak (3,16,39), (3,158,387) (3,1564, 3831),....
ve (3,4,9), (3,38,93), (3,376,921),....
bulunur. Şimdi bu üçlülere karşılık gelen $\{1,b,c\}$ cümleleri olarakta sırasıyla

$A_{x_j} = \{\{1,6,253\}, \{1,6,24961\}, \{1,6,2446093\}, \{1,6,13\}, \{1,6,1441\}, \{1,6,141373\} ...\}$ bulunur.

Yine (2.5) dolayısıyla (2.6) ifadesi $x = x_k = 4$ için

$$z^2 - 13y^2 = -36 \qquad (2.11)$$

şeklinde bir Pell denklemine dönüşür. Bu denklemde sonsuz (z,y) çözümlerine sahiptir. Bu çözümleri bulmak için

$$z^2 - 13y^2 = 1 \qquad (2.12)$$

ve

$$\xi^2 - 13\eta^2 = -1 \qquad (2.13)$$

denklemlerinin çözümlerinden faydalanmak zorundayız.

(2.13) denkleminin minimal çözümüne (ξ_0, η_0) dersek $(\xi_0, \eta_0) = (18,5)$ dir.

$$\xi_n + \eta_n\sqrt{13} = (18 + 5\sqrt{13})^n \qquad (2.14)$$

yazarsak

$$\xi_n = 18^n + \sum_{k=1}^{n} \binom{n}{2k} 18^{n-2k}\, 5^{2k}\, 13^{k} \qquad (2.15)$$

$$\eta_n = \sum_{k=1}^{n} \binom{n}{2k-1} 18^{n-2k+1}\, 5^{2k-1}\, 13^{k-1}$$

ifadelerine sahiptir. Şimdi

i) Eğer n ler pozitif tek tamsayıları tarıyorsa (2.15) ile birlikte verilen (2.14) eşitliği (2.13) denkleminin bütün pozitif tamsayılı çözümlerini verecektir.

ii) Eğer n ler pozitif çift tamsayıları tarıyorsa (2.15) ile birlikte verilen (2.14) ifadesi (2.12) denkleminin bütün pozitif tamsayılı çözümlerini verecektir. (Teorem 1.14).

Buna göre (2.12) ve (2.13) denklemini sağlayan değerler için aşağıdaki tabloyu teşkil edebiliriz.

n	A	B
0	1	0
1	18	5
2	649	180
3	23382	6485
4	842401	233640
5	30349818	8417525
6	1093435849	303264540
.	.	.
.	.	.
.	.	.

Tablo : 4

(2.12) denkleminin çözümlerini $(\bar{z},\bar{y})$ ile gösterirsek $n=0,2,4,6,\ldots$ değerleri için A, B sütunları $(\bar{z},\bar{y})$ çözümlerine, $n = 1,2,3.5,\ldots$ degerleri için (2.13) denkeliminin (ξ,η) çözümlerine karşılık getirilecektir.

(2.11) denkleminin çözüm sınıf numarası bulunur, her sınıfın temel çözümü bulunursa Tablo 4 ten de faydalanarak (2.11) denkleminin bütün çözümleri bulunabilir. Buna göre (2.11) denkleminin bütün çözümleri, $n = 0,1,2,\ldots$ için

$$z_n + y_n\sqrt{13} = (4 + 2\sqrt{13})(649 + 180\sqrt{13})^n$$

$$z_n + y_n\sqrt{13} = (-4 + 2\sqrt{13})(649 + 180\sqrt{13})^n$$

$$z_n + y_n\sqrt{13} = (17 + 5\sqrt{13})(649 + 180\sqrt{13})^n$$

$$z_n + y_n\sqrt{13} = (-17 + 5\sqrt{13})(649 + 180\sqrt{13})^n$$

$$z_n + y_n\sqrt{13} = (61 + 17\sqrt{13})(649 + 180\sqrt{13})^n$$

$$z_n + y_n\sqrt{13} = (-61 + 17\sqrt{13})(649 + 180\sqrt{13})^n$$

$$z_n + y_n\sqrt{13} = (108 + 30\sqrt{13})(649 + 180\sqrt{13})^n$$

ile verilir. Her bir sınıf için tablo 2 ve tablo 3 e benzer tablolar oluşturulabilir. $4 < y < z$ olacak şekilde (2.11) denklemini sağlayan (z,y) ikililerinden birkaçı

z	y
17	5
61	17
108	30
191	53
667	185
1084	578
7276	2018
22733	6305
79369	22013
140292	38910

olarak verilebilir. Şu halde (2.5) denklemini sağlayan $(4,y,z)$ üçlüleri olarak (4,5,17), (4,17,61), (4,30,108), (4,53,191), (4,185,667), (4,578,2084), (4,2018,7276), (4,6305,22733), (4,22013,79369), (4,38910,140292), ... bulunur. Bu üçlülere karşılık olarakta

A_{x_K} = {{1,13,22}, {1,13,286}, {1,13,897}, {1,13,2806}, {1,13,34222}, {1,13,334081}, {1,13,4072321} {1,13,39753022}, {1,13,516789286} . {1,13,1513988100}, ...}

elde edilir. Bu ailenin herbir elemanı P_3 cümlesidir.

Benzer düşünce tekrarlanabilir. Yani $x = x_e = 5$, v.s.

seçilebilir. A_{xj} lerin teşkil tarzından görüleceği üzere $\forall\ x_j \neq x_k$ için $b(x_j) \neq b(x_k)$ olduğundan $A_{xj} \cap A_{x_k} = \Phi$ dir. Böylece aşağıdaki teoremi ispatlamış olduk.

Teorem 2.2. $x = x_j \geqslant 3$ eşitsizliğini sağlayan herbir x_j doğal sayısına karşılık P_3 özelliğini sağlayan sonsuz elemanlı bir

$$A_{xj} = \{\{1, b(x_j), c_i\}\} \quad i \in I_o, \ I_o \subset N$$

ailesi vardır. Üstelik $x_j \neq x_k$ için $A_{xj} \cap Ax_k = \Phi$ dir.

şimdi (2.1) sisteminde a=2 seçerek aşağıdaki teoremi ifade ve ispat edebiliriz.

Teorem 2.3. Bazı x,y,z tamsayıları ve a=2 için (2.1) sistemini sağlayan sonsuz çoklukta {2,b,c} cümleleri vardır.

Ispat. (2.1) sisteminde a=2 alınmakla

$$\begin{aligned} 2b + 3 &= x^2 \\ 2c + 3 &= y^2 \\ bc + 3 &= z^2 \end{aligned} \tag{2.16}$$

sistemi elde edilir. Buradan

$$b = \frac{x^2 - 3}{2} \qquad c = \frac{y^2 - 3}{2}$$

olur. $2 < b < c$ olduğu gözönüne alınırsa $x = 2n + 1$, ve $y = 2n + 3$, $n \geqslant 1$ için b,c pozitif tamsayılardır. b ve c nin bu değerleri (2.16) sisteminin 3. denkleminde kullanılırsa

$$(x^2 - 3)(y^2 - 3) + 12 = (2z)^2 \tag{2.17}$$

olur. Bu ifade

$$(xy - 3)^2 - 3[(x - y)^2 - 4] = (2z)^2 \qquad (2.18)$$

olarak tekrar düzenlenirse $y - x = \mp 2$ için ,bu ifadenin sol tarafı daima bir tamkaredir, maksadımıza uygun (x,y,z) üçlüleri her zaman bulunabilir.

$x = 2n + 1$, $y = 2n + 3$ için $z = 2n(n + 2)$, $n \in N$ olur. Dolayısıyle (2.18) denklemini sağlayan (x,y,z) üçlüleri $n \in N$ olmak üzere $(2n+1,\ 2n+3,\ 2n(n+2))$ olarak genelleştirilebilir. Her bir n doğal sayısı için bir (x,y,z) üçlüsü ve bu üçlüye karşılıkta bir $\{2,b,c\}$ cümlesi bulunabilecektir. $x = 2n + 1$ için $b = 2n^2+2n-1$, $y = 2n + 3$ için $c = 2n^2+6n+3$ bulunur. O halde $\{2,b,c\}$ cümleleri $n \in N$ olmak üzere

$$\{2,\ 2n^2 + 2n - 1,\ 2n^2 + 6n + 3\}$$

formunda ifade edilebilirler. Bu da ispatı tamamlar.

(2.17) ifadesi $Z = 2z$ olmak üzere

$$Z^2 - (x^2 - 3)y^2 = -3(x^2 - 7) \qquad (2.19)$$

olarak yeniden düzenlenebilir. Bu denklemin temel çözümleri $(x,y,Z) = (2n + 1,\ 2n + 3,\ 4n(n + 2))$, $n \in N$ şeklindedir.

Bu çözümler (2.19)'un bütün çözümlerini kapsamaz. $x=x_j \geqslant 3$ seçilerek Pell denklemleri elde edilir. Elde edilen denklemler sonsuz (Z,y) çözümlerine sahip olacaktır. Böylece aşağıdaki teorem ifade edilebilir.

Teorem 2.4. $x = x_j \geqslant 3$ eşitsizliğini sağlayan her bir x_j doğal sayısına karşılık P_3 özelliğini sağlayan sonsuz elemanlı bir

$$B_{x_j} = \{\{2, b(x_j),\ c_i\}\}\ i \in I_o,\ I_o \subset N$$

ailesi vardır. Üstelik $x_j \neq x_k$ için $Bx_j \cap Bx_k = \Phi$ dir.

Ispat. Teorem 2.2 de olduğu gibi yapılır.

Buraya kadar (2.1) sisteminde a = 1 ve a = 2 seçmekle karşımıza çıkabilecek durumlar incelendi. Şimdi a nın 3 olması halinde de benzer tipteki cümlelerin teşkiline imkan veren bir teoremi ifade ve ispat edelim. Aynı sistemde a = 3 seçersek

$$\begin{aligned} 3b + 3 &= x^2 \\ 3c + 3 &= y^2 \\ bc + 3 &= z^2 \end{aligned} \qquad (2.20)$$

sistemini elde ederiz.

Teorem 2.5. Bazı x,y,z tamsayıları için (2.20) sistemini sağlayan sonsuz çoklukta $\{3,b,c\}$ cümleleri vardır.

Ispat. (2.20) sisteminden $b = \dfrac{x^2 - 3}{3}$, $c = \dfrac{y^2 - 3}{3}$

bulunur. $3 < b < c$ olduğu dikkate alınırsa $x=3n$ ve $y=3(n+1)$ $n > 1$, $n \in N$ için b ve c daima maksadımıza uygun bir tamsayıdır. b ve c nin bulunan bu değerlerini (2.20) sisteminin üçüncü denkleminde kullanır ..., gerekli düzenlemeleri yaparsak

$$(x^2 - 3)(y^2 - 3) + 27 = (3z)^2 \qquad (2.21)$$

olur. Bu ifadenin sağ tarafı her z için bir tamkaredir. Sol tarafınında bir tamkare olması gerekir. (2.21) ifadesi

$$(xy - 3)^2 - 3[(x - y)^2 - 9] = (3z)^2 \qquad (2.22)$$

olarak yeniden düzenlenirse, $y - x = \mp 3$ için sol tarafta daima bir tamkaredir. Uygun (x,y,z) üçlüleri her zaman bulunabilir. $y - x = \mp 3$ için (2.22) ifadesi

$$(xy - 3)^2 = (3z)^2$$

olur. $n > 1$, $n \in N$ olmak üzere $x = 3n$, $y = 3(n+1)$ olarak alınırsa $z = 3n^2 + 3n - 1$ bulunur. O zaman (x,y,z) üçlülerimiz; $(3n, 3n+3, 3n^2+3n-1)$, $n > 1$, $n \in N$ olarak ifade edilebilir.

(x,y,z) üçlüleri ve bunlara karşılık $\{3,b,c\}$ cümlelerinden birkaç tanesi aşagıda verilmiştir.

(6,9,17) ....{3,11,26}
(9,12,35) ....{3,26,47}
(12,15,59) ....{3,47,74}
(15,18,89) ....{3,74,107}
.   .
.   .
.   .

Bunlara (2.20) sisteminin temel çözümleri adı verilir. Bu çözümler

$$\{3,\ 3n^2 - 1,\ 3n^2 + 6n + 2\} \quad n > 1, \quad n \in N$$

olarak genelleştirilebilir. Her n doğal sayısına karşılık bir tane üçlü karşılık getirilebileceğinden çözümlerin sayısının sonsuz olduğu görülmüş olur.

Şimdi $a = 3$ olması halinde elde edilen üçlüler ailesinden meydana gelen cümleler ailesinin bazı özelliklerini inceleyelim.

(2.21) eşitliği $Z = 3z$ olmak üzere

$$Z^2 - (x^2 - 3)y^2 = -3(x^2 - 12) \qquad (2.23)$$

olarak yazılabilir. Bu denklemin temel çözümleri $n > 1$, $n \in N$ olmak üzere $(x,y,z) = (3n,\ 3n+3,\ 9n^2+9n-3)$ şeklindedir. Bu çözümler (2.23) ün bütün çözümlerini kapsamaz. $x = x_j \geqslant 6$ seçilmek suretiyle Pell denklemleri elde edilir. Buna göre aşağıdaki teoremi verebiliriz.

Teorem 2.6. $x = x_j \geqslant 6$ eşitsizliğini gerçekleyen her bir x_j doğal sayısına karşılık P_3 özelliğini sağlayan sonsuz elemanlı bir

$$C_{x_j} = \{\{3,\ b(x_j),\ c_i\}\},\ i \in I_0,\ I_0 \subset N$$

ailesi vardır. Üstelik $x_j \neq x_k$ için $C_{x_j} \cap C_{x_k} = \emptyset$ dir.

İspat. Bunun ispatı tamamen teorem 2.2 de olduğu gibi yapılır.

Buraya kadar ispatı yapılan teoremlerde $a = 1,2,3$ seçilerek $\{a,b,c\}$ cümlelerinin teşkili üzerinde duruldu. Acaba a doğal sayılar cümlesinin bütün elemanları üzerinden değerler alabilir mi sorusuna cevap aramak zorundayız ki bu çalışmamızın önemli bir kısmını oluşturacaktır. Hemen görülebileceği gibi (2.1) sisteminden $ab = x^2-3$, $ac = y^2-3$ olacaktır. $a = 4$ seçmekle $4 < b < c$ şartını sağlayacak hiçbir b,c doğal sayısı yoktur ki $\{4,b,c\}$ cümlesi P_3 özelliğine sahip olsun. Keza $a = 5$ seçmekle de P_3 özelliğini sağlayan bir $\{5,b,c\}$ şeklinde cümle kurulamaz. a elemanının seçilmesi problemi biraz daha yakından tetkik edilirse, a nın seçilmesi probleminin

$$x^2 \equiv 3 \pmod{a}$$

kongrüansının çözülebilir olmasına denk olduğu görülür. Buna göre problemimiz bu kongrüansın hangi a lar için çözülebilir olduğuna indirgenmiş olmaktadır. Şimdi bu kongrüans hangi a lar için çözülebilir onu araştıralım.

Teorem 1.6 dan bu kongrüansın $\left(\frac{3}{a}\right) = 1$ olan a doğal sayıları için çözülebilir olacağını hemen söyleyebiliriz. Böyle a sayıları $12k\mp1$ şeklindeki asal sayılardır. Keza $12k\mp5$, $k = 0,1,2,\ldots$ şeklindeki asallar için kongrüans çözülemezdir. O halde a sayısı $12k\mp5$ şeklindeki hiçbir asal ve böyle asalların pozitif tam kuvvetleri olamaz.

$12k\mp1$ şeklindeki asallar; 11,13,23,37,47,... v.s. gibi asallardır. Böyle elemanların oluşturduğu cümleyi E_1, ile gösterirsek

$$E_1 = \{(12k\mp1) : 12k\mp1 \text{ asal}, \ k = 1,2,\ldots\}$$

olarak ifade edebiliriz.

Yine Teorem 1.10 dan a, $12k\mp1$ şeklindeki bir asal olmak üzere

$$x^2 \equiv 3 \ (\mathrm{mod}\, a^{\alpha}), \quad \alpha \geqslant 2$$

kongrüansında çözülebilirdir. Dolayısıyla a olarak $12k\mp1$ şeklindeki asalların 2 den büyük bütün pozitif kuvvetleri de seçilebilir. 11^2, $11^3,\ldots$, 13^2, $13^3,\ldots$, v.s. Böyle elemanların oluşturduğu cümleyi E_2 ile gösterirsek

$$E_2 = \{(12k\mp1)^{\alpha} : 12k\mp1 \text{ asal}, \ \alpha \geqslant 2, \ \alpha \in N, \ k = 1,2,\ldots\}$$

olarak ifade edilebilir.

a sayısı $(12k\mp1)$ şeklindeki asalların pozitif tam kuvvetleri olarak seçilebildiği gibi böyle asalların ve pozitif tam kuvvetlerinin 2 ve 3 katları dolayısıyla 6 katları olarakta seçilebilir. Zira teorem 1.2 den

$$x^2 \equiv 3 \ (\mathrm{mod}\, 6a^{\alpha})$$

kongrüansının çözülebilir olması için

$$x^2 - 3 \equiv 0 \pmod{2}$$
$$x^2 - 3 \equiv 0 \pmod{3}$$
$$x^2 - 3 \equiv 0 \pmod{a^{\alpha}}$$

kongrüanslarının ayrı ayrı çözülebilir olması gerektir. Bu kongrüanslarda ayrı ayrı çözülebilirdir. O zaman aşağıdaki cümleler teşkil edilebilir.

$$E_3 = \{ 2.(12k\mp1)^{\alpha} : 12k\mp1 \text{ asal}, \ \alpha = 0,1,2,\ldots\}$$
$$E_4 = \{ 3.(12k\mp1)^{\alpha} : 12k\mp1 \text{ asal}, \ \alpha = 0,1,2,\ldots\}$$
$$E_5 = \{ 6.(12k\mp1)^{\alpha} : 12k\mp1 \text{ asal}, \ \alpha = 0,1,2,\ldots\}$$
$$E_6 = \{ (12k\mp1)^{\alpha}.(12k\mp1)^{\beta} : 12k\mp1 \text{ asal}, \ \alpha \ , \beta = 0,1,2,\ldots\}$$

Şimdi a elemanlarının bulunabileceği cümle

$$E = E_1 U E_2 U E_3 U E_4 U E_5 U E_6$$

olarak düşünülebilir.

a elemanının seçilmesi problemini bu şekilde kareterize ettikten sonra tekrar (2.1) sistemine dönelim. (2.1) sistemi

$$(xy - 3)^2 - 3[(x - y)^2 - a^2] = (az)^2 \qquad (2.24)$$

olarak düzenlenirse $y - x = \mp a$ için sol taraf daima bir tamkaredir. $a \in E$ ve $a > 3$ olmak üzere öyle bir s elemanı seçelimki

$$3 < s < \frac{a}{2} \text{ ve } s^2 \equiv 3 \pmod{a}$$

olsun. O zaman

$$x = an \mp s, \ y = x \mp a, \ n \in N \text{ için}$$

$$b = n(an \mp 2s) + (s^2-3)/a$$

$$c = (n + 1)[an + a \mp 2s] + (s^2-3)/a$$

olur. Böylece aşağıdaki teorem ıspatlanmış olur.

Teorem 2.7. $a \in E$, $n \in N$ olmak üzere

$$\{a,\ n(an\mp 2s)+t,\ (n+1)[an+a\mp 2s]+t\},\ t=(s^2-3)/a$$

cümlesinin herhangi iki elemanı birbiri ile çarpılır üç eklenirse bir tamkare olur. Burada s, $3 < s < \frac{a}{2}$ ve $s^2 \equiv 3$ (moda) olacak şekilde bir tamsayıdır.

Bu teoremin ifadesinde kullanılan s nin nasıl seçilebileceğini açık bir şekilde görmek için bir örnek verelim.

Örnek. $a = 6.13^2 = 1014 \in E$ olsun.

$3 < s < 1014/2$ olmalı ve $s^2 \equiv 3 \ (mod 1014)$ kongrüansı çözülmelidir. $s^2 \equiv 3 \ (mod 1014)$ kongrüansının çözülmesi için

$$s^2 \equiv 3 \ (mod 2)$$
$$s^2 \equiv 3 \ (mod 3)$$
$$s^2 \equiv 3 \ (mod 13^2)$$

kongrüansları ayrı ayrı çözülmelidir. İlk iki kongrüans

$$s^2 \equiv 1 \ (mod 2)$$
$$s^2 \equiv 0 \ (mod 3) \quad \text{olur.}$$

Bunları sağlayan s, $s \equiv 3 \ (mod 6)$ şeklindedir.

$s^2 \equiv 3 \ (mod 13^2)$ kongrüansının çözümünede Teorem 1.3. uygulanırsa;

$s^2 - 3 \equiv 0 \ (mod 13)$ kongrüansının çözümleri $a_1 = 4$, $a_2 = 9$ dir. Y_0,

$$f(4)/13 + y.f'(4) \equiv 0 \ (mod 13)$$

kongrüansının bir çözümü ise

$1 + 8y \equiv 0 \pmod{13}$
$y = 8 + 13k,\ k \quad \mathbb{Z}$ olur.

$s = a_1 + 13Y_o$
$s = 4 + 13(8 + 13k)$
$s = 108 + 13^2.k$ Buradan $s \equiv 108 \pmod{13^2}$ dir.

Benzer olarak
$s = a_2 + 13Y_o$ için

$f(9)/13 + y.f'(9) \equiv 0 \pmod{13}$
$6 + 18y \equiv 0 \pmod{13}$
$y = 4 + 13n,\ n$ olur.

$s = 9 + 13(4 + 13n)$
$s \equiv 61 \pmod{13^2}$ olur.

Şimdi verilen kongrüansı sağlayan s leri bulabiliriz. Bunun için de

$s \equiv 3 \pmod{6}$ $\qquad$ $s \equiv 3 \pmod{6}$
ve
$s \equiv 61 \pmod{169}$ $\qquad$ $s \equiv 108 \pmod{169}$

sistemlerini ayrı ayrı çözmeliyiz. Bunların çözümleri de sırasıyla $s \equiv 399 \pmod{1014}$ ve $s \equiv 615 \pmod{1014}$ şeklindedir. $3 < s < 507$ olacagı düşünülürse $s = 399$ olur. Şimdi

$\{a,\ n(an \mp 2s) + t,\ (n + 1)[an + a \mp 2s] + t\}$

cümlesinde $a = 1014,\ s = 399,\ n = 1$ alırsak

$\{1014,\ 1969,\ 5809\}$ P_3 cümlesi bulunur.

$n = 2$ alırsak

$\{1014,\ 5809,\ 11677\}$ bulunur.

Cümledeki - işareti alınırsa $n = 1$ için

$$\{1014, 373, 2617\}$$

P_3 cümlesi bulunur.

Böylece P_3 özelliğine sahip cümlelerin elemanlarının nasıl bulunacakları hakkında teoremler ıspatlanmış oldu. Şimdi P_3 cümlelerinin elemanlarını karekterize eden hatta $k \equiv 3 \pmod 4$ olmak üzere bütün P_k cümlelerinin elemanlarını karakterize edebiliriz.

2.2. P_k CÜMLELERİNİN ELEMANLARININ KAREKTERİZASYONU

$k \equiv 3 \pmod 4$ olmak üzere P_k cümlelerinin elemanlarını karekterize eden aşağıdaki teoremi verelim.

Teorem 2.8. $k \equiv 3 \pmod 4$ ve $X = \{x_1, x_2, x_3\}$ cümlesi bir P_k cümlesi olsun. $1 \leqslant i \leqslant 3$ olmak üzere en fazla bir x_i çift olup $x_i = 4m + 2$, $m = 0, 1, 2, \ldots$ formundadır. Geriye kalan elemanlar tek olup ya ikiside $4m + 1$ formunda ya da $4m + 3$ formundadır.

Ispat. $k \equiv 3 \pmod 4$ ve $X = \{x_1, x_2, x_3\}$ P_k cümlesi olsun. O zaman $i \neq j$ olmak üzere

$$x_i\, x_j + k = C^2$$

olacak şekilde bir C tamsayısı vardır. $C^2 \equiv 0 \vee 1 \pmod 4$ olacağından

$$x_i \cdot x_j + k \equiv 0 \pmod 4$$

veya

$$x_i \cdot x_j + k \equiv 1 \pmod 4$$

olur. Buradan da

$$x_i . x_j \equiv 1 \pmod 4$$

ya da

$$x_i . x_j \equiv 2 \pmod 4$$

olur.

Yani P_K cümlelerinin her hangi iki elemanı birbiri ile çarpıldığında 4 modülüne göre ya 1 kalanını ya da 2 kalanını bırakabilir.

P_K cümlelerinin herbir elemanı (mod4) e göre 4m, 4m+1, 4m+2, 4m+3 formunda olabilir. $x_i x_j$ çarpımı için olabilecek durumlar şunlardır.

Eğer bir eleman 4m formunda ise başka bir elemanla çarpıldığında 4 modülüne göre sıfıra denk olur. O halde hiçbir eleman 4m formunda olamaz. Herhangi iki eleman 4m+2 formunda da olamaz. Zira ikisi aynı formda olsa çarpımları yine sıfıra denk olur. Çarpımları 2 ye denk olan elemanlar

$$(4m + 1)(4m + 2) \equiv 2 \pmod 4$$
$$(4m + 3)(4m + 2) \equiv 2 \pmod 4$$

şeklindeki elemanlardır. O halde en fazla bir eleman çifttir ve o da 4m+2 formundadır. Geriye kalan iki eleman tektir. Bunlarda 4 modülüne göre ayrı ayrı formda olsalar çarpımları 1 e denk olamaz. O halde bunların ikiside aynı formda olmalıdır.

Ispatladığımız teoremlerde ve kaynak [10] da verilen P_K cümlelerinde bu özelliği daha açık şekilde görmek mümkündür.

2.3. P_3 CÜMLELERİNİN GENİŞLETİLMESİ

Şimdi P_3 cümlelerinin genişletilmesi problemi üzerinde duralım. Önce genişletilebilme tanımını verelim.

Tanım 2.2. X bir P_3 cümlesi olsun. $y \in X$ oldugunda $X \cup \{y\}$ cümlesi P_3 özelligini koruyorsa P_3 cümlesi genişletilebilirdir denir.

İki elemanlı bir P_3 cümlesi $\{a,b\}$ ise $x^2 = ab + 3$ olmak üzere bu cümle $\{a, b, a + b + 2x\}$ olarak üçlülere genişletilebilirdir. Biz üç elemanlı P_3 cümlelerinin 4 elemanlı olup olamayacakları üzerinde duracağız.

$X = \{a,b,c\}$ bir P_k cümlesi olsun. X in genişletilmesi demek $ad + k = x^2$, $bd + k = y^2$, $cd + k = z^2$ olacak şekilde x,y,z,d tamsayılarının bulunması demektir. Yani $\{a,b,c,d\}$ cümlesinin bir P_k cümlesi olması demektir. Bu denklemler arasında d yok edilirse

$$
\begin{aligned}
ay^2 - bx^2 &= (a - b)k \\
az^2 - cx^2 &= (a - c)k \qquad (2.25) \\
bz^2 - cy^2 &= (b - c)k
\end{aligned}
$$

sistemi elde edilir. Bu sistemin $xyz = 0$, $xyz = 1$ şartlarının dışında x,y,z tamsayılarını bulmalıyız. Şimdi aşağıdaki teoremi ifade edebiliriz.

Teorem 2.9. $n \equiv 1 \pmod 4$ ise

$$\{2,\ 2n^2 + 2n-1,\ 2n^2 + 6n + 3\}$$

cümlesi ki bu bir P_3 cümlesidir, genişletilemezdir.

Ispat. Kabul edelimki genişletilebilsin. O zaman öyle bir pozitif d tamsayısı vardır ki

$$\{2,\ 2n^2+2n-1,\ 2n^2 + 6n + 3,\ d\}$$

cümlesi bir P_3 cümlesidir. (2.25) sisteminde $a = 2$, $b = 2n^2 + 2n - 1$, $c = 2n^2 + 6n + 3$, $k = 3$ alınırsa

$$
\begin{aligned}
2y^2 - (2n^2 + 2n - 1)x^2 &= 9 - 6n^2 - 6n \\
2z^2 - (2n^2 + 6n + 3)x^2 &= -6n^2 - 18n - 3 \qquad (2.26)\\
(2n^2 + 2n - 1)z^2 - (2n^2 + 6n + 3)\, y^2 &= -12 - 12n
\end{aligned}
$$

sistemi elde edilir.

$n \equiv 1 \pmod{4}$ olduğunda $n^2 \equiv 1 \pmod{4}$ olur. (2.26) sisteminin birinci ve ikinci denklemleri

$$
\begin{aligned}
2y^2 + x^2 &\equiv 1 \pmod{4} \\
2z^2 - 3x^2 &\equiv -3 \pmod{4}
\end{aligned}
$$

olur. Bu sistemin x in tek y ve z nin çift olduğunda çözümü vardır. x in çift olması durumunda sistem çözümsüzdür.(2.26) nın üçüncü denkleminde $y = 2u$, $z = 2v$ yazılırsa

$$
\begin{aligned}
(2n^2 + 2n - 1)4v^2 - (2n^2 + 6n + 3)4u^2 &= -12(1+n) \\
(2n^2 + 2n - 1)v^2 - (2n^2 + 6n + 3)u^2 &= -3(1+n)
\end{aligned}
$$

olur. $n \equiv 1 \pmod{4}$ olduğu dikkate alınırsa

$$
\begin{aligned}
-v^2 - 3u^2 &\equiv 2 \pmod{4} \\
3u^2 + v^2 &\equiv 2 \pmod{4}
\end{aligned}
$$

elde edilir. $v^2 \equiv 0 \pmod{4}$ veya $v^2 \equiv 1 \pmod{4}$ olur.
$v^2 \equiv 0 \pmod{4}$ ise yani v çift ise

$$
\begin{aligned}
3u^2 &\equiv 2 \pmod{4} \\
u^2 &\equiv 2 \pmod{4}
\end{aligned}
$$

olurki bu kongrüansın çözümü yoktur.
$v^2 \equiv 1 \pmod{4}$ ise yani v tek ise

$$
\begin{aligned}
3u^2 &\equiv 1 \pmod{4} \\
u^2 &\equiv -1 \pmod{4}
\end{aligned}
$$

olurki bu kongrüansta çözümsüzdür. Dolayısıyle $y=2u$, $z=2v$

olacak şekilde u,v tamsayıları yoktur. O halde $n \equiv 1 \pmod 4$ iken

$$\{2,\ 2n^2 + 2n - 1,\ 2n^2 + 6n + 3\}$$

cümlesi genişletilemezdir.

KAYNAKLAR

[1] GELFOND, A.O. "Denklemlerin Tamsayılarla Çözülmesi" Çeviren : Orhan İçen. Türk Matematik Dernegi Yayınları Istanbul (1962).

[2] DICKSON, L.E. "History of the Theory of Numbers" Vol.II, Canegie Institute, Washington (1920).

[3] BAKER, A, DAVENPORT, H. "The Equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$" Quart.J.Math.Oxford Ser.(3). V.20, (19690, pp.129-137.

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

[5] HOGGATT, V.E; BERGUM, G.E. "A Problem of Fermat and The Fibonacci Sequence" The Fibonacci Quarterly 15 (1977), pp 323-330.

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

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

[8] THAMOTHERAMPILLAI, N. "The Set of Numebrs 1,2,7 " Bull.Calcutta Math.Soc. V.72, (1980) pp.195-197

[9] MOHANTY, S.P; RAMASAMY, A.M.S. "The Simultaneous Diophantine Equations $5Y^2 - 20 = X^2$ and $2Y^2 + 1 = Z^2$" J.Number Theory, V.18, (1984), pp 356-359.

[10] BROWN, E. "Sets in Which xy + k is Always a Square" Mathematics of Computation, V.45, N.172,(1985), pp. 613-620.

[11] MOHANTY, S.P.; RAMASAMY, A.M.S."The Characteristics Number of Two Simultaneous Pell's Equations and it's Application" Simon Stevin, A Quarterly J. of Pure and Applied Mathematics V.59, (1985), N.2, pp. 203-214.

[12] NUTT, M. "Generalizations of Thamotherampillai's {1,2,7}." Bull.Cal.Math.Soc.78, pp.7-9, (1986).

[13] APOSTOL, T.M. "Introduction to Analytic Number Theory" Springer Verlag, (1984).

[14] VINDGRADOV, I.M. "An Introduction to the Theory of Numbers" Pergamon Press. Oxford. (1961).

[15] NAGELL, T. "Introduction to Number Theory" Wiley, New York, (1951).

[16] LONG, C.T. "Elementary Introduction to Number Theory" D.c. Heath and Company, Boston, (1965).

[17] HARDY, G.H. and WRIGHT, E.M. "An Introduction to the Theory of Numbers" Oxford University Press, Ely House London, (1975).

[18] LEVEQUE, W.J. "Topics In Number Theory" Vol.I., Addison-Wesley Publishing C. INC, U.S.A.(1965.)

[19] MORDELL, L.J. "Diophantine Equations" Academic Press, London, (1968).

[20] COHN, H. "Advanced Number Theory" Dover Puplications, Inc, New York, (1962).