$Q(\sqrt{m})$ CİSMİNDE BAZI DIOPHANTINE DENKLEMLERİNİN ÇÖZÜM METODLARI

TEZİ HAZIRLAYAN
Muzaffer ATASOY

TEZ YÖNETİCİSİ
Doç. Dr. Hüseyin ALTINDİŞ

Erciyes Üniversitesi
Fen Bilimleri Enstitüsü' ne
Matematik Anabilim Dalında Doktora Tezi olarak
sunulmuştur.

Temmuz - 1995
KAYSERİ

Erciyes Üniversitesi
Fen Bilimleri Enstitüsü Müdürlüğü' ne

Bu çalışma jürimiz tarafından **Matematik** Anabilim Dalında **Doktora** Tezi olarak kabul edilmiştir.

10./ 7./ 1995

Başkan : Prof. Dr. Ekrem Öztürk

Üye : Doç. Dr. Hüseyin Altındiş

Üye : Yrd. Doç. Dr. Bilal Vatansever

ONAY :

Yukarıdaki imzaların, adı geçen öğretim üyelerine ait olduğunu onaylarım.

12 TEMMUZ 1995

T.C.

Fen Bilimleri Enstitüsü Müdürü

Prof. Dr. Mehmet GÜNDÜZ
MÜDÜR V.

TEŞEKKÜR

Bu çalışma konusunu bana veren, çalışmalarım boyunca yakın ilgi ve yardımlarını esirgemeyen muhterem Hocam, Sayın **Doç. Dr. Hüseyin ALTINDİŞ**' e teşekkür ederim.

Muzaffer ATASOY

ÖZGEÇMİŞ

Adı Soyadı : Muzaffer ATASOY

Baba Adı : Şakir

Ana Adı : Hatice

Doğum Yeri : Yozgat

Doğum Tarihi : 03. 01. 1964

İlk ve orta öğrenimini Şefaatli' de tamamladı. Erciyes Üniversitesi Fen-Edebiyat Fakültesi Matematik Bölümü' nden lisans diploması alarak 1988 yılında mezun oldu. 08. 11. 1989 tarihinde Erciyes Üniversitesi Matematik Bölümü " Cebir ve Sayılar Teorisi " Anabilim Dalı' na Araştırma Görevlisi olarak atandı. Ağustos 1991 de " Diophantine Denklemleri " isimli Yüksek Lisans tezini tamamladı. Halen aynı üniversitede Araştırma Görevlisi olarak çalışmaktadır.

ÖZET

Bu çalışma üç bölümden ibaret olup;

Birinci bölümde, İleriki bölümlerde kullanılacak bazı temel kavramlar ve sonuçlar verildi.

İkinci bölümde, iki, üç ve n bilinmeyenli Diophantine Denklemlerinin, $Q(\sqrt{5})$ kuadratik cismindeki çözüm metotları incelendi.

Üçüncü bölümde, Lineer olmayan bazı Diophantine Denklemlerin, $Q(\sqrt{m})$ kuadratik cisminde çözüm metotları araştırıldı.

ABSTRACT

This study consists of three chapters:

In the first chapter, some basic concepts and results are given for later use. In the second chapter, the solution methods of Linear Diophantine Equations with two, three and n unknowns in the $Q(\sqrt{5})$ quadratic field are examined. In the third chapter, the solution methods of some non-Linear Diophantine Equations in the $Q(\sqrt{m})$ quadratic field are sought.

İÇİNDEKİLER

BÖLÜM I

Sayfa

1.1 SÜREKLİ KESİRLER 1
1.2 KUADRATİK CİSİMLER 4

BÖLÜM II

2.1 $ax + by = c$ LİNEER DIOPHANTINE DENKLEMLERİNİN $Q(\sqrt{5})$ CİSMİNDE ÇÖZÜMLERİ 12
2.2 $ax + by + cz = e$ LİNEER DIOPHANTINE DENKLEMLERİNİN $(Q\sqrt{5})$ CİSMİNDE ÇÖZÜMÜ. 14
2.3 n BİLİNMEYENLİ LİNEER DIOPHANTINE DENKLEMLERİNİN $Q(\sqrt{5})$ CİSMİNDE ÇÖZÜMÜ 18

BÖLÜM III

3.1 $Q(\sqrt{m})$ CİSMİNDE $x^2 + y^2 = z^2$ DIOPHANTINE DENKLEMİ 23
3.2 $Q(\sqrt{m})$ CİSMİNDE $ax^2 - b\,y^2 = c$ DIOPHANTINE DENKLEMİ 26
3.3 $Q(\sqrt{m})$ CİSMİNDE $x^3 + y^3 = z^3$ DIOPHANTINE DENKLEMİ 30
3.4 $Q(\sqrt{m})$ CİSMİNDE $x^4 - y^4 = z^2$ DIOPHANTINE DENKLEMİ 41
3.5 $Q(\sqrt{m})$ CİSMİNDE $x^4 + y^4 = z^2$ DIOPHANTINE DENKLEMİ 43
KAYNAKLAR 46

BÖLÜM I

Bu bölümde ; Lineer Diophantine Denklemlerinin çözümlerinin bulunmasında yararlanılan sürekli kesir, sürekli kesirlerle ilgili temel teoremler, Kuadratik cisimlerin tamsayıları, birimleri gibi diğer bölümlerde kullanılacak olan temel tanım ve teoremler verildi.

1.1. SÜREKLİ KESİRLER

Tanım 1.1.1 $a_0, a_1, a_2, \ldots, a_n$ ler reel sayılar ve $a_1, a_2, \ldots, a_n$ ler pozitif reel sayılar olmak üzere ,

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}$$

ifadesine sonlu sürekli kesir denir. Burada $a_1, a_2, \ldots, a_n$ reel sayılarına, sürekli kesrin kısmi bölenleri denir. Eğer $a_0, a_1, a_2, \ldots, a_n$ ler tamsayılar ise o zaman bu sürekli kesre basittir denir. Sürekli kesrin bu gösterimi,

$$a_0 + \frac{1}{a_1 +}\,\frac{1}{a_2 +} \cdots + \frac{1}{a_n} \quad \text{veya} \quad [a_0, a_1, \ldots, a_n]$$

şeklindedir.
Sonlu sürekli kesirler için,

$$[a_0] = (a_0 / 1) = a_0$$

$$[a_0, a_1] = a_0 + (1 / a_n)$$

ve $1 \leq k < n$ için,

$$[a_0, a_1, \ldots, a_{k-1}, a_k] = [a_0, a_1, \ldots, a_{k-2}, a_{k-1} + (1/a_k)]$$

$$= a_0 + (1/ [a_1, a_2, \ldots, a_k])$$

eşitlikleri vardır. Bu eşitlikler daha genel olarak $1 \leq m \leq k \leq n$ olmak üzere,

$$[a_0, a_1, \ldots, a_{k-1}, a_k] = [[a_0, a_1, \ldots, a_{m-1}], [a_m, a_{m+1}, \ldots, a_{k-1}, a_k]]$$

şeklinde tanımlanır.

Tanım 1.1.2 $0 < k \leq n$ olmak üzere $[a_0, a_1, \ldots, a_{k-1}, a_k]$ sürekli kesrine, $[a_0, a_1, \ldots, a_{n-1}, a_n]$ sürekli kesrinin k. yakınsayanı denir ve c_k ile gösterilir. Bir sürekli kesrin n. yakınsayanı, kesrin değerini verir.

Teorem 1.1.1 $a_0, a_1, \ldots, a_{n-1}, a_n$ ler reel sayılar ve $a_1, \ldots, a_{n-1}, a_n$ ler pozitif olsun. $p_0, p_1, \ldots, p_n$ ve $q_0, q_1, \ldots, q_n$ dizileri,

$$p_0 = a_0 \qquad q_0 = 1$$

$$p_1 = a_0 a_1 + 1 \qquad q_1 = a_1$$

ve

$$p_k = a_k p_{k-1} + p_{k-2} \qquad q_k = a_k q_{k-1} + q_{k-2}, \quad k = 2, 3, \ldots, n$$

ile tanımlansın. O zaman k. yakınsayan $c_k = [a_0, a_1, \ldots, a_{k-1}, a_k]$ veya $c_k = (p_k / q_k)$ ile verilir.

İspat . Bu teoremin ispatını tümevarım metodunu kullanarak gösterelim.
$k = 0$ için ,

$$c_0 = [a_0] = (a_0 / 1) = (p_0 / q_0).$$

$k = 1$ için ,

$$c_1 = [a_0, a_1] = a_0 + (1 / a_n) = (a_0 a_1 + 1) / a_1$$

$$= (p_1 / q_1).$$

$2 \leq k < n$ için doğru olduğunu kabul edelim. Yani ,

$$c_k = [a_0, a_1, \ldots, a_k] = (p_k / q_k) = (a_k p_{k-1} + p_{k-2}) / (a_k q_{k-1} + q_{k-2})$$

olsun.
$k = k + 1$ için doğruluğunu gösterelim.

$$c_{k+1} = [a_0, a_1, \ldots, a_k, a_{k+1}] = [a_0, a_1, \ldots, a_{k-1}, a_k + (1/a_{k+1})]$$

$$= \frac{\left(a_k + \dfrac{1}{a_{k+1}}\right) p_{k-1} + p_{k-2}}{\left(a_k + \dfrac{1}{a_{k+1}}\right) q_{k-1} + q_{k-2}}$$

$$= \frac{a_{k+1}\left(a_k p_{k-1} + p_{k-2}\right) + p_{k-1}}{a_{k+1}\left(a_k q_{k-1} + q_{k-2}\right) + q_{k-1}}$$

$$= \frac{a_{k+1} p_k + p_{k-1}}{a_{k+1} q_k + q_{k-1}}$$

$$= (p_{k+1} / q_{k+1})$$

olur ki, bu da her k doğal sayısı için doğruluğunu gösterir. Dolayısıyla bu teorem yardımıyla verilen sürekli kesrin yakınsayanları bulunur.

Şimdi sürekli kesrin yakınsayanlarıyla ilgili bir kaç teoremi ispatsız verelim.

Teorem 1.1.2 p_k ve q_k değerleri,

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}$$

veya

$$(p_k / q_k) - (p_{k-1} / q_{k-1}) = ((-1)^{k-1}) / q_k q_{k-1}$$

eşitliklerini sağlar [17].

Teorem 1.1.3 p_k ve q_k değerleri için,

$$p_k q_{k-2} - p_{k-2} q_k = (-1)^k a_k$$

veya

$$(p_k / q_k) - (p_{k-2} / q_{k-2}) = (-1)^k a_k / q_k q_{k-2}$$

eşitlikleri sağlanır.

Teorem 1.1.4 Her rasyonel sayı sonlu sürekli kesirle temsil edilebilir [17].

1.2 KUADRATİK CİSİMLER

F bir cisim olmak üzere katsayıları F den alınan ve x değişkenli polinomların cümlesi F[x] ile tanımlanır. Eğer F = Q alınırsa o zaman Q[x] ile katsayıları rasyonel sayılar olan x değişkenli polinomlar cümlesi tanımlanır. $a_i \in Q$, $i = 1,2,3,\dots,n$ olmak üzere,

$$f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_n \tag{1.2.1}$$

polinomunu gözönüne alalım. Burada $a_0 \neq 0$ olmak üzere, n ye polinomun derecesi ve a_0 a başlangıç katsayısı denir. Eğer $a_0 = 1$ ise o zaman bu polinoma monik polinom, $(a_0, a_1, a_2, \dots, a_n) = 1$ ise f(x) e ilkel polinom adı verilir.

Tanım 1.2.1 $f(x)$ özdeş olarak sıfır olmayan bir polinom olsun . $f(x) = g(x)h(x)$ olacak şekilde derecesi $f(x)$ den küçük olan pozitif dereceli $g(x)$ ve $h(x)$ elemanları $Q[x]$ de bulunamıyorsa , $f(x)$ polinomuna Q da indirgenemez veya asaldır denir.

Tanım 1.2.2 Herhangi bir F cisminde $\alpha \neq 0$ olmak üzere, $\beta = \alpha\gamma$ olacak şekilde γ tamsayısı varsa α ya β nın bir böleni denir ve $\alpha | \beta$ şeklinde gösterilir.
1 in herhangi bir bölenine F nin birimi denir. Sıfırdan farklı α ve β tamsayıları için α/β bir birim ise bu sayılara birbiriyle ilgilidir denir.

Tanım 1.2.3 $a_0 , a_1 , a_2 , \ldots , a_n$ ler sıfırdan farklı tamsayılar olmak üzere ,

$$a_0\alpha^n + a_1\alpha^{n-1} + \ldots + a_n = 0 \qquad (1.2.2)$$

denklemini sağlayan α sayısına Cebirsel sayı denir. ($a_0 , a_1 , a_2 , \ldots , a_n$ ler rasyonel sayılar ise, bunların en küçük ortak katları bulunarak tamsayı yapılabileceğinden $a_0 , a_1 , a_2 , \ldots , a_n \in Z$ alınabilir.) Eğer α, n. dereceden bir cebirsel denklemi sağlıyor, fakat daha yüksek mertebeden bir denklemi sağlamıyor ise α ya n. dereceden cebirseldir denir.

Teorem 1.2.1 Bir α cebirsel sayısı Q üzerinde bir tek $g(x) = 0$ indirgenemez monik polinomu sağlar. Üstelik Q üzerinde α nın sağladığı her polinom denklemi $g(x)$ ile bölünebilir.
Bu teoremde bahsedilen $g(x) = 0$ denklemine , α cebirsel sayısının minimal denklemi denir.

Tanım 1.2.4 Bir α cebirsel sayısı, $a_0 = 1$ olması durumunda (1.2.2) denklemini sağlıyor ise o zaman α cebirsel sayısına cebirsel tamsayı denir.

Teorem 1.2.2 Rasyonel sayılar arasında sadece $0 , \pm 1 , \pm 2 , \pm 3 , \ldots$ tamsayıları cebirsel tamsayılar olup, bu sayılara rasyonel tamsayılar ve bu sayılar arasındaki asallara da rasyonel asal sayılar denir.

Teorem 1.2.3 α ve β cebirsel sayı ise $\alpha \pm \beta$, $\alpha.\beta$ da cebirsel sayılardır. Eğer α ve β cebirsel tamsayılar ise $\alpha \pm \beta$, $\alpha.\beta$ da cebirsel tamsayılardır [11].

(1.2.2) denkleminde ;

n = 1 olması durumunda $\alpha = a_1 / a_0$ olup, rasyonel sayılar cümlesini oluşturur.

n = 2 olması durumunda α kuadratik olup,

$$a_0x^2 + a_1x + a_2 = 0 \tag{1.2.3}$$

denkleminin bir köküdür. Dolayısıyla bazı a , b , c tamsayıları ve içerisinde karesel çarpan ihtiva etmeyen m tamsayısı için,

$$\alpha = \frac{a+b\sqrt{m}}{c} \quad , \quad \sqrt{m} = \frac{c\alpha - a}{b} \tag{1.2.4}$$

dir.

Bu takdirde $Q(\sqrt{m})$ ile $Q(\alpha)$ cismi aynı elemana sahip olduğundan, içerisinde karesel çarpan ihtiva etmeyen her m rasyonel tamsayısı için $Q(\sqrt{m})$ kuadratik cismini gözönüne almamız yeterli olacaktır. $Q(\sqrt{m})$ cisminin herhangi bir α elemanı, t , u , v , w , a , b , c rasyonel tamsayılar olmak üzere,

$$\alpha = \frac{t+u\sqrt{m}}{v+w\sqrt{m}} = \frac{\left(t+u\sqrt{m}\right)\left(v-w\sqrt{m}\right)}{v^2-mw^2}$$

$$= \frac{a+b\sqrt{m}}{c}$$

formuna sahip olsun. (1.2.4) den $(c\alpha - a)^2 = mb^2$ olduğundan α elemanı

$$c^2x^2 - 2acx + a^2 - mb^2 = 0 \tag{1.2.5}$$

denkleminin bir kökü olup α , ya rasyonel ya da kuadratiktir. Yani, kuadratik cismin her elemanı ya rasyoneldir ya da kuadratiktir. Bu durumda $Q(\sqrt{m})$ cismi, cebirsel tamsayıların oluşturduğu bir alt cismi ihtiva eder.

Şimdi bu cebirsel sayılar arasından $Q(\sqrt{m})$ kuadratik cisminin tamsayılarını (tamlarını) bulalım.

$\alpha = \dfrac{a+b\sqrt{m}}{c}$, $Q(\sqrt{m})$ cisminin bir tamsayısı olsun. Burada $c \geqslant 1$ ve $(a, b, c) = 1$ olduğunu kabul edelim. $b = 0$ olduğunda $\alpha = a / c$ olup $c = 1$ için $\alpha = a$ sayısı herhangi bir tamsayıdır.

Eğer $b \neq 0$ ise o zaman α kuadratiktir. Dolayısıyla (1.2.5) denklemini sağlar. Bu denklemi c^2 ile böldüğümüzde, katsayısı 1 olan monik denklemi elde ederiz. Buradan $c \mid 2a$ ve $c^2 \mid a^2 - mb^2$ dir.

Eğer $(a, c) = d$ ise,

$$d^2 \mid a^2 \; , \; d^2 \mid c^2 \; , \; d^2 \mid a^2 - mb^2$$

olduğundan

$$d^2 \mid mb^2$$

olur. m içerisinde karesel çarpan ihtiva etmediğinden $d^2 \mid b^2$ den $d \mid b$ dir. $(a, b, c) = 1$ olduğundan $d = 1$ olmalıdır. $(a, c) = 1$ olması nedeniyle $c \mid 2a$ ifadesinden $c \mid 2$ elde edilir. Bu sebeple $c = 1$ veya $c = 2$ olmalıdır.

Eğer $c = 2$ ise a tek ve $mb^2 \equiv a^2 \equiv 1 \pmod 4$ dür. Yani, $m \equiv 1 \pmod 4$ ve b tek olmalıdır. Her nekadar $(a, b, c) = 1$ şartını sağlamasa da, $c^2 \mid a^2 - mb^2$ nin $a^2 - mb^2 = c^2k \equiv 0 \pmod 4$ şeklinde ifade edildiğinden, bu kongrüansın a ve b nin herikisinin çift olması durumunda çözülebilir olması, c tamsayısının çift olmasını veya $4 \mid m$ olmasını gerektirir. Fakat $m = 4k + 1$ şeklinde olduğundan $4 \mid m$ olamaz. Dolayısıyla a, b, c tamsayılarının her üçü birden çift olmalıdır.

o halde m nin iki durumunu inceleyelim.

i) $m \not\equiv 1 \pmod 4$ ise o zaman $c = 1$ olup, $Q(\sqrt{m})$ kuadratik cisminin tamsayıları, a, b rasyonel tamsayılar olmak üzere

$$\alpha = a + b\sqrt{m} \qquad (1.2.6)$$

formunda olur ki bu $m \equiv 2 \pmod 4$ ve $m \equiv 3 \pmod 4$ olmasıdır.
ii) $m \equiv 1 \pmod 4$ ise o zaman $c = 2$ olup, $Q(\sqrt{m})$ cisminin tamsayıları, a , b ler her ikisi birden çift veya tek olan rasyonel tamsayılar olmak üzere,

$$\alpha = \frac{a+b\sqrt{m}}{2} \tag{1.2.7}$$

formundadır.

Her iki durumda da $\lambda = \frac{1+\sqrt{m}}{2}$, $a_1 , b_1 \in Z$ olmak üzere $a_1 + b_1\lambda$ formunda yazılabilir .

$Q(\sqrt{m})$ kuadratik cismine $m<0$ ise imajiner kuadratik cisim, $m>0$ ise reel kuadratik cisim adı verilir [9].

Tanım 1.2.5 $Q(\sqrt{m})$ kuadratik cisminde $\alpha = \frac{a+b\sqrt{m}}{c}$ tamsayısının normu, α ile α nın eşleniğinin çarpımına eşitir. Yani,

$$N(\alpha) = \alpha.\bar{\alpha} = \frac{a^2-mb^2}{c^2}$$

dir.

Teorem 1.2.4 Çarpımın normu, çarpanların normlarının çarpımına eşittir. $N(\alpha) = 0$ olması için gerek ve yeter şart $\alpha = 0$ olmasıdır. $Q(\sqrt{m})$ cismindeki tamsayıların normu rasyonel sayılardır. θ, $Q(\sqrt{m})$ cisminin bir tamsayısı olmak üzere $N(\theta) = \pm 1$ olması için gerek ve yeter şart θ nın birim olmasıdır.

Teorem 1.2.5 m, içerisinde karesel çarpan ihtiva etmeyen negatif rasyonel tamsayı olsun. Bu takdirde $Q(\sqrt{m})$ kuadratik cisminin birimleri, $m = -1$ ve $m = -3$ durumları hariç sadece ± 1 dir. $Q(\sqrt{-1})$ cisminin birimleri ± 1 ve $\pm i$, $Q(\sqrt{-3})$ cisminin birimleri ± 1 , $\frac{1 \pm \sqrt{-3}}{2}$, $\frac{-1 \pm \sqrt{-3}}{2}$ dir.

Teorem 1.2.6 Herhangi bir reel kuadratik cismin sonsuz sayıda birimleri vardır.

Tanım 1.2.6 $Q(\sqrt{m})$ kuadratik cisminde birimden farklı olan α cebirsel tamsayının bölenleri, sadece cismin birimleri ve kendisiyle ilgili olanı ise α ya asaldır denir.

Teorem 1.2.7 Eğer $Q(\sqrt{m})$ cisminin herhangi bir α tamsayısının normu, p rasyonel asal olmak üzere,

$$N(\alpha) = \pm p$$

ise o zaman α tamsayısına $Q(\sqrt{m})$ de asaldır denir.

Teorem 1.2.8 $Q(\sqrt{m})$ cisminin sıfırdan ve birimden farklı her tamsayısı ya asaldır ya da asalların çarpımı olarak yazılabilir [15].

Tanım 1.2.7 $\varepsilon_i = \pm 1$, $r_i \in Z^+$, $1 \leq i$, $r_0 \in Z$ ve $\lambda = 2\mathrm{Cos}(\pi/q)$, $3 \leq q \in Z$ olmak üzere,

$$r_0\lambda + \cfrac{\varepsilon_1}{r_1\lambda + \cfrac{\varepsilon_2}{r_2\lambda + \ddots}}$$

ifadesine λ_q- kesri denir ve $\left[r_0\lambda, \frac{\varepsilon_1}{r_1\lambda}, \frac{\varepsilon_2}{r_2\lambda}, \ldots\right]$ formunda gösterilir.

Eğer α herhangibir reel sayı ise λ nın en yakın tam katının bulunması gerekir . Yani, $\{\ \}$ en yakın tamsayı ise o zaman $\left\{\frac{\alpha}{\lambda}\right\} = r_0$ yazılır. Burada $\frac{-1}{2} \leq r_0 - \frac{\alpha}{\lambda} < \frac{1}{2}$ özelliği sağlanır ve r_0,

$$r_0\lambda - \frac{\lambda}{2} < \alpha \leq r_0\lambda + \frac{\lambda}{2} \qquad (1.2.8)$$

eşitliğinden tek türlü hesaplanır. Böylece $\alpha = r_0\lambda + \frac{\varepsilon_1}{\alpha_1}$ yazılır ki burada

$r_0\lambda < \alpha$ ise $\varepsilon_1 > 0$, $r_0\lambda > \alpha$ ise $\varepsilon_1 < 0$ alındığında $\alpha_1 = \frac{\varepsilon_1}{\alpha - r_0\lambda} > 0$ olur.

Bu şekilde devam edildiğinde $\alpha_m > \frac{\lambda}{2}$ bulunur ki, bu da $1 \leq r_m$ olmasını gerektirir.($1 \leq m$).

λ_q- kesri aşağıdaki özellikleri sağlar.

i) $\lambda - \frac{1}{r\lambda}$ olduğunda $2 \leq r$ dir.

ii) $$\cfrac{\varepsilon_1}{\lambda - \cfrac{1}{2\lambda - \cfrac{1}{\lambda + \cfrac{\varepsilon_2}{\ddots}}}}$$

olduğunda $\varepsilon_1 = \varepsilon_2 = 1$ ve $\lambda - \cfrac{1}{2\lambda - \frac{1}{\lambda}} = \frac{2}{\lambda}$ dır.

iii) Eğer λ_q- kesri

$$\cfrac{\varepsilon}{\lambda - \frac{1}{\lambda}}$$

ile bitiyorsa o zaman $\varepsilon = 1$ dir. $Q(\sqrt{5})$ de $\lambda - \frac{1}{\lambda} = 1$ olduğundan

$$\lambda^2 - \lambda - 1 = 0 \qquad (1.2.9)$$

denklemi sağlanır. α, $\beta \in Q(\sqrt{5})$ olmak üzere $\alpha x + \beta y = 1$ denkleminin çözümü α / β ifadesi λ_q- kesrine açıldığında sondan bir önceki yakınsayanı p_{n-1} / q_{n-1} olmak üzere,

$$x = (-1)^{n+1} q_{n-1}, \quad y = (-1)^n p_{n-1}$$

olup $\alpha x + \beta y = \gamma$ denkleminin çözümü

$$x = (-1)^{n+1} \gamma q_{n-1}, \quad y = (-1)^n \gamma p_{n-1} \qquad (1.2.10)$$

dir [16].

BÖLÜM II

Şimdiye kadar yapılan çalışmalarda Lineer Diophantine Denklemlerinin tamsayılardaki çözümlerinin varlığı ve çözümleri sürekli kesirler yardımıyla [17] , [15] , [19] de incelenmiştir. Katsayıları $Q(\sqrt{5})$ kuadratik cisminden alınan iki ve üç bilinmeyenli Lineer Diophantine Denklemlerinin $Q(\sqrt{5})$ de çözüm metodu ve bütün çözümlerinin bulunması [16], [1] de, Lineer olmayan ikinci dereceden bazı Diophantine Denklemlerinin çözümleri, dereceleri üçden büyük olan homojen veya homojen olmayan Diophantine Denklemlerinin çözümlerinin incelenmesi, Fermat' ın son teoremi olarak bilinen $x^n + y^n = z^n$, $(n>2)$ denkleminin $xyz \neq 0$ olması durumunda hiçbir çözüme sahip olmadığı ve $x^3 + y^3 = z^3$ denkleminin $Q(\sqrt{-3})$ kuadratik cisminde aşikar çözümü haricinde hiçbir çözümünün olmadığı [13] , [11] , [4], [14] , [9] de araştırılmıştır. Pell denklemi için indirgeme bağıntıları [5] , [12], D içerisinde karesel çarpan ihtiva etmeyen bir tamsayı olmak üzere, $x^2 - Dy^2 = -1, -4$ denkleminin D nin durumlarına göre çözümlerinin incelenmesi ve çözümlerinin bulunması [10], $x^2 - Dy^2 = nz^2$ denkleminin $D = -11$ ve $n = 3$ olması halindeki çözümü [3] de incelenmiştir.

a, içerisinde $p \equiv \pm 3 \pmod 8$ şeklinde bir asal çarpan ihtiva eden bir tamsayı ve m , n pozitif çift tamsayılar olmak üzere $x^2 + a^2y^m = z^{2n}$

denkleminin, y tek tamsayı ve $(x , ay) = 1$ olacak şekildeki tamsayı çözümünün olmadığı K. D. Zelator tarafından, $x^2 - 2y^2 = 1$ ve $y^2 - Dz^2 = 4$ Pell denkleminin tamsayılarda ortak çözümlerinin varlığı ve çözümlerin bulunması J. H. Chen tarafından gösterilmiştir [21] , [2]. $ax^2 - by^2 = c$ Diophantine denkleminin matris metoduyla tamsayılardaki çözümleri 1994 yılında A. Grelak ve A. Grytczuk tarafından ve p tek asal olmak üzere $x^4 + dy^4 = z^p$ denkleminin çözümleri ve çözüm metotları, $d = -1$ için, 1993 yılında H. Daimon tarafından, d içerisinde karesel çarpan ihtiva etmeyen bir tamsayı olması durumunda 1992 yılında N. O . H. Terai tarafından gösterilmiştir [8] , [7] , [22]. G, Gausian tamsayıların cümlesini göstermek üzere $\pm\alpha^4 \pm\beta^4 = \gamma^4$ $\alpha,\beta,\gamma \in G$ denkleminin $(\alpha , \beta) = 1$ olacak şekilde çözüme sahip olmadığı Fermat' ın sonsuz indirgeme metoduyla [6], $x , y \in Q$ olmak üzere $x^y = y^x$ denkleminin çözümlerinin sadece $(x , y) = ((1 + (1/n))^n , (1 + (1/n))^{n+1}) , (x < y$ ve $n = 1 , 2 , ...)$ şeklinde olduğu [18] de gösterilmiştir.

Bu bölümde katsayıları $Q(\sqrt{5})$ kuadratik cisminin elemanları olan iki , üç ve n bilinmeyenli Lineer Diophantine denklemlerinin $Q(\sqrt{5})$ cisminde çözümleri verildi.

2.1 $ax + by = c$ LİNEER DİOPHANTİNE DENKLEMLERİNİN $Q(\sqrt{5})$ CİSMİNDE ÇÖZÜMLERİ

$Q(\sqrt{5})$ kuadratik cisminin cebirsel tamsayıları, $m \equiv 1 \pmod 4$ olduğunda, $\lambda = \frac{1+\sqrt{5}}{2}$ ve $s , t \in Z$ olmak üzere $s + t\lambda$ formundadır [8]. $ax + by = c$ Diophantine denkleminin çözümünün olduğunu kabul edelim. Yani $(a , b) \mid c$ olsun. Bu takdirde a / b sayısı (1.2.8) yardımıyla λ_q-kesrine açıldığında (1.2.9) dan dolayı bu kesrin toplamı λ ya göre iki polinomun bölümünü verir ki, bu da $s_1 , s_2 , t_1 , t_2 \in Z$ olmak üzere,

$$\frac{s_1 + t_1\lambda}{s_2 + t_2\lambda} \qquad (2.1.1)$$

formuna indirgenebilir. Bu ifadenin pay ve paydası $s_2 + t_2\lambda$ nın konjigesi olan $(s_2 + t_2) - t_2\lambda$ ile çarpılırsa ,

$$\frac{s_3+t_3\lambda}{t_4}$$

şekline gelir. Burada $s_3 = s_1s_2 + s_1t_2 - t_1s_1$, $t_3 = t_1s_1 - s_1t_2$, $t_4 = s_2^2 + s_2t_2 - t_2^2$ dir. λ_q- kesri, (2.1.1) şekline yuvarlandığında ve indirgendiğinde pay ve paydasında uygun bir birim çarpan bulunmadıkça orjinal kesre benzemez. Orjinal kesre benzetmek için, pay ve payda için ortak birim çarpan bulunması gerekir. Böylece sürekli kesrin ardışık son iki yakınsayanı teorem 1.1.1 kullanılarak hesaplandığında, $ax + by = 1$ Diophantine Denkleminin bir çözümü, teorem 1.1.2 den

$$x = (-1)^{n+1} q_{n-1} \ , \ y = (-1)^n p_{n-1} \tag{2.1.2}$$

Olur. Verilen denklemin çözümü, x ve y nin bu değerleri c ile çarpılırsa,

$$x = (-1)^{n+1} cq_{n-1} \ , y = (-1)^n cp_{n-1} \tag{2.1.3}$$

olarak bulunur.

Teorem 2.1.1 p , q , r ler $Z(\sqrt{5})$ in, birimden farklı ve aralarında asal olan elemanları olsun. Bu durumda

$$px + qy = r$$

denklemi $Q(\sqrt{5})$ kuadratik cisminde tamsayı çözüme sahiptir. Eğer x_0 , y_0 özel çözüm ise herhangi bir çözümü

$$x = x_0 + qt \quad , \quad y = y_0 - pt \quad , \quad t \in Q(\sqrt{5})$$

formuna sahiptir. $(p, q) = d$ ve $d \mid r$ ise o zaman,

$$\frac{p}{d}x + \frac{q}{d}y = \frac{r}{d}$$

denklemi $Q(\sqrt{5})$ cisminde çözülebilirdir.

İspat. Rasyonel sayılarda olduğu gibi, önce $px + qy = 1$ denklemi çözülür. Bu da p / q nun λ_q - kesrine açılımı ile yapılır ve sondan bir önceki yakınsayan hesaplanarak $px + qy = 1$ denkleminin çözümü (2.1.2) den ve $px + qy = r$ denkleminin çözümü de (2.1.3) den hesaplanır. Eğer x_0 , y_0 verilen denklemin temel çözümü ise o zaman sonsuz çözümleri $t \in Z(\sqrt{5})$ olmak üzere $x = x_0 + qt$, $y = y_0 - pt$ ile elde edilir. Üstelik $a , b \in Z(\sqrt{5})$ herhangi bir çözüm ve x_0 , y_0 temel çözüm ise bu durumda $pa + qb = r$ ve $px_0 + qy_0 = r$ olup,

$$p(a - x_0) + q(b - y_0) = 0$$

dır. Buradan

$$p \mid -(b - y_0) \Rightarrow -b + y_0 = pt$$

$$\Rightarrow b = y_0 - pt$$

ve

$$p (a - x_0) = qpt \Rightarrow a - x_0 = qt$$

$$\Rightarrow a = x_0 + qt$$

elde edilir. Teoremin son iddiası $\left(\frac{p}{d}, \frac{q}{d}, \frac{r}{d}\right) = 1$ olduğundan, teoremin birinci iddiasından kolaylıkla görülür. Bu da teoremin ispatını tamamlar.

Teorem 2.1.2 $4 \leq q$ için $\lambda_q = 2Cos(\pi/q)$ ve $a , b \in Z(\lambda_q)$ ise o zaman $ax + by = 1$ Diophantine Denkleminin $Z(\lambda_q)$ da çözülebilir olması için gerek ve yeter şart $(a , b) = d \mid c$ ve a / b nin sonlu bir λ_q- kesriyle temsil edilebilmesidir [16].

Bu metod, eğer uygun bir sürekli kesirle temsili mevcut ise diğer cisimlerede genişletilebilir. Fakat $Q(\lambda_q)$ cisminde sonlu bir λ_q- kesrine, bütün rasyonel tamsayılar içinde mümkün olan q ların sadece $q = 3$ ve $q = 5$ olduğunu wolfart [20] göstermiştir. Bu yüzden $Q(\sqrt{5})$ kuadratik cismi haricindeki cisimlerde, λ_q- kesrine açılım mümkün olmadığından çözümü yoktur.

2.2 $ax + by + cz = e$ LİNEER DİOPHANTİNE DENKLEMİNİN $Q(\sqrt{5})$ CİSMİNDE ÇÖZÜMÜ

a, b, c, e ler $Q(\sqrt{5})$ cisminin tamsayıları olmak üzere,

$$ax + by + cz = e \tag{2.2.1}$$

denkleminin çözümleri incelenecektir.

Teorem 2.2.1 Eğer p, q, r, s ler $Z(\sqrt{5})$ de $(q, r) = 1$ olacak şekildeki elemanlar ise o zaman,

$$px + qy + rz = s \tag{2.2.2}$$

Diophantine Denklemi, $Q(\sqrt{5})$ kuadratik cisminde tamsayı çözümlerine sahiptir. Eğer x_0, y_0, z_0 bu denklemin özel bir çözüm ise o zaman herhangi bir çözümü

$$x = x_0 + Av$$

$$y = y_0 + Bu + Cv$$

$$z = z_0 + Du + Ev$$

formuna sahiptir. Burada A, B, C, D, E ler $Q(\sqrt{5})$ kuadratik cisminde bilinen tamsayılar ve u, v de uygun bir algoritma ile hesaplanan keyfi tamsayılardır.

İspat. $\alpha, \delta, \gamma, \beta$ lar, $\alpha\delta - \gamma\beta = 1$ şartını sağlayan tamsayılar olmak üzere,

$$y = \alpha t + \beta u$$

$$z = \gamma t + \delta u \tag{2.2.3}$$

olsun. Bu eşitlikler (2.2.2) de yerine yazılırsa

$$px + (q\alpha + r\gamma)\, t + (q\beta + r\delta)\, u = s \tag{2.2.4}$$

denklemi elde edilir. Bu denklemin cismin x , t , u tamsayılarına göre çözümü ile (2.2.2) denkleminin x , y , z tamsayılarına göre çözümleri aynıdır.
$(q , r) = 1$ olduğundan $q\beta + r\delta = 0$ denkleminin çözümü $\beta = -r$, $\delta = q$ olur. Bu takdirde $\alpha\delta - \gamma\beta = 1$ denklemi, teorem 2.1.1 den cismin α , γ tamsayılarına göre çözülebilirdir. α , β , γ ve δ nın bu değerleri (2.2.4) de kullanılırsa elde edilen dönüşüm denklemi

$$px + t = s \tag{2.2.5}$$

şekline dönüşür ki bu denklem sadece x , t gibi iki değişken ihtiva eder. Bu son denklemin çözümü, $(p/1)$ ifadesi λ_q- kesrine açılırsa (2.1.3) formunda olduğu görülür. Bütün çözümleri de, teorem 2.1.1 den

$$x = x_0 + Av$$

$$t = t_0 + B_0 v$$

olarak bulunur. Böylece (2.2.2) denkleminin bütün çözümleri, t' nin bu değeri (2.2.3) de yerine yazılarak elde edilir. Bu da teoremin ispatını tamamlar [1].

ÖRNEK 2.1.1

$$(2 + \lambda)x + (6\lambda - 1)y + (1 + 3\lambda)z = 3 + \lambda \tag{2.2.6}$$

denklemini gözönüne alalım. Burada $q = 6\lambda - 1$, $r = 1 + 3\lambda$, $(q , r) = 1$.
$y = \alpha t + \beta u$ ve $z = \gamma t + \delta u$ olsun. $(q , r) = 1$ olduğundan $\beta = -r = -(1 + 3\lambda)$ ve $\delta = q = 6\lambda - 1$ olup,

$$(6\lambda - 1)\alpha + (1 + 3\lambda)\gamma = 1 \tag{2.2.7}$$

denklemini sağlayan α , γ tamsayılarının sadece bir değerini bulalım. $(6\lambda - 1) / (1 + 3\lambda)$ sayısı λ_q - kesrine açıldığında,

$$\frac{6\lambda - 1}{3\lambda + 1} = \left[\lambda, \frac{-1}{5\lambda}, \frac{-1}{\lambda}, \frac{1}{\lambda}, \frac{-1}{3\lambda}, \frac{-1}{\lambda}\right]$$

elde edilir. Eşitliğin sağ tarafı , (1.2.9) bağıntısı kullanılarak yuvarlandığında $(113\,\lambda + 70\,) \,/\, (\,76\,\lambda + 47)$ elde edilir. Pay $(8 + 13\,\lambda)(6\lambda -1)$ ve payda $(8 + 13\,\lambda)(6\lambda -1)$ formunda olduğundan pay ve payda ortak bir birim çarpan $(8 +13\,\lambda) = \lambda^7)$ ihtiva eder. Bu sürekli kesrin sondan bir önceki yakınsayanı

$$\left[\lambda, \frac{-1}{5\lambda}, \frac{-1}{\lambda}, \frac{1}{\lambda}, \frac{-1}{3\lambda}\right] = \frac{82\lambda+49}{52+38\lambda}$$

dır. Böylece (2.1.2) den $(113\,\lambda + 70\,)\alpha + (\,76\,\lambda + 47)\gamma = 1$ denkleminin çözümü $\alpha' = -(52\alpha + 38)$ ve $\gamma' = -(82\alpha + 49)$ olur. $(6\lambda -1)\,\alpha + (3\lambda +1)\,\gamma = 1$ denkleminin çözümü α' ve γ' çözümlerinin $(8 + 13\,\lambda)$ ile çarpılmasıyla elde edilir. Yani,

$$\alpha = (52\alpha + 38)\,(8 + 13\,\lambda) = 1586\lambda + 980$$

$$\gamma = -(82\alpha + 49)\,(8 + 13\,\lambda) = -(2359\,\lambda + 1458\,)$$

(2.2.7) denkleminin bir çözümüdür. α ve γ nın bu değerleri alındığında

$$y = (1586\lambda + 980)\,t - (1 + 3\lambda\,)\,u$$

$$z = -(2359\,\lambda + 1458\,)\,t + (6\lambda - 1)\,u$$

elde edilir. y ve z nin bu değerleri (2.2.6) da kullanılırsa,

$$(2 + \lambda)\,x + t = (3 + \lambda\,) \qquad (2.2.8)$$

denklemi bulunur.Bu denklemin çözümünü hesaplamak için,
$(2 +\lambda)$ ifadesi sürekli kesre açılırsa,

$$2+\lambda = \left[2\lambda, \frac{1}{2\lambda}, \frac{-1}{\lambda}\right]$$

olduğu kolaylıkla görülür. Bu eşitliğin sağ tarafını yine (1.2.9) bağıntısı kullanılarak yuvarlandığında $(7\lambda +4) \,/\, (1 + 2\lambda)$ bulunur ve

$(2+\lambda)x'+t'=1$ denklemin çözümü $x'=6\lambda+4$ ve $t'=-(22\lambda+13)$ olur. Dolayısıyla $(2+\lambda)x+t=(3+\lambda)$ denklemin çözümü (2.1.3) den $x=(6\lambda+4)(3+\lambda)=(28\lambda+18)$ ve $t=-(22\lambda+13)(3+\lambda)=-(101\lambda+61)$ olarak elde edilir. Buradan (2.2.8.) denkleminin genel çözümü,

$$x=(28\lambda+18)+v$$

$$t=-(101\lambda+61)-(2+\lambda)v\ ,\quad v\in Q(\sqrt{5})$$

olur.

Böylece (2.2.6) nın bütün çözümleri,

$$x=(28\lambda+18)+v$$

$$y=-[(355912\lambda+219966)+(14564\lambda+2940)v]-(1+3\lambda)u$$

$$z=[(529416\lambda+327197)+(8535\lambda+5275)v]+(6\lambda-1)u$$

olarak bulunur. Burada u, v cismin keyfi iki tamsayısıdır.

2.3 n BİLİNMEYENLİ LİNEER DİOPHANTİNE DENKLEMİNİN $Q(\sqrt{5})$ CİSMİNDE ÇÖZÜMÜ

$a_i\neq 0$, $i>3$ olmak üzere

$$a_0x_0+a_1x_1+\dots+a_{n-1}x_{n-1}=c\quad(n>3)\qquad(2.3.1)$$

denklemini gözönüne alalım. Burada a_0, $a_1,\dots,a_{n-1}\in Q(\sqrt{5})$. (2.3.1) denkleminin çözümünün olduğunu kabul edelim. Bu durumda $\alpha,\beta,\gamma,\delta$ lar $\alpha\delta-\gamma\beta=1$ şartını sağlayan kuadratik cismin tamsayıları olmak üzere,

$$x_{n-2}=\alpha u+\beta v$$

$$x_{n-1}=\gamma u+\delta v\qquad(2.3.2)$$

dönüşümünü uygulayalım. O zaman (2.3.2) denkleminden

$$u = \delta x_{n-2} - \beta x_{n-1}$$

$$v = -\gamma x_{n-2} + \alpha x_{n-1}$$

eşitlikleri elde edilir. Burada u , v nin $Q(\sqrt{5})$ in tamsayıları olması için gerek ve yeter şart x_{n-2} ve x_{n-1} sayılarının cismin tamsayıları olmasıdır. Eğer

$$\beta = \frac{a_{n-1}}{(a_{n-2}, a_{n-1})} \quad \text{ve} \quad \delta = -\frac{a_{n-2}}{(a_{n-2}, a_{n-1})}$$

olarak seçilirse $(\beta, \delta) = 1$ olup $\alpha\delta - \gamma\beta = 1$ denklemi, α ve γ ya göre çözülebilirdir. Bu çözüm (2.1.3) den bulunur. Bununla beraber α ve γ nın sonsuz çözümlerinden sadece bir çözümüne ihtiyacımız vardır. (2.3.2) eşitlikleri (2.3.1) denkleminde yerine yazılırsa,

$$a_0x_0 + a_1x_1 + \dots + a_{n-3}x_{n-3} + (a_{n-2}\alpha + a_{n-1}\gamma)\, u = c \qquad (2.3.3)$$

şeklinde bir eksik bilinmeyen ihtiva eden denklem elde edilir. Burada

$$(a_{n-2}\alpha + a_{n-1}\gamma) = -(a_{n-2}, a_{n-1})\alpha\delta + (a_{n-2}, a_{n-1})\gamma\beta$$

$$= -(a_{n-2}, a_{n-1})$$

ve

$$(a_0, a_1, \dots, a_{n-3}, (a_{n-2}, a_{n-1})) = (a_0, a_1, \dots, a_{n-1})$$

dir. Bu dönüşümlerle elde edilen (2.3.3) denklemi (2.3.1) denklemi ile aynı özelliğe sahip olup, katsayılarının en büyük ortak böleni, c yi böler ve katsayılar, $Q(\sqrt{5})$ kuadratik cisminin sıfırdan farklı tamsayılarıdır.

Eğer $n > 4$ ise (2.3.3) denklemine indirgeme metodu tekrar uygulanarak (n-2) bilinmeyenli Lineer Diophantine Denklemine indirgenir, böyle devam edilerek iki bilinmeyen ihtiva eden Lineer Diophantine denklemine indirgenmiş olur. Elde edilen bu iki bilinmeyen ihtiva eden Lineer Diophantine Denklemi bir çözüme sahipse katsayıları λ_q- kesrine açılarak bir çözümü bulunur. Bu denklemin bütün çözümleri bir tek parametreye bağlı olarak verildiği gibi (2.3.1) Lineer Diophantine Denkleminin bütün çözümü, (n-1) parametreye bağlı olarak ifade edilir. Eğer (2.3.3) denklemi gibi, (n-1) bilinmeyen ihtiva eden herhangi bir Lineer Diophantine Denklemi $v_0, v_1, \ldots, v_{n-3}$ şeklinde (n-2) parametreye bağlı olarak $x_0, x_1, \ldots, x_{n-3}, u$ çözümlerine sahipse o zaman (2.3.1) denkleminin çözümleri,

$$x_0,\ x_1, \ldots, x_{n-3},\ \alpha u + \beta v,\ \gamma u + \delta v$$

ile verilir. Bu çözümler $v_0, v_1, \ldots, v_{n-3}, v$ parametrilerini ihtiva eder ve bu çözümler,

$$x_i = b_i + d_{i,0} v_0 + d_{i,1} v_1 + \ldots + d_{i,n-2} v_{n-2}$$

formunda ifade edilir.

$3 \leq q \in Z$ ve $\lambda = 2Cos(\pi/q)$ olmak üzere sadece $Q(\lambda_q) = Q(\sqrt{5})$ olduğu, yani kuadratik cismin tamsayılarının λ_q- kesrine açılabilmesi için gerek ve yeter şart kuadratik cismin $Q(\sqrt{5})$ olması gerektiği [20] gösterildi. Dolayısıyla aşağıdaki sonucu verebiliriz.

Sonuç 2.3.1 n bilinmeyenli Lineer Diophantine Denkleminin kuadratik cisimlerde bir çözüme sahip olması için gerek ve yeter şart $Q(\lambda_q) = Q(\sqrt{5})$ olmasıdır. Burada $3 \leq q \in Z$, $\lambda = 2Cos(\pi/q)$.

BÖLÜM III

Bu bölümde $Q(\sqrt{m})$ kuadratik cisminde lineer olmayan bazı Diophantine Denklemlerinin çözümleri incelendi. Birinci bölümde kuadratik cismin cebirsel tamsayıları, m nin durumuna göre belirlenmişti. İçerisinde karesel çarpan ihtiva etmeyen pozitif m tamsayısı için $Q(\sqrt{m})$ kuadratik cisminin birimlerini inceleyelim.

$m \equiv 1 \pmod 4$ ise $Q(\sqrt{m})$ nin tamları, a , b ler her ikisi birden çift veya tek tamsayılar olmak üzere, $(a + b\sqrt{m})/2$ formunda bulunuyordu. Herhangi bir $\theta \in Q(\sqrt{m})$ nin birim olabilmesi için teorem 1.2.1 den $N(\theta) = \pm 1$ olmalıdır. Dolayısıyla,

$$N(\theta) = \frac{a+b\sqrt{m}}{2} \cdot \frac{a-b\sqrt{m}}{2} = \frac{a^2-b^2m}{4} \quad \pm 1$$

elde edilir.

Eğer $m \equiv 1 \pmod 4$ ise $Q(\sqrt{m})$ kuadratik cismin birimleri, $\theta = \dfrac{a+b\sqrt{m}}{2}$ den $a^2 - mb^2 \equiv \pm 4 \pmod 4$ bulunur. Buradan $a^2 - b^2 \equiv 0 \pmod 4$ kongrüansı elde edilir ki, bu kongrüansın çözülebilir olması için, a ve b nin her ikisinin çift veya tek olması gerekir. Eğer $m \equiv 1 \pmod 8$ olacak şekilde bir tamsayı ise o zaman,

$$a^2 - b^2 \equiv \pm 4 \pmod 8$$

olup, bu kongrüansın çözülebilir olması için, ya $a = 4k + 2$, $b = 4k$ şeklinde ya da tersi olmalıdır. Bu yüzden $m = 8k + 1$ olması durumunda $Q(\sqrt{m})$ kuadratik cisminin birimi, $a = 4k + 2$, $b = 4k$ şeklinde veya tersi olmak üzere,

$$\theta = \frac{a + b\sqrt{m}}{2} \quad \text{formundadır.}$$

Eğer $m \equiv 2 \pmod 4$ ise kuadratik cismin elemanları $a + b\sqrt{m}$ formunda olduğundan $\theta \in Q(\sqrt{m})$ elemanı için, $\theta = a + b\sqrt{m}$ olmak üzere,

$$N(\theta) = (a + b\sqrt{m})(a - b\sqrt{m})$$

$$= a^2 - mb^2 \equiv \pm 1 \pmod 4$$

$$a^2 - 2b^2 \equiv \pm 1 \pmod 4$$

olup, bu kongrüans, a ve b tek tamsayılar veya a tek, b çift olduğunda bir çözüme sahipdir. Bu nedenle a , b nin diğer durumları için çözülemezdir.
Eğer $m \equiv 3 \pmod 4$ ise, $a , b \in Z$ olmak üzere, kuadratik cismin tamları $a + b\sqrt{m}$ formunda olduğundan $\theta \in Q(\sqrt{m})$ elemanı için,

$$N(\theta) = a^2 - mb^2 \equiv \pm 1 \pmod 4$$

$$a^2 + b^2 \equiv \pm 1 \pmod 4$$

olup, bu kongrüans, a ve b çift veya tek tamsayılar olduğunda bir çözüme sahip değildir. Bu nedenle a , b nin diğer durumları için çözülebilirdir. Şimdi aşağıdaki sonucu verelim.

Sonuç 3.1.1 m içerisinde karesel çarpan ihtiva etmeyen pozitif tamsayı olmak üzere, $Q(\sqrt{m})$ kuadratik cisminin birimleri,

i) $m \equiv 1 \pmod 4$ ise o zaman a , b nin herikisi birden çift veya tek olmak üzere, $\theta = \dfrac{a + b\sqrt{m}}{2}$ formunda.

ii) $m \equiv 1 \pmod 8$ ise o zaman $a = 4k + 2$, $b = 4k$ şeklinde veya tersi olmak üzere, $\theta = \dfrac{a + b\sqrt{m}}{2}$ formunda.

iii) $m \equiv 2 \pmod 4$ ise o zaman a, b ler her ikisi birden çift veya b tek olmamak üzere $\theta = a + b\sqrt{m}$ formunda,
iv) $m \equiv 3 \pmod 4$ ise, a ve b ler, biri tek diğeri çift tamsayı olmak üzere, $\theta = a + b\sqrt{m}$ formunda,
olmalıdır.

3.1.1 $Q(\sqrt{m})$ CİSMİNDE $x^2 + y^2 = z^2$ DİOPHANTİNE DENKLEMİ

Bu denklemin, $Q(\sqrt{m})$ kuadratik cisminde çözümlerini incelerken $(x,y,z) = 1$ kabule debiliriz. Eğer $(x, y, z) = d$ ise o zaman $d \mid x$, $d \mid y$, $d \mid z$ olup $x = x_1 d$, $y = y_1 d$, $z = z_1 d$ olacak şekilde $x_1, y_1, z_1 \in Q(\sqrt{m})$ vardır. Bu değerler

$$x^2 + y^2 = z^2 \tag{3.1.1}$$

denkleminde yerine yazılırsa

$$(x_1 d)^2 + (y_1 d)^2 = (z_1 d)^2$$

elde edilir ve $(x_1, y_1, z_1) = 1$ dir. Dolayısıyla $(x,y,z) = 1$ olarak kabul edebiliriz. (3.1.1) denkleminin çözümüne geçmeden önce aşağıdaki teoremleri verelim.

Teorem 3.1.1 r, s, t ler $(r,s) = 1$ ve $rs = t^2$ olacak şekilde $Q(\sqrt{m})$ kuadratik cisminin tamsayıları ise o zaman, $r = m^2$, $s = n^2$ olacak şekilde cismin m ve n tamsayıları vardır.

İspat. $r = 1$ veya $s = 1$ içn teoremin doğruluğu aşikardır. $r > 1$ ve $s > 1$ kabul edelim. r, s ve t ler cismin herhangi tamsayıları olduğundan, p_i ve q_i ler, $Q(\sqrt{m})$ kuadratik cisminin asalları olmak üzere,

$$r = p_1^{a_1} p_2^{a_2} \cdots p_u^{a_u}$$

$$s = p_{u+1}^{a_{u+1}} p_{u+2}^{a_{u+2}} \cdots p_v^{a_v}$$

$$t = q_1^{b_1} q_2^{b_2} \cdots q_k^{b_k}$$

şeklinde yazmak mümkündür. $(r, s) = 1$ olduğundan r ve s nin çarpımları farklıdır. $rs = t^2$ olduğundan,

$$p_1^{a_1} p_2^{a_2} \ldots p_u^{a_u} p_{u+1}^{a_{u+1}} p_{u+2}^{a_{u+2}} \ldots p_v^{a_v} = q_1^{2b_1} q_2^{2b_2} \ldots q_k^{2b_k} \qquad (3.1.2)$$

dir. Aritmetiğin temel teoreminden (3.1.2) eşitliğindeki asal kuvvetler aynı olmalıdır. Böylece herbir p_i, bazı j ler için q_j ye eşit olmalıdır.
Yani, $a_i = 2b_j$ dir. Tersine olarak herbir a_i üssü çift ve bu yüzden $(a_i/2)$ bir tamsayıdır.

$$m = p_1^{\frac{a_1}{2}} p_2^{\frac{a_2}{2}} \ldots p_u^{\frac{a_u}{2}} \quad \text{ve} \quad n = p_{u+1}^{\frac{a_{u+1}}{2}} p_{u+2}^{\frac{a_{u+2}}{2}} \ldots p_v^{\frac{a_v}{2}}$$

olmak üzere $r = m^2$ ve $s = n^2$ elde edilir. Bu da ispatı tamamlar.

Teorem 3.1.2 $(x, y, z) = 1$ ise o zaman $(x, y) = (y, z) = (x, z) = 1$ dir.

İspat. Kabul edelim ki $(x, y, z) = 1$ ve $(x, y) > 1$ olsun. o zaman $p \mid (x, y)$ olacak şekilde kuadratik cisminde bir p asalı vardır. Yani, $p \mid x$ ve $p \mid y$ dir. Bu durumda $p \mid x^2 + y^2$ ve $p \mid z^2$ olduğundan $p \mid z$ olur ki, bu da kabulümüze bir tezat teşkil eder. O halde $(x, y) = 1$ dir. Benzer şekilde $(y, z) = 1$ ve $(x, z) = 1$ olduğu gösterilir.

Teorem 3.1.3 Eğer $(x, y, z) = 1$ ise o zaman ya $x = 2\alpha$, $y = 2\beta + \theta$ şeklinde veya tersi olmalıdır. ($\alpha, \beta \in Q(\sqrt{m})$, θ cismin birimidir.)

İspat. $(x, y, z) = 1$ olsun. Teorem 3.1.2 den $(x, y) = 1$ dir. Yani, x ve y nin herikisi birden 2α formunda değildir. Ayrıca x ve y nin herikisi birden $2\alpha + \theta$ formunda da değildir. Eğer x ve y nin herikisi birden $2\alpha + \theta$ formunda olsaydı o zaman,

$$x^2 \equiv \theta \pmod 4$$

$$y^2 \equiv \theta \pmod 4$$

olması $z^2 \equiv 2\theta \pmod 4$ olmasını gerektirir ki, bu mümkün olmazdı. Bu yüzden $x = 2\alpha$, $y = 2\beta + \theta$ veya tersi olmalıdır. Bu da ispatı tamamlar.

Teorem 3.1.4 x, y, z ler $Q(\sqrt{m})$ in pozitif tamsayıları olmak üzere, y nin, $y = 2\alpha$ formunda olması için gerek ve yeter şart,

$$x = m^2 - n^2$$

$$y = 2mn$$

$$z = m^2 + n^2$$

olacak şekilde kuadratik cismin, $m>n$, $m = 2\gamma$, $n = 2\beta + \theta$ veya tersi olan m, n pozitif tamsayıları vardır. Burada $(m, n) = 1$ dir.

İspat. $(x, y, z) = 1$ olsun. Teorem 3.1.3 den $x = 2\alpha$, $y = 2\beta + \theta$ veya tersi olmalıdır. $y = 2\beta$, x ve z de $2\alpha + \theta$ şeklinde olsun. Böylece $z + x$ ve $z - x$, 2 nin bir katı olduğundan $r = (z + x)/2$, $s = (z - x)/2$ olacak şekilde $Q(\sqrt{m})$ in pozitif tamsayıları vardır. $x^2 + y^2 = z^2$ olduğunda,

$$y^2 = z^2 - x^2$$

$$\left(\frac{y}{2}\right)^2 = \frac{z+x}{2}\,\frac{z-x}{2} = rs$$

olup $(r, s) = 1$ dir. Eğer $(r, s) = d$ olsaydı $d | r$, $d | s$ ve $d | (r + s)$ olurdu. Buradan $d | z$, $d | x$ ve $d | (x, z)$ olup $d | 1$ olması $d = 1$ olmasını gerektirir. Teorem 3.1.1 den $r = m^2$, $s = n^2$ olacak şekilde m ve n tamsayıları vardır. Bu durumda x, y, z ler, m ve n ye bağlı olarak,

$$x = r - s = m^2 - n^2$$

$$y = \sqrt{4rs} = 2mn$$

$$z = r + s = m^2 + n^2$$

ile verilip $(m, n) = 1$ dir. m ve n nin herhangi bir ortak böleni, x, y, z nin de bir ortak böleni olmalıdır. Halbuki $(x, y, z) = 1$ dir. Yine m ve n nin herikisi de $2\beta + \theta$ formunda değildir. Eğer bu formda olsa x, y, z nin

hepsi 2 nin katı olmak zorunda olur ki, bu da yine $(x, y, z) = 1$ olmasıyla çelişir.
$(m, n) = 1$ ve bunların herikisi $2\beta + \theta$ formunda olmadığından, biri 2α ve diğeri $2\beta + \theta$ şeklinde olmalıdır.

Sonuç 3.1.2 $x^2 + y^2 = z^2$ Diophantine Denkleminin $Q(\sqrt{m})$ kuadratik cismindeki bütün çözümleri, m, n ler, $(m, n) = 1$, $m>n$ ve sadece bir tanesi 2α formunda olan $Q(\sqrt{m})$ kuadratik cismin pozitif tamsayıları olmak üzere,

$$x = m^2 - n^2$$

$$y = 2mn$$

$$z = m^2 + n^2$$

ile verilir.

3.2 $Q(\sqrt{m})$ CİSMİNDE $ax^2 - by^2 = c$ DİOPHANTİNE DENKLEMİ

Bu kısımda a, b, c ler $Q(\sqrt{m})$ kuadratik cisminin tamsayıları olmak üzere,

$$ax^2 - by^2 = c \qquad (3.2.1)$$

Diophantine Denkleminin çözümlerini inceleyeceğiz. Bu denklemin çözümüne geçmeden önce $d = ab$ olmak üzere,

$$x^2 - dy^2 = z^2 \qquad (3.2.2)$$

denkleminin çözümünü verelim.

Teorem 3.2.1 $d = ab = 2\alpha$ formunda ise, (3.2.2) Diophantine Denkleminin bütün çözümleri,

$$x = (am^2 + b\,n^2)\rho$$

$$y = 2mn\rho$$

$$z = (am^2 - bn^2)\rho \qquad (3.2.3)$$

formülü ile, $d = ab = 2\alpha + \theta$ formunda ise,

$$x = (1/2)(am^2 + b\,n^2)\rho$$

$$y = mn\rho$$

$$z = (1/2)(am^2 - bn^2)\rho \qquad (3.2.4)$$

formülüyle verilir. Burada ρ tamsayısı, m ve n ler $2\alpha + \theta$ şeklinde ise, kuadratik cismin herhangi bir tamsayısı, m ve n den biri 2γ diğeri $2\beta + \theta$ ise o zaman ρ tamsayısı 2δ formundadır. Her iki durumda da $(m, n) = 1$ ve pozitif tamsayılardır.

İspat. $(x, y) = (y, z) = (x, z) = 1$ olduğunu kabul edebiliriz. Çünkü $(x,y,z) = k$ olsa,
$k|x$, $k|y$ ve $k|z$ olduğundan (3.2.2) denklemi,

$$k^2 x_1^2 - dk^2 y_1^2 = k^2 z_1^2$$

ve

$$x_1^2 - dy_1^2 = z_1^2$$

olur ki, burada $(x_1, y_1, z_1) = 1$ dir. Şimdi,

$$x^2 - z^2 = dy^2, \quad (x - z)(x + z) = dy^2$$

olduğundan teorem 3.1.3 den, x ve z ler, $2\beta + \theta$ formunda ve $y = 2\alpha$ formundadır. $x = 2\beta_1 + \theta$, $z = 2\beta_2 + \theta$ şeklinde olduğundan $(x + z, x - z) = 2$ dir. Böylece $((x + z)/2, (x - z)/2) = 1$ olur. Eğer $(x + z, x - z) = 2$ ise o zaman $(x + z)/2 = u$ ve $(x - z)/2 = v$ dersek $(u, v) = 1$ elde edilir.
$y = 2\alpha$ formunda olduğunda

$$uv = ((x + z)/2)((x - z)/2) = (x^2 - z^2)/4 = d\alpha^2$$

dir. $(u, v) = 1$ olduğundan bu eşitliğin sağlanması için, u ve v nin karesel çarpan ihtiva etmesi gerekir. o halde $u = am^2$ ve $v = bn^2$ şeklindedir.

Eğer p, m nin bir asal çarpanı ise o zaman $p^2 \mid d\alpha^2$ dir. fakat $p^2 \nmid d$ olduğundan $p \mid \alpha$ olmalıdır. Bu düşünceden, α tamsayısı, m, n ve mn ile bölünebildiğinden $\alpha = mnq$ olacak şekilde q tamsayısı vardır. $a = (u/m^2)$, $b = (v/n^2)$ aldığımızda, bunların çarpımından dq^2 elde edilir ki, buradan $q^2 = 1$ olmalıdır.
$y = 2\alpha$ ve $\alpha = mnq$ olduğundan,

$$x = (am^2 + b n^2)\rho$$

$$y = 2mn\rho$$

$$z = (am^2 - bn^2)\rho \qquad (3.2.5)$$

elde edilir. Burada ρ kuadratik cismin herhangi bir tamsayısı, m ve n de, $(m , n) = 1$ olan pozitif tamsayılarıdır.
Eğer $(x + z , x - z) = 1$ ise o zaman kuadratik cismin x , z tamsayıları $2\beta + \theta$ şeklindedir. Bu yüzden $d = 2\alpha + \theta$ şeklinde olması gerekir. Yine

$$x + z = u \quad , \quad x - z = v \qquad (3.2.6)$$

alınarak, bu eşitlikler taraf tarafa toplanır ve çıkarılırsa,

$$x = (1/2)(am^2 + b n^2)\rho$$

$$y = mn\rho$$

$$z = (1/2)(am^2 - bn^2)\rho \qquad (3.2.7)$$

elde edilir. Böylece d nin her iki durumu için de teorem ispatlanmış olur.

Teorem 3.2.2 a , b ve c ler, $(a , b) = (a , c) = (b , c) = 1$, $c>2$ olacak şekilde $Q(\sqrt{m})$ kuadratik cisminin pozitif tamsayıları ve $d = ab$ olsun.

$$ax^2 - by^2 = c \qquad (3.2.8)$$

denkleminin $(x , y) = 1$ olacak şekilde, $Q(\sqrt{m})$ de tamsayı çözümlere sahip olması için,

$$u^2 - dv^2 = c^2 \qquad (3.2.9)$$

denkleminin çözülebilir olması gerekir.

İspat. Teoremin şartlarının sağlandığını ve (3.2.9) denkleminin (u, v) tamsayılarına göre çözüme sahip olduğunu kabul edelim. Teorem 3.2.1 den (3.2.9) denkleminin $Q(\sqrt{m})$ deki bütün çözümleri,
$d = ab = 2\alpha$ formunda olması durumunda,

$$u = (am^2 + bn^2)\rho$$

$$v = 2mn\rho$$

$$c = (am^2 - bn^2)\rho \quad , \qquad (3.2.10)$$

$d = ab = 2\alpha + \theta$ formunda olması durumunda,

$$u = (1/2)(am^2 + bn^2)\rho$$

$$v = mn\rho$$

$$c = (1/2)(am^2 - bn^2)\rho \qquad (3.2.11)$$

şeklindedir. Burada cismin ρ tamsayısı, m ve n nin herikisi $2\beta + \theta$ şeklinde ise, cismin herhangi bir tamsayısı, m ve n den sadece biri 2β şeklinde ise, 2γ formunda olan bir tamsayısıdır.
$d = ab = 2\alpha$ şeklinde olsun. o zaman $\rho = 1$ olması durumunda (3.2.10) dan

$$u = (am^2 + bn^2)$$

$$c = (am^2 - bn^2) \qquad (3.2.12)$$

elde edilir. Sonuç olarak (3.2.12) den $(u + c)/2 - (u - c)/2 = am^2 - bn^2 = c$ bulunur. Bunun anlamı ise, (3.2.9) denkleminin $(m, n) = 1$ olacak şekilde m ve n tamsayı çözümüne sahip olmasıdır.
$d = ab = 2\alpha + \theta$ olsun. $\rho = 2\rho_1$ olması durumunda (3.2.11) denkleminden

$$u = (am^2 + bn^2)\rho_1$$

$$c = (am^2 - bn^2)\rho_1 \qquad (3.2.13)$$

olup, $(m, n) = 1$ ve m, n ler birimden farklıdır. Böylece $\rho_1 = 1$ için,

$(u+c)/2 - (u-c)/2 = am^2 - bn^2 = c$ dir. Bu ise (3.3.9) denkleminin $Q(\sqrt{m})$ kuadratik cisminde, m ve n tamsayılarına göre bir çözümünün olduğunu verir ki, bu da ispatı tamamlar.

Tanım 3.2.1 (3.2.9) denklemini sağlayan, kuadratik cismin herhangi bir x tamsayısı için, $ax_0^2 - by_0^2 = c$ ve $x_0 \leq x$ ise o zaman (x_0, y_0) çözümüne, (3.2.9) denkleminin tekil çözümü adı verilir.

3.3 $Q(\sqrt{m})$ CİSMİNDE $x^3 + y^3 = z^3$ DİOPHATİNE DENKLEMİ

Bu denklemin çözümünü incelemeye geçmeden önce, aşağıdaki teoremleri ifade ve ispat edelim.

Teorem 3.3.1 a, Z de karesel olmayan bir tamsayısı ve m de,

$$x^2 \equiv a \pmod{m} \qquad (3.3.1)$$

kongrüansının çözüme sahip olacak şekildeki kuadratik cismin bir tamsayısı ve bu kongrüansın herhangi bir kökü N olsun. Bu takdirde $\sqrt{\frac{4}{3}|a|}$ yı geçmeyen, cismin bazı λ tamsayısı için, $Q(\sqrt{m})$ cisminde

$$\lambda m = x^2 - ay^2 \quad \text{ve} \quad x - Ny \equiv 0 \pmod{m}$$

kongrüansını sağlayan x , y tamsayıları bulunur.

İspat. İlk olarak $|m| > \sqrt{\frac{4}{3}|a|}$ kabul edelim. $N^2 \equiv a \pmod{m}$ nin kökü de, $(1/2)\,|m|$ yi geçmeyen tamsayıların cümlesinde olsun. $m \mid N^2 - a$ olduğundan, $N^2 - a = mm_1$ olacak şekilde $m_1 \in Q(\sqrt{m})$ tamsayısı var ve $m_1 = (N^2 - a)/m$ dir. Buradan;

$$|m_1| \leq \frac{|m|}{4} + \frac{|a|}{|m|}$$

dir. $\frac{|m|}{4} + \frac{|a|}{|m|} < |m|$ eşitsizliği, kabul ettiğimiz $|m| > \sqrt{\frac{4}{3}|a|}$ eşitsizliğini sağlar. Dolayısıyla $|m_1| < |m|$ dir. N nin (mod m_1) e göre en küçük kalanı N_1 ise, δ_1 tamsayısı, $|N_1| \leq (1/2)|m_1|$ olacak şekildeki tamsayıların cümlesinden alınmak üzere, $N_1 = N - \delta_1 m_1$ dir.

$$N^2 - a \equiv 0 \pmod{m_1}$$

olduğundan

$$N_1^2 \equiv a \pmod{m_1}$$

dir. yani, $m_2 \neq 0$ olmak üzere $N_1^2 - a = m_1 m_2$, $m_2 \in Q(\sqrt{m})$ dir. Yine,

$$|m_2| \leq \frac{|m_1|}{4} + \frac{|a|}{|m_1|} \quad , \quad |m_1| > \sqrt{\frac{4}{3}|a|}$$

oluyorsa $|m_2| < |m_1|$ dir. $|N_2| \leq \frac{1}{2}|m_2|$ olacak şekildeki sayıların cümlesinden seçilen δ_2 tamsayısı,

$$N_2 = N_1 - \delta_2 m_2$$

denklemini sağlar. O zaman, $N_2^2 - a = m_2 m_3$ ve $|m_2| > \sqrt{\frac{4}{3}|a|}$ olduğu sürece $|m_3| < |m_2|$ dir. Bu yolla devam edildiğinde

$$|m| > |m_1| > |m_2| > |m_3| > \dots,$$

şeklinde cismin tamsayılarının pozitif azalan bir dizisi oluşur. Böylece m, m_1, m_1, ... tamsayıları m_{k+1} e geldiğinde, ifadenin tamdeğeri, bir sonraki terimi olan m_{k+2} değildir. Bunun anlamı ise,

$$|m_{k+1}| \leq \sqrt{\frac{4}{3}|a|}$$

olması, m, m_1, m_1, ..., m_k ların hepsinin $\sqrt{\frac{4}{3}|a|}$ den daha büyük sayılar olmasını gerektirir. m_{k+1} yerine λ alınırsa,

$$\lambda m_k = N_k^2 - a$$

denkleminden $y_k = 1$, $z_k = 0$ ile sağlanan $\lambda m_k = (m_k z_k + N_k y_k)^2 - a y_k^2$ denklemi bulunur. Bu denklemde $N_k = N_{k-1} - \delta_k m_k$ ve $y_{k-1} = z_k - \delta_k y_k$, $z_{k-1} = y_k$ alınırsa,

$$\lambda m_k = (m_k y_{k-1} + N_{k-1} z_{k-1})^2 - a z_{k-1}^2$$

olup, $m_k m_{k-1} = N_{k-1}^2 - a$ olduğundan,

$$\lambda = m_k y_{k-1}^2 + 2N_{k-1} y_{k-1} z_{k-1} + m_{k-1} z_{k-1}^2$$

ve

$$\lambda m_{k-1} = (m_{k-1} z_{k-1} + N_{k-1} y_{k-1})^2 - a y_{k-1}^2$$

elde edilir. Burada $(y_k , z_k) = 1$ olduğundan $(y_{k-1} , z_{k-1}) = 1$ dir.
$N_{k-1} = N_{k-2} - \delta_{k-1} m_{k-1}$, $y_{k-2} = z_{k-1} - \delta_{k-1} y_{k-1}$, $z_{k-2} = y_{k-1}$ alınırsa,

$$\lambda m_{k-1} = (m_{k-1} y_{k-2} + N_{k-2} z_{k-2})^2 - a z_{k-2}^2 .$$

Aynı düşünceyle,

$$\lambda m_{k-2} = (m_{k-2} z_{k-2} + N_{k-2} y_{k-2})^2 - a y_{k-2}^2$$

olur. $(y_{k-1} , z_{k-1}) = 1$ olduğundan $(y_{k-2} , z_{k-2}) = 1$ dir . Aynı yolla devam edilirse,

$$\lambda m = (mz + Ny)^2 - ay^2$$

denklemini sağlayan ve $(y , z) = 1$ olan y , z tamsayıları bulunur. Eğer başlangıçta $|m| \le \sqrt{\frac{4}{3}|a|}$ ve $|m_1| \le \sqrt{\frac{4}{3}|a|}$ olarak kabul edilse, aynı düşünce uygulanırdı. $|m_1| > \sqrt{\frac{4}{3}|a|}$ ise, o zaman $(y , z) = 1$ olmak üzere, $\lambda m_1 = (m_1 y + N_1 z)^2 - az^2$ ve $\lambda m = (mz + Ny)^2 - ay^2$ olur. Burada, $x = mz + Ny$, $y = y$ alınırsa,

$$\lambda m = x^2 - ay^2 \quad , \quad x - Ny \equiv 0 \pmod m$$

yi sağlayan kuadratik cismin tamsayıları şu şekilde elde edilir.
$x = N_k$, $y_k = 1$ olarak başlayıp, x_{k-1}, y_{k-1} ; x_{k-2}, y_{k-2} ; ... ; x_1 , y_1 ; x , y çiftleri ,

$$y_{i-1} = \frac{x_i - N_{i-1} y_i}{m_i} \;, \quad x_{i-1} = m_{i-1} y_i + N_{i-1} y_{i-1} \qquad i = k\,, k-1, \dots, 2, 1$$

Formülünden hesaplanır.. Bu formüller, $x_i = m_i z_i + N_i y_i$ ve z_i nin bu eşitlikteki değeri,

$$y_{i-1} = z_i - \delta_i y_i \;, \quad z_{i-1} = y_i$$

de yerine yazılarak elde edilir.

Şimdi $a, n \in Z$ olmak üzere a nın bazı özel değerleri için ,

$$x^2 + ay^2 = z^n \tag{3.3.2}$$

denkleminin, kuadratik cisimdeki x , y , z tamsayılarına göre çözümlerini inceleyelem. Bu denklemin, $Q(\sqrt{m})$ kuadratik cismindeki çözümü olan x , y tamsayıları,

$$N^2 \equiv -a \pmod{z^n} \tag{3.3.3}$$

kongrüansının bazı köklerine bağlıdır. Yani ,

$$x - Ny \equiv 0 \pmod{z^n} \tag{3.3.4}$$

olduğundan,teorem 3.3.1 den

$$t^2 + au^2 = \lambda z \;, \quad t - Nu \equiv 0 \pmod{z^n} \tag{3.3.5}$$

yi sağlayan kuadratik cismin t , u tamsayıları ve $|\lambda| \leq \sqrt{\frac{4}{3}|a|}$ olacak şekilde $\lambda \in Z$ vardır.
Şimdi $\sqrt{-a}$, imajiner veya irrasyonel olmak üzere,

$$P - Q\sqrt{-a} = (t - u\sqrt{-a})^n \;, \quad n \in N \tag{3.3.6}$$

eşitliğinin sağ tarafı açıldığında, rasyonel kısmı, rasyonel kısma ve $\sqrt{-a}$ nın katsayısını, $\sqrt{-a}$ nın katsayısına eşitleyerek elde edilen, cismin P , Q tamsayılarını gözönüne alalım. (3.3.3) ve (3.3.5) den,

$$P - QN \equiv (t - Nu)^n \equiv 0 \pmod{z^n} \qquad (3.3.7)$$

yazılır. (3.3.4) ve (3.3.7) den

$$Px + aQy \equiv 0 \pmod{z^n} \;,\; Py - Qx \equiv 0 \pmod{z^n}$$

elde edilir ve $\rho , \sigma \in Q(\sqrt{m})$ olmak üzere,

$$Px + aQy = \rho z^n \;,\quad Py - Qx = \sigma z^n$$

yazılır.

$$\frac{x+y\sqrt{-a}}{P+Q\sqrt{-a}} = \frac{Px+aQy+\sqrt{-a}(Py-Qx)}{P^2+aQ^2}$$

alınırsa, (3.3.5) den $P^2 + aQ^2 = \lambda^n z^n$ elde edilir. Dolayısıyla,

$$x + y\sqrt{-a} = (1/\lambda^n)(\rho + \sigma\sqrt{-a})(P + Q\sqrt{-a})$$

olur. Böylece

$$x^2 + ay^2 = \frac{(\rho^2+a\sigma^2)(P^2+aQ^2)}{\lambda^{2n}}$$

veya

$$z^n = \frac{(\rho^2+a\sigma^2)\lambda^n z^n}{\lambda^{2n}} \;.$$

Buradan

$$\rho^2 + a\sigma^2 = \lambda^n \qquad (3.3.8)$$

denklemi bulunur.Şimdi $\lambda = \pm 1$ olacak şekildeki, a nın değerlerine dönelim. Bu durumda (3.3.2) denkleminin kuadratik cisimde herhangi bir çözümü, $(x , y) = 1$ olmak üzere,

$$x + y\sqrt{-a} = (\rho + \sigma\sqrt{-a})(t + u\sqrt{-a})^n \qquad (3.3.9)$$

ile verilir. Burada $(t, u) = 1$ dir.
Tersine olarak, kuadratik cismin keyfi t, u tamsayıları için, $\pm z = t^2 + au^2$ olmak üzere, (3.3.2) denkleminin çözümleri, (3.3.9) ile verilir.
$(t, au) = 1$ olmak üzere, kuadratik cismin (3.3.6) ile elde edilen P, Q tamsayıları, cismin herhangi bir asalı ile bölünsün. O zaman

$$r^2 \equiv -a \pmod p$$

kongrüansının bazı kökleri için,

$$t^2 + au^2 \equiv 0 \pmod p \quad \text{ve} \quad t \equiv ru \pmod p \qquad (3.3.10)$$

dir. Fakat $P + Qr \equiv (t + ru)^n \pmod p$ olduğundan,

$$t \equiv -ru \pmod p \qquad (3.3.11)$$

yazılır. (3.3.10) ve (3.3.11) den, $2t \equiv 0 \pmod p$ bulunur. Bu ise $p \mid au^2$ olmasıdır ki, $(t, au) = 1$ olduğundan dolayı bu imkansızdır. Bu ise $(x, y) = 1$.
O halde $(t, au) = 1$ ise $(x, y) = 1$ dir.
$a = 1$ olsun. O zaman

$$N^2 \equiv -1 \pmod{z^n}$$

kongrüansı, $n \geq 2$ ve $z = 2\beta$ olması durumunda çözümü imkansız olur. Bu yüzden $x^2 + y^2 = z^n$ denkleminde x, y tamsayıları farklı olmak zorundadır. Ayrıca $z > 0$ ise $\lambda = 1$ olup, $t^2 + u^2 = z$ denkleminde t, u lar, $(t, u) = 1$ olan farklı tamsayılardır. Dolayısıyla $x^2 + y^2 = z^n$ denkleminin bütün çözümleri $i = \sqrt{-1}$, $\varepsilon = \pm 1$, $\pm i$ ve $(t, u) = 1$ olmak üzere,

$$x + iy = \varepsilon(t + iu)^n$$

ile verilir. $(i)^2 = -1$ olduğundan $n = 2$ için denklemin çözümleri

$$x + iy = (p + iq)^2 \quad \text{veya} \quad x + iy = i(p - iq)^2$$

den $x = r^2 - q^2$, $y = 2pq$ veya $x = 2pq$, $y = r^2 - q^2$ şeklinde verilir.
Burada $(p, q) = 1$ dir.

$n = 3$ için,

$$x + iy = (p + iq)^3$$

olur. Yani , $x^2 + y^2 = z^n$ denklemin bütün çözümleri, $(p\ ,\ q) = 1$ olmak üzere,

$$x = p^3 - 3pq^2\ ,\quad y = 3p^2 q - q^3\ ,\quad z = p^2 + q^2$$

ile verilir.
$a = 2$ olsun. O zaman,

$$N^2 \equiv -2 \pmod{z^n}$$

kongrüansı, $z = 2\beta$ ve $\lambda = 1$ için çözüme sahip olmayacağından $(t\ ,\ 2u) = 1$ olmak zorundadır. Bu durumda $x^2 + 2y^2 = z^n$ denkleminin bütün çözümleri, $(p\ ,\ 2q) = 1$ olmak üzere,

$$x + y\sqrt{-2} = \pm(p + q\sqrt{-2})^n\ ,\quad z = p^2 + 2q^2$$

ile verilir.
$a = 3$ olsun. Bu takdirde,

$$N^2 \equiv -3 \pmod{z^n}$$

kongrüansı, $n \geqslant 3$ ve $z = 2\beta$ ise bir çözüme sahip olmadığından $z = 2\beta + \theta$ formunda ve $\lambda = 1$ olmalıdır. Böylece $(x\ ,\ y) = 1$ olan farklı tamsayılar ve $z = 2\beta + \theta$ olmak üzere, $x^2 + 3y^2 = z^n$ denkleminin bütün çözümleri,

$$x + y\sqrt{-3} = \pm(p + q\sqrt{-3})^n\ ,\quad z = p^2 + 3q^2$$

ile verilir. Burada p ve 3q , $(p\ ,\ 3q) = 1$ olan farklı tamsayılardır.
$n = 2$ olması durumunda $(x\ ,\ y) = 1$ olmasına rağmen $z = 2\beta$ olabilir. Bu durumda $\lambda = 2$ ve

$$x + y\sqrt{-3} = (1/4)(\rho + \sigma\sqrt{-3})\ \ (t + u\sqrt{-3})^2\ ,\quad z = (1/2)\,(p^2 + 3q^2)$$

olup, (3.3.8) den ,

$$\rho^2 + 3\sigma^2 = 4 \qquad (3.3.12)$$

elde edilir.

ρ , $\sigma \in Q(\sqrt{m})$ olduğundan, (1.2.7) den $\rho = (1/2)(a + b\sqrt{m})$, $\sigma = (1/2)(c + d\sqrt{m})$ şeklinde olup, (3.3.12) denkleminin sağlanması için $\rho = \pm 2$, $\sigma = 0$ veya $\rho = \pm 1$, $\rho = \pm 1$ olmalıdır.

Yine (1.2.6) dan $\rho = (a + b\sqrt{m})$ ve $\sigma = c + d\sqrt{m}$ formunda olup, (3.3.12) denkleminin sağlanması için $\rho = \pm 2$, $\sigma = 0$ veya $\rho = \pm 1$ $\sigma = \pm 1$ olmalıdır. O halde $\rho = \pm 2$, $\sigma = 0$ olduğunda t , u lar, $2\beta + \theta$ şeklindedir.

$\rho = \pm 1, \sigma = \pm 1$ olması durumunda, $\left(\frac{\rho + \sigma\sqrt{-3}}{2}\right)^2 = \frac{-1 + \sqrt{-3}}{2}$ ve $\rho = \mp 1$, $\sigma = \pm 1$ olması durumunda, $\left(\frac{\rho + \sigma\sqrt{-3}}{2}\right)^2 = \frac{-1 - \sqrt{-3}}{2}$ olduğundan,

$$x + y\sqrt{-3} = \frac{-1 \pm \sqrt{-3}}{4}(t + u\sqrt{-3})^2 = \frac{1}{2}\left(\frac{t \mp 3u + (u \pm t)\sqrt{-3}}{2}\right)^2$$

$$= (1/2)(p + q\sqrt{-3})^2$$

elde edilir ki burada, $p = (1/2)(t \mp 3u)$, $q = (1/2)(u \pm t)$ ve $p^2 + 3q^2 = t^2 + 3u^2$ dir. Şimdi aşağıdaki sonucu verelim.

Sonuç 3.3.1 $x^2 + 3y^2 = z^n$ denkleminin bütün çözümleri, $(p, 3q) = 1$ olmak üzere, $\lambda = 1$,p ve q lar cismin herhangi bir tamsayısı ise,

$$x + y\sqrt{-3} = \pm(p + q\sqrt{-3})^n \;, \quad z = p^2 + 3q^2 \;, \quad (3.3.13)$$

ve $\lambda = 2$,p ve q tamsayılarının her ikisi birden $2\beta + \theta$ formunda ise,

$$x + y\sqrt{-3} = \pm\ (1/2)(p + q\sqrt{-3})^n \;, \quad z = (1/2)\ p^2 + 3q^2$$

ile verilir.

Teorem 3.3.2 $x^3 + y^3 = z^3$ Diophantine denklemi, $xyz \neq 0$ olmak üzere, $Q(\sqrt{m})$ kuadratik cisminde hiç bir tamsayı çözüme sahip değildir.

İspat. $Q(\sqrt{m})$ kuadratik cisminin, x_1 , y_1 , z_1 tamsayıları,

$$x^3 + y^3 = z^3 \tag{3.3.14}$$

denklemini sağlasın, Ayrıca z_1 in, bu denklemi sağlayan en küçük pozitif tamsayı olduğunu kabul edelim. Burada $(x, y) = 1$ kabul edilirse, $(x_1, y_1) = (x_1, z_1) = (y_1, z_1) = 1$ olur. Teorem 3.1.3 den bu tamsayıların ikisi $2\beta + \theta$ şeklinde olmalıdır. x_1 ve y_1 tamsayılarının $2\beta + \theta$ formunda olduğunu kabul edelim. Eğer x_1, z_1 bu formda olsaydı (3.3.14) denklemi $x^3 + (-z)^3 = (-y)^3$ formunda yazılırdı ki, bu da (3.3.14) denklemiyle aynı olurdu. Şimdi p ve q lar, $(p, q) = 1$ olacak şekilde biri 2α ve diğeri $2\beta + \theta$ formunda kuadratik cismin tamsayıları olmak üzere,

$$x_1 = p + q \ , \quad y_1 = p - q$$

alalım. Dolayısıyla,

$$x_1 = 2\alpha + 2\beta + \theta = 2(\alpha + \beta) + \theta$$

ve

$$y_1 = 2\alpha - 2\beta - \theta = 2(\alpha - \beta - \theta) + \theta$$

formunda olur. Bunlar (3.3.14) denkleminde yerlerine yazılırsa,

$$2p(p^2 + 3q^2) = z_1^3 \tag{3.3.15}$$

elde edilir ve $p \neq 0$ dır. Şimdi z_1 nin, 3 ile bölünebildiğini veya bölünemediğini inceleyelim. Önce kabul edelim ki z_1, 3 ile bölünemesin. Bu durumda $(2p, p^2 + 3q^2) = 1$ olduğundan, teorem 3.1.1 den,

$$p = 4\gamma^3 \ , \quad p^2 + 3q^2 = \delta^3 \ , \quad z_1 = 2\gamma\delta$$

yazılır. $(p, q) = 1$ olması sebebiyle teorem 3.3.1 den,

$$p^2 + 3q^2 = \delta^3 \tag{3.3.16}$$

denkleminin,

$$p + q\sqrt{-3} = (r + s\sqrt{-3})^3 \tag{3.3.17}$$

şeklinde çözümü vardır. Buradan,

$$p = r(r^2 + 9s^2)\ , \quad q = 3s(r^2 - s^2)$$

elde edilir. Fakat $p = 4\gamma^3$ şeklinde olduğundan,

$$r(r^2 - 9s^2) = r(r + 3s)(r - 3s) = 4\gamma^3$$

olmalıdır. r ve s, $(r\ , 3s) = 1$ olacak şekilde, $r = 2\alpha$, $s = 2\beta + \theta$ formunda kuadratik cismin tamsayıları ve

$$(r\ , r + 3s) = (r\ , r - 3s) = (r + 3s\ , r - 3s) = 1$$

olmaları nedeniyle teorem 3.1.1 den dolayı,

$$r + 3s = \xi^3\ , \quad r - 3s = \eta^3\ , \quad r = (1/2)\,\mu^3 \qquad (3.3.18)$$

olmalıdır. (3.3.18) den,

$$\xi^3 + \eta^3 = \mu^3$$

elde edilir. Burada ξ , η ve μ nün sıfırdan farklı oldukları açıktır.
$z_1 = 2\gamma\delta$ ve $r(r + 3s)(r - 3s) = 4\gamma^3$ olmasından dolayı

$$z_1 = \xi\eta\mu\delta \quad \text{ve} \quad \delta = r^2 + 3s^2 > 16$$

dır. Bu nedenle , $|z_1| > |\mu|16$ olup, buradan $|\mu| < (1/16)\,|z_1| < |z_1|$ bulunur. Bu ise (3.3.14) denklemini sağlayan, z_1 den daha küçük pozitif bir sayısının varlığını gösterir ki, bu da z_1 tamsayısının tanımına tezat teşkil eder. Bu sebeple z_1 tamsayısının 3 ile bölünememesi durumunda (3.3.14) denkleminin, $Q(\sqrt{m})$ kuadratik cisimde çözümü yoktur.
Kabul edelim ki, z_1 , 3 ile bölünebilsin. O zaman (3.3.15) den dolayı $3|\ p$ olmalıdır. (3.3.15) ifadesinin her iki yanını 9 ile kısaltırsak ,

$$(2/9)p\,(p^2 + 3q^2) = \frac{z_1^3}{9}$$

$$(2/3)p(3(\frac{p}{3})^2 + q^2) = 3(\frac{z_1}{3})^3$$

olur. Burada $((2/3)p, 3(\frac{p}{3})^2 + q^2) = 1$ olup, teorem 3.1.1 den,

$$p = 36\gamma^3 , \quad 3(\frac{p}{3})^2 + q^2 = \delta^3 , \quad z = 6\gamma\delta$$

olmalıdır. Yine teorem 3.3.1 den dolayı $3(\frac{p}{3})^2 + q^2 = \delta^3$ denkleminin çözümleri, sonuç 3.3.1 den,

$$q + (1/3)p\sqrt{-3} = (r + s\sqrt{-3})^3$$

şeklindedir. Bu denklemden

$$p = 9s(r^2 - s^2) = 36\gamma^3 \quad \text{veya} \quad p = s(r^2 - s^2) = 4\gamma^3$$

elde edilir. Fakat r, $r+s$, $r-s$ sayıları $(r, s) = 1$ olduğundan $(s, r+s) = (s, r-s) = (r+s, r-s) = 1$ dir. Böylece, $r + s = \xi^3$, $r - s = -\eta^3$, $s = (1/2)\mu^3$ alındığında,

$$\xi^3 + \eta^3 = \mu^3$$

elde edilir. Burada ξ, η ve μ ler cismin sıfırdan farklı tamsayılar olup, (3.3.14) denklemini sağlarlar.

$z_1 = 6\gamma\delta$, $4\gamma^3 = s(r+s)(r-s)$ ve $s = (1/2)\mu^3$, $r + s = \xi^3$, $r - s = -\eta^3$ olmalarından dolayı,

$$z_1 = -3\xi\eta\mu\delta \quad \text{ve} \quad \delta = r^2 + 3s^2 > 48$$

olup,

$$144|\mu| < |z_1| , \quad |\mu| < (1/144)|z_1| < |z_1|$$

dir. Dolayısıyla z_1 den daha küçük kuadratik cismin bir μ tamsayısı elde edilir. Bu ise z_1 tamsayısının tanımıyla çelişir. Bu yüzden $3 | z$ için (3.3.14) denklemi, $Q(\sqrt{m})$ kuadratik cisminde hiç bir çözüme sahip değildir.

Sonuç olarak, z_1 tamsayısının, 3 ile bölünübildiği veya bölünemediği durumların herikisi için de, (3.3.14) denkleminin, $Q(\sqrt{m})$ kuadratik cisminde bir çözüme sahip olmadığı gösterilmiş olur. Böylece teoremin ispatı tamamlanmış olur.

3. 4 $Q(\sqrt{m})$ CİSMİNDE $x^4 - y^4 = z^2$ DİOPHANTİNE DENKLEMİ

Teorem 3.4.1 $x^4 - y^4 = z^2$ Diophantine Denklemi, $Q(\sqrt{m})$ kuadratik cisminde hiç bir çözüme sahip değildir.

İspat. x, y ve z nin pozitif olduklarını kabul edelim. Eğer $(x , y) = d$ ise $x = x_1 d$, $y = y_1 d$, $z = z_1 d$ olacak şekilde $x_1 , y_1 , z_1 \in Q(\sqrt{m})$ tamsayıları vardır. Bu durumda,

$$(x_1 d)^4 - (y_1 d)^4 = (z_1 d)^2$$

$$x_1^4 - y_1^4 = z_1^2$$

elde edilir ki, $(x_1, y_1) = 1$ olduğundan $(x_1, z_1) = (y_1, z_1) = 1$ dir. Bu yüzden kuadratik cismin x , y ve z tamsayılarını $(x, y) = (x , z) = (y , z) = 1$ olarak kabul edebiliriz. Teorem 3.1.3 den $x = 2\alpha + \theta$ fomunda olduğundan, $y^4 + z^2$, 4 ile bölünemez. Kabul edelim ki,

$$x^4 - y^4 = z^2 \tag{3.4.1}$$

denklemi $Q(\sqrt{m})$ kuadratik cisminde bir (x , y ,z) çözümüne sahip olsun ve x tamsayısı da bu denklemi sağlayan en küçük pozitif tamsayı olsun. İlk olarak $y = 2\beta$ şeklinde olmasını gözönüne alalım. Bu durumda $(x^2 + z , x^2 - z) = 2$ dir. $y = 2\beta$ formunda olduğundan $16 \mid (x^2 + z)(x^2 - z)$ dir. Dolayısıyla bu sayılardan biri 2, diğeri 8 ile bölünebilir. Bu yüzden,

$$\left(\frac{1}{2}(x^2 \pm z), \frac{1}{8}(x^2 \mp z)\right) = 1$$

olup, bu sayılar teorem 3.1.1 den, dördüncü kuvvetten olmalıdır.

Bu nedenle $(a , b) = 1$ ve $a = 2\beta + \theta$ formunda olmak üzere,

$$\begin{aligned}(x^2 \pm z) &= 2a^4 \\ (x^2 \mp z) &= 8b^4\end{aligned} \tag{3.4.2}$$

olup $y = 2ab$ bulunur. (3.4.2) ifadesinden,

$$x^2 = a^4 + 4b^4 \tag{3.4.3}$$

elde edilir ve bu denklem,

$$(x + a^2)(x - a^2) = 4b^2 \tag{3.4.4}$$

olarak yazılır. Yine burada $(x + a^2, x - a^2) = 2$ olduğundan

$$x + a^2 = 2c^4 \ , \quad x - a^2 = 2d^4 \tag{3.4.5}$$

olup, $b = cd$ ve $(c\ ,\ d) = 1$ olacak şekilde kuadratik cisminin c , d tamsayıları vardır. (3.4.5) den

$$a^2 = c^4 - d^4 \tag{3.4.6}$$

denklemi elde edilir ki, $y = 2\beta$ olması durumunda (3.4.1) denkleminin (x , y , z) çözümünden hareket ederek yeni bir (c , d , a) çözümünün varlığını göstermiş oluruz. Kuadratik cismin a , b , c , d tamsayıları sıfırdan farklı olduklarından,

$$c < 2acd = y < x$$

olduğundan, bulduğumuz $Q(\sqrt{m})$ kuadratik cismin bu c tamsayısı x tamsayısının tanımına bir tezat teşkil eder. O halde $y = 2\beta$ olması durumunda , (3.4.1) denkleminin $Q(\sqrt{m})$ kuadratik cisminde çözümü yoktur.

$y = 2\beta + \theta$ formunda olduğunu kabul edelim. Bu durumda $(x^2 - y^2 , x^2 + y^2) = 2$ olması nedeniyle δ, $Q(\sqrt{m})$ kuadratik cisminin bir tamsayısı olmak üzere $z = 2\delta$ formundadır. Böylece $\left(\frac{x^2+y^2}{2} , \frac{x^2-y^2}{2}\right) = 1$ olması sebebiyle teorem 3.1.1 den,

$$x^2 + y^2 = 2a^2 \ , \quad x^2 - y^2 = 2b^2 \tag{3.4.7}$$

yazılır. Burada a ve b ler, kuadratik cismin $(a, b) = 1$ ve $2z = ab$ olacak şekildeki tamsayılarıdır. (3.4.7) den $x^2 = a^2 + b^2$ $y^2 = a^2 - b^2$ buluruz. Bu son eşitlikler taraf tarafa çarpılırsa,

$$(xy)^2 = a^4 - b^4 \tag{3.4.8}$$

denklemi elde edilir. $y = 2\beta + \theta$ formunda olduğunda (3.4.1) denkleminin yeni bir (a, b, xy) çözümü elde edildi. Fakat a, b kuadratik cismin sıfırdan farklı pozitif tamsayıları olduğundan,

$$a^2 < a^2 + b^2 \quad , \quad a < \sqrt{a^2+b^2} = x$$

olup, bu da x in tanımına bir tezattır. o halde (3.4.1) denklemi $Q(\sqrt{m})$ de çözülemez.

Sonuç olarak, $y = 2\beta$ ve $y = 2\beta + \theta$ formunda olması durumlarının herikisinde de, (3.4.1) denkleminin, $z \neq 0$ olması durumunda, $Q(\sqrt{m})$ kuadratik cisminde, hiç bir çözümü yoktur.

3.5 $Q(\sqrt{m})$ CİSMİNDE $x^4 + y^4 = z^2$ DİOPHANTİNE DENKLEMİ

Teorem 3.5.1 $x^4 + y^4 = z^2$ Diophantine Denkleminin $Q(\sqrt{m})$ kuadratik cisminde sıfırdan farklı hiç bir çözümü yoktur.

İspat. $xyz \neq 0$ olmak üzere,

$$x^4 + y^4 = z^2 \tag{3.5.1}$$

denkleminin $Q(\sqrt{m})$ cisminde çözümünün olduğunu kabul edelim. Burada $(x, y) = 1$ kabul edebiliriz. Eğer $(x, y) = d$ ise o zaman $x = x_1 d$, $y = y_1 d$ olduğundan $(x_1, y_1) = 1$ olur. Dolayısıyla,

$$(x_1 d)^4 + (y_1 d)^4 = (z)^2$$

$$d(x_1^4 + y_1^4) = (z)^2$$

olur. Buradan $d^4 | z^2$ ve dolayısıyla $d^2 | z$ bulunur. Bu sebeple $z = d^2 z_1$ olup $z_1 > 0$ dir. z nin bu değeri yerine yazılırsa,

$$x_1^4 + y_1^4 = z_1^2 \qquad (3.5.2)$$

elde edilir ki, bu da $(x_1 , y_1) = 1$ olmak şartıyla (3.5.1) denklemiyle aynıdır. Kabul edelim ki, $Q(\sqrt{m})$ kuadratik cisminin x_0 , y_0 , z_0 tamsayıları (3.5.1) denklemini sağlasın ve z_0, bu eşitliği sağlayan en küçük pozitif tamsayı olsun. $((x_0 , y_0) = 1)$ Bu takdirde,

$$x_0^4 + y_0^4 = z_0^2$$

olduğundan $(x_0^2)^2 + (y_0^2)^2 = z_0^2$ olur. Bu ise x_0^2 , y_0^2 , z_0 tamsayılarının (3.1.1) denkleminin bir çözümü olmasıdır. Dolayısıyla $(x_0^2 , y_0^2) = 1$ olması nedeniyle sonuç 3.1.2 den,

$$x_0^2 = m^2 - n^2$$

$$y_0^2 = 2mn$$

$$z_0 = m^2 + n^2 \qquad (3.5.3)$$

olacak şekilde, $Q(\sqrt{m})$ kuadratik cisminin, $(m , n) = 1$ olacak şekilde m ve n tamsayıları vardır. Burada eğer gerekirse x ve y nin yerlerini değiştire- biliriz. (3.5.3) den ,

$$m^2 = x_0^2 + n^2 \qquad (3.5.4)$$

olur ki, teorem 3.1.4 den bu denklemin çözümü vardır ve bu çözümler sonuç 3.1.2 den,

$$x_0 = r^2 - s^2$$
$$n = 2rs$$
$$m = r^2 + s^2$$

dir. Burada r ve s ler, $(r, s) = 1$ olan, $Q(\sqrt{m})$ kuadratik cisminin pozitif tamsayılarıdır. $m = 2\beta+\theta$ formunda olduğundan, $(m, 2n) = 1$ olup, $y_0^2 = 2mn$ olması nedeniyle teorem 3.1.1 den dolayı $m = z_1^2$ ve $2n = w^2$ olacak şekilde $z_1, w \in Q(\sqrt{m})$ vardır. w, n nin 2 katı olduğundan $w = 2v$ yazılabilir. Burada v, $v^2 = (n/2) = rs$ olan, cismin pozitif tamsayısıdır. $(r, s) = 1$ olduğundan teorem 3.1.1 den $r = x_1^2$, $s = y_1^2$ olacak şekilde, kuadratik cismin, x_1, y_1 pozitif tamsayıları vardır. $(r, s) = 1$ olduğundan $(x_1, y_1) = 1$ dir. Bu değerler sırasıyla yerle-rine yazılırsa (3.5.2) denklemi elde edilir ki, cismin x_1, y_1, z_1 pozitif tamsayıları (3.5.1) denklemini sağlar. $Q(\sqrt{m})$ cisminin bu tamsayılarının hepsi sıfırdan farklı olduklarından,

$$z_1 < z_1^4 = m^2 < m^2 + n^2 = z_0$$

elde edilir. Bu z_0 tamsayısının, $Q(\sqrt{m})$ kuadratik cisminin en küçük tamsayısı olmasıyla çelişir.

Sonuç olarak, (3.5.1) denkleminin, $xyz \neq 0$ olması durumunda $Q(\sqrt{m})$ kuadratik cisminde çözümü yoktur.

KAYNAKLAR

[1]. H. Altındiş and M. Atasoy, The Linear Diophantine Equation $ax + by + cz = e$ in $Q(\sqrt{5})$, Indian Journal of Pure and applied Mathematics, (Baskıda)

[2]. J. H. Chen, Common Solution of Pell Equation $x^2 - 2y^2 = 1$ and $y^2 - Dz^2 = 4$, J. Wuha univ. Natur. Sci. ed., 1 , 8-12 , (1990)

[3]. E. L. Cohen, On the Diophantine Equation $x^2 - Dy^2 = nz^2$, Journal of Number Theory, 40, 86-91, (1992)

[4]. H. Cohn , Advanced Number Theory, p.44-45, Dover Publications, inc., New York, (1961)

[5]. G. N. Copley , Recurrence relations for solutions of Pell's Equation, Amer. Math. Monthly 66, 288-290, (1959)

[6]. J. T. Crass, In the Gaussian integers, $\alpha^4 + \beta^4 = \gamma^4$, Math. Mag. vol. 66, 2, 105-108 , (1993)

[7]. H. Darmon, The Equation $x^4 - y^4 = z^p$, C.R. Math. Rep. Acad. Sci., Canada vol. 15, 6 , 286-290, (1993)

[8]. A. Grelak and A. Grytczuk, On the Diophantine Equation $ax^2 - by^2 = c$, Publ. Math. Debrecen 44/ 3-4 , 291- 299, (1994)

[9]. G. H. Hardi, An Indroduction to the Theory of Number, p. 204-209, Oxsfortd at the Clarenden Press, (1960)

[10]. P. Kaplan, Pell's Equations $x^2 - my^2 = -1$, -4 and Continued Fractions, Journal of Number Theory , 23, 169-182, (1986)

[11]. W. J. Leveque, Topics in Numbers Theory, p. 20-22 , Printed in the United States of America , (1956)

[12]. S. P. Mohanty and A. M. S. Ramasamy, The Characteristic number of two simultaneous Pell's equations and its application, A Quarterly Journal of Pure and Applied Math. 59, 203-214, (1985)

[13]. L. J. Mordel, Diophantine Equation, p.30-34, London and New York, (1969)

[14]. T. Nagel, Indroduction to Number Theory , p. 227-245, Wiley, New York, (1951)

[15]. I. Niven, An indroduction to the Theory of Numbers, p.373-379 John wiley sons inc., New York, (1972)

[16]. D. Rosen, The Diophantine Equation $ax + by = c$ in $Q(\sqrt{5})$ and other Number Field, Pacific Journal of Math. , vol.119 , 2, 465-472, (1985)

[17]. K. H. Rosen, Elementary Number Theory and its Applications, p.353 - 363, Reprinted with Corrections, (1988)

[18]. M. Sved, On the Rational Solutions of $x^y = y^x$, Math. Mag. Vol.63 , 1, 330-33 , (1990)

[19]. J. Uspensky , M. A. Heaslet, Elementary Numbers Theory, p. 389-396, Mcgraw Hill Book Campany inc., New York and London, (1939)

[20]. J. Wolfort, Eine Bemerkung Uber Heckes Modulgruppen, Arch. Der. Math. ,1 ,72-77 ,(1977)

[21]. K. D. Zelator, The Diophantine Equation $x^2 + a^2y^m = z^{2n}$ With $(x,ay) = 1$, Fibonacci Quart. 30, 305-309, (1992)

[22]. N. O. Zelator, The Diophantine Equation $x^4 + dy^4 = z^p$, C. R. Math. Rep. Acad. Sci. , Canada vol.14, 1 , 55-58 , (1992)