T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

DIOPHANT DENKLEMLERİ

YÜKSEK LİSANS TEZİ

Sündüz KELEŞ

Enstitü Anabilim Dalı : MATEMATİK
Tez Danışmanı : Doç. Dr. Refik KESKİN

Mayıs 2007

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

DIOPHANT DENKLEMLERİ

YÜKSEK LİSANS TEZİ

Sündüz KELEŞ

Enstitü Anabilim Dalı : MATEMATİK

Tez Danışmanı : Doç. Dr. Refik KESKİN

Bu tez 11/05/2007 tarihinde aşağıdaki jüri tarafından Oybirliği ile kabul edilmiştir.

Doç. Dr. Refik KESKİN	Yrd. Doç. Dr. Mehmet ÖZEN	DOÇ. DR. ELMAN ALİYEV
Jüri Başkanı	Jüri Üyesi	Jüri Üyesi

TEŞEKKÜR

Tez çalışmamız boyunca bana zaman ayıran, üstün bilgi ve birikimlerini paylaşan ve de desteğini esirgemeyen kıymetli hocam Doç. Dr. Refik KESKİN'e; düşünce ve tavsiyelerini paylaşmaktan çekinmeyen Araş. Gör. Bahar DEMİRTÜRK'e; sadece tezimi hazırlarken değil bugüne kadar her ihtiyaç duyduğumda hiç karşılık beklemeden yanımda olan sevgili anneme; hiçbir fedakarlıktan kaçınmayarak bugünlere gelmemi sağlayan sevgili babama; hayatım boyunca zor anlarımı paylaşan, bana her konuda yardımcı ve destek olan kardeşim Sevil'e; hayatın akışına ayak uydurmaya çalışırken zamanın sınırlı olduğunu hissettiğim ve bunun sıkıntısını yaşadığım anlarda imdadıma yetişen kardeşlerim Uğur ve Yaşar'a; maddi ve manevi desteğini hiçbir zaman esirgemeyen canım eşim Engin'e; varlığıyla bana güç veren biricik oğlum Aybars Yağız'a desteklerinden dolayı teşekkürü bir borç bilirim.

Sündüz KELEŞ

İÇİNDEKİLER

SİMGELER VE KISALTMALAR LİSTESİ

$a \mid b$: a böler b

$a \nmid b$: a bölmez b

$a \sim b$: a ilgili b

$a \not\sim b$: a ilgili değil b

$| \, |$: Mutlak değer

$\Leftrightarrow$: Ancak ve ancak

$\Rightarrow$: İse

$\mathbb{N}$: Doğal sayılar kümesi

$\mathbb{Z}$: Tamsayılar *kümesi*

$[\![\,]\!]$: Tamdeğer

$\equiv$: Denktir

$\not\equiv$: Denk değildir

$\in$: Elemanıdır

$\subset$: Altküme

$\cup$: Birleşim

$\left(\frac{m}{p}\right)$: Legendre sembolü

ÖZET

Anahtar kelimeler: Kareler toplamı, Pisagor üçlüleri, Tek türlü parçalanmalı bölge.

Bu tezde bazı Diophant denklemleri incelenmiştir. Birinci bölümde bazı asal sayıların, iki sayının karelerinin toplamı biçiminde yazılabileceği gösterildi. Ayrıca bu bölümde her n doğal sayısının dört tamsayının kareleri toplamı biçiminde yazılabileceği gösterildi. İkinci bölümde de pisagor üçlüleri incelenmiş ve bazı denklemlerin çözümlerinin olmadığı gösterilmiştir. Üçüncü bölümde ise $x^3 + y^3 = z^3$ denkleminin çözümünün olmadığı gösterilmiştir. Son olarak dördüncü bölümde tek türlü parçalanmalı bölgeler ele alınarak bazı Diophant denklemlerinin çözümleri incelenmiştir.

DIOPHANT EQUATIONS

SUMMARY

Key Words: Sum of squares, Pytheporian triples, Unique factorization domain.

In this thesis, we investigated some Diophant equations. In the first chapter, it is shown that the primes of the form $4n+1$, is a sums of two squares. Moreover it is shown that every natural number is a sum of four squares. Second chapter is devoted to the Pythegorion triples. In this chapter it is shown that some Diophant equations has not got a solution. In the thirth chapter, the equation $x^3+y^3=z^3$, is considered and it shown that is no solution to this equation. Lastly, in the fourth chapter by considering the unique factorization domain, solutions of Diophant equations are investigated.

BÖLÜM 1. GİRİŞ

1.1. Güvercin Yuvası İlkesi ve Bazı Uygulamaları

Lemma 1.1.1(Güvercin yuvası ilkesi): Eğer n elemanlı bir küme alt kümelerinin m tanesinin birleşimine eşit ve $n > m$ ise en az bir alt küme birden fazla elemana sahiptir.

Sonuç 1.1.2: $x_1,\ldots,x_n$ tamsayılar ve n>m olsun. Bu taktirde, $x_i \equiv x_j (\text{modm})$ olacak biçimde $i \neq j$ vardır.

Lemma1.1.3 (Thue'nin Lemması): $n \geq 2$ doğal sayısı bir tam kare olmasın. Bu durumda a bir tamsayı olmak üzere $(a,n)=1$ ise $ax \equiv y (\text{mod}\, n)$ olacak biçimde $0<|x|<\sqrt{n}$ ve $0<|y|<\sqrt{n}$ şartlarını sağlayan x ve y tamsayıları vardır.

İspat: k=$\left[\!\left[\sqrt{n}\right]\!\right]$ olsun. $\sqrt{n}$ tamsayı olmadığından , $\left[\!\left[\sqrt{n}\right]\!\right]<\sqrt{n}<\left[\!\left[\sqrt{n}\right]\!\right]+1$ dir.Yani k<$\sqrt{n}$ <k+1 olur. Dolayısıyla $(k+1)^2$>n olur. $0 \leq |x_1| < \sqrt{n}, 0 \leq |y_1| < \sqrt{n}$ olmak üzere $ax_1 + y_1$ tamsayılarının sayısı $(k+1)^2$ dir ve $(k+1)^2 > n$ dir. O halde, $ax_1 + y_1 \equiv ax_2 + y_2 (\text{mod}\, n)$ olan $(x_1,x_2) \neq (y_1,y_2)$ vardır. Bu durumda $a(x_1 - x_2) \equiv y_2 - y_1 (\text{mod}\, n)$ olur. $x = x_1 - x_2, y = y_2 - y_1$ alırsak, $ax \equiv y (\text{mod}\, n)$ bulunur. Burada,

$$|x| = |x_1 - x_2| \leq k \text{ , } |y| = |y_2 - y_1| \leq k$$

olduğundan

$$0 \le |x| < \sqrt{n}, 0 \le |y| < \sqrt{n}$$

elde edilir.

$x = 0$ ise $a.0 \equiv y \pmod{n}$ olur ve $n \mid y$ elde edilir. Bu ise $n \le |y|$ olmasını gerektirir. Ancak $|y| < \sqrt{n}$ olduğundan çelişki elde edilir. Dolayısıyla $x \neq 0$ dır. $y = 0$ ise $ax \equiv 0 \pmod{n}$ olur. $(a,n) = 1$ olduğundan $n \mid x$ dir. $x \neq 0$ olduğundan $n \le |x|$ olur. Fakat bu $|x| < \sqrt{n}$ ile çelişir. Dolayısıyla $y \neq 0$ dır. Böylece,

$$0 < |x| < \sqrt{n}, \quad 0 < |y| < \sqrt{n}$$

bulunur.

Teorem 1.1.4: $p > 2$ ve p asal sayı olsun. Bu taktirde $p \equiv 1 \pmod{4}$ tür $\Leftrightarrow$ $p \mid x^2 + 1$ olacak biçimde bir x tam sayısı vardır [5].

Teorem 1.1.5: $p > 2$ ve p asal sayı olmak üzere $p = a^2 + b^2$ olacak biçimde a ve b tam sayıları vardır $\Leftrightarrow$ $p \equiv 1 \pmod{4}$ tür.

İspat: $(\Leftarrow)$ $p \equiv 1 \pmod{4}$ olsun. O zaman $(a,p) = 1$ olmak üzere $a^2 \equiv -1 \pmod{p}$ olan bir a tamsayısı vardır. $(a,p) = 1$ ise Lemma 1.1.3 e göre $a\, x_0 \equiv y_0 \pmod{p}$ olacak biçimde $0 < |x_0| < \sqrt{p}$ ve $0 < |y_0| < \sqrt{p}$ şartını sağlayan x_0, y_0 tam sayıları vardır. $a^2 x_0^2 \equiv y_0^2 \pmod{p}$ ve $a^2 \equiv -1 \pmod{p}$ olduğundan $x_0^2 + y_0^2 \equiv 0 \pmod{p}$ dir. $x_0^2 + y_0^2 = kp$ olsun. $0 < |x_0| < \sqrt{p}$ ve $0 < |y_0| < \sqrt{p}$ olduğundan $x_0^2 + y_0^2 < 2p$ dir. $kp = x_0^2 + y_0^2 < 2p$ ise $k = 1$ dir. Dolayısıyla $p = x_0^2 + y_0^2$ bulunur.

$(\Rightarrow:)$ $p=a^2+b^2$ olan a ve b tamsayıları mevcut olsun. p tek olduğundan a ve b nin ikisi aynı anda tek veya aynı anda çift olamaz. a tamsayısı tek, b tamsayısı çift olsun. Bu durumda,

$$a^2 \equiv 1 \pmod 4,\ b^2 \equiv 0 \pmod 4$$

biçimindedir. O zaman,

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

olur. Bu durumda,

$$p \equiv 1 \pmod 4$$

elde edilir.

Önerme 1.1.6 : m ve n iki sayının kareleri toplamı biçiminde ise mn de iki sayının kareleri toplamı biçimindedir.

İspat: a,b,c,d tamsayılar olmak üzere $m=a^2+b^2, n=c^2+d^2$ ise

$$mn=\left(a^2+b^2\right)\left(c^2+d^2\right)=\left(ac-bd\right)^2+\left(ad+bc\right)^2$$

olur. Yani mn de iki sayının kareleri toplamı biçimindedir.

Önerme 1.1.7: $p>2$ bir asal sayı ve $p \equiv 3 \pmod 4$ olsun. Eğer $p \mid a^2+b^2$ ise $p \mid a$ ve $p \mid b$ dir [5] .

Teorem 1.1.8: $n=a^2+b^2$ olacak biçimde a ve b tamsayıları vardır $\Leftrightarrow$ n nin asal çarpanlarına ayrılışındaki asal sayılardan $4k+3$ biçiminde olanların (eğer varsa) üssü çifttir.

İspat: $(\Rightarrow:)$ n nin üssü tek olan $4k+3$ biçiminde bir p asal çarpanı olsun. Yani $(p,m)=1$ olmak üzere $n=p^{2l+1}m$ olsun. Dolayısıyla $p \mid a^2+b^2$ dir. Yani $p \mid a$ ve $p \mid b$ dir. O zaman $a=p^r k, b=p^s t,\quad (k,p)=(t,p)=1$ olacak biçimde k ve t tamsayıları vardır. $r \le s$ olsun.

$$a^2+b^2=p^{2r}k^2+p^{2s}t^2=p^{2r}\left(k^2+p^{2s-2r}t^2\right)=p^{2r}\left(k^2+\left(p^{s-r}t\right)^2\right)$$

dir. Böylece $p^{2r} \mid n$ olur. Dolayısıyla $2r \le 2l+1$ dir. $2r$ çift ve $2l+1$ tek olduğundan $2r<2l+1$ bulunur. Şu halde,

$$\text{n}=p^{2l+1}\,m=p^{2r}\left(k^2+\left(p^{s-r}t\right)^2\right)$$

ise

$$p^{2l+1-2r}\,m=\,k^2+\left(p^{s-r}t\right)^2$$

elde edilir. Böylece, $2l+1-2r>0$ ise $p \mid k^2+\left(p^{r-s}t\right)^2$ dir. Dolayısıyla $p \mid k$ ve $p \mid p^{s-r}t$ olur. $p \mid k$ bir çelişkidir. Çünkü $(p,k)=1$ dir.

$(\Leftarrow:)$ $n=2^k q_1^{\beta_1}q_2^{\beta_2}...q_s^{\beta_s}p_1^{2\alpha_1}p_2^{2\alpha_2}...p_k^{2\alpha_k}$ ve $q_i \equiv 1 \pmod 4$, $1 \le i \le s$ ve $p_j \equiv 3 \pmod 4, 1 \le j \le k$ olsun . 2 ve $q_1,q_2,,,,,,q_s$ asal sayıları iki sayının kareleri toplamı biçiminde yazılabildiğinden, $2^k, q_1^{\beta_1}, q_2^{\beta_2},...,q_s^{\beta_s}$ lerde iki sayının kareleri toplamı biçiminde yazılabilir. Dolayısıyla, $2^k q_1^{\beta_1}q_2^{\beta_2}...q_s^{\beta_s}$ de iki sayının kareleri toplamı biçimin de yazılabilir.

$2^k q_1^{\beta_1}q_2^{\beta_2}...q_s^{\beta_s}=a_1^2+b_1^2$ olsun. Bu taktirde, $x=p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}$ olmak üzere

$$n=2^k q_1^{\beta_1}q_2^{\beta_2}...q_s^{\beta_s}\;p_1^{2\alpha_1}...p_k^{2\alpha_k}$$

$$=(a_1^2+b_1^2)\left(p_1^{\alpha_1}...p_k^{\alpha_k}\right)^2=(a_1^2+b_1^2)x^2$$

$$=a_1^2x^2+b_1^2x^2=\left(a_1x\right)^2+\left(b_1x\right)^2$$

bulunur. $a = a_1 x, b = b_1 x$ alınırsa,

$$n = a^2 + b^2$$

olur.

Önerme1.1.9: $p > 2$ bir asal sayı ise $kp = x^2 + y^2 + z^2 + w^2$ olacak biçimde $k < p$ tamsayısı vardır.

İspat: Önce $x^2 + y^2 + 1 \equiv 0 (\mathrm{mod}\, p)$ ve $0 \le x < p/2$ ve $0 \le y < p/2$ olacak biçimde x ve y tamsayılarının var olduğunu gösterelim.

$$S = \left\{0^2, 1^2, ..., \left(\frac{p-1}{2}\right)^2\right\} \text{ ve } T = \left\{-1-0^2, -1-1^2, ..., -1-\left(\frac{p-1}{2}\right)^2\right\}$$

olsun. S nin herhangi iki elemanı p modülüne göre birbirine konguru değildir. Çünkü $x^2 \equiv y^2 \pmod p$ ise $p \mid x^2 - y^2$, yani $p \mid x - y$ veya $p \mid x + y$ dir.

$0 \le x < p/2$ ve $0 \le y < p/2$ olduğundan bu mümkün değildir. Benzer biçimde T nin herhangi iki elemanı p modülüne göre birbirine konguru olamaz.

$S \cup T$ nin $p+1$ tane eleman içerdiğini görmek kolaydır. Dolayısıyla $S \cup T$ de farklı iki elemanın p ye bölümünden kalan aynıdır. Böylece Lemma 1.1.1 e göre x ve y tamsayıları $x^2 \equiv -1 - y^2 \pmod p$, $0 \le x < \frac{p-1}{2}$ ve $0 \le y < \frac{p-1}{2}$ olacak biçimde vardır. Böylece, $x^2 + y^2 + 1 \equiv 0 (\mathrm{mod}\, p)$ bulunur. Buradan $x^2 + y^2 + 1 + 0^2 = kp$ olacak biçimde bir k tamsayısının olduğu görülür.

$$x^2 + y^2 + 1 < 2\left(\frac{p-1}{2}\right)^2 + 1 < p^2$$

olduğundan, $k < p$ dir.

Önerme 1.1.10: m tek ise $-\left(\frac{m-1}{2}\right),-\left(\frac{m-1}{2}\right)+1,...,-1,0,1,...,\frac{m-1}{2}$ tamsayıları m modülüne göre bir tam kalanlar sistemidir.

İspat : Bu sayılar ardışık m tane tamsayı olduğundan bunların m modülüne göre bir tam kalanlar sistemi oluşturduğunu görmek kolaydır.

Teorem 1.1.11: Her p asal sayısı için $p=x^2+y^2+z^2+w^2$ olacak biçimde x,y,z,w tamsayıları vardır.

İspat: $2=1^2+1^2+0^2+0^2$ olduğundan 2 için teorem doğrudur. $p>2$ için inceleyelim. Yani p nin tek asal sayı olduğunu kabul edelim.

Önerme 1.1.9 a göre $x^2+y^2+z^2+w^2=kp$ olacak biçimde x,y,z,w ve k tamsayıları vardır.

$$S=\{k\in\mathbb{N}\mid k<p \text{ ve } kp=x^2+y^2+z^2+w^2,\ x,y,z,w\in\mathbb{Z}\}$$

olsun. S nin en küçük elemanı m olsun. Dolayısıyla $m<p$ ve $mp=x^2+y^2+z^2+w^2$ olacak biçimde x,y,z,w tam sayıları vardır. $m=1$ olduğunu gösterirsek ispat biter. Bunun için $m>1$ olduğunu kabul edelim. Şimdi m nin çift olduğunu varsayalım. Bu durumda, x,y,z,w tamsayılarının hepsi çifttir veya hepsi tektir ya da ikisi tek ikisi çifttir. Tüm bu durumda bu sayılar yeniden düzenlenerek, $x\equiv y(\mathrm{mod}\,2)$, $z\equiv w(\mathrm{mod}\,2)$ olduğu kabul edilebilir. Bu durumda, $\frac{x-y}{2},\frac{x+y}{2},\frac{z-w}{2},\frac{z+w}{2}$ tamsayılarıdır ve

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

$$= \frac{x^2 + y^2 + z^2 + w^2}{2}$$

$$= \frac{m}{2} p$$

olur. Bu durum m nin en küçük olması ile çelişir. Şimdi de m nin tek olduğunu kabul edelim. Önerme 1.1.10 u kullanırsak $a \equiv x \pmod{m}, b \equiv y \pmod{m}$, $c \equiv z \pmod{m}, d \equiv w \pmod{m}$ ve $\frac{-m}{2} < a,b,c,d < \frac{m}{2}$ olacak biçimde a,b,c,d tamsayılarının bulunduğunu görürüz. Buradan,

$$a^2 + b^2 + c^2 + d^2 \equiv x^2 + y^2 + z^2 + w^2 \pmod{m}$$

elde edilir. Böylece

$$a^2 + b^2 + c^2 + d^2 = km$$

olacak biçimde bir k tamsayısının var olduğu görülür ve

$$0 \le a^2 + b^2 + c^2 + d^2 < 4\left(\frac{m}{2}\right)^2$$

dir. Sonuç olarak $0 \le k < m$ bulunur. Eğer $k = 0$ ise $a = b = c = d = 0$ dır ve dolayısıyla $x \equiv y \equiv z \equiv w \equiv 0 \pmod{m}$ olur. Bu ise $x^2 + y^2 + z^2 + w^2 \equiv 0 \pmod{m^2}$ olduğunu gösterir.

Buradan $m^2 \mid mp$ olduğu görülür. Bu bir çelişkidir. Çünkü $1 < m < p$ dir. Dolayısıyla $k > 0$ olur. Ayrıca ,

$$\left(x^2 + y^2 + z^2 + w^2\right)\left(a^2 + b^2 + c^2 + d^2\right) = mp.km = m^2 kp$$

dir. Diğer yandan,

$$ax + by + cz + dw \equiv x^2 + y^2 + z^2 + w^2 \equiv 0 \pmod{m}$$

$$bx - ay - dz - cw \equiv yz - xy + wz - zw \equiv 0 \pmod{m}$$

$$cx-dy-az+bw \equiv zx-wy-xz+yw \equiv 0 \pmod{m}$$

$$dx+cy-bz-aw \equiv wx+zy-yz-xw \equiv 0 \pmod{m}$$

olur. Sonuç olarak,

$$X=(ax+by+cz+dw)/m,$$

$$Y=(bx-ay+dz-cw)/m,$$

$$Z=(cx-dy-az+bw)/m,$$

$$W=(dx+cy-bz-zw)/m$$

ise X,Y,Z,W lar birer tamsayıdır.

Böylece $X^2+Y^2+Z^2+W^2=m^2kp/m^2=kp$ elde edilir. $0<k<m$ olduğundan bu bir çelişkidir. Dolayısıyla kabulümüz yanlıştır. Yani $m=1$ dir. Bu ise, $p=x^2+y^2+z^2+w^2$ olacak biçimde x,y,z,w tamsayılarının olduğunu gösterir.

Önerme 1.1.12: Eğer m ve n pozitif tamsayılar ve m sayısı ile n sayısı dört sayının kareleri toplamı biçiminde ise mn de dört sayının kareleri toplamı biçimindedir. Daha genel olarak $m_1,m_2,...,m_n$ tam sayıları dört tam sayının kareleri toplamı biçiminde yazılabilirse $m_1m_2...m_n$ de dört tam sayının kareleri toplamı biçiminde yazılabilir.

İspat: $m=a^2+b^2+c^2+d^2$, $n=x^2+y^2+z^2+w^2$ ve a,b,c,d, x,y,z,t ler tamsayılar olsun. O zaman,

$$mn=(a^2+b^2+c^2+d^2).(x^2+y^2+z^2+t^2)$$

$$=(ax+by+cz+dt)^2+(ay-bx-ct-dz)^2+$$

$$(az-bt-cx-dy)^2+(at-bz-cy-dx)^2$$

olur. Burada,

$$ax+by+cz+dt=u,$$

$$ay-bx-ct-dz=v,$$

$$az-bt-cx-dy=k,$$

$$at-bz-cy-dx=l$$

alınırsa,

$$mn=u^2+v^2+k^2+l^2$$

olur.

Örnek 1.1.13: $7=2^2+1^2+1^2+1^2$ ve $10=3^2+1^2+0^2+0^2$ ise

$$70=7.10=\left(2^2+1^2+1^2+1^2\right)\left(3^2+1^2+0^2+0^2\right)$$

$$=(3.3+1.1+1.0+1.0)^2+(2.1-1.3-1.0-1.0)^2$$

$$+(2.0-1.0-1.3+1.1)^2+(2.0+1.0-1.1-1.3)^2$$

$$=7^2+1^2+2^2+4^2$$

olarak yazabileceğimizi görürüz.

Teorem 1.1.14: Her n pozitif tamsayısı için $n=a^2+b^2+c^2+d^2$ olacak biçimde a,b,c,d tamsayıları vardır. Yani her tamsayı dört tam karenin toplamı biçiminde yazılabilir.

İspat: $1=1^2+0^2+0^2+0^2$ olduğundan 1 in dört tam karenin toplamı biçiminde yazılabileceği açıktır. $n>1$ kabul edelim. n sayısı $n=p_1p_2...p_r$ olacak biçimde asal çarpanlarına ayrılsın. $1\le i\le r$ için her bir p_i dört tam kare toplamı olarak ifade edilebilir. Önerme 1.1.12 ye göre n tamsayısı dört tam sayının kareleri toplamı biçiminde yazılabilir.

Teorem 1.1.15: $4^n(8m+7)$ biçimindeki bir tamsayı üç sayının kareleri toplamı biçiminde yazılamaz.

İspat: $n=0$ için $4^0(8m+7)=8m+7$ olur. $8m+7$ üç sayının kareleri toplamı biçiminde yazılamaz. Çünkü, $a^2\equiv 0,1,4(\mathrm{mod}\,8)$ dir. Dolayısıyla, $a^2+b^2+c^2\equiv 0,1,2,3,4,5,6\,(\mathrm{mod}\,8)$ olur. Ancak, $8m+7\equiv 7(\mathrm{mod}\,8)$ olduğundan $8m+7\equiv a^2+b^2+c^2$ olması mümkün değildir. $4^n(8m+7)$ biçiminde olup üç sayının kareleri toplamı biçiminde yazılan sayılar olduğunu kabul edelim.

$S=\{n\in N|m$ tamsayısı, $4^n(8m+7)$ sayısı üç sayının kareleri toplamı olarak yazılacak biçimde vardır $\}$ olsun.

$S\neq\varnothing$ ve $S\subset\mathbb{N}$ dir. S nin en küçük elemanı k olsun. Bu durumda, $4^k(8m_1+7)=a^2+b^2+c^2$ olan m_1 vardır. Burada a,b,c tamsayılarından her biri çift olmalıdır. Çünkü, a tek, b tek, c tek olursa,

$$a^2\equiv 1\ (\mathrm{mod}\,4),\ b^2\equiv 1\ (\mathrm{mod}\,4),\ c^2\equiv 1\ (\mathrm{mod}\,4)$$

ise

$$a^2+b^2+c^2\equiv 3\,(\mathrm{mod}\,4)$$

bulunur ve çelişki elde edilir. a tek, b çift, c çift olsun.

$$a^2\equiv 1\ (\mathrm{mod}\,4),\ b^2\equiv 0\ (\mathrm{mod}\,4),\ c^2\equiv 0\ (\mathrm{mod}\,4)$$

ise

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

olur ve çelişki elde edilir. a tek, b tek, c çift olsun.

$$a^2 \equiv 1 \pmod 4,\ b^2 \equiv 1 \pmod 4,\ c^2 \equiv 0 \pmod 4$$

ise

$$a^2+b^2+c^2 \equiv 2 \pmod 4$$

olur ve çelişki elde edilir. Şu halde a,b,c lerin hepsi çift olmalıdır. $a=2a,b=2b,c=2c$ olarak alırsak,

$$4^{k-1}(8m+7)=a_1^2+b_1^2+c_1^2$$

elde ederiz. $(k-1)\in S$ olur. $k-1<k$ olduğundan k nın en küçük olması ile çelişir.

BÖLÜM 2. PİSAGOR ÜÇLÜLERİ

Tanım 2.1.1: $x^2+y^2=z^2$ denklemini sağlayan bir (x,y,z) pozitif tamsayı üçlüsüne bir pisagor üçlüsü denir. $x\neq 0, y\neq 0, z\neq 0$ olmak üzere eğer (x,y,z) tamsayı üçlüsü $x^2+y^2=z^2$ denklemini sağlıyorsa, o zaman bu denklemi $(|x|,|y|,|z|)$ tamsayı üçlüsü de sağlar.

Eğer $(x,y,z)=1$ ise, o zaman bu üçlüye primitif pisagor üçlüsü denir.

Primitif pisagor üçlülerinin en çok bilinen örnekleri; $(3,4,5)$ ve $(5,12,13)$ tür. Daha az bilinen örneği ise $(12,35,37)$ dir.

(x,y,z) herhangi bir pisagor üçlüsü olsun ve $d=(x,y,z)$ alalım. Bu durumda $x=dx_1, y=dy_1, z=dz_1$ ve $(x_1,y_1,z_1)=1$ olur. Ayrıca

$$x_1^2+y_1^2=\frac{x^2+y^2}{d^2}=\frac{z^2}{d^2}=z_1^2$$

elde edilir. Kısaca, her pisagor üçlüsü bir primitif pisagor üçlüsüne dönüştürülebilir.

Lemma 2.1.2: (x,y,z) bir primitif pisagor üçlüsü ise x ve y den biri tek diğeri çifttir.

İspat: x ve y nin her ikisinin de çift olduğunu kabul edelim. O zaman $2\mid x^2+y^2$ olur. Bu durumda $2\mid z^2$ dir. Buradan da, $2\mid z$ bulunur. Dolayısıyla, $(x,y,z)\geq 2$ sonucu elde edilir. Bu ise $(x,y,z)=1$ olduğundan çelişkidir. Şimdi de, x ve y nin

her ikisinin de tek olduğunu kabul edelim. Dolayısıyla $x^2 \equiv 1 (\mathrm{mod}\, 4)$ ve $y^2 \equiv 1 (\mathrm{mod}\, 4)$ olur. Bu ise

$$z^2 = x^2 + y^2 \equiv 1+1 \equiv 2 (\mathrm{mod}\, 4)$$

olduğunu gösterir. Bu olamaz. Çünkü herhangi bir a tamsayısı için $a^2 \equiv 1 (\mathrm{mod}\, 4)$ veya $a^2 \equiv 0 (\mathrm{mod}\, 4)$ tür. Bundan dolayı x ve y den biri tek diğeri çifttir.

Bir primitif pisagor üçlüsü olarak verilen (x, y, z) tamsayılarından biri çift ve diğer ikisi tektir.

(x, y, z) bir primitif pisagor üçlüsü olduğunda,

$$(x, y) = (y, z) = (x, z) = 1$$

olduğunu gösterelim. $(x, y) = d > 1$ olsun. O zaman $p \mid d$ olan bir p asal sayısı vardır. $d \mid x$ ve $d \mid y$ olduğundan, $p \mid x$ ve $p \mid y$ dir. Dolayısıyla, $p \mid x^2 + y^2$ olur. Buradan da $p \mid z^2$ olur. Yani $p \mid z$ bulunur. Bu ise (x, y, z) =1 olması ile çelişir. O halde d =1 dir. Aynı şekilde $(y, z) = (x, z) = 1$ olduğu kolayca görülür.

Bütün sayıları asal sayı olan hiçbir primitif pisagor üçlüsü yoktur.

Önerme 2.1.3: (x, y, z) bir pisagor üçlüsü olsun. O zaman, $(x, y, z) = (dx_1, dy_1, dz_1)$ olacak biçimde bir $d > 0$ tamsayısı ve primitif bir (x_1, y_1, z_1) pisagor üçlüsü vardır.

Önerme 2.1.4: (a, b) = 1, $a > 0$, $b > 0$ tamsayılar olmak üzere $ab = x^2$ ise $a = u^2$, $b = v^2$ olan u ve v tamsayıları vardır.

Genel olarak, $ab = x^n$ ise, $a = u^n$ ve $b = v^n$ olacak biçimde u ve v tamsayıları vardır.

İspat: $a>0$, $b>0$ olmak üzere $ab=x^2$ olsun. $(x,a)=u,(x,b)=v$ alalım.

$$uv=(x,a)(x,b)=(x,ab)=(x,x^2)=x$$

olduğundan $u^2v^2=x^2$ dir. Yani

$$u^2v^2=x^2=ab$$

olur. $(a,v)=(b,u)=1$ olduğundan,

$$(a,v^2)=(b,u^2)=1$$

dir. Bu durumda $ab=u^2v^2$ ve $(a,v^2)=1$ olduğundan $a\mid u^2$ dir. Aynı biçimde, $u^2\mid ab$ ve $(b,u^2)=1$ olduğundan $u^2\mid a$ dır. $a\mid u^2$ ve $u^2\mid a$ olduğundan $a=u^2$ elde edilir. $ab=u^2v^2$ ve $a=u^2$ ise $b=v^2$ dir.

Önerme 2.1.5 : $a>0,b>0,(a,b)=1$ ve $ab=2x^2$ olsun. Bu durumda $a=2u^2,b=v^2$ veya $a=u^2,b=2v^2$ olacak biçimde u ve v tamsayıları vardır [5] .

Teorem 2.1.6: $x>0,y>0,z>0$ olmak üzere (x,y,z) bir primitif pisagor üçlüsüdür $\Leftrightarrow s>t,(s,t)=1$ ve s ile t den biri tek diğeri çift olmak üzere, $x=2st,y=s^2-t^2,z=s^2+t^2$ olacak biçimde s,t tamsayıları vardır.

İspat:($\Rightarrow$:) $x^2+y^2=z^2$ ve (x,y,z)=1 ise, x ve y tamsayılarından biri tek diğeri çift ve z tektir. x in çift, y ve z nin tek olduğunu kabul edelim. $x^2+y^2=z^2$ ise $x^2=z^2-y^2$ yani $x^2=(z-y)(z+y)$ olarak yazabiliriz. Burada $(z-y)$ ve $(z+y)$ çifttir. O zaman $\frac{z-y}{2}$ ve $\frac{z+y}{2}$ birer tamsayıdır. $x^2=(z-y)(z+y)$

denklemini, $(\frac{x}{2})^2 = (\frac{z-y}{2})(\frac{z+y}{2})$ olarak yazalım. Şimdi de, $(\frac{z-y}{2}, \frac{z+y}{2})=1$ olduğunu gösterelim. $(\frac{z-y}{2}, \frac{z+y}{2}) = d > 1$ ise $p|d$ olacak biçimde bir p asalı vardır. $d|\frac{z-y}{2}$ ve $d|\frac{z+y}{2}$ olduğundan $p|\frac{z-y}{2}$ ve $p|\frac{z+y}{2}$ olur. $p|\frac{z-y}{2}$ ve $p|\frac{z+y}{2}$ olduğundan $p|\frac{z-y}{2}+\frac{z+y}{2}$ yani $p|z$ bulunur. Yine, $p|\frac{z-y}{2}$ ve $p|\frac{z+y}{2}$ olduğundan, $p|-\frac{z-y}{2}+\frac{z+y}{2}$ yani $p|y$ elde edilir. $p|y$ ve $p|z$ ise $p|z^2-y^2$ olur ve buradan da $p|x^2$ bulunur. Bu ise, $p|x$ demektir. $(x,y,z)=1$ olduğundan $p|x$, $p|y$, $p|z$ olması imkansızdır. Dolayısıyla, $(\frac{z-y}{2}, \frac{z+y}{2}) = 1$ dir. $\frac{z-y}{2}=u$, $\frac{z+y}{2}=v$ dersek, $(u,v)=1$ ve $(x/2)^2=uv$ olur. Önerme 2.1.4 e göre, $u=t^2$, $v=s^2$ olan t,s tamsayıları vardır. $(u,v)=1$ ise $(t^2,s^2)=1$ dir. Dolayısıyla, $(t,s)=1$ olur. $\frac{z-y}{2}=t^2$, $\frac{z+y}{2}=s^2$ ise,

$$z=t^2+s^2, y=s^2-t^2, x=2st$$

bulunur. $(x,y,z)=1$ olduğundan s ve t nin biri çift, diğeri tektir. Ayrıca, $v>u$ olduğundan, $s>t$ dir.

$(\Leftarrow:)\ x=2st, y=s^2-t^2, z=s^2+t^2, s>t, (s,t)=1$ ve s ile t den biri tek diğeri çift olsun. $x^2+y^2=z^2$ olduğunu gösterelim:

$$x^2+y^2=(2st)^2+(s^2-t^2)^2$$

$$=4s^2t^2+s^4-2s^2t^2+t^4$$

$$=s^4+2t^2+t^4=(s^2+t^2)=z^2$$

olur. Şimdi de $(x,y,z)=1$ olduğunu gösterelim. Bunun için $p|x$, $p|y$, ve $p|z$ olacak biçimde bir p asal sayısının olmadığını gösterelim. Aksini kabul edip çelişki elde edelim. $p|x$, $p|y$, ve $p|z$ olacak biçimde bir p asal sayısı

bulunsun. $p \mid x$ ise $p \mid 2st$ dir. $p = 2$ olsun. $p \mid$ y olduğundan 2|y yani $2 \mid s^2 - t^2$ olur. s ve t den biri tek diğeri çift olduğundan $s^2 - t^2$ tektir. Dolayısıyla $2 \mid s^2 - t^2$ bir çelişkidir. O zaman $p > 2$ olmalıdır. $p \mid 2st$ ve $p \nmid 2$ olduğundan $p \mid st$ dir. Bu durumda $p \mid s$ veya $p \mid t$ dir. $p \mid s$ olsun. O zaman $p \mid s^2$ olur. $p \mid s^2$ ve $p \mid y$ olduğundan $p \mid s^2 - t^2$ dir. Yani $p \mid s^2 - \left(s^2 - t^2\right)$ ise $p \mid t^2$ dolayısıyla $p \mid t$ olur. Bu ise $(s,t) = 1$ olmasına aykırıdır. Benzer biçimde $p \mid t$ ise $p \mid s$ bulunur. Yine çelişki elde edilir. Dolayısıyla $(x, y, z) = 1$ dir.

Sonuç 2.1.7: k bir pozitif tamsayı ve s ile t Teorem 2.1.6 daki şartları sağlıyorsa, pisagor üçlülerinin tümü; $x = k\left(s^2 - t^2\right), y = 2kst, z = k\left(s^2 + t^2\right)$ olarak verilir.

s ve t nin küçük değerlerinden oluşan bazı primitif pisagor üçlülerinin listesi aşağıdaki tabloda verilmiştir.

$t < s, (t,s) = 1$, s ve t den biri tek diğeri çift olacak biçimdeki $s = 2, 3, 4$ değerleri için liste yapılmıştır.

		x	y	z
s	t	$2st$	$s^2 - t^2$	$s^2 + t^2$
2	1	4	3	5
3	2	12	5	14
4	1	8	15	17
4	3	24	7	25

Örnek2.1.8: Hipotenüsü ve dik kenarlarından biri arasındaki fark, pozitif bir k tamsayısı olan ve kenarları primitif pisagor üçlülerinden oluşan dik üçgenlerin kenar uzunluklarını bulunuz.

Çözüm: k yı tek veya çift alarak iki durumda inceleyelim.

Durum 1: k tek olsun. Dik kenar uzunluklarından biri tek ve diğeri çift olduğundan x tek ve y çift kabul edilebilir. O halde y ve z (hipotenüs) k dan farklı olmalıdır. Teorem 2.1.6 ya göre $u^2+v^2=2uv+k$ yani $(u-v)^2=k$ dır. Dolayısıyla k bir tamkare olmalıdır. q bir pozitif tamsayı olmak üzere $k=q^2$ alalım. $u>v$ olduğundan $u=v+q$ dur. O zaman, $v,q>0$ ve v ile q dan biri tek, diğeri çift olmak üzere,

$$x=q(2v+q), y=2v(v+q)$$

ve

$$z=2v^2+2qv+q^2$$

olarak bulunur.

Eğer $q=1$ ise $k=1$ ve $x=2v+1, y=2v(v+1), z=2v^2+2v+1$ dir. Buradan da, $(3,4,5);(5,12,13);(7,24,25);(9,40,41)$, ... üçlüleri elde edilir.

Durum 2 : k çift olsun. z tek olduğundan z ve x ile y den tek olanı k dan farklı olmalıdır. Teorem 2.1.6 ya göre, $u^2+v^2=u^2-v^2+k$ ise $2v^2=k$ olur. Yani eğer bir çözüm varsa, q bir tamsayı olmak üzere $k=2q^2$ olmalıdır. $v=q$ ve u keyfî alındığında, $u>q$ ve u ile q dan biri tek, diğeri çift olmalıdır. Buradan da, $x=u^2-q^2, y=2uq$ ve $z=u^2+q^2$ elde edilir. Özellikle, $k=2$ için $x=u^2-1, y=2u, z=u^2+1$ olur.

Burada u çift ve $u>2$ dir. w pozitif bir tamsayı olmak üzere $u=2w$ alırsak,

$$x=4w^2-1, y=4w \text{ ve } z=4w^2+1$$

olur. Bu ise $(3,4,5),(15,8,17),(35,12,37),(63,16,65)$, ... üçlülerini verir.

Örnek 2.1.9: Aritmetik olarak artan tüm (x,y,z) pisagor üçlülerini bulunuz.

Çözüm: k ortak fark olmak üzere x ve k tamsayıları, $(x-k)^2+x^2=(x+k)^2$ olacak biçimde var olsun. $(x-k)^2+x^2=(x+k)^2$ ise,

$$x^2-2xk+k^2+x^2=x^2+2xk+k^2$$

olur ve $x^2=4xk$ bulunur. Dolayısıyla $x=0$ veya $x=4k$ dır. $x\neq 0$ olduğundan $x=4k$ olmalıdır.

Dolayısıyla,

$$x-k=4k-k=3k, x=4k, x+4k=5k$$

olduğundan bu üçlüler $(3k,4k,5k)$ biçiminde bulunurlar. Primitif üçlü ise sadece $(3,4,5)$ tir.

Örnek 2.1.10: Kenarlarından biri bir tamkare olan tüm primitif pisagor üçlülerini bulunuz.

Çözüm: 3 durumda inceleyelim:

1. Durum: Hipotenüs bir tamkare olsun. Yani $x^2+y^2=(z^2)^2=z^4$ olsun. Teorem 2.1.6 ya göre $u>v$ olmak üzere u ile v den biri tek, diğeri çift olmak üzere $z^2=u^2+v^2$, $x=u^2-v^2$, $y=2uv$ dir. u çift ve v tek olursa $u=2mn$, $v=m^2-n^2$ dir. Bu durumda $(m,n)=1$, $m>n$ m ve n den biri tek, diğeri çift olmak üzere, $x=u^2-v^2=(2mn)^2-(m^2-n^2)^2=4m^2n^2-m^4+2m^2n^2-n^4=$

$-\left(m^4-6m^2n^2+n^4\right)$ olur. Eğer u tek ve v çift olursa $u=m^2-n^2$, $v=2mn$ dir.

Böylece $x=u^2-v^2=\left(m^2-n^2\right)^2-\left(2mn\right)^2=m^4-6m^2n^2+n^4$ ve

$y=2uv=4mn\left(m^2-n^2\right)$ olur. O halde

Dolayısıyla her iki durumuda göz önüne alırsak ,

$$x=\left|m^4-6m^2n^2+n^4\right|,$$

$$y=2uv=2.2mn\left(m^2-n^2\right)=4mn\left(m^2-n^2\right),$$

$$z^2=u^2+v^2=\left(2mn\right)^2+\left(m^2-n^2\right)^2=4m^2n^2+m^4-2m^2n^2+n^4=\left(m^2+n^2\right)^2$$

olduğundan ,

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

elde edilir.

Bu ise, $(7,24,25);(119,120,169)$, ... üçlülerini verir.

2. Durum: Dik kenarlardan tek olanı bir tamkare olsun. Yani $\left(x^2\right)^2+y^2=x^4+y^2=z^2$ olsun. Teorem 2.1.6 ya göre, $u>v$ olmak üzere $x^2=u^2-v^2$ yani $x^2+v^2=u^2$ dir. x tek olduğundan, u tek ve v çift olmalıdır. O zaman $(m,n)=1, m>n>0$ ve m ve n den biri tek, diğeri çift olmak üzere,

$$x=m^2-n^2,\ v=2mn \text{ ve } u=m^2+n^2$$

olur. Yani,

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

$$y=2uv=2\left(m^2+n^2\right)2mn=4mn\left(m^2+n^2\right),$$

$$z=u^2+v^2=\left(m^2+n^2\right)^2+\left(2mn\right)^2=m^4+2m^2n^2+n^4+4m^2n^2=m^4+6m^2n^2+n^4$$

bulunur. Bu ise, $(9,40,41),(25,312,313)$ üçlülerini verir.

3. Durum: Dik kenarlardan çift olanı bir tamkare olsun. Teorem 2.1.6 ya göre $y^2 = 2uv$ dir. Şimdi $(u,v)=1$ ve u ile v den biri çift olsun. y çift olduğundan, w bir tamsayı olmak üzere $y=2w$ alabiliriz. Buradan da, $uv=2w^2$ olur. Önerme 2.1.5 ten, $(m,2n)=1$ veya $(n,2m)=1$ olmak üzere $u=m^2$ ve $v=2n^2$ veya $u=2m^2$ ve $v=n^2$ elde edilir. Dolayısıyla, $(m,2n)=1$ olduğunda,

$x=u^2-v^2=\left(2m^2\right)^2-\left(n^2\right)^2=4m^4-n^4$ veya $x=u^2-v^2=m^2-\left(2n^2\right)^2=m^4-4n^4$

olduğundan, m veya n olması durumu değiştirmediğinden dolayı,

$$x=\left|4m^4-n^4\right|,$$

$y^2=2uv=2\left(2m^2\right)n^2=4m^2n^2$ veya $y^2=2uv=2m^2\left(2n^2\right)=4m^2n^2$ olduğundan,

$$y=2mn,$$

$z=u^2+v^2=\left(2m^2\right)^2+\left(n^2\right)^2=n^4+4m^4$ veya $z=u^2+v^2=\left(2n^2\right)^2+\left(m^2\right)^2=4n^4+m^4$

olduğundan,

$$z=n^4+4m^4$$

bulunur. Bu ise $(3,4,5),(77,36,85)$, ... üçlülerini verir.

Teorem 2.1.11: (x,y,z) bir pisagor üçlüsü ise, $r=(xy)/(x+y+z)$ her zaman bir tamsayıdır.

İspat: Uygun olan k,s,t tamsayıları için,

$$x=2kst, y=k\left(s^2-t^2\right), z=k\left(s^2+t^2\right)$$

olduğunu biliyoruz. O halde,

$$r=\frac{xy}{x+y+z}=\frac{2k^2st(s^2-t^2)}{k(2st+s^2-t^2+s^2+t^2)}=\frac{kt(s^2-t^2)}{s+t}=kt(s-t)$$

dir. Yani r bir tamsayıdır.

Teorem 2.1.12: $x^4+y^4=z^2$ denklemini sağlayan $x>0,y>0,z>0$ tamsayıları yoktur.

İspat: $x^4+y^4=z^2$ denklemini sağlayan $x>0,y>0,z>0$ tamsayıları varsa, $(x,y,z)=d$ alınırsa $x=da,y=db,z=dc$ olarak yazılabilir. $d^4(a^4+b^4)=d^2c^2$ ise $d^2(a^4+b^4)=c^2$ dir. Buradan da $d^2\mid c^2$ yani $d\mid c$ olur. $a^4+b^4=(c/d)^2$, c/d bir tamsayıdır. $(a,b,c)=1$ ise $(a,b,c/d)=1$ dir. Şu halde genelliği bozmadan $x^4+y^4=z^2$ ve $(x,y,z)=1$ olan $x>0,y>0,z>0$ tamsayılarının olduğunu kabul edebiliriz.

$$S=\{z\mid x^4+y^4=z^2 \text{ ve } (x,y,z)=1 \text{ olan } x>0,y>0,z>0 \text{ vardır }\}$$

olsun. $S\neq\varnothing$ dir. $S\subset\mathbb{N}$ olduğundan S nin bir en küçük elemanı vardır. Bunu z ile gösterelim. Yani, $x^4+y^4=z^2$ ise $(x^2)^2+(y^2)^2=z^2$ ve (x^2,y^2,z) olup (x^2,y^2,z) bir primitif pisagor üçlüsüdür. Teorem 2.1.6 ya göre, $a>b,(a,b)=1$, a ile b den biri tek, diğeri çift olmak üzere,

$$x^2=a^2-b^2,y^2=2ab,z=a^2+b^2$$

dir. $x^2=a^2-b^2$ ise $x^2+b^2=a^2$ ve $(x,b,a)=1$ dir. Yani, (x,b,a) bir primitif pisagor üçlüsü olur. Dolayısıyla, a tek ve b çift olmalıdır. Buradan da, $c>d>0,(c,d)=1$, c ve d den biri tek, diğeri çift olmak üzere,

$$x=c^2-d^2,b=2cd,a=c^2+d^2$$

biçiminde yazılabilir. Buradan,

$$y^2=2ab=2(2cd)(c^2+d^2)=4cd(c^2+d^2)$$

yani

$$(y/2)^2 = cd(c^2+d^2)$$

elde edilir. Burada y^2 çift olduğundan y çift ve dolayısıyla $y/2$ bir tamsayıdır. Diğer yandan, $(c,d)=1$ olduğundan $(cd, c^2+d^2)=1$ dir. Dolayısıyla $cd=r^2, c^2+d^2=w^2$ olan $r>0$ ve $w>0$ tamsayıları vardır. $(c,d)=1$ olduğundan $c=u^2, d=v^2$ olan u ve v tamsayıları vardır. Böylece $(u^2)^2+(v^2)^2=w^2$ olur. Yani, $u^4+v^4=w^2$ dir. Dolayısıyla, $z=a^2+b^2$ olduğundan $a^2<z$ olur ve $w \le w^2=c^2+d^2=a \le a^2<z$ dir. Yani $w<z$ bulunur. Bu ise z nin tanımına aykırıdır.

Sonuç 2.1.13: $x^4+y^4=z^4$ olacak biçimde x ve y tamsayıları yoktur.

İspat: Eğer (x_0, y_0, z_0) üçlüsü $x^4+y^4=z^4$ ün bir pozitif çözümü ise (x_0, y_0, z_0^2) üçlüsü de $x^4+y^4=z^2$ denklemini sağlar ve bu Teorem 2.1.12 ile çelişir. Yani $x^4+y^4=z^4$ olacak biçimde x ve y tamsayıları yoktur.

Teorem 2.1.14: $x^4-y^4=z^2$ denklemini sağlayan $x>0, y>0, z>0$ tamsayıları yoktur.

İspat: $x^4-y^4=z^2$ nin x_0, y_0, z_0 gibi bir çözümünün olduğunu ve ayrıca x_0 ın en küçük olduğunu kabul edelim.

$(x_0, y_0)=d>1$ ise $x_0=dx_1, y_0=dy_1$ olacak biçimde x_1, y_1 tamsayıları vardır. $d^4(x_1^4-y_1^4)=z_0^2$ ise $d^2 \mid z_0$ dır. Yani $z_0=d^2 z_1$ olan bir $z_1>0$ vardır. Buradan $x_1^4-y_1^4=z_1^2$ bulunur. Bu durumda $0<x_1<x_0$ olan (x_1, y_1, z_1) bir çözüm oldu. Bu bir çelişkidir. O halde $(x_0, y_0)=1$ dir.

y_0 tek olsun. ${x_0}^4 - {y_0}^4 = {z_0}^2$ ise ${z_0}^2 + \left({y_0}^2\right)^2 = \left({x_0}^2\right)^2$ olarak yazarsak, $\left(z_0, {y_0}^2, {x_0}^2\right)$ bir primitif pisagor üçlüsü olur. Teorem 2.1.6 ya göre $s > t > 0, (s,t) = 1$ olmak üzere $z_0 = 2st, {y_0}^2 = s^2 - t^2, {x_0}^2 = s^2 + t^2$ olur. Böylece,

$$s^4 - t^4 = \left(s^2 + t^2\right)\left(s^2 - t^2\right) = {x_0}^2 {y_0}^2$$

olur. O zaman s, t, x_0, y_0 tamsayıları $x^4 - y^4 = z^2$ nin pozitif çözümüdür. $0 < s < \sqrt{s^2 + t^2} = x_0$ olduğundan çelişki elde edilir. y_0 çift olsun. O zaman, s çift ve t tek olmak üzere

$$ {y_0}^2 = 2st, z_0 = s^2 - t^2, {x_0}^2 = s^2 + t^2$$

olacak biçimde $s > 0, t > 0$ tamsayıları vardır.

${y_0}^2 = 2st$ ve genelliği bozmadan s yi çift, t yi tek kabul edebiliriz. Bu durumda $(2s,t) = 1$ olur. Önerme 2.1.5 ten $2s$ ve t nin ikisi de pozitif tamsayıların karesi olmalıdır. w, v tamsayılar olmak üzere $2s = w^2, t = v^2$ olsun. Dolayısıyla w çifttir. $w = 2u$ alırsak, $s = 2u^2$ elde edilir. ${x_0}^2 = s^2 + t^2 = 4u^4 + v^4$ tür ve $\left(2u^2, v^2, x_0\right)$ bir primitif pisagor üçlüsüdür. Teorem 2.1.6 dan $a > b > 0$ ve $(a,b) = 1$ olmak üzere

$$2u^2 = 2ab, v^2 = a^2 - b^2, x_0 = a^2 + b^2$$

olur.

$u^2 = ab$ olduğu için a ve b birer tam karedir. c ve d tamsayılar olmak üzere $a = c^2, b = d^2$ alalım. $v^2 = a^2 - b^2 = c^4 - d^4$ yazarsak, $x^4 - y^4 = z^2$ nin yeni çözümleri elde edilir.

$$0 < c \le \sqrt{a} < a^2 + b^2 = x_0$$

olduğundan bu bir çelişkidir. Yani, $x^4 - y^4 = z^2$ denkleminin tamsayılarda çözümü yoktur.

Teorem 2.1.15: $x>0, y>0, z>0$ ve (x,y,z) bir pisagor üçlüsü ise $(1/2)xy$ hiçbir zaman bir tamkareye eşit olamaz.

İspat: $x>0, y>0, z>0$, (x,y,z) bir pisagor üçlüsü ise $(1/2)xy$ bir tamkare olsun. Yani u bir tamsayı olmak üzere $(1/2)xy=u^2$ olsun. O zaman $2xy=4u^2$ dir.

$x^2+y^2=z^2$ ye $2xy=4u^2$ eklenirse $(x+y)^2=z^2+4u^2$ elde edilir. Yine $x^2+y^2=z^2$ den $2xy=4u^2$ çıkarılırsa $(x-y)^2=z^2-4u^2$ elde edilir. Elde edilen bu iki denklemi çarptığımızda

$$(x+y)^2(x-y)^2=(z^2+4u^2)(z^2-4u^2)$$

yani

$$(x^2-y^2)^2=z^4-16u^4=z^4-(2u)^4$$

bulunur. Bu ise Teorem 2.1.13 ile çelişir. Yani $(1/2)xy$ bir tamkareye eşit olamaz.

Örnek 2.1.16: x,y,z sıfırdan farklı tamsayılar ve $x^4+y^4=2z^2$ olsun. O zaman $x^2=y^2$ ve $z^2=x^4$ tür.

Çözüm: Verilen denklemin her iki tarafının karesini alırsak,

$$4z^4=(x^4+y^4)^2=(x^4-y^4)^2+4x^4y^4$$

olur ve buradan da ,

$$z^4-x^4y^4=\left(\frac{x^4-y^4}{2}\right)^2$$

elde edilir. Bu durumda $x^4+y^4=2z^2$ olduğundan x ve y nin ikisi de tek veya ikisi de çifttir. Dolayısıyla x^4-y^4 ifadesi de çift olur. O halde $\frac{x^4-y^4}{2}$ bir

tamsayıdır. Teorem 2.1.16 ya göre $x^4 = y^4$ olmalıdır. Böylece $x^2 = y^2$ olur. Yani, $z^2 = x^4$ tür.

Örnek 2.1.17: x, y, z sıfırdan farklı tamsayılar ve $2x^4 + 2y^4 = z^2$ ise $x^2 = y^2$, $z^2 = 4x^4$ tür.

Çözüm: $2x^4 + 2y^4 = z^2$ denkleminin her iki tarafını 8 ile çarparsak,

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

bulunur. Örnek 2.1.17 ye göre, $(2x)^2 = (2y)^2$ ve $(2z)^2 = (2x)^4$ tür. Yani $x^2 = y^2$ ve $z^2 = 4x^4$ elde edilir.

Teorem 2.1.18: $(x, y, z) = 1$ olduğunda $x^2 + 2y^2 = z^2$ nin pozitif tamsayılardaki çözümleri, $u, v > 0$ ve $(u, 2v) = 1$ olmak üzere, $x = |u^2 - 2v^2|$, $y = 2uv$ ve $z = u^2 + 2v^2$ dir.

İspat: $(x, y, z) = 1$ ise x tek, dolayısıyla z tek olmalıdır. Dolayısıyla $x^2 \equiv 1 \pmod 4$, $z^2 \equiv 1 \pmod 4$ ve $2y^2 \equiv 0 \pmod 4$ bulunur. Yani y çifttir. w bir tamsayı olmak üzere $y = 2w$ olsun. O zaman, $x^2 + 8w^2 = z^2$ yani $8w^2 = z^2 - x^2$ olur. z tek ve x tek olduğundan $z+x$ ve $z-x$ ler çifttir. Dolayısıyla, $\frac{z+x}{2}$ ve $\frac{z-x}{2}$ ler tamsayılardır. $8w^2 = z^2 - x^2$ ve böylece $2w^2 = \left(\frac{z-x}{2}\right)\left(\frac{z+x}{2}\right)$ olur. Ayrıca, burada $\left(\frac{z+x}{2}, \frac{z-x}{2}\right) = 1$ dir. Aksini kabul

edelim. $\left(\frac{z+x}{2},\frac{z-x}{2}\right)=d>1$ olsun. Bu durumda $p\mid d$ olacak şekilde bir p asal sayısı vardır. $d\mid\frac{z+x}{2}$ ve $d\mid\frac{z-x}{2}$ olduğundan $p\mid\frac{z+x}{2}$ ve $p\mid\frac{z-x}{2}$ dir.

Buradan da $p\mid\frac{z+x}{2}+\frac{z-x}{2}$, yani $p\mid z$ ve $p\mid\frac{z+x}{2}-\frac{z-x}{2}$ den $p\mid x$ bulunur. $p\mid z$ ve $p\mid x$ olduğu için $p\mid z^2-x^2$ yani $p\mid 2y^2$ dir. z ve x tek olduğundan p de tektir.

p tek ve $p\mid 2y^2$ ise $p\mid y^2$ ve dolayısıyla $p\mid y$ dir. Bu ise $(x,y,z)=1$ olması ile çelişir. Yani $\left(\frac{z+x}{2},\frac{z-x}{2}\right)=1$ dir. Önerme 2.1.5 e göre u,v birer tamsayı olmak üzere $\frac{z+x}{2}=u^2$ ve $\frac{z-x}{2}=2v^2$ veya $\frac{z+x}{2}=2u^2$ ve $\frac{z-x}{2}=v^2$ olmalıdır. Burada $(u,2v)=1$ veya $(2u,v)=1$ dir. Bu durumda, $\frac{z-x}{2}=2v^2$, $\frac{z+x}{2}=u^2$ alırsak, $\frac{z+x}{2}-\frac{z-x}{2}=u^2-2v^2$ yani $x=u^2-2v^2$ ve $\frac{z+x}{2}+\frac{z-x}{2}=u^2+2v^2$ yani $z=u^2+2v^2$ olur. Ayrıca $2y^2=z^2-x^2$ olduğundan $2y^2=\left(u^2+2v^2\right)^2-\left(u^2-2v^2\right)^2=\left(u^2+2v^2+u^2-2v^2\right).\left(u^2+2v^2-u^2+2v^2\right)$ yani $2y^2=2u^2.4v^2$ elde edilir. Bu durumda $y=2uv$ bulunur. $\frac{z+x}{2}=2u^2,\frac{z-x}{2}=v^2$ alırsak, $\frac{z+x}{2}-\frac{z-x}{2}=2u^2-v^2$ yani $x=2u^2-v^2$, $\frac{z+x}{2}+\frac{z-x}{2}=2u^2+v^2$ yani $z=2u^2+v^2$ bulunur. Ayrıca, $2y^2=z^2-x^2$ olduğundan, $2y^2=\left(2u^2+v^2\right)^2-\left(2u^2-v^2\right)=\left(2u^2+v^2-2u^2+v^2\right)\left(2u^2+v^2+2u^2-v^2\right)=2v^2 4u^2v^2$ yani $y^2=4u^2v^2$ elde edilir. Bu durumda $y=2uv$ bulunur. Yani $u,v>0,(u,2v)=1$ için $x^2+2y^2=z^2$ denkleminin çözümleri,

$$x=\left|u^2-2v^2\right|,\ y=2uv \text{ ve } z=u^2+2v^2$$

biçimindedir.

Teorem 2.1.19: $x^2+y^2=2z^2$ nin aralarında asal pozitif tamsayılardaki çözümü;

$(u,v)=1$ ve u ile v den biri tek diğeri çift tamsayılar olmak üzere,

$$x=u^2-v^2+2uv,\ y=\left|u^2-v^2-2uv\right|,\ z=u^2+v^2$$

biçimindedir.

İspat: x,y,z aralarında asal olduğundan modül 4'e göre kongruansları göz önüne aldığımızda z nin çift olamayacağını görürüz. x çift, y çift ise $x^2\equiv 0(\mathrm{mod}\,4)$, $y^2\equiv 0(\mathrm{mod}\,4)$ olur. Buradan da $x^2+y^2\equiv 0(\mathrm{mod}\,4)$ olduğundan $2z^2\equiv 0(\mathrm{mod}\,4)$ bulunur. Yani $z^2\equiv 0(\mathrm{mod}\,4)$ ve z çift olur. Bu ise $(x,y,z)=1$ olması ile çelişir. x çift, y tek (y çift, x tek) ise $x^2\equiv 0(\mathrm{mod}\,4)$, $y^2\equiv 1(\mathrm{mod}\,4)$ tür. $x^2+y^2\equiv 0+1\equiv 1(\mathrm{mod}\,4)$ olur. $2z^2\equiv 1(\mathrm{mod}\,4)$ olamıyacağı için çelişki elde edilir.

x tek ve y tek ise $x^2\equiv 1(\mathrm{mod}\,4)$, $y^2\equiv 1(\mathrm{mod}\,4)$ tür. O zaman $x^2+y^2\equiv 2(\mathrm{mod}\,4)$ yani $2z^2\equiv 2(\mathrm{mod}\,4)$ olur. Dolayısıyla, z tektir. O halde x tek, y tek ve z tektir. O zaman $x+y$ ve $x-y$ çift olur. Dolayısıyla $\frac{x+y}{2}$ ve $\frac{x-y}{2}$ ler tamsayılardır. $x^2+y^2=2z^2$ ise $\left(\frac{x+y}{2}\right)^2+\left(\frac{x-y}{2}\right)^2=2z^2$ olur. Eğer $x=y$ ise o zaman $x=y=z=1$ bir primitif çözümdür. Teorem 2.1.6 ya göre $u>v$, $(u,v)=1$ ve u ile v den biri tek diğeri çift olmak üzere

$$\frac{x+y}{2}=u^2-v^2\ ,\ \frac{x-y}{2}=2uv \text{ ve } z=u^2+v^2$$

veya

$$\frac{x+y}{2}=2uv\ ,\ \frac{x-y}{2}=u^2-v^2 \text{ ve } z=u^2+v^2$$

dir.

$$\frac{x+y}{2}=u^2-v^2\ ,\quad \frac{x-y}{2}=2uv\ ,\quad z=u^2+v^2$$

olsun.

$$\frac{x+y}{2}+\frac{x-y}{2}=u^2-v^2+2uv$$

yani

$$x=u^2-v^2+2uv$$

bulunur.

$$\frac{x+y}{2}-\frac{x-y}{2}=u^2-v^2-2uv$$

yani

$$y=u^2-v^2-2uv$$

olur.

$$\frac{x+y}{2}=2uv\,,\quad \frac{x-y}{2}=u^2-v^2\,,\quad z=u^2+v^2$$

olsun.

$$\frac{x+y}{2}+\frac{x-y}{2}=2uv+u^2-v^2$$

yani

$$x=u^2-v^2+2uv$$

bulunur.

$$\frac{x+y}{2}-\frac{x-y}{2}=2uv-u^2+v^2$$

yani $y=-u^2+v^2+2uv$ olur. Her iki durumu da gözönüne alırsak,

$$x=u^2-v^2+2uv\,,\quad y=\left|u^2-v^2-2uv\right|\,,\quad z=u^2+v^2$$

olarak bulunur.

Teorem 2.1.20: $x^4-4y^4=\pm z^2$ denkleminin sıfırdan farklı tamsayılarda çözümü yoktur.

İspat: $x^4-4y^4=z^2$ denklemini göz önüne almak yeterlidir. Çünkü, eğer x,y,z sıfırdan farklı tamsayıları $x^4-4y^4=-z^2$ olacak biçimde varsa, o zaman $4x^4-(2y)^4=-(2z)^2$ olur. Böylece $(2y)^4-4x^4=(2z)^2$ olur ve $(2y,x,2z)$ üçlüsü $x^4-4y^4=z^2$ denkleminin bir çözümüdür. Şimdi, eğer x,y,z pozitif tamsayıları $x^4-4y^4=z^2$ mevcut olsun. $d=(x,y,z)$ olarak alınırsa $\left(\frac{x}{d}\right)^2-4\left(\frac{y}{d}\right)^2=\left(\frac{z}{d^2}\right)^2$ ve $\left(\frac{x}{d},\frac{y}{d},\frac{z}{d^2}\right)=1$ olduğunu görmek kolaydır. Şu halde genelliği bozmadan $(x,y,z)=1$ kabul edebiliriz. Eğer $x^4-4y^4=z^2$ ise $4y^4+z^2=x^4$, yani $(2y)^2+z^2=(x^2)^2$ olur. Şimdi $(2y,z,x^2)^2=1$ olduğunu gösterelim. Bunun için $p\mid 2y, p\mid z, p\mid x^2$ olan bir p asal sayısının mevcut olduğunu kabul edelim. Eğer $p>2$ ise $p\mid y, p\mid z, p\mid x$ olur. Bu ise $(x,y,z)=1$ olmasını aykırıdır. $p=2$ ise $2\mid z, 2\mid x^2$ olur. Dolayısıyla z ve x çifttir. $z=2a, x=2b$ olsun. Böylece $x^4-4y^4=z^2$ olduğu kullanılırsa $16b^4-4y^4=4a^2$ elde edilir. Bu ise $4b^4-y^4=a^2$ olduğunu gösterir. Bu durumda y çift olmalıdır. Eğer y tekse $y^4\equiv 1(\mathrm{mod}\,4)$ olduğundan $a^2\equiv -y^4(\mathrm{mod}\,4)$, $a^2\equiv -1(\mathrm{mod}\,4)$, yani $a^2\equiv 3(\mathrm{mod}\,4)$ olur. Bu olamaz. y çift ise bu durum $(x,y,z)=1$ olmasına aykırıdır. Şu halde $(2y^2,z,x^2)=1$ olur. Böylece $x^2=a^2+b$, $2y^2=2ab$, $z=a^2-b^2$ olacak biçimde aralarında asal a ve b tamsayıları vardır. $y^2=ab$ olduğundan $a=c^2, b=d^2$ olur. Böylece $x^2=c^4+d^4$ elde edilir. Bu ise Sonuç 2.1.13 e göre olamaz.

Teorem 2.1.21: $4x^4-1=3y^4$ denkleminin tamsayılarda sadece $(\pm1,\pm1)$ çözümleri vardır.

İspat : Eğer x,y tamsayıları $(2x^2+1,2x^2-1)=1$ olmak üzere $3y^4=4x^4-1=(2x^2+1)(2x^2-1)$ olacak biçimde varsa, $2x^2-1\not\equiv 0(\mathrm{mod}3)$ olduğundan

$$2x^2+1=3a^4,\ 2x^2-1=b^4$$

olan a,b tamsayıları vardır. $2x^2-1=b^4$ denklemi $2x^2=b^4+1$ olarak yazılırsa Örnek 2.1.16 ya göre $b^2=1$ ve $x^2=b^4$ elde edilir. $b^2=1$ ise $b=\pm1$ dir. Böylece $x=\pm1$ olur.Buradan da $4x^4-1=3y^4$ olduğundan $y=\pm1$ bulunur. Yani, $4x^4-1=3y^4$ denkleminin çözümleri sadece $(\pm 1,\pm 1)$ dir.

Önerme 2.1.22: a,b,r,x pozitif tam sayılar ve $(a,b)=1$, $ab=rx^n$ olsun. Bu durunda $a=se^n, b=tf^n$ ve $st=r$ olacak biçimde s,t,e,f tamsayıları vardır

İspat: $s=(a,r), t=(b,r)$ olsun. $st=(a,r)(b,r)=(ab,r)=r$ olur. Ayrıca $a=su, b=tv$ ise

$$ab=stuv=ruv=rx^n$$

bulunur. $uv=x^n$ olup $(u,v)=1$ olduğundan $u=e^n, v=f^n$ olan e ve f vardır. Böylece

$$a=su=se^n, b=tv=tf^n$$

elde edilir.

Teorem 2.1.23: En az iki kenarı tam kare olan bir primitif pisagor üçlüsü yoktur.

İspat: $x^4+y^4=z^2$ ve $x^2+y^4=z^4$ olmak üzere iki durumu göz önüne alalım. Teorem 2.1.12 ye göre $x^4+y^4=z^2$ yi sağlayan $x>0, y>0, z>0$ tamsayıları yoktur. Yine Teorem 2.1.14 e göre $z^4-y^4=x^2$ yi sağlayan $x>0, y>0, z>0$ tamsayıları yoktur.

Sonuç 2.1.24: Bir pisagor üçlüsünde dik kenarlardan biri ve hipotenüs, bir başka pisagor üçlüsünde x ve y olacak biçimde pisagor üçlüleri yoktur.

İspat: Aksini kabul edelim. $x^2+y^2=z^2$ ve $x^2+z^2=u^2$ denklemlerinin çözümleri mevcut olsun. O zaman $x^2-z^2=-y^2$ ve $x^2+z^2=u^2$ olduğundan

$$\left(x^2-z^2\right)\left(x^2+z^2\right)=x^4-z^4=-y^2u^2$$

yani $x^4+(uy)^2=z^4$ dür. Bu ise Teorem 2.1.23 ile çelişir.

Teorem 2.1.25: $x>u$ olmak üzere $x^2+y^2=u^2+v^2$ denkleminin tamsayılardaki çözümü, $x=(ms+nr)/2, u=(ms-nr)/2, v=(ns+mr)/2, y=(ns-mr)/2$ olarak verilir. Burada m ve n nin ikisi de tek ise r ve s ya aynı anda tektir ya da aynı anda çifttir.

İspat: $s=(x+u, y+v)$ olsun. O zaman $(m,n)=1$ olmak üzere, $x+u=ms$ ve $y+v=ns$ olarak yazabiliriz. Eğer $x^2+y^2=u^2+v^2$ denklemini $x^2-u^2=v^2-y^2$ olarak yazarsak, $(x-u)m=(v-y)n$ olduğunu görürüz. Bundan da $(m,n)=1$

olduğundan $n \mid x-u$ ve $m \mid v-y$ olur. O halde $\frac{x-u}{n}, \frac{v-y}{m}$ birer tam sayıdır.

$(x-u)m=(v-y)n$ eşitliği $\frac{x-u}{n}=\frac{v-y}{m}$ olarak yazılırsa, $x-u=nr$ ve $v-y=mr$ olacak biçimde bir r tamsayısının varlığı görülür. Bu durumda,

$$x+u=ms, y+v=ns,\ x-u=nr, v-y=mr$$

olduğundan

$$x=(ms+nr)/2, u=(ms-nr)/2,$$

$$v=(ns+mr)/2, y=(ns-mr)/2$$

elde edilir. Eğer m ve n nin ikisi de tek ise o zaman $2 \mid mr+ns$ olduğundan $r+s \equiv 0 (\mathrm{mod}\, 2)$ dir. Yani, r ve s ya aynı anda tektir yada aynı anda çifttir.

BÖLÜM 3. KÜP DENKLEMLERİ

Önerme 3.1.1: $S=\{a^2+3b^2 \mid a,b\in\mathbb{Z}\}$, k sıfırdan farklı bir tamsayı ve p bir asal sayı olmak üzere, $p=c^2+3d^2\in S$, $pk=a^2+3b^2\in S$ ise o zaman $p\mid ac+3bd, p\mid ad-bc$ ve $k=\left(\frac{ac+3bd}{p}\right)^2+3\left(\frac{ad-bc}{p}\right)^2$, veya $p\mid ac-3bd, p\mid ad+bc$ ve $k=\left(\frac{ac-3bd}{p}\right)^2+3\left(\frac{ad+bc}{p}\right)^2$ yani $k\in S$ dir.

İspat: $k=a^2+3b^2$ yi $k=\frac{(a^2+3b^2)\left(c^2+3d^2\right)}{\left(c^2+3d^2\right)^2}$ olarak yazabiliriz.

Buradan ,

$$k=\frac{(a+\sqrt{3}bi)(a-\sqrt{3}bi)(c+\sqrt{3}di)(c-\sqrt{3}di)}{\left(c^2+3d^2\right)^2}$$

$$=\frac{\left[(a+\sqrt{3}bi)(c-\sqrt{3}di)\right]\left[(a-\sqrt{3}bi)(c+\sqrt{3}di)\right]}{\left(c^2+3d^2\right)^2}$$

$$=\frac{\left[(ac+3bd)-\sqrt{3}(ad-bc)i\right]\left[(ac+3bd)+\sqrt{3}(ad-bc)i\right]}{\left(c^2+3d^2\right)^2}$$

$$=\frac{\left[(ac+3bd)^2+3(ad-bc)^2\right]}{\left(c^2+3d^2\right)^2}$$

veya

$$k=\frac{\left[(a+\sqrt{3}bi)(c+\sqrt{3}di)\right]\left[(a-\sqrt{3}bi)(c-\sqrt{3}di)\right]}{\left(c^2+3d^2\right)^2}$$

olduğu kullanılırsa

$$k=\frac{\left[(ac-3bd)^2+3(ad+bc)^2\right]}{\left(c^2+3d^2\right)^2}$$

elde edilir. Fakat,

$$\begin{aligned}&(ac+3bd)(ac-3bd)\\&=a^2c^2-9b^2d^2\\&=a^2(c^2+3d^2)-3(a^2+3b^2)d^2\\&=(a^2-3d^2)(c^2+3d^2)\end{aligned}$$

olur. $c^2+3d^2=p$ bir asal olduğundan $p\mid ac+3bd$ veya $p\mid ac-3bd$ dir. Bu durumda $p\mid ac+3bd$ alınırsa $\frac{ac+3bd}{p}$ bir tamsayı olur. Ayrıca, k bir tamsayı olduğundan $3\left(\frac{(ad-bc)}{p}\right)^2$ de bir tamsayıdır. Dolayısıyla, $\frac{(ad-bc)}{p}$ bir tamsayı olur. Bu durumda,

$$u=\frac{ac+3bd}{p},$$

$$v=\frac{ad-bc}{p}$$

olmak üzere, $k=u^2+3v^2$ biçiminde bulunur. Yani $k\in S$ dir. Benzer biçimde, eğer $p\mid ac-3bd$ ise $k=\frac{\left[(ac-3bd)^2+3(ad+bc)^2\right]}{\left(c^2+3d^2\right)^2}$ olduğu kullanılarak istenen elde edilir.

Önerme 3.1.2: p bir asal sayı olsun. $p=x^2+3y^2$ olacak biçimde x ve y tamsayıları vardır $\Leftrightarrow p=3$ veya $p\equiv 1\pmod 3$ tür.

İspat: $p\equiv 1\pmod 3$ ise $(-3/p)=(-1/p)(3/p)$ olduğunu kullanalım.

Bu durumda,

$$(-3/p)=(-1/p)\,(-1)^{\frac{3-1}{2}\cdot\frac{p-1}{2}}\,(p/3)$$

$$=(-1/p)\,(-1)^{(p-1)/2}\,(p/3)$$

$$=(-1)^{(p-1)/2}\,(-1)^{(p-1)/2}=1$$

elde edilir. Dolayısıyla $x^2\equiv -3\pmod p$ kongrüansının bir çözümü vardır. Bu ise $p\nmid a$ olmak üzere $a^2+3\equiv 0\pmod p$ olacak biçimde bir a tamsayısının mevcut olduğunu gösterir. O halde Lemma 1.1.3 e göre $0<|x|<\sqrt{p}$ ve $0<|y|<\sqrt{p}$ olmak üzere $ay\equiv x\pmod p$ olacak biçimde x ve y tamsayıları vardır. Buradan $a^2y^2\equiv x^2\pmod p$ yazılabilir. $a^2+3\equiv 0\pmod p$ olduğundan $x^2+3y^2\equiv 0\pmod p$ elde edilir.

$0<x^2<p$ ve $0<y^2<p$ olduğundan $0<x^2+3y^2<p+3p=4p$ bulunur. $p\mid x^2+3y^2$ olduğundan $x^2+3y^2=pk$ olacak biçimde k doğal sayısı vardır ve k doğal sayısı 1, 2, 3 değerlerini alabilir. $k=1$ ise $x^2+3y^2=p$ olur. $k=2$ ise x ve y tamsayılarının ikisi de çifttir veya ikisi de tektir. Her iki durumda da $4\mid 2p$ elde edilir. Bu ise mümkün değildir. $k=3$ ise $x^2+3y^2=3p$ olacağından $3\mid x$ olur. $x=3z$ olsun. Bu durumda $3p=x^2+3y^2=9z^2+3y^2=3(y^2+3z^2)$, yani $p=y^2+3z^2$ elde edilir.

$(\Leftarrow:)$ $p=3$ ise $p=0^2+3.1^2$ dir. $p>3$ ve $p\equiv 1\pmod 3$ olsun. $p=x^2+3y^2$ ise $3\nmid x$ dir. Bu durumda $3\mid x^2-1$ yani $x^2\equiv 1\pmod 3$ tür. Ayrıca $p\equiv x^2\pmod 3$ olduğundan $p\equiv 1\pmod 3$ bulunur.

Lemma 3.1.3: $u,v\neq 0$, $(u,v)=1$ olmak üzere $m=u^2+3v^2$ olsun. Eğer p bir tek asal sayı ve $p\mid m$ ise $a,b\neq 0,(a,b)=1$ olmak üzere $p=a^2+3b^2$ biçimindedir.

İspat: $p=3$ ise $3=0^2+3.1^2$ olduğundan $3=c^2+3d^2$ biçimindedir. $p\neq 3$ olsun. $p\mid m$ olduğundan $p\nmid v$ dir. $p\mid v$ ise $p\mid u^2+3v^2$ olduğundan $p\mid u^2+3v^2-3v^2$ yani $p\mid u^2$ olup $p\mid u$ bulunur ve bu hipotezle yani $(u,v)=1$ olması ile çelişir. $vv_1\equiv 1\pmod p$ olacak biçimde bir v_1 alalım. Böylece $p\mid u^2+3v^2$ ise $u^2\equiv -3v^2\pmod p$ olup $u^2v_1^2\equiv -3v^2v_1^2\pmod p$ yani $(uv_1)^2=-3(vv_1)^2\pmod p$ bulunur. Bu ise $(uv_1)^2=-3\pmod p$ olduğunu gösterir. O halde $(uv_1)^2=-3\pmod p$ olduğundan $\left(\frac{-3}{p}\right)=1$ yani $p=1\pmod 3$ olur. Önerme 3.1.2 ye göre $p=a^2+3b^2$ olacak biçimde a,b tamsayıları vardır.

Önerme 3.1.4: p bir asal sayı olsun. $a\geq 0,b\geq 0$, $c\geq 0,d\geq 0$ olmak üzere

$$p=a^2+3b^2=c^2+3d^2$$

ise $a=c$ ve $b=d$ dir.

İspat: $k=1$ için Önerme 3.1.1 i uygulayalım.

$a\geq 0,b\geq 0,c\geq 0,d\geq 0$ için $p=a^2+3b^2=c^2+3d^2$ olsun. O zaman,

$$1=\left(\frac{ac+3bd}{p}\right)^2+3\left(\frac{ad-bc}{p}\right)^2$$

olur.

Böylece $p=ac+3bd$ ve $ad=bc$ olur. Dolayısıyla,

$$pd=acd+3bd^2=\ bc^2+3bd^2=b(c^2+3d^2)=bp$$

bulunur. Yani $b=d$ olur. O halde $ad=bc$ olduğundan $a=c$ dir.

Önerme 3.1.5: $m=3$ veya $u,v\neq 0,(u,v)=1$ olmak üzere $m=u^2+3v^2$ olsun. Eğer m tek ve $p_1,p_2,...,p_n$ ler asallar ve $e_i\geq 1$ olmak üzere $m=\prod_{i=1}^{n}p_i^{e_i}$ ise o zaman $i=1,2,...,n$ için a_i,b_i tamsayıları, $p_i=a_i^2+3b_i^2$ ve $u+v\sqrt{3}i=\prod_{i=1}^{n}(a_i+b_i\sqrt{3}i)^{e_i}$ olacak biçimde vardır $[4]$.

Önerme 3.1.6: s tek, $(u,v)=1$ olmak üzere $s^3=u^2+3v^2$ olan (u,v,s) üçlülerinin tümünün kümesini E ile gösterelim. $(t,w)=1$ ve $t\not\equiv w\pmod 2$ olan (t,w) ikililerinin tümünün kümesini F ile gösterelim. O zaman, $u=t(t^2-9w^2),v=3w(t^2-w^2),s=t^2+3w^2$ olmak üzere;

$\Phi : F\rightarrow E$

$\Phi\ (t,w)=(u,v,s)$

olarak verilen Φ fonksiyonu örtendir.

İspat: İlk olarak $u^2+3v^2=s^3$ olduğunu gösterelim;

$$u^2+3v^2=t^2(t^2-9w^2)^2+3(3w(t^2-w^2))^2$$

$$=t^2(t^4-18t^2w^2+81w^4)+27w^2(t^4-2t^2w^2+w^4)$$

$$= t^6 - 18t^4w^2 + 81w^4t^2 + 27t^4w^2 - 54t^2w^4 + 27w^6$$

$$= t^6 + 9t^4w^2 + 27t^2w^4 + 27w^6 = (t^2 + 3w^2)^3 = s^3$$

bulunur.

t ve w dan biri tek diğeri çift olduğundan s tektir. Şimdi, $(u,v)=1$ olduğunu gösterelim. Bunun için önce $(t^2-9w^2, t^2-w^2)=1$ olduğunu göstermeliyiz. $p \mid t^2-9w^2$ ve $p \mid t^2-w^2$ olacak biçimde bir p asal sayısı bulunsun. Şu halde t ve w dan biri tek diğeri çift olduğundan p tektir. $p \mid t^2-9w^2$ ve $p \mid t^2-w^2$ olduğundan $p \mid -t^2+9w^2+9t^2-9w^2$ yani $p \mid 8t^2$ olur. Bu durumda p tek olduğundan $p \mid t^2$ yani $p \mid t$ dir. $p \mid t$ ve $p \mid t^2-w^2$ den $p \mid -(t^2-w^2)+t^2$ bulunur. Böylece $p \mid w^2$ yani $p \mid w$ elde edilir. Bu ise $(t,w)=1$ olması ile çelişir. O halde, $(t^2-9w^2, t^2-w^2)=1$ dir. Şimdi de, $(u,v)=1$ olmadığını kabul edelim. Bu taktirde, $q \mid u$ ve $q \mid v$ olacak biçimde bir q asalı vardır. u ve v den biri tek diğeri çift olduğundan q asal sayısı da tek olur. $u = t(t^2-9w^2)$ olduğundan $q \mid u$ ise $q \mid t$ veya $q \mid t^2-9w^2$ dir. $q \mid t$ olsun. $q \mid t$ ve $(t,w)=1$ olduğundan $q \nmid w$ dur. Dolayısıyla $q \mid t^2-9w^2$ dir. $q \mid t^2-w^2$ olduğundan $q \mid 9t^2-9w^2-\left(t^2-9w^2\right)$, yani $q \mid 8t^2$ olur. q tek olduğundan $q \mid t^2$ elde edilir. $q \mid t^2-w^2$ olduğu kullanılırsa $q \mid w^2$ bulunur. Bu ise $(t,w)=1$ olmasına aykırıdır. Eğer $q=3$ ise $3 \mid u$ ve $3 \mid v$ olur. $3 \mid t$ ve $3 \nmid w$ olduğundan $3 \mid s$ elde edilir. Fakat $3^2 \nmid s$ dir. Bununla beraber kolay bir hesaplamayla, $3 \mid s$, $s^3 = u^2+3v^2$ olduğu kullanılırsa $3^2 \mid s$ elde edilir. Bu ise $3^2 \nmid s$ olmasına aykırıdır. Dolayısıyla $(u,v)=1$ dir. Böylece $\Phi(t,w)=(u,v,s) \in E$ olur. Tersine $(u,v,s) \in E$ verildiğinde $p_1, p_2, ..., p_n$ ler farklı asallar ve $e_1, e_2, ..., e_n \geq 1$ olmak üzere $s^3 = \prod_{i=1}^{n} p_i^{e_i}$ olsun. Böylece her i için $e_i = 3e_i^*$ olur. Önerme 3.1.5 ten i = 1, 2, ..., n için $p_i = a_i^2 + 3b_i^2$ olacak biçimde a_i, b_i tamsayıları vardır. Bu durumda,

$$u + v\sqrt{3}i = \prod_{i=1}^{n} (a_i + b_i\sqrt{3}i)^{e_i}$$

dir. t, w tamsayıları,

$$\prod_{i=1}^{n}(a_i+b_i\sqrt{3}i)^{e_i^*}=t+w\sqrt{3}i$$

olarak tanımlansın. Böylece,

$$u+v\sqrt{3}i=(t+w\sqrt{3}i)^3$$

olur. Ayrıca,

$$u+v\sqrt{3}i=(t+w\sqrt{3}i)^3$$

$$=t^3+3t^2w\sqrt{3}i-9tw^2-3\sqrt{3}w_i^3$$

dir. Buradan,

$$u=t^3-9tw^2=t(t^2-9w^2),$$

$$v=3w(t^2-w^2)$$

bulunur. Sonuç olarak $u+v\sqrt{3}i$ nin eşleniğini alırsak,

$$u-v\sqrt{3}i=(t-w\sqrt{3}i)^3$$

elde edilir. Buradan da,

$$s^3=u^2+3v^2=(t^2+3w^2)^3$$

yani $s=t^2+3w^2$ olur. t,w tamsayılarından biri tek diğeri çift ve $(t,w)=1$ olduğundan,

$$\Phi(t,w)=(u,v,s)$$

olur. Bu ise Önermenin ispatını tamamlar.

Önerme 3.1.7: $a,b\in\mathbb{Z}$ ve $(a,b)=1$ olmak üzere $ab=c^3$ olsun. O zaman $a=u^3, b=v^3$ olacak biçimde u ve v tamsayıları vardır.

İspat: $(a,c)=u_1,(b,c)=v_1$ olsun.

$$u_1^3=(a,c)^3=(a^3,c^3)=(a^3,ab)=|a|\ (a^2,b)=|a|$$

olur. Çünkü $(a, b)=1$ olduğundan $(a^2,b)=1$ dir. Ayrıca,

$$v_1^3=(b,c)^3=(b^3,c^3)=(b^3,ab)=|b|\ (b^2,a)=|b|$$

olur. Çünkü $(b^2,a)=1$ dir. O halde $|a|=u_1^3$ ise $a=\mp u_1^3=(\mp u_1)^3$ dür. $\mp u_1=u$ dersek, $a=u^3$ olur. $|b|=v_1^3$ ise $b=\mp v_1^3=(\mp v_1)^3$'dür. $\mp v_1=v$ dersek, $b=v^3$ olur.

Teorem 3.1.8: $x^3+y^3+z^3=0$ olacak biçimde x,y,z tamsayıları varsa, $x=y=z=0$ dır.

İspat: Sıfırdan farklı ve aralarında asal x,y,z tamsayıları, $x^3+y^3+z^3=0$ denklemini sağlasın. Bu durumda $(x,y)=1$ olduğunu görmek kolaydır. O zaman $2=a^3$ olacak biçimde bir $a\in\mathbb{Z}$ olmadığı için x,y,z farklı olmalıdır. Bu x,y,z tamsayılarından biri çift, diğer ikisi tek olmalıdır. x ve y yi tek, z yi de çift alalım. Yukarıdaki şartları sağlayan tüm çözümlerin içinden x,y,z yi $|z|$ en küçük olacak biçimde seçelim. $x+y$ ve $x-y$ çift olduğundan $2a=x+y$, $2b=x-y$ olacak biçimde a ve b tamsayıları vardır. Buradan, $x=a+b$, $y=a-b$ bulunur. Dolayısıyla, $a,b\neq 0$, $(a,b)=1$ ve a ile b den birinin tek, diğerinin çift olduğunu gösterelim. a,b aynı anda tek veya aynı anda çift olunca x ve y çift olur. Bu ise olamaz. $(a,b)=d$ olsun. $d|a$ ve $d|b$ olduğundan, $d|a+b$ ve $d|a-b$ bulunur. Yani $d|x$ ve $d|y$ olur. Ancak $(x,y,z)=1$ olduğu için bu durum $(x,y)=1$ olması ile çelişir. Eğer $a=0$ ise $x=-y$ olur. O zaman $x^3+y^3+z^3=0$ yani $-y^3+y^3+z^3=0$ böylece $z^3=0$ bulunur. O halde $z=0$ olur. Bu ise x,y,z lerin sıfırdan farklı olması ile çelişir. Eğer $b=0$ ise $x=y$ olur. O zaman $x^3+y^3+z^3=0$ yani $x^3+x^3+z^3=0$ böylece $2x^3=-z^3$ bulunur. Ancak

$2=a^3$ olacak biçimde bir $a\in\mathbb{Z}$ olmadığı için bu mümkün değildir. $x^3+y^3+z^3=0$ denklemi $-z^3=x^3+y^3$ olarak yazılır, x ve y nin değerleri yerine konulursa,

$$-z^3=x^3+y^3=(a+b)^3+(a-b)^3=2a(a^2+3b^2)$$

elde edilir. Şu halde z çift ve a ile b den biri tek, diğeri çift olduğundan a^2+3b^2 de tek, dolayısıyla z çift olduğundan $8|z^3$ yani $8|2a$ olur. Bu durumda a çift ve b tek olur. $(2a,a^2+3b^2)=d$ olsun. a^2+3b^2 tek olduğundan d tektir. Eğer $d|2a$ ise $d|a$ dır. O halde $d|a^2$ elde edilir. Bu durumda $d|a^2$ ise $d|3a^2$ bulunur. $d|a^2+3b^2$ ve $d|a^2$ olduğundan $d|a^2+3b^2-a^2$ yani $d|3b^2$ olur. Böylece, $d|3a^2$ ve $d|3b^2$ ise $d|(3a^2,3b^2)$ yani $d|3(a^2,b^2)$ bulunur. $(a,b)=1$ olduğundan $(a^2,b^2)=1$ dir. Dolayısıyla, $d|3$ olur. Yani d ya 1 ya da 3 tür.

1. Durum: $(2a,a^2+3b^2)=1$ olsun. O zaman $3\nmid a$ dır. $-z^3=2a.(a^2+3b^2)$ olduğundan $2a$ ve a^2+3b^2 birer küptür. Dolayısıyla s tek ve $3\nmid s$ olmak üzere

$$2a=r^3,$$

$$a^2+3b^2=s^3$$

olacak biçimde r ve s tamsayıları vardır. s tek ve $(a,b)=1$ olmak üzere $s^3=a^2+3b^2$ ise, o zaman Önerme 3.1.6 ya göre $u,v\in\mathbb{Z}$ tamsayıları $a=u(u^2-9v^2)$, $b=3v(u^2-v^2)$ ve $s=u^2+3v^2$ olacak biçiminde vardır. Burada b tek olduğundan v tek, a çift olduğundan u çifttir. $u\neq 0$ ve $3\nmid u$ dur. Eğer $3|u$ ise $3|s$ yani $3|s^3$ olur. Buradan da $3|a^2$ yani $3|a$ bulunur. Bu ise olamaz. $u=0$ ise $a=0$ olur. Böylece $x=-y$ yani $z=0$ bulunur. Bu ise olamaz. Önerme 3.1.6 ya göre $(u,v)=1$ dir. $(u,v)=1$, v tek, u çift olduğundan $2u,u+3v,u-3v$ sayıları aralarında asaldır. Dolayısıyla, $r^3=2a=2u(u-3v)(u+3v)$ ve $2u,u+3v,u-3v$ aralarında asal olduğundan bunlar birer küptür. $l,m,n\neq 0$ ve aralarında asal sayılar olmak üzere,

$$2u=-n^3,$$

$$u-3v=l^3,$$

$$u+3v=m^3$$

olsun. Böylece n çift ve $l^3+m^3+n^3=0$ sonucuna varılır.. Şimdi $|z|>|n|$ olduğunu gösterelim. Gerçekten, $u^2-9v^2=l^3m^3\neq 0$ ve b tek olduğundan $b\neq 0$ dır. Bu durumda, $|z^3|=|2a(a^2+3b^2)|=|n^3(u^2-9v^2)(a^2+3b^2)|\geq 3|n|^3>|n^3|$ olur. Yani $|z|>|n|$ bulunur. Bu ise z nin en küçük olması ile çelişir.

2. Durum: $(2a,a^2+3b^2)=3$ olsun. $3|2a$ ise $a=3c$ olacak biçimde bir $c\in\mathbb{Z}$ vardır ve a çift olduğundan c de çifttir. Ayrıca $(a,b)=1$ olduğundan $3\nmid b$ dir. O zaman, $-z^3=2a(a^2+3b^2)=6c(9c^2+3b^2)=18c(3c^2+b^2)$ olur. Burada $(18c,3c^2+b^2)=1$ dir. O halde, c çift ve b tek olduğundan $3c^2+b^2$ tek, $3\nmid 3c^2+b^2$ ve $(b,c)=1$ dir. $-z^3=18c(3c^2+b^2)$ ve $(18c,3c^2+b^2)=1$ olduğundan, s tek ve $3|r$ olmak üzere,

$$18c=r^3,$$

$$3c^2+b^2=s^3$$

olacak biçimde r ve s tamsayıları vardır. $v\in\mathbb{Z}$ ve $b=u(u^2-9v^2),c=3v(u^2-v^2)$ olmak üzere $s=u^2+3v^2$ dir. Böylece, b tek olduğundan u tek ve v çift, $u\neq 0,(u,v)=1$ olur. Ayrıca, $2v,u+v,u-v$ aralarında asaldırlar. $r^3=18c=54v(u+v)(u-v)$ den $(r/3)^3=2v(u+v)(u-v)$ bulunur. Burada $2v,u+v,u-v$ aralarında asal olduklarından birer küptürler. $l,m,n\neq 0$ ve n çift olmak üzere,

$$2v=-n^3,$$

$$u+v=p^3,$$

$$u-v=-m^3$$

olacak biçimde l,m,n tamsayıları vardır. O zaman $l^3+m^3+n^3=0$ olur. Şimdi $|z|>|n|$ olduğunu gösterelim:

$|z|^3=18|c|\left(3c^2+b^2\right)=54\left|v\left(u^2-v^2\right)\right|\left(3c^2+b^2\right)=27|n|^3\left|u^2-v^2\right|\left(3c^2+b^2\right)>|n|^3$ ve $u^2-v^2=-l^3m^3\neq 0$, $\left|3c^2+b^2\right|\geq 1$ olduğundan $|z|>|n|$ bulunur. Bu ise yine $|z|$ nin en küçük olması ile çelişir. Şu halde $x^3+y^3+z^3=0$ olacak biçimde sıfırdan farklı x,y,z tamsayıları yoktur.

BÖLÜM 4. KUADRATİK CİSİMLER

4.1. Kuadratik Cisimler ve Kuadratik Tamsayılar

Tanım 4.1.1: d tamkare olmayan sabit bir rasyonel sayı olsun. a,b keyfi rasyonel sayılar olmak üzere $a+b\sqrt{d}$ biçimindeki sayıların kümesini $Q\left(\sqrt{d}\right)$ ile gösterelim. O zaman, $Q\left(\sqrt{d}\right)$ ye kuadratik cisim denir. Eğer $d>0$ ise, $Q\left(\sqrt{d}\right)$ ye reel kuadratik cisim, eğer $d<0$ ise $Q\left(\sqrt{d}\right)$ ye kompleks (sanal) kuadratik cisim denir.

$$Q\left(\sqrt{d}\right)=\left\{a+b\sqrt{d}\,,\ \ a \text{ ve } b \text{ rasyonel sayılardır } \right\}.$$

$d<0$ ise $a+b\sqrt{d}=a+b\sqrt{-di}$ dir.

Teorem 4.1.2: $a+b\sqrt{d}=c+e\sqrt{d}$ dir $\Leftrightarrow$ a = c ve b = e dir.

Ayrıca, $a+b\sqrt{d}=0$ dır $\Leftrightarrow$ $a=b=0$ dır.

İspat: ($\Rightarrow$:) $d>0$ ve $a+b\sqrt{d}=c+e\sqrt{d}$ olsun. O zaman,

$$(a-c)+(b-e)\sqrt{d}=0$$

olur. Buradan da, $a-c=0$ ve $b-e=0$ olduğu görülür.

$b-e\neq 0$ olsun. $\sqrt{d}=\dfrac{a-c}{b-e}$ ve $\sqrt{d}$ irrasyonel olduğundan, $\dfrac{a-c}{b-e}$ rasyonel ve $\sqrt{d}$ irrasyonel olduğundan bu olamaz. O halde $b-e=0$ dır. Yani $b=e$ bulunur.

Aynı zamanda, $a-c=0$ dan $a=c$ olur.

$(\Leftarrow:)$ $a=c$ ve $b=e$ olsun. O zaman $a-c=0$ ve $b-e=0$ dır.

$$(a-c)+(b-e)\sqrt{d}=0$$

ise

$$a+b\sqrt{d}=c+e\sqrt{d}$$

bulunur.

$d<0$ ise benzer ispat yapılır.

Teorem 4.1.3: α ve β $Q(\sqrt{d})$ nin elemanları ise;

$\alpha+\beta,\alpha-\beta,\alpha\beta$ ve $\beta\neq 0$ olduğunda $\dfrac{\alpha}{\beta}$ lar da $Q(\sqrt{d})$ nin elemanlarıdır.

İspat: $a,b,c,e\in Q$ olmak üzere, $\alpha=a+b\sqrt{d}$ ve $\beta=c+e\sqrt{d}$ olsun.

$$\alpha+\beta=(a+c)+(b+e)\sqrt{d},$$

$$\alpha-\beta=(a-c)+(b-e)\sqrt{d},$$

$$\alpha\beta=(ac+bed)+(ae+bc)\sqrt{d}$$

ler $Q(\sqrt{d})$ nin elemanlarıdır. Çünkü, $a+c,b+e,a-c,b-e,ac+bed,ae+bc$ lerin hepsi rasyoneldir. $\beta\neq 0$ ise c ve e nin ikisi de sıfırdan farklıdır. Dolayısıyla, $c-e\sqrt{d}\neq 0$ dır. Yani,

$$c^2-e^2d=\left(c+e\sqrt{d}\right)\left(c-e\sqrt{d}\right)\neq 0$$

olur. O halde

$$\frac{\alpha}{\beta}=\frac{(a+b\sqrt{d})(c-e\sqrt{d})}{(c+e\sqrt{d})(c-e\sqrt{d})}=(\frac{ac-bed}{c^2-e^2d})+(\frac{bc-ae}{c^2-e^2d})\sqrt{d}$$

de $Q\left(\sqrt{d}\right)$ nin elemanıdır.

Tanım 4.1.4: $\alpha=a+b\sqrt{d}$ olsun. $\overline{\alpha}=a-b\sqrt{d}$ ye α nın eşleniği denir.

Teorem 4.1.5: α ve β $Q\left(\sqrt{d}\right)$ nin iki elemanı ise,

$$\overline{(\overline{\alpha})}=\alpha,\ \ \overline{(\alpha+\beta)}=\overline{\alpha}+\overline{\beta},\overline{(\alpha-\beta)}=\overline{\alpha}-\overline{\beta},\overline{(\alpha\beta)}=\overline{\alpha}.\overline{\beta}$$

dir. $\beta\neq 0$ ise $\overline{\beta}\neq 0$ dır ve

$$\overline{\left(\frac{\alpha}{\beta}\right)}=\frac{\overline{\alpha}}{\overline{\beta}}$$

dir. Ayrıca $\alpha=\overline{\alpha}$ dır $\Leftrightarrow \alpha$ bir rasyonel sayıdır.

İspat: $\alpha=a+b\sqrt{d}$, $\beta=c+e\sqrt{d}$ olsun.

$$\overline{(\overline{\alpha})}=\overline{\overline{(a+b\sqrt{d})}}=\overline{(a-b\sqrt{d})}=a+b\sqrt{d}=\alpha,$$

,

$$\overline{(\alpha+\beta)}=\overline{\left((a+c)+(b+e)\sqrt{d}\right)}=(a+c)-(b+e)\sqrt{d}=\overline{\alpha}+\overline{\beta}$$
$$\overline{(\alpha-\beta)}=\overline{\left((a-c)+(b-e)\sqrt{d}\right)}=(a-c)-(b-e)\sqrt{d}=\overline{\alpha}-\overline{\beta},$$

$$\overline{\alpha\beta}=\overline{\left((ac+bed)+(ae+bc)\sqrt{d}\right)}=(ac+bed)-(ae+bc)\sqrt{d}=\overline{\alpha}.\overline{\beta}$$

olarak bulunur. Eğer $\beta \neq 0$ ise $c \neq 0$ ve $e \neq 0$ dır. O zaman $\overline{\beta} = c - e\sqrt{d} \neq 0$ olur. Dolayısıyla,

$$\frac{1}{(\beta\overline{\beta})} = \frac{1}{c^2 - e^2 d}$$

bir rasyonel sayıdır. O zaman,

$$\overline{\left(\frac{\alpha}{\beta}\right)} = \overline{\left(\frac{1}{\beta.\overline{\beta}}.\alpha\overline{\beta}\right)} = \overline{\left(\frac{1}{\beta\overline{\beta}}\right)}.\overline{\alpha}.\overline{(\beta)} = \frac{1}{\beta\overline{\beta}}.\overline{\alpha}.\beta = \frac{\overline{\alpha}}{\overline{\beta}}$$

olur.

$(\Leftarrow:)$ Eğer $\alpha = a + 0\sqrt{d}$ rasyonel sayı ise $\overline{\alpha} = a - 0\sqrt{d} = \alpha$ dır.

$(\Rightarrow:)$ Eğer $\alpha = \overline{\alpha}$ ise $a + b\sqrt{d} = a - b\sqrt{d}$ dir. Teorem 4.1.2 ye göre, $b = -b$ dir.

Yani $b = 0$ ve $\alpha = a$ dır. Dolayısıyla, α bir rasyonel sayıdır.

Tanım 4.1.6: $\alpha, Q\left(\sqrt{d}\right)$ de bir irrasyonel sayı olsun. a,b,c ler tamsayılar ve $a > 0$ olmak üzere, $(a,b,c) = 1$ olsun. Bu durumda α, $ax^2 + bx + c = 0$ denklemini sağlıyorsa bu denkleme α nın tanımlayıcı denklemi denir.

Örneğin, $\frac{3+\sqrt{17}}{4}$ sayısı $8x^2 + 12x - 4 = 0, -10x^2 + 15x + 5 = 0, -2x^2 + 3x + 1$ denklemlerini sağlar. $\frac{3+\sqrt{17}}{4}$ ün tanımlayıcı denklemi $2x^2 - 3x - 1 = 0$ dır.

Tanım 4.1.7: Eğer $\alpha \in Q\left(\sqrt{d}\right)$ ise, α nın normu $\mathrm{N}(\alpha) = \alpha\overline{\alpha}$ olarak tanımlanır.

Teorem 4.1.8: $\alpha = a$ ise $N(a) = a^2$ dir. Eğer $\alpha, Q\left(\sqrt{d}\right)$ nin elemanı ise $N(\alpha)$ rasyoneldir. $N(\alpha) = 0$ dır $\Leftrightarrow$ $\alpha = 0$ dır. Eğer $d < 0$ ise $N(\alpha) \geq 0$ dır. Eğer β

da $Q(\sqrt{d})$ nin elemanı ise $N(\alpha\beta)=N(\alpha)N(\beta)$ dır. $\beta\neq 0$ ise $N\left(\frac{\alpha}{\beta}\right)=\frac{N(\alpha)}{N(\beta)}$ dır.

İspat: $\alpha=a$ bir rasyonel sayı ise $\overline{a}=a$ dır. O zaman, $N(\alpha)=a\overline{a}=a^2$ olur. Eğer $\alpha=a+b\sqrt{d}$ ise, $N(\alpha)=\alpha\overline{\alpha}=\left(a+b\sqrt{d}\right)\left(a-b\sqrt{d}\right)=a^2-b^2d=a^2+(-d)b^2$ dir.

$d<0$ ise $(-d)\geq 0$ olur. $a^2\geq 0, b^2\geq 0$ ve $(-d)\geq 0$ olduğundan, $N(\alpha)\geq 0$ bir rasyonel sayıdır. $N(\alpha)$ rasyonel sayı ise Teorem 4.1.5 e göre $N(0)=0.\overline{0}=0.0=0$ dır. $\alpha\neq 0$ ise $\overline{\alpha}\neq 0$ dır. Dolayısıyla $N(\alpha)=\alpha\overline{\alpha}\neq 0$ olur. Yani $N(\alpha)=0$ dır $\Leftrightarrow \alpha=0$ dır. $N(\alpha\beta)=(\alpha\beta)\left(\overline{\alpha\beta}\right)=\alpha\beta.\overline{\alpha}\,\overline{\beta}=\left(\alpha\overline{\alpha}\right)\left(\beta\overline{\beta}\right)=N(\alpha)N(\beta)$ dır. $\beta\neq 0$ ise

$$N\left(\frac{\alpha}{\beta}\right)=\left(\frac{\alpha}{\beta}\right)\left(\frac{\overline{\alpha}}{\overline{\beta}}\right)=\frac{\alpha}{\beta}.\frac{\overline{\alpha}}{\overline{\beta}}=\frac{\alpha\overline{\alpha}}{\beta\overline{\beta}}=\frac{N(\alpha)}{N(\beta)}$$

olur.

Tanım 4.1.9: $\alpha\in Q(\sqrt{d})$ olsun. $\alpha\in\mathbb{Z}$ veya α irrasyonel iken α nın tanımlayıcı denklemindeki x^2 nin katsayısı 1 ise, α ya bir kuadratik tamsayı (veya kısaca tamsayı) denir.

$\mathbb{Z}$ nin elemanlarına da rasyonel tamsayılar diyeceğiz.

Teorem 4.1.10: Eğer $d\not\equiv 1\pmod 4$ ise $Q(\sqrt{d})$ nin tamsayıları a,b rasyonel tamsayılar olmak üzere $a+b\sqrt{d}$ biçimindeki sayılardır. Eğer $d\equiv 1\pmod 4$ ise

$Q(\sqrt{d})$ nin tamsayıları a ve b rasyonel tamsayılarının ikisi de çift veya ikisi de tek olmak üzere $\frac{a+b\sqrt{d}}{2}$ biçimindeki sayılardır.

İspat: $\alpha \in Q(\sqrt{d})$ ise a,b rasyonel tamsayılar olmak üzere $\alpha = a+b\sqrt{d}$ biçimindedir. O zaman $\overline{\alpha} = a-b\sqrt{d}$ şeklinde olur. Ayrıca α nın tanımlayıcı denklemi

$$(x-\alpha)(x-\overline{\alpha}) = (x-a-b\sqrt{d})(x-a+b\sqrt{d}) = (x-a)^2 - (b\sqrt{d})^2 = x^2 - 2ax + a^2 - b^2 d$$

dir. α, $Q(\sqrt{d})$ de bir tamsayı ise Tanım 4.1.6 ya göre $2a$ ve $a^2 - b^2 d$ birer tamsayı olmalıdır. Bu durumda $2a = n \in \mathbb{Z}$, $m = 2b$ alınırsa,

$$4(a^2 - b^2 d) = 4a^2 - 4b^2 d = (n^2 - m^2 d) \in 4\mathbb{Z}$$

bulunur. $n \in \mathbb{Z}$ olduğundan $m^2 d \in \mathbb{Z}$ olur. $m = \frac{r}{s}, (r,s) = 1$ olsun. $\frac{r^2}{s^2} d \in \mathbb{Z}$ ve $r^2 d = s^2 k$ olan $k \in \mathbb{Z}$ vardır. Eğer $s > 1$ ise $p \mid s$ olan bir p asalı vardır. Böylece $p^2 \mid s^2$ olur. Yani $p^2 \mid r^2 d$ bulunur. $(p,r) = 1$ olduğundan $(p^2, r^2) = 1$ dir. O halde $p^2 \mid d$ olur. Bu ise d nin karesiz olması ile çelişir. Şu halde $r = 1$ dir. Yani $m = \frac{r}{1} = r$ olup m tamsayı olur. Ayrıca, d karesiz tamsayı olduğundan $d \not\equiv 0 \pmod 4$ tür. O halde $d \equiv 1,2,3 \pmod 4$ durumlarını incelemek yeterlidir.

1. Durum: $d \equiv 2,3 \pmod 4$ olsun. $n,m \in \mathbb{Z}$ için $n^2 - dm^2 \equiv 0 \pmod 4$ olduğundan m ve n nin her ikisi de çift olmalıdır. Yani $2a = 2x$ ve $2b = 2y$ olan x ve y rasyonel tamsayıları vardır. Buradan a ve b nin rasyonel tamsayılar olduğu görülür. Yani α, $Q(\sqrt{d})$ de bir tamsayı ise $d \equiv 2,3 \pmod 4$ olduğunda a ve b rasyonel tamsayılar olmak üzere $\alpha = a+b\sqrt{d}$ olmalıdır.

2. Durum : $d \equiv 1 \pmod 4$ olsun. $m,n \in \mathbb{Z}$ için $n^2 - dm^2 \equiv n^2 - m^2 \equiv 0 \pmod 4$ olur. Yani $n^2 \equiv m^2 \pmod 4$ bulunur. Bu ise m ve n nin her ikisinin de tek veya her ikisinin de çift olmasını gerektirir. O halde α, $Q(\sqrt{d})$ de bir tamsayı ise m ve n nin her ikisi de tek veya her ikisi de çift olmak üzere $\alpha = a + b\sqrt{d} = \frac{2a}{2} + \frac{2b}{2}\sqrt{d} = \frac{m}{2} + \frac{n}{2}\sqrt{d} = \frac{m + n\sqrt{d}}{2}$ olmalıdır.

Tersine $d \equiv 2,3 \pmod 4$ olduğunda a ve b rasyonel tamsayılar olmak üzere $\alpha = a + b\sqrt{d}$ nin bir tamsayı ve $d \equiv 1 \pmod 4$ olduğunda a ve b rasyonel tamsayılarının her ikisi de tek veya her ikisi de çift olmak üzere $\alpha = \frac{a + b\sqrt{d}}{2}$ nin bir tamsayı olduğunu görmek kolaydır.

Sonuç 4.1.11: $d \equiv 1 \pmod 4$ ise $Q(\sqrt{d})$ nin bir α elemanı bir tamsayıdır $\Leftrightarrow$ a ve b ler rasyonel tamsayılar olmak üzere

$$\alpha = a + b\left(\frac{1+\sqrt{d}}{2}\right)$$

olarak yazılabilir.

İspat: ($\Leftarrow$:) $a,b \in \mathbb{Z}$ ise

$$a + b\left(\frac{1+\sqrt{d}}{2}\right) = \frac{(2a+b) + b\sqrt{d}}{2}$$

olarak bulunur. $2a+b$ ve b sayıları aynı anda çift veya aynı anda tek olduğundan $a + b\left(\frac{1+\sqrt{d}}{2}\right)$ bir tamsayı olur.

($\Rightarrow$:) α bir tamsayı olsun. $a,b \in \mathbb{Z}$ lerin ikisi de tek veya ikisi de çift olduğundan $\frac{a-b}{2}$ ve b tamsayıdır. O zaman, $\frac{a+b\sqrt{d}}{2} = \frac{a-b}{2} + b\left(\frac{1+\sqrt{d}}{2}\right)$ bulunur.

Örnek 4.1.12 : $Q(i)$, $Q(\sqrt{3}i)$ ve $Q(\sqrt{5}i)$ nin tamsayılarını belirleyiniz.

Çözüm: $i=\sqrt{-1}$ olduğundan $d=-1\equiv 3(\text{mod}\,4)$ tür. Yani, $Q(i)$ nin tamsayılarının kümesi $\{a+bi \mid a,b\in\mathbb{Z}\}$ olarak bulunur.

$-3\equiv 1(\text{mod}\,4)$ olduğundan $Q(\sqrt{3}i)$ nin tamsayılarının kümesi $\left\{a+b\left(\frac{1+\sqrt{3}i}{2}\right) \mid a,b\in\mathbb{Z}\right\}$ olur.

$-5\equiv 3(\text{mod}\,4)$ olduğundan $Q(\sqrt{5}i)$ nin tamsayılarının kümesi $\{a+b\sqrt{5}i \mid a,b\in\mathbb{Z}\}$ olarak bulunur.

Teorem 4.1.13: α ve β $Q(\sqrt{d})$ de tamsayılar ise; $\alpha+\beta$, $\alpha-\beta$, $\alpha\,\beta$ da $Q(\sqrt{d})$ de tamsayılardır.

İspat: Teoremi $d\not\equiv 1\,(\text{mod}\,4)$ ve $d\equiv 1\,(\text{mod}\,4)$ durumlarının her ikisi için de ispatlayalım.

$$w=\begin{cases}\sqrt{d}, d\not\equiv 1(\text{mod}\,4) ise\\ \dfrac{1+\sqrt{d}}{2}, d\equiv 1(\text{mod}\,4) ise\end{cases}$$

alalım.

Teorem 4.1.10 ve Sonuç 4.1.11 den $Q(\sqrt{d})$ de bir α sayısının tamsayı olması için gerekli ve yeterli şart α nın,

$$\gamma = \text{(rasyonel tamsayı)} + \text{(rasyonel tamsayı)}\ w \qquad ...(1)$$

biçiminde olmasıdır. $\alpha,\beta\in Q(\sqrt{d})$ ise $a,b,c,e\in\mathbb{Z}$ olmak üzere $\alpha=a+bw, \beta=c+ew$ alalım. O zaman,

$$\alpha+\beta=(a+c)+(b+e)w,$$

$$\alpha-\beta=(a-c)+(b-e)w$$

olur. Böylece $\alpha+\beta$ ve $\alpha-\beta$ nın (1) formunda olduğu görülür. Yani $\alpha+\beta$ ve $\alpha-\beta$ $Q(\sqrt{d})$ de tamsayılardır.

$s,t\in\mathbb{Z}$ için $w^2=sw+t$ olarak yazabiliriz. Burada $d\not\equiv 1 \pmod 4$ ise $s=0$, $t=d$ dir ve $d\equiv 1 \pmod 4$ ise $s=1$, $t=\dfrac{d-1}{4}$ tür. Ayrıca $d\equiv 1 \pmod 4$ olduğundan, t bir tamsayıdır.

$$\alpha\beta=ac+(ae+bc)w+bew^2$$

$$=ac+(ae+bc)w+be(sw+t)$$

$$=(ac+bet)+(ae+bc+bes)w$$

(1) formunda olduğundan $\alpha\beta$ da bir tamsayıdır.

Teorem 4.1.14: $\alpha,Q(\sqrt{d})$ de bir tamsayı ise, o zaman $N(\alpha)$ bir rasyonel tamsayıdır.

İspat: α bir tamsayı ise, eşleniği olan $\overline{\alpha}$ de bir tamsayıdır. Teorem 4.1.13 ye göre $N(\alpha)=\alpha\overline{\alpha}$ çarpımı da bir tamsayıdır. Fakat $N(\alpha)$ ayrıca rasyonel olduğundan $N(\alpha)$ bir rasyonel tamsayıdır.

4.2. Kuadratik Cisimlerde Birimler ve Asallar

Tanım 4.2.1: $\alpha \neq 0$ ve α, β $Q(\sqrt{d})$ de tamsayılar olsun. $\beta = \alpha\gamma$ olacak biçimde $Q(\sqrt{d})$ de bir γ tamsayısı varsa α, β yı böler denir ve bu durum $\alpha \mid \beta$ ile gösterilir. Eğer $\alpha \mid \beta$ ise $\frac{\beta}{\alpha}$ bir tamsayıdır.

$\alpha \mid \beta$ denildiğinde $\alpha \neq 0$ olmak üzere α, β nın $Q(\sqrt{d})$ de tamsayılar olduğunu kabul edeceğiz.

Teorem 4.2.2: $\alpha \mid \beta$ ve $\alpha \mid \gamma$ ise $\bar{\gamma} \mid \bar{\beta}$ ve ε, δ $Q(\sqrt{d})$ de keyfi, tamsayılar olmak üzere $\alpha \mid (\beta\,\delta + \gamma\,\varepsilon)$ dur.

Özel olarak $\varepsilon = \delta = 1$ alınırsa

$$\alpha \mid \beta + \gamma\ ;$$

$\delta = 1$, $\varepsilon = -1$ alınırsa,

$$\alpha \mid \beta - \gamma\ ;$$

$\varepsilon = 0$ alınırsa,

$$\alpha \mid \beta\,\delta$$

dır. Eğer $\alpha \mid \beta$ ve $\beta \mid \gamma$ ise o zaman

$$\alpha \mid \gamma$$

dır.

İspat: Tanımdan $\beta = \alpha\lambda, \gamma = \alpha\eta$ olacak biçimde λ, η tamsayıları vardır. $\beta = \alpha\lambda$ ise $\bar{\beta} = \overline{\alpha\lambda}$ olur. Dolayısıyla $\bar{\alpha} \mid \bar{\beta}$ olduğu görülür. Ayrıca,

$\beta\delta+\gamma\varepsilon=\alpha\lambda\delta+\alpha\eta\varepsilon=\alpha(\lambda\delta+\eta\varepsilon)$ olarak bulunur. λ bir tamsayı olduğundan, $\overline{\lambda}$ da bir tamsayıdır. Ayrıca, δ,η,ε lar da tamsayılar olduğundan Teorem 4.1.12 ye göre $\lambda\delta+\eta\varepsilon$ da bir tamsayıdır. Tanımdan $\alpha\,|\,(\beta\delta+\gamma\varepsilon)$ olur. Eğer $\alpha\,|\,\beta$ ve $\beta\,|\,\gamma$ ise $\beta=\alpha\lambda$ ve $\gamma=\beta\eta$ olacak şekilde λ ve η tamsayıları vardır. Bu durumda $\gamma=\alpha\lambda\eta$ olur. Yani $\alpha\,|\,\gamma$ dır.

Tanım 4.2.3: $Q(\sqrt{d})$ deki bir ε tamsayısına $\varepsilon\,|\,1$ ise bir birim denir.

Özellikle 1 ve - 1 $Q(\sqrt{d})$ de her zaman birimdirler.

Uyarı : ε sayısını bir tamsayı olarak sınırlandırmak gereklidir. Örneğin, $N\left(\frac{3}{5}+\frac{4}{5}\sqrt{-1}\right)=1$ dir. Fakat $\frac{3}{5}+\frac{4}{5}\mathrm{i}$, $Q(i)$ de bir tamsayı değildir. Dolayısıyla bir birim değildir.

Teorem 4.2.4: Eğer ε_1 ve ε_2 ler $Q(\sqrt{d})$ de birimler ise, o zaman $\overline{\varepsilon_1}$, $\varepsilon_1\varepsilon_2$, $\varepsilon_1/\varepsilon_2$ ler de $Q(\sqrt{d})$ de birimlerdir.

Ayrıca, $Q(\sqrt{d})$ nin bir ε tamsayısı bir birimdir $\Leftrightarrow$ $N(\varepsilon)=\pm1$ dir.

İspat : ε_1 ve ε_2 birim olduklarından tamsayılardır ve $\varepsilon_1\delta_1=\varepsilon_2\delta_2=1$ olacak biçimde $Q(\sqrt{d})$ de δ_1 ve δ_2 tamsayıları vardır. Bu durumda $\overline{\varepsilon_1}$, $\varepsilon_1\,\varepsilon_2$, $\overline{\delta_1}$ ve $\delta_1\,\delta_2$ tamsayılardır. Bununla beraber

$$\overline{\varepsilon_1}\;\overline{\delta_1}=\overline{(\varepsilon_1\delta_1)}=\overline{1}=1,$$

$$(\varepsilon_1\varepsilon_2)(\delta_1\delta_2)=(\varepsilon_1\delta_1)(\varepsilon_2\delta_2)=1$$

olduğundan $\overline{\varepsilon_1}$ ve $\varepsilon_1\,\varepsilon_2$ birer birimdir. Ayrıca $\varepsilon_2\,\delta_1$ de bir tamsayı olduğundan,

$$\frac{\varepsilon_1}{\varepsilon_2}(\varepsilon_2\,\delta_1)=(\varepsilon_1\,\delta_2)(\varepsilon_2\,\delta_1)=(\varepsilon_1\,\varepsilon_2)(\delta_1\,\delta_2)=1$$

dir. Yani $\frac{\varepsilon_1}{\varepsilon_2}$ de bir birimdir.

($\Leftarrow$:) ε bir tamsayı ve $N(\varepsilon)=\pm 1$ olsun. ε bir tamsayı ise $\bar{\varepsilon}$, $-\bar{\varepsilon}$ ler de tamsayılardır. $N(\varepsilon)=1$ ise $\varepsilon\bar{\varepsilon}=N(\varepsilon)=1$ ya da $N(\varepsilon)=-1$ ise $\varepsilon(-\bar{\varepsilon})$ $=-N(\varepsilon)=1$ olur.

($\Rightarrow$:) ε bir birim olsun. Bir δ tamsayısı $\varepsilon\,\delta=1$ olacak şekilde vardır. Bu durumda, $N(\varepsilon)N(\delta)=N(\varepsilon\delta)=N(1)=-1$ olur. $N(\varepsilon)$ ve $N(\delta)$ rasyonel tamsayılar ve çarpımları 1 olduğundan ya $N(\varepsilon)=N(\delta)=1$ ya da $N(\varepsilon)=N(\delta)=-1$ dir. Yani $N(\varepsilon)=\pm 1$ olarak bulunur.

Teorem 4.2.5: $d<0, d\neq 1, d\neq -3$ ise $Q(\sqrt{d})$ nin birimleri ± 1 olmak üzere iki tanedir. Ayrıca $Q(i)$ nin birimleri $\pm 1, \pm\sqrt{-1}$ olmak üzere dört tane; $Q(\sqrt{3i})$ nin $\pm$ 1, $\pm$(-1 +$\sqrt{3i}$) / 2 $\pm$ (- 1 - $\sqrt{3i}$) / 2 olmak üzere altı tane birimi vardır. Eğer $d>0$ ise $Q(\sqrt{d})$ sonsuz çoklukta birime sahiptir.

İspat : $d<0$ ve $d\not\equiv 1 \pmod 4$ olsun. O zaman $Q(\sqrt{d})$ nin tamsayıları a ve b rasyonel tamsayılar olmak üzere, $\gamma=a+b\sqrt{d}$ biçimindedir. Eğer γ bir birim ise $N(\gamma)=1$ dir. $d<0$ olduğunda normlar negatif olmadığından $N(\gamma)=1$ olur.

$$N(\gamma)=a^2-b^2d=a^2+b^2(-d)$$

olduğunu hatırlayalım. $d\leq 2$ yani $-d\geq 2$ için,

$$N(\gamma)\geq a^2+2b^2$$

dir. Eğer $b \neq 0$ ise $b^2 \geq 1$ olur. Dolayısıyla,

$$N(\gamma) \geq a^2 + 2.1 \geq 2$$

bulunur. Bu durumda γ bir birim değildir. O zaman γ bir birim ve $d \leq -2$ ise $b = 0$ olmalıdır. $N(\gamma) = a^2 = 1$ ise $a = \pm 1$ ve $\gamma = \pm 1$ dir. Böylece, $d \leq 2$ ve $d \not\equiv 1 (\mathrm{mod}\, 4)$ olduğunda $Q(\sqrt{d})$ nin birimlerinin sadece ± 1 olduğu görülür.

$d = -1$ olsun. γ yı bir birim olarak kabul edersek, $1 = N(\gamma) = a^2 + b^2$ olur. Buradan $|a| \leq 1, |b| \leq 1$ ve böylece $a = \pm 1$, $b = 0$ veya $a = 0$, $b = \pm 1$ olduğu görülür. O halde $Q(i)$ nin birimleri $\pm$ 1, $\pm$ $\sqrt{-1}$ dir. $d < 0$ ve $d \equiv 1 (\mathrm{mod}\, 4)$ olsun. Bu durumda $Q(\sqrt{d})$ nin γ tamsayıları, a ve b ler $\mathbb{Z}$ de ikisi de tek veya ikisi de çift olmak üzere $\gamma = \dfrac{a + b\sqrt{d}}{2}$ biçimindedir. Şu halde $N(\gamma) = \dfrac{a^2 + b^2(-d)}{4}$ tür. $d < 0$ ve γ bir birim ise $N(\gamma) = 1$ olduğundan $a^2 + b^2(-d) = 4$ tür. O halde $d \leq -7$ yani $-d \geq 7$ ve $b \neq 0$ için, $a^2 + b^2(-d) \geq a^2 + 7b^2 \geq a^2 + 7.1 > 4$ bulunur. Eğer $b = 0$ ise $4 = N(a) = a^2$ olduğundan $a = \pm 2$ ve $\gamma = \pm 1$ dir. Bu durum γ nın bir birim olduğunu gösterir. Eğer $d < 0, d \equiv 1 (\mathrm{mod}\, 4)$ ve $-7 < d$ iken $d = -3$ alınırsa γ bir birim olduğundan $a^2 + 3b^2 = 4$ olur. Burada $|b| \geq 2$ alınırsa $a^2 + 3b^2 \geq 12$ olur. Bu mümkün değildir. O halde $|b| < 2$ olmalıdır. Bu taktirde $b = \pm 1$ veya $b = 0$ olabilir.

$$b = 0 \text{ ise } a = \pm 2 \text{ ve } \gamma = \pm 1,$$

$$b = 1 \text{ ise } a = \pm 1 \text{ ve } \gamma = \left(\pm 1 + \sqrt{3}\right)/2,$$

$$b = -1 \text{ ise } a = \pm 1 \text{ ve } \gamma = \left(\pm 1 + \sqrt{3}\right)/2$$

elde edilir. Yani $Q(\sqrt{3}i)$ nin birimleri sadece, $\pm 1, \left(\pm 1 + \sqrt{3}i\right)/2, \left(\pm 1 - \sqrt{3}i\right)/2$ dir.

$d>0$ olsun. a ve b rasyonel tamsayılar olmak üzere $\gamma=a+b\sqrt{d}$ biçimindeki birimlerin sonsuz çoklukta olduğunu gösterelim. $d\equiv 1(\mathrm{mod}\,4)$ ve c ile e aynı anda tek veya aynı anda çift olduğunda $\left(c+e\sqrt{d}\right)/2$ biçimindeki potansiyel birimleri bir kenara bırakalım. $N(\gamma)=1$ olan sonsuz tane γ biriminin olduğunu gösterelim. $N(\gamma)=-1$ olan birimleri dikkate almayalım. $N(\gamma)=1$ olsun. $N(\gamma)=1$ dir $\Leftrightarrow$ $a^2-db^2=1$ dir. Bu ise Fermat ın Pell denklemidir. $\sqrt{d}$ irrasyonel olduğundan, a ve b tamsayılar olduğunda bu denklemin sonsuz tane çözümü vardır. Bunun için $[3]$ numaralı kaynağa bakılabilir. Dolayısıyla $Q\left(\sqrt{d}\right)$ nin $d>0$ olduğunda sonsuz tane biriminin olduğu gösterilmiş olur.

Tanım 4.2.6 : ε, $Q\left(\sqrt{d}\right)$ de bir birim olsun. $Q\left(\sqrt{d}\right)$ de α ve β tamsayıları $\alpha=\beta\varepsilon$ olacak biçimde varsa , α ya β nın ilgilisidir veya α ile β ilgilidir denir. Bu durum $\alpha\sim\beta$ ile gösterilir. Eğer α ile β ilgili değilse bu durum $\alpha\nsim\beta$ ile gösterilir.

α,β nın ilgisidir $\Leftrightarrow$ α/β bir birimdir.

Teorem 4.2.7: α,β $Q\left(\sqrt{d}\right)$ de tam sayılar olsun. O zaman,

(i) α,β nın bir ilgisidir $\Leftrightarrow$ β,α nın bir ilgisidir.

(ii) α ile β ilgilidir $\Leftrightarrow$ $\alpha\mid\beta$ ve $\beta\mid\alpha$ dır.

(iii) α ile β ilgili ve $\gamma\mid\alpha$ ise $\gamma\mid\beta$ dır. Ayrıca $\alpha\mid\delta$ ise $\beta\mid\delta$ dır.

(iv) α bir asal ise α nın tüm ilgilileri asaldır

(v) α asal değilse α nın asal ilgilisi yoktur.

İspat : (i) ε bir birim ise $1/\varepsilon$ da bir birimdir. Yani eğer $\alpha = \beta\varepsilon$ ise $\beta = \alpha(1/\varepsilon)$ dur. Dolayısıyla tanımdan β da α nın bir ilgilisidir. Aynı şekilde β, α nın bir ilgilisi ise α da β nın bir ilgilisi olur.

(ii) ($\Rightarrow$:) Eğer α ve β tam sayıları ilgililerse bir ε birimi $\alpha = \beta\varepsilon$ ve $\beta = \alpha(1/\varepsilon)$ olacak biçimde vardır. ε ve $1/\varepsilon$ birim olduklarından bölünebilirlik tanımından β/α ve α/β tamsayılardır. Yani $\beta|\alpha$ ve $\alpha|\beta$ dır.

($\Leftarrow$:) Diğer taraftan $\alpha|\beta$ ve $\beta|\alpha$ ise tanımdan ε ve δ tamsayılar olmak üzere $\beta = \alpha\varepsilon$ ve $\alpha = \beta\delta$ dır. Dolayısıyla $\varepsilon\delta = (\beta/\alpha)(\alpha/\beta) = 1$ olur. Yani ε ile δ birimdirler. Böylece α ve β nın ilgili oldukları görülür.

(iii) Eğer α ve β ilgili, $\gamma|\alpha$ ise $\alpha|\beta$ olduğundan $\gamma|\beta$ dır. Eğer α ve β ilgili, $\alpha|\delta$ ise $\beta|\alpha$ olduğundan $\beta|\delta$ dır.

(iv, v) Birimlerin bütün ilgilileri birimler olduğu için bir birimin birimden farklı bir ilgilisi olmayacağı açıktır.

α ve β $Q(\sqrt{d})$ de sıfırdan farklı birim olmayan ilgili tamsayılar olsun. O zaman α ya asaldır ya da yada asal değildir. β da aynı şekildedir. Her ikisinin de asal ya da her ikisinin de asal olmadığını gösterelim. α ve β nın biri asal olsun diğeri asal olmasın. Fark etmediği için α asal olsun ve β asal olmasın. γ ve δ lar birim olmadığında $\beta = \gamma\delta$ olarak yazabiliriz. α ve β lar ilgili olduklarından, bir ε birimi $\alpha = \beta\varepsilon$ olacak biçimde vardır. Yani, $\alpha = \gamma(\delta\varepsilon)$ olur. γ bir birim olmasın. Ayrıca, $(\delta\varepsilon)$ birim olmayanın bir ilgilisi olduğundan, kendisi de bir birim değildir. α nın birimden farklı iki çarpanını bulmamız α nın bir asal sayı olması varsayımı ile çelişir. Dolayısıyla α ve β nın her ikisi de asal değildir.

Tanım 4. 2.8 : $Q(\sqrt{d})$ de sıfırdan ve birimden farklı bir π tamsayısı sadece ilgililerine ve birimlere bölünüyorsa bu π tamsayısına $Q(\sqrt{d})$ de bir asaldır denir. Eğer π, $Q(\sqrt{d})$ de bir asal ise, ε bir birim olduğunda, $\varepsilon\,\pi$ de π nin ilgilisidir ve dolayısıyla asalıdır. Eğer $\pi=\alpha\beta$ olarak iki tamsayının çarpımı biçiminde ise, ya α ya da β bir birimdir.

Burada $\mathbb{Z}$ nin asallarına rasyonel asal diyeceğiz.

Teorem 4.2.9: $Q(\sqrt{d})$ de bir α tamsayısının normu bir rasyonel asal ise α bir asaldır.

İspat: $N(\alpha)$ bir rasyonel asal olduğundan α sıfır veya bir birim değildir. α ve β $Q(\sqrt{d})$ de tamsayılar olmak üzere $\alpha=\beta\gamma$ olsun. O zaman $N(\beta)$ ve $N(\gamma)$ lar rasyonel tamsayılar olmak üzere $N(\alpha)=N(\beta)N(\gamma)$ dır. Bir rasyonel asalın tanımından $N(\beta)$ ve $N(\gamma)$ dan biri bir rasyonel birimdir. Rasyonel birimler ±1 olduğundan ya $N(\beta)=\pm1$ ya da $N(\gamma)=\pm1$ dir. Yani β veya γ bir birimdir. Dolayısıyla tanımdan α bir asaldır.

Örnek 4.2.10 : Teorem 4.2.9 un tersinin doğru olmadığını gösteriniz.

Çözüm: $Q(i)$ yi göz önüne alalım. Burada $N(3)=9$ dur. $3=(a+bi)(c+di)$ olarak yazarsak $9=(a^2+b^2)(c^2+d^2)$ olur. Buradan da $3=a^2+b^2=c^2+d^2$ olamayacağı görülür. Yani $a^2+b^2=1$ veya $c^2+d^2=1$ olmalıdır. O halde Teorem 4.2.4 e göre $a+bi$ veya $c+di$ bir birimdir. Dolayısıyla 3, $Q(i)$ de bir asaldır. Fakat 3 ün normu asal değildir.

Örnek 4.2.11: $N(7)=49$ un bir rasyonel asal olmamasına rağmen, 7 nin $Q(\sqrt{6})$ da bir asal olduğunu gösteriniz.

Çözüm: 7, $Q(\sqrt{6})$ da bir asal olmasın. O zaman $Q(\sqrt{6})$ da α ve β sayıları bir birim olmadığı takdirde $7=\alpha\beta$ olarak yazılır. Buradan, $|N(\alpha)|\geq 2, |N(\beta)|\geq 2$ sonucu çıkar. Böylece,

$$|N(\alpha)||N(\beta)|=|N(\alpha)N(\beta)|=|N(\alpha\beta)|=|N(7)|=49$$

olur. $|N(\alpha)|$ ve $|N(\beta)|$ pozitif rasyonel tamsayılar olduğundan, $|N(\alpha)|=|N(\beta)|=7$ olmalıdır. 7 nin $Q(\sqrt{6})$ da bir asal olduğunu göstermek için ± 7 normunun $Q(\sqrt{6})$ da tamsayılarının olmadığını göstermek yeterlidir. $\gamma, Q(\sqrt{6})$ da bir tamsayı olsun. O zaman a ve b ler $\mathbb{Z}$ de olmak üzere, $\gamma=a+b\sqrt{6}$ biçimindedir. $N(\gamma)=\pm 7$ olsun. $a^2-6b^2=\pm 7$ olur. $a^2+b^2\equiv a^2-6b^2\equiv \pm 7\equiv 0 \pmod 7$ dir. Dolayısıyla $7\mid a^2+b^2$ dir. Bu ise $7\mid a$ ve $7\mid b$ demektir. O zaman $49\mid a^2$ ve $49\mid b^2$ bulunur. $49\mid a^2-6b^2$ olur. Bu ise, $a^2-6b^2=\pm 7$ olması ile çelişir. Sonuç olarak $a^2-6b^2=\pm 7$ denkleminin tamsayı çözümleri yoktur. Böylece $N(\alpha)=\pm 7$ normunun $Q(\sqrt{6})$ da olan tamsayıları yoktur. Dolayısıyla $7, Q(\sqrt{6})$ da bir asaldır.

Tanım 4.2.12: $\alpha,\beta,\delta\in Q(\sqrt{d})$ de tamsayılar olsun. Eğer $\alpha=\beta\delta$ iken β veya δ tamsayılarından biri $Q(\sqrt{d})$ de bir birim oluyorsa α elemanına indirgenemezdir denir.

Teorem 4.2.13 : $Q(\sqrt{d})$ de sıfırdan farklı, birim olmayan her bir eleman indirgenemezdir veya indirgenemez elemanların çarpımı biçiminde yazılabilir.

İspat : α indirgenemez ise ispat biter. Şimdi n üzerinden tümevarımla ispat yapalım. $n \geq 2$ olmak üzere $P(n)$ önermesi şöyle tanımlansın; α, $Q(\sqrt{d})$ de sıfırdan farklı, birim olmayan bir eleman ve $|N(\alpha)| \leq n$ ise α indirgenemez olsun veya α, indirgenemez elemanların çarpımı biçiminde yazılsın.

$n=2$ olsun. $|N(\alpha)| \leq 2$ olur. $N(\alpha)$ birim olmadığından $N(\alpha)=2$ dir. α indirgenemez olmasın. Bu durumda $\alpha = \beta\gamma$ olarak yazılabilir. Öyleyse

$$|N(\alpha)| = |N(\beta)||N(\gamma)| \geq 2.2 = 4$$

tür. Bu ise olamaz. Şu halde α indirgenemezdir. Yani $n=2$ için ifade doğru olur.

Teorem n için doğru olsun. Yani α sıfırdan farklı ve birim olmayan $|N(\alpha)| \leq n$ şartını sağlayan bir eleman ise α ya indirgenemez ya da indirgenemez elemanların çarpımı biçiminde olsun.

Şimdi iddianın $(n+1)$ için doğru olduğunu gösterelim. α sıfırdan farklı, birim olmayan bir eleman ve $|N(\alpha)| \leq n$ olsun. $|N(\alpha)| \leq n$ ise tümevarım kabulüne göre iddia doğrudur. O zaman $n < |N(\alpha)| \leq n+1$ kabul edelim. α indirgenemez ise ispat biter. Şu halde α indirgenemez olmasın. $\alpha = \beta\gamma$ olup $N(\alpha) = N(\beta)N(\gamma) = n+1$ olduğundan $|N(\beta)| \leq n$ ve $|N(\gamma)| \leq n$ olur. Tümevarım kabulüne göre β ve γ elemanları ya indirgenemez ya da indirgenemez elemanların çarpımı biçimindedir. Böylece α nın indirgenemez elemanların çarpımı biçiminde yazıldığı görülür.

Örnek 4.2.14: $Q(\sqrt{5i})$ de 2 indirgenemezdir, ancak asal değildir.

Çözüm: İlk olarak 2 nin $Q(\sqrt{5i})$ de indirgenemez olduğunu gösterelim. $a,b,c,d \in \mathbb{Z}$ için $2 = (a+b\sqrt{5i})(c+d\sqrt{5i})$ olduğunu varsayalım. Bu denklemin

her iki tarafının modülünü alınırsa $4=\left(a^2+5b^2\right)\left(c^2+5d^2\right)$ elde edilir. Bu durumda a^2+5b^2, 4 ü bölen bir pozitif rasyonel tamsayıdır ve $a^2+5b^2=1,2$ veya 4 olmalıdır. Dolayısıyla $(a,b)=(\mp 1,0)$ ya da $(a,b)=(\mp 2,0)$ dır. Yani $a+b\sqrt{5}i=\mp 1$ ya da $a+b\sqrt{5}i=\mp 2$ dir. $a+b\sqrt{5}i=\mp 1$ ise $a+b\sqrt{5}i$ elemanı $Q\left(\sqrt{5}i\right)$ nin bir birimidir. Diğer taraftan, $a+b\sqrt{5}i=\mp 2$ için $c+d\sqrt{5}i=\dfrac{2}{a+b\sqrt{5}i}=\dfrac{2}{\mp 2}=\mp 1$ elde edilir. Öyleyse $c+d\sqrt{5}i$ sayısı $Q\left(\sqrt{5}i\right)$ de bir birimdir. Sonuç olarak 2, $Q\left(\sqrt{5}i\right)$ de indirgenemezdir. Şimdi de 2 nin $Q\left(\sqrt{5}i\right)$ asal olmadığını gösterelim. $2\mid\left(1+\sqrt{5}i\right)\left(1-\sqrt{5}i\right)$ olmasına rağmen $2\nmid\left(1+\sqrt{5}i\right)$ ve $2\nmid\left(1-\sqrt{5}i\right)$ olduğundan 2, $Q\left(\sqrt{5}i\right)$ de asal değildir.

4.3.3 Tek Türlü Parçalanmalı Bölgeler ve Euclid Cisimleri

Tanım 4.3.1: $Q\left(\sqrt{d}\right)$ aşağıdaki özellikleri sağlıyorsa, $Q\left(\sqrt{d}\right)$ ye tek türlü parçalanmalı bölge denir. $\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s$ asallar ve ε bir birim olmak üzere, $\alpha_1\,\alpha_2 \ldots . \alpha_r = \varepsilon\,\beta_1\beta_2 \ldots . \beta_s$ olsun. Bu durumda $r=s$ dir ve $\sigma:\{1,2,\ldots r\}\to\{1,2,\ldots r\}$ bir permütasyon (birebir örten dönüşüm) olmak üzere, α_i sayısı $\beta_{\sigma(i)}$ sayısı ile ilgilidir.

Örnek 4.3.2: $Q\left(\sqrt{13}i\right)$ tek türlü parçalanmalı bölge değildir.

Çözüm: $\left(1-\sqrt{13}i\right),\left(1+\sqrt{13}i\right)\in Q\left(\sqrt{13}i\right)$ nin tamsayıları için $\left(1-\sqrt{13}i\right)\left(1+\sqrt{13}i\right)=14=2.7$ dir. $\left(1-\sqrt{13}i\right)$ asal olmasın.

$1-\sqrt{13}i=\left(a+b\sqrt{13}i\right)\left(c+d\sqrt{13}i\right)$ olacak biçimde birimden farklı $\left(a+b\sqrt{13}i\right),\left(c+d\sqrt{13}i\right)\in Q\left(\sqrt{13}i\right)$ nin tamsayıları vardır. Her iki tarafın normunu alırsak, $14=\left(a^2+13b^2\right)\left(c^2+13d^2\right)$ olur. $a^2+13b^2=2$ ve $c^2+13d^2=7$ olmalıdır. Fakat iki eşitliğin de çözümü yoktur. Öyleyse, $1-\sqrt{13}i$ asaldır. Benzer şekilde 2 sayısının da asal olduğu gösterilir. Şimdi 2 asal olmasın. Dolayısıyla $2=\left(a+b\sqrt{13}i\right)\left(c+d\sqrt{13}i\right)$ olacak şekilde birimden farklı $\left(a+b\sqrt{13}i\right),\left(c+d\sqrt{13}i\right)\in Q\left(\sqrt{13}i\right)$ nin tamsayıları vardır. Her iki tarafın normunu alırsak, $4=\left(a^2+13b^2\right)\left(c^2+13d^2\right)$ olur.

Dolayısıyla $a^2+13b^2=2$ ve $c^2+13d^2=2$ olmalıdır. Fakat iki eşitliğin de çözümü yoktur. Öyleyse 2 asaldır. Benzer şekilde 7 nin asal olduğu görülür. Sonuç olarak, 2, 7, $1+\sqrt{13}i$, $1-\sqrt{13}i$ asal elemanlardır. Şimdi $2\sim 1+\sqrt{13}i$ olsun. Bu durumda $2\mid\left(1+\sqrt{13}i\right)$ ise $1+\sqrt{13}i=2\left(a+b\sqrt{13}i\right)$ olur. Böylece $1=2a$ ve $1=2b$ elde edilir. Bu ise $a,b\in\mathbb{Z}$ olması ile çelişir. Dolayısıyla $2\neq 1+\sqrt{13}i$ dir. Öyleyse $Q\left(\sqrt{13}i\right)$ tek türlü parçalanmalı bölge değildir.

Teorem 4.3.3: $Q\left(\sqrt{d}\right)$ tek türlü parçalanmalı bölgedir $\Leftrightarrow$ $Q\left(\sqrt{d}\right)$ de π bir asal, α ile β tamsayılar olmak üzere $\pi\mid\alpha\beta$ ise $\pi\mid\alpha$ veya $\pi\mid\beta$ dır [3].

Aşağıdaki teoremin ispatı bir önceki teorem kullanılarak kolayca yapılabilir.

Teorem 4.3.4: $Q\left(\sqrt{d}\right)$ tek türlü parçalanmalı bölge, α,β,γ $Q\left(\sqrt{d}\right)$ nin tamsayıları ve $\alpha\mid\beta\gamma$ olsun. Eğer α ile β nın birimden başka ortak böleni yoksa $\alpha\mid\gamma$ dır [3].

Teorem 4.3.5: $Q\left(\sqrt{d}\right)$ tek türlü parçalanmalı bölgedir $\Leftrightarrow$ $Q\left(\sqrt{d}\right)$ nin indirgenemez her elemanı asaldır $[3]$.

Teorem 4.3.6: $Q\left(\sqrt{d}\right)$ tek türlü parçalanmalı bölge olsun. $\alpha,\beta \in Q(\sqrt{d})$ nin tamsayıları olmak üzere α ve β nın birimden başka ortak böleni olmasın. Eğer n pozitif tamsayısı için $\alpha\beta = \varepsilon\gamma^n$ eşitliğini sağlayan bir $\gamma \in Q(\sqrt{d})$ tamsayısı varsa,

$$\alpha = \varepsilon_1\gamma_1^n,$$

$$\beta = \varepsilon_2\gamma_2^n$$

olacak biçimde $\varepsilon_1,\varepsilon_2$ birimleri ve $\gamma_1,\gamma_2 \in Q(\sqrt{d})$ tamsayıları vardır $[3]$.

Teorem 4.3.7: a ve b $Q(\sqrt{d})$ de sıfırdan farklı tamsayılar ve $(a,b)=c$ olsun. $\alpha \mid a$ ve $\alpha \mid b$ olacak biçimde $\alpha \in Q\left(\sqrt{d}\right)$ tamsayısı varsa, $\alpha \mid c$ dir. Özel olarak, a ve b aralarında asal ise a ve b nin $Q\left(\sqrt{d}\right)$ de birimden başka ortak asal böleni yoktur.

İspat: $(a,b)=c$ ise $ar+bs=c$ olacak biçimde r ve s rasyonel tamsayıları vardır. $\alpha \mid a$ ve $\alpha \mid b$ ise $\alpha \mid ar+bs$ dir. Diğer bir deyişle $\alpha \mid c$ olur. Ayrıca a ve b aralarında asal ise $\alpha \mid 1$ olacağından α bir birim olur.

Örnek 4.3.8: $Q\left(\sqrt{47i}\right)$ tek türlü parçalanmalı bölge değildir.

Çözüm: Önce $Q\left(\sqrt{47i}\right)$ de 2 nin asal olduğunu görelim.

$$2=\left(\frac{a+b\sqrt{47i}}{2}\right).\left(\frac{c+d\sqrt{47i}}{2}\right)=\alpha\beta$$

olsun. Buradan

$$4=\left(\frac{a^2+47b^2}{4}\right).\left(\frac{c^2+47d^2}{4}\right)$$

olur. $2=\alpha\beta$ ise $4=N(\alpha)N(\beta)$ dır. Eğer $N(\alpha)=1$ ise α birimdir. Eğer $N(\alpha)=2$ ise $\frac{a^2+47b^2}{4}=2$ ve böylece $a^2+47b^2=8$ bulunur. $b\neq 0$ ise $8=a^2+47b^2\geq 47$ veya $b=0$ ise $a^2=8$ dir. Bu iki durum için de çözüm yoktur. Öyleyse 2 indirgenemezdir. Ayrıca, $2\mid\left(\frac{1+\sqrt{47i}}{2}\right)\left(\frac{1-\sqrt{47i}}{2}\right)$ dir. Fakat $2\nmid\left(\frac{1+\sqrt{47i}}{2}\right)$ ve $2\nmid\left(\frac{1-\sqrt{47i}}{2}\right)$ dir. Dolayısıyla 2 asal değildir. Dolayısıyla Teorem 4.3.5 e göre $Q\left(\sqrt{47i}\right)$ tek türlü parçalanmalı bölge değildir.

Tanım 4.3.9: $\beta\neq 0$, $\alpha,\beta\in Q\left(\sqrt{d}\right)$ tamsayıları için, $\alpha=\gamma\beta+\delta$ ve $|N(\delta)|<|N(\beta)|$ olacak biçimde $\gamma,\delta\in Q\left(\sqrt{d}\right)$ tamsayıları varsa bu $Q\left(\sqrt{d}\right)$ kuadratik cismine bir Euclid cismi denir.

Teorem 4.3.10: Eğer α ve β, $Q\left(\sqrt{d}\right)$ de sıfırdan farklı tamsayılar ve $Q\left(\sqrt{d}\right)$ bir Euclid cismi ise, $Q\left(\sqrt{d}\right)$ de aşağıdaki özellikleri sağlayan bir δ tamsayısı vardır.

(i) $\delta \mid \alpha$ ve $\delta \mid \beta$,

(ii) $\gamma \mid \alpha$ ve $\gamma \mid \beta$ ise $\gamma \mid \delta$ dır.

Ayrıca, bir δ' tamsayısı yukarıdaki iki özelliğe sahiptir $\Leftrightarrow$ $\delta' \sim \delta$ dır [3].

Teorem 4.3.11: Bir kuadratik Euclid cismi tek türlü parçalanmalı bölgedir.

İspat: α ve β, $Q(\sqrt{d})$ de birimlerden başka ortak böleni olmayan tamsayılar olsun. O zaman $Q(\sqrt{d})$ de λ_0 ve μ_0 tamsayılarının $\alpha\lambda_0 + \beta\mu_0 = 1$ olacak biçimde mevcut olduğunu gösterelim. $S = \{|N(\alpha\lambda + \beta\mu)| : \lambda, \mu \in Q(\sqrt{d})$ nin tamsayıları $\}$ olarak tanımlansın. Bu taktirde S nin bir en küçük elemanı vardır. Bu en küçük eleman $\varepsilon = \alpha\lambda_1 + \beta\mu_1$ olmak üzere $|N(\alpha\lambda_1 + \beta\mu_1)|$ olsun. α ve ε sayılarına Euclid algoritmasını uygularsak, $|N(\delta)| < |N(\varepsilon)|$ olmak üzere $\alpha = \varepsilon\gamma + \delta$ olarak yazabiliriz. Burada $\delta = \alpha - \varepsilon\gamma = \alpha - \gamma(\alpha\lambda_1 + \beta\mu_1) = \alpha(1 - \gamma\lambda_1) + \beta(-\gamma\mu_1)$ olduğundan δ, $Q(\sqrt{d})$ de bir tamsayıdır. ε un tanımı ve $|N(\delta)| < |N(\varepsilon)|$ olduğu kullanılırsa $|N(\delta)| = 0$ elde edilir. Böylece Teorem 4.1.13 e göre $\delta = 0$ dır. Yani $\alpha = \varepsilon\gamma$ olur ve bu durumda $\varepsilon \mid \alpha$ dır. Benzer şekilde $\varepsilon \mid \beta$ bulunur ve dolayısıyla ε bir birim olur. ε bir birim olduğundan ε^{-1} de bir birimdir. Böylece $1 = \varepsilon\varepsilon^{-1} = \varepsilon^{-1}(\alpha\lambda_1 + \beta\mu_1) = \alpha(\varepsilon^{-1}\lambda_1) + \beta(\varepsilon^{-1}\mu_1) = \alpha\lambda_0 + \beta\mu_0$ bulunur. Şimdi de π, $Q(\sqrt{d})$ de bir asal ve $\pi \mid \alpha\beta$ ise $\pi \mid \alpha$ veya $\pi \mid \beta$ olduğu ispatlanırsa Teorem 4.3.3 e göre $Q(\sqrt{d})$ nin tek türlü parçalanmalı bölge olduğu görülür. $\pi \nmid \alpha$ olsun. Bu durumda π ve α nın birimden başka ortak böleni yoktur. Dolayısıyla $1 = \pi\lambda_0 + \alpha\mu_0$ olacak biçimde λ_0 ve μ_0 tamsayıları vardır. Son denklemin her iki tarafını β ile çarparsak $\beta = \pi\beta\lambda_0 + \alpha\beta\mu_0$ olur. Böylece $\pi \mid \alpha\beta$ olduğu

kulanılırsa $\pi \mid \beta$ elde edilir. Benzer biçimde $\pi \nmid \beta$ ise $\pi \mid \alpha$ olduğu gösterilir. Dolayısıyla $Q(\sqrt{d})$ cismi tek türlü parçalanmalı bölgedir.

Önerme 4.3.12: $s>0$ olmak üzere $\frac{r}{s} \neq 0$ bir rasyonel sayı olsun. Bu durumda bir $c \in \mathbb{Z}$ tamsayısı $\left|\frac{r}{s}-c\right| \leq \frac{1}{2}$ olacak biçimde vardır.

İspat: r tamsayısı s ye bölünerek $r=sq+t, 0 \leq t<s$ biçiminde yazılabilir. Bu durumda $\frac{r}{s}=q+\frac{t}{s}=q+t*, 0 \leq t<1$ olarak yazılabilir. Eğer $t* \leq \frac{1}{2}$ ise $\left|\frac{r}{s}-q\right|=\left|t^*\right| \leq \frac{1}{2}$ elde edilir. Eğer $\frac{1}{2}<t^*<1$ ise $\frac{r}{s}=q+1+t^*-1$ olup $\left|t^*-1\right|<\frac{1}{2}$ olduğu görülür. Bu ise $\left|\frac{r}{s}-(q+1)\right|=\left|t^*-1\right|<\frac{1}{2}$ olduğunu gösterir. Dolayısıyla $\left|\frac{r}{s}-c\right| \leq \frac{1}{2}$ olacak biçimde bir c tamsayısı vardır.

Teorem 4.3.13: Eğer $d=-11,-7,-3,-2,-1,2,3,5$ ise $Q(\sqrt{d})$ Euclid cismidir.

İspat: Teoremi iki adımda ispatlayalım. Birinci olarak, $d \not\equiv 1 (\mathrm{mod}\, 4)$ olanlar için, ikinci olarak $d \equiv 1 (\mathrm{mod}\, 4)$ olanlar için ispat yapalım. Şimdi d nin ya -2, -1, 2 ya da 3 olduğunu kabul edelim. $b \neq 0$ olmak üzere α ve β $Q(\sqrt{d})$ de tamsayılar olsun. x ve y rasyonel olmak üzere, $\frac{\alpha}{\beta}=x+y\sqrt{d}$ olsun. Önerme 4.3.12 ye göre r ve s tamsayıları;

$$|x-r| \leq \frac{1}{2}, |y-s| \leq \frac{1}{2}$$

olacak biçimde vardır.

$$\gamma = r + s\sqrt{d}, \delta = \beta\left[(x-r)+(y-s)\sqrt{d}\right]$$

alınırsa, $\alpha = \beta\left(x+y\sqrt{d}\right) = \beta\gamma + \delta$ olsun. r ve s rasyonel tamsayılar olduklarından γ bir tamsayıdır. $\delta = \alpha - \beta\gamma$ olduğundan δ da bir tamsayıdır. Ayrıca,

$$|N(\delta)| = |N(\beta)|\left|N\left[(x-r)+(y-s)\sqrt{d}\right]\right| = |N(\beta)|\left|(x-r)^2 - d(y-s)^2\right|$$

dir ve $|d|<3$ ise

$$\left|(x-r)^2 - d(y-s)^2\right| \le |x-r|^2 + |-d||y-s|^2 < \left(\frac{1}{2}\right)^2 + 3\left(\frac{1}{2}\right)^2 = 1$$

olur. Şimdi $d=3$ olsun. Eğer $|x-r|<\frac{1}{2}$ veya $|y-s|<\frac{1}{2}$ ise

$$\left|(x-r)^2 - d(y-s)^2\right| < \left(\frac{1}{2}\right)^2 + 3\left(\frac{1}{2}\right)^2 = 1$$

olur. Eğer $|x-r| = |y-s| = \frac{1}{2}$ ve $d=3$ ise

$$\left|(x-r)^2 - d(y-s)^2\right| = \left|\frac{1}{4} - 3.\frac{1}{4}\right| = \frac{1}{2} < 1$$

dir. Dolayısıyla, $\left|(x-r)^2 - d(y-s)^2\right| < 1$ olur. Böylece,

$$|N(\delta)| = |N(\beta)|\left|(x-r)^2 - d(y-s)^2\right| < |N(\beta)|.1 = |N(\beta)|$$

bulunur. Şu halde $Q\left(\sqrt{d}\right)$ bir Euclid cismidir.

Şimdi de d ya -11, -7, -3 ya da 5 olsun. $\beta \neq 0$ iken α ve β lar $Q\left(\sqrt{d}\right)$ de tamsayılar olsun. x ve y ler rasyonel sayılar olmak üzere, $\alpha/\beta = x + y\sqrt{d}$ olsun. Önerme 4.3.12 ye göre $|2y-s| \le \frac{1}{2}$ olacak biçimde bir s rasyonel

tamsayısı vardır. O halde $\left|y-\frac{s}{2}\right|\leq\frac{1}{4}$ tür. Benzer olarak bir r rasyonel tamsayısı için $\left|\left(x-\frac{r}{2}-r\right)\right|\leq\frac{1}{2}$ olur. Sonuç 4.1.11 e göre $\gamma=r+s\left[\frac{\left(1+\sqrt{d}\right)}{2}\right]$ bir tamsayıdır.

$$\delta=\beta\left\{\left[\left(x-r-\frac{s}{2}\right)\right]+\left[y-\frac{s}{2}\right]\sqrt{d}\right\}$$

olsun. Bu durumda,

$$\alpha=\beta\left(x+y\sqrt{d}\right)=\beta\gamma+\delta,\delta=\alpha-\beta\gamma$$

bir tamsayıdır.

$$|N(\delta)|=|N(\beta)|\left|\left(x-r-\frac{s}{2}\right)^2-d\left(y-\frac{d}{2}\right)^2\right|$$

dir ve

$$\left|\left(x-r-\frac{s}{2}\right)^2-d\left(y-\frac{s}{2}\right)^2\right|\leq\left|x-r-\frac{s}{2}\right|^2+|d|\left|y-\frac{s}{2}\right|^2\leq\left(\frac{1}{2}\right)^2+11\left(\frac{1}{4}\right)^2<1$$

olur.

Yani, $|N(\delta)|<|N(\beta)|$ dır ve $Q\left(\sqrt{d}\right)$ yine bir Euclid cismidir.

Teorem 4.3.14: $Q\left(\sqrt{d}\right)$ Euclid cismidir $\Leftrightarrow$ d, -11,-7,-3,-2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57 veya 73 sayılarından biridir [3].

Teorem 4.3.15: $d<0$ ise $Q\left(\sqrt{d}\right)$ tek türlü parçalanmalı bölgedir $\Leftrightarrow$ d, -1,-2,-3,-7,-19,-43,-67 veya -163 sayılarından biridir [3].

Teorem 4.3.16: $2 \le d \le 100$ olmak üzere d nin 38 değeri için $Q(\sqrt{d})$ tek türlü parçalanmalı bölgedir. Bunlar 2, 3, 5, 6, 7, 11, 13, 14, 17, 19, 21, 22, 23, 29, 31, 33, 37, 38, 41, 43, 46, 47, 53, 57, 59, 61, 62, 67, 69, 71, 73, 77, 83, 86, 89, 93, 94, 97 dir. [3]

Önerme 4.3.17 : a) α, $Q(\sqrt{d})$ de bir tamsayı olsun. α nın normu asal ise α indirgenemezdir.

b) $Q(\sqrt{d})$ tek türlü parçalanmalı bölge ve $N(\alpha)$ asal ise α asaldır.

İspat : a) $N(\alpha)$ asal olsun. α nın indirgenemez olmadığını kabul edelim. Bu durumda β ve γ birimden farklı tamsayılar olmak üzere $\alpha = \beta\gamma$ biçiminde yazılabilir. Buradan $N(\alpha) = N(\beta)N(\gamma)$ elde edilir. β ve γ birimden farklı olduğundan $N(\beta) > 1$ ve $N(\gamma) > 1$ dir. Bu ise $N(\alpha)$ nın asal sayı olması ile çelişir.

b) $N(\alpha)$ asal ise (a) şıkkına göre α indirgenemezdir ve Teorem 4.3.5 e göre α asal eleman olur.

Önerme 4.3.18 : a) $Q(\sqrt{d})$ tek türlü parçalanmalı bölge, $\alpha \in Q(\sqrt{d})$ bir tamsayı, $\alpha \neq 0$ ve α bir birim olmasın. Bu taktirde $\pi \mid \alpha$ olan bir π asal elemanı vardır.

b) $Q(\sqrt{d})$ tek türlü parçalanmalı bölge olsun. α ve β nın birimden başka ortak böleni yoktur $\Leftrightarrow$ α ve β nın hiçbir ortak asal böleni yoktur.

İspat : a) Teorem 4.2.12 den α ya indirgenemez ya da indirgenemez elemanların çarpımı biçimindedir. Bir tek türlü parçalanmalı bölgede indirgenemez her eleman asal olduğundan ispat açıktır.

b) $(\Rightarrow:)$ α ve β nın birimden başka ortak böleni yoksa α ve β nın ortak asal böleni olmadığı açıktır.

$(\Leftarrow:)$ α ve β nın ortak asal böleni olmasın. Şimdi α ve β nın birimden farklı bir γ ortak böleninin mevcut olduğunu kabul edelim. γ birimden farklı olduğundan

(a) şıkkına göre, α nın bir π asal böleni vardır. Dolayısıyla, $\pi \mid \alpha$ ve $\pi \mid \beta$ olur. Bu ise hipotezle çelişir.

Teorem 4.3.19 : $Q(\sqrt{d})$ bir tek türlü parçalanmalı bölge ve π , $Q(\sqrt{d})$ da bir asal ise π pozitif rasyonel asalların en az birini böler.

İspat : $\pi \mid N(\pi)$, yani $\pi \mid |N(\pi)|$ dir. Dolayısıyla π pozitif bir rasyonel sayının bölenidir. $p = \min\{a \in \mathbb{N} : \pi \mid a, a > 1\}$ olsun. Bu taktirde p bir rasyonel tamsayıdır. $\pi \mid p$ olduğu açıktır. p nin asal sayı olmadığını kabul edelim. Bu durumda $p = ab$, $1 < a < p$, $1 < b < p$ olacak biçimde a ve b tamsayıları vardır. $\pi \mid ab$ ve π asal olduğundan $\pi \mid a$ veya $\pi \mid b$ olur. Fakat bu durum p nin tanımına aykırıdır. Çünkü a ve b, p den küçüktür.

Teorem 4.3.20 : $Q(\sqrt{d})$ bir tek türlü parçalanmalı bölge olsun.

a) Herhangi bir p rasyonel asalı ya $Q(\sqrt{d})$ nin bir asalıdır ya da $Q(\sqrt{d})$ nin farklı olmaları gerekmeyen π_1, π_2 gibi iki asalının çarpımıdır.

b) Tüm rasyonel asallara (a) yı uyguladığımızda elde edilen p, π_1, π_2 asallarının tamamı ve bunların ilgilileri $Q(\sqrt{d})$ nin tüm asallarının kümesini oluşturur.

c) $(p,d) = 1$ olan bir p tek asalı $Q(\sqrt{d})$ deki iki π_1, π_2 asallarının $(p = \pi_1 \pi_2)$ çarpımıdır $\Leftrightarrow \left(\frac{d}{p}\right) = +1$ dir. Ayrıca, $p = \pi_1 \pi_2$ olacak biçimde iki asal mevcutsa π_1 ve π_2 ilgili değildir. Ancak π_1 ile $\overline{\pi_2}$ ve π_2 ile $\overline{\pi_1}$ ilgili olabilir.

d) $(2,d) = 1$ ve $d \equiv 3 \pmod 4$ ise 2, bir asalın karesinin ilgilisidir. $d \equiv 5 \pmod 8$ ise 2 , bir asaldır. $d \equiv 1 \pmod 8$ ise 2, farklı iki asalın çarpımıdır.

e) Herhangi bir p rasyonel asalı d yi bölüyorsa, o zaman p , $Q(\sqrt{d})$ de bir asalın karesinin ilgilisidir.

İspat: a) Eğer p bir rasyonel asal ise p nin $Q(\sqrt{d})$ de bir asal böleni vardır. Yani β, $Q(\sqrt{d})$ de tamsayı ve π, $Q(\sqrt{d})$ nin bir asalı olmak üzere $p=\pi\beta$ dır. Her iki tarafın normunu alırsak, $N(\pi)N(\beta)=N(p)=p^2$ olur. π bir asal olduğu için $N(\pi)\neq\mp 1$ dir. Bu durumda $N(\beta)=\mp 1$ veya $N(\beta)=\mp p$ olmalıdır. Eğer $N(\beta)=\mp 1$ ise Teoerem 4.2.4 e göre β bir birimdir. Böylece π, p nin bir ilgilisi olur.. O halde Teoerem 4.2.7 nin (iv) maddesine göre p, $Q(\sqrt{d})$ de bir asal olmalıdır. Eğer $N(\beta)=\mp p$ ise Teorem 4.2.9 a göre β bir asaldır. Böylece p $Q(\sqrt{d})$ de $p=\pi\beta$ olacak biçimde iki asalın çarpımıdır.

b) Teoerem 4.3.19 ve 4.3.20 nin (a) şıkkından doğruluğu açıktır.

c) $(\Leftarrow)$ $(p,d)=1$ ve $\left(\frac{d}{p}\right)=+1$ olmak üzere p bir tek rasyonel asal ise, $x^2\equiv d(\bmod p)$ olacak biçimde bir x rasyonel tamsayısı vardır. Yani $p\mid(x^2-d)$ dir. O halde $p\mid(x-d)(x+d)$ olur. Eğer p, $Q(\sqrt{d})$ de bir asal ise Teoerem 4.3.3' e göre p sayısı $x-\sqrt{d}$ veya $x+\sqrt{d}$ çarpanlarından birini böler. Dolayısıyla $\frac{x}{p}-\frac{\sqrt{d}}{p}$ veya $\frac{x}{p}+\frac{\sqrt{d}}{p}$ $Q(\sqrt{d})$ de bir tamsayı olur. Burada $a+b\sqrt{d}=\frac{x}{p}\pm\frac{1}{p}\sqrt{d}$ ise $a=\frac{x}{p}$ ve $b=\pm\frac{1}{p}$ dir. Ancak $\frac{1}{p}$ bir rasyonel tamsayı olmadığından Teorem 4.1.10 a göre bu imkansızdır. Şu halde, p sayısı $Q(\sqrt{d})$ de bir asal değildir. Böylece (a) ya göre $\left(\frac{d}{p}\right)=+1$ ise π_1 ve π_2 $Q(\sqrt{d})$ de iki asal olmak üzere $p=\pi_1\pi_2$ biçimindedir.

$(\Rightarrow)$ $(d,p)=1$ ve p bir tek rasyonel asal olsun. Ancak p, $Q(\sqrt{d})$ de bir asal olmasın. (a) nın ispatından $N(\pi)=N(\beta)=\mp p$ olmak üzere $p=\pi\beta$ biçiminde olduğunu görürüz. $d\not\equiv 1(\bmod 4)$ ise a ve b rasyonel tamsayılar olmak üzere

$\pi = a + b\sqrt{d}$ veya $d \equiv 1 \pmod 4$ ise a ve b rasyonel tamsayıları aynı türden olmak üzere $\pi = \frac{1}{2}\left(a + b\sqrt{d}\right)$ olarak yazabiliriz. Eğer $\pi = a + b\sqrt{d}$ ise

$$a^2 - db^2 = N(\pi) = \mp p \quad \ldots (1)$$

olur. Her iki tarafı 4 ile çarparsak,

$$(2a)^2 - d(2b)^2 = \mp 4p \quad \ldots (2)$$

elde edilir. Yani,

$$(2a)^2 \equiv d(2b)^2 \pmod p$$

dir. Bu ise $\left(\frac{d}{p}\right) = 1$ olduğunu gösterir. Ayrıca, π ile $\overline{\beta}$ ve $\overline{\pi}$ ile β ilgili olabilirler. $p = \pi\beta$ ve $N(\pi) = a^2 - db^2$ olduğundan

$$\beta = \frac{p}{\pi} = \frac{p}{\left(a + b\sqrt{d}\right)} = \frac{p\left(a - b\sqrt{d}\right)}{a^2 - db^2} = \mp\left(a - b\sqrt{d}\right)$$

olur. Böylece $\overline{\beta} = \mp\left(a - b\sqrt{d}\right)$ dir. Yani π ve $\overline{\beta}$ ilgilidirler. Benzer biçimde $\overline{\pi}$ ile β nın ilgili oldukları gösterilir. Diğer yandan

$$\frac{\pi}{\beta} = \mp\frac{\left(a + b\sqrt{m}\right)}{\left(a - b\sqrt{d}\right)} = \frac{\left[(2a)^2 + d(2b)^2\right]}{4p} + \frac{8ab\sqrt{d}}{4p}$$

olur. Burada $p \nmid 8ab$ olduğundan π / β $Q\left(\sqrt{d}\right)$ de bir tamsayı değildir. Dolayısıyla bir birim değidir. Yani π ve β ilgili değillerdir.

d) Eğer $d \equiv 3 \pmod 4$ ise $Q\left(\sqrt{d}\right)$ nin tamsayıları $a + b\sqrt{d}$ biçimindedir.

$\left(d+\sqrt{d}\right)\left(d-\sqrt{d}\right)=d^2-d=2\dfrac{d^2-d}{2}$ ve $2\nmid\left(d\mp\sqrt{d}\right)$ dir. Aksini kabul edelim. $2\mid\left(d\mp\sqrt{d}\right)$ olsun. O zaman $Q\left(\sqrt{d}\right)$ de $d+\sqrt{d}=2\left(a+b\sqrt{d}\right)$ olacak biçimde bir $a+b\sqrt{d}$ tamsayısı vardır. Burada $2a=d, 2b=1$ olur. Bu ise mümkün değildir. Benzer biçimde $2\nmid d-\sqrt{d}$ olduğu görülür. O halde $Q\left(\sqrt{d}\right)$ de 2 bir asal değildir. Dolayısıyla 2 sayısı bir π asalı ile bölünebilir. $x+y\sqrt{d}=\pi$ olsun. $\pi\mid 2$ ise $2=\pi\pi^*$ olacak biçimde bir π^* tamsayısı vardır. Her iki tarafın normunu alırsak $4=N(\pi)N\left(\pi^*\right)$ olur. π asal olduğundan $N(\pi)=\mp 1$ olamaz. $N(\pi)=\mp 4$ ise $N\left(\pi^*\right)=\mp 1$ olur. Yani π^* bir birim olur. O halde π ile 2 ilgilidir. Dolayısıyla 2 de bir asal olur. Çelişki elde edilir. Şu halde $N(\pi)=\mp 2$ yani $x^2-dy^2=\pm 2$ dir. Böylece

$$\mp\frac{x-y\sqrt{d}}{x+y\sqrt{d}}=\frac{x^2+dy^2}{2}-xy\sqrt{d}$$

ve benzer olarak,

$$\mp\frac{x+y\sqrt{d}}{x-y\sqrt{d}}=\frac{x^2+dy^2}{2}+xy\sqrt{d}$$

olur. Burada $x^2+dy^2=x^2-dy^2+2dy^2=2+2dy^2=2\left(1+dy^2\right)$ olduğundan $2\mid x^2+dy^2$ dir. Yani $\left(x-y\sqrt{d}\right)\left(x+y\sqrt{d}\right)^{-1}$ ve $\left(x+y\sqrt{d}\right)\left(x-y\sqrt{d}\right)^{-1}$ sayılarının her ikisi de $Q\left(\sqrt{d}\right)$ de tamsayılardır. Böylece bu sayılar birim olmalıdır. Yani $x-y\sqrt{d}$ ve $x+y\sqrt{d}$ ilgilidirler. Eğer $d\equiv 1(\bmod 4)$ ve 2, $Q\left(\sqrt{d}\right)$ de bir asal değilse o zaman yukarıda gösterildiği gibi 2, x ve y tamsayılarının ikisi de tek veya ikisi de çift olmak üzere, normu ∓ 2 olan $\dfrac{1}{2}\left(x+y\sqrt{d}\right)$ asalı ile bölünebilir. O halde $\dfrac{1}{4}\left(x^2-dy^2\right)=\mp 2$ yani

$$x^2-dy^2=\mp 8 \quad \ldots(3)$$

bulunur. Eğer x ve y çift ise $x=2x_0$ ve $y=2y_0$ olacak biçimde x_0, y_0 rasyonel tamsayıları vardır. Bu değerleri (3) de yazarsak $x_0^2-dy_0^2=\mp 2$ elde edilir. Ancak $d\equiv 1(\mathrm{mod}\,4)$ olduğundan

$$\mp 2\equiv x_0^2-dy_0^2\equiv x_0^2-y_0^2\equiv 0,+1,-1(\mathrm{mod}\,4)$$

bulunur. Bu ise mümkün değildir. Yani (3) sadece x ve y tek olduğunda çözüme sahiptir. O zaman $x^2\equiv y^2\equiv 1(\mathrm{mod}\,8)$ dir, $x^2\equiv y^2\equiv 1(\mathrm{mod}\,8)$ ve (3) den $x^2-dy^2\equiv 1-d\equiv 0(\mathrm{mod}\,8)$ olur. Bu ise $d\equiv 1(\mathrm{mod}\,8)$ olmasını gerektirir. Yani $d\equiv 5(\mathrm{mod}\,8)$ ise 2, $Q(\sqrt{d})$ de bir asaldır. Eğer $d\equiv 1(\mathrm{mod}\,8)$ ise

$$\frac{1}{2}\left(1-\sqrt{d}\right)\frac{1}{2}\left(1+\sqrt{d}\right)=\frac{1}{4}(1-d)=2\frac{1-d}{8} \text{ dir ve } 2\nmid\left(1\mp\sqrt{d}\right)/2$$

olduğundan 2 nin $Q(\sqrt{d})$ de bir asal olmadığını görürüz. ($2\mid\left(1\mp\sqrt{d}\right)/2$

olsun. O zaman $Q(\sqrt{d})$ de $\frac{1+\sqrt{d}}{2}=2.\frac{1}{2}\left(a+b\sqrt{d}\right)$ olacak biçimde bir $\frac{1}{2}\left(a+b\sqrt{d}\right)$ tamsayısı vardır. $\frac{1+\sqrt{d}}{2}=a+b\sqrt{d}$ olduğundan $a=\frac{1}{2}$, $b=\frac{1}{2}$ olur. a ve b ler rasyonel tamsayılar olduğundan bu imkansızdır. Yani $2\nmid\left(1\mp\sqrt{d}\right)/2$ dir. Yani x ve y tek rasyonel sayılar olduğunda (3) ün çözülebilir olduğunu biliyoruz. Şimdi $\frac{1}{2}\left(x+y\sqrt{d}\right)$ ve $\frac{1}{2}\left(x-y\sqrt{d}\right)$ asallarının $Q(\sqrt{d})$ de ilgili olmadıklarını, yani onların bölümlerinin bir birim olmadığını gösterelim. Gerçekten, onların bölümü $\frac{x+y\sqrt{d}}{x-y\sqrt{d}}=\mp\frac{x^2+dy^2}{8}\mp\frac{xy}{4}\sqrt{d}$ olup x ve y tek rasyonel tamsayılar ise $x^2\equiv 1(\mathrm{mod}\,8), y^2\equiv 1(\mathrm{mod}\,8)$ dir. Böylece $x^2+dy^2\equiv 1+1\equiv 2(\mathrm{mod}\,8)$ olur. Yani $8\nmid x^2+dy^2$ dir. Dolayısıyla $\frac{x+y\sqrt{d}}{x-y\sqrt{d}}$, $Q(\sqrt{d})$ de bir tamsayı değildir. Dolayısıyla bir birim değildir. Sonuç olarak $d\equiv 1(\mathrm{mod}\,8)$ ise (a) şıkkına göre 2 sayısı iki farklı asalın çarpımı biçimindedir.

e) p, d nin bir rasyonel asal böleni olsun. Eğer, $p=|d|$ ise $p=\mp\sqrt{d}\sqrt{d}$ olarak yazılabilir ve Teorem 4.2.7 ye göre p nin $Q(\sqrt{d})$ de bir asalın karesinin ilgilisi olduğu açıkça görülür.

Eğer $p<|d|$ ise

$$\sqrt{d}\sqrt{d}=d=p(d/p) \quad ...(4)$$

olarak yazabiliriz. Teorem 4.1.10 a göre d karesiz olduğundan p, $Q(\sqrt{d})$ de $\sqrt{d}$ nin bir böleni değildir. Şu halde p, $Q(\sqrt{d})$ de bir asal değildir. Yani p, $N(\pi)=\mp p$ olan bir π asalı ile bölünebilir. (4) e göre π, $\sqrt{d}$ nin de bir bölenidir. O halde $\pi^2 \mid d$ ve böylece $\pi^2 \mid p$ olur. Bu ise (a) şıkkına göre ispatı tamamlar.

Sonuç 4.3.21 : $Q(\sqrt{d})$ bir tek türlü parçalanmalı bölge olsun.

a) $(p,2d)=1$ ve $\left(\frac{d}{p}\right)=-1$ olmak üzere p bir rasyonel asal ise p, $Q(\sqrt{d})$ de bir asaldır.

b) $(p,2d)=1$ ve $\left(\frac{d}{p}\right)=+1$ olmak üzere p bir rasyonel asal ise p, $Q(\sqrt{d})$ de farklı iki asalın çarpımı biçimindedir.

İspat: a) p bir rasyonel asal olmak üzere $(p,2d)=1$ ve $\left(\frac{d}{p}\right)=-1$ olsun. p nin asal olmadığını kabul edelim. O zaman Teorem 4.3.20 nin (a) şıkkına göre $p=\pi_1\pi_2$ olmak üzere p sayısı iki farklı asalın çarpımı biçimindedir. Her iki tarafın normu alınırsa $p_2=N(\pi_1)N(\pi_2)$ elde edilir. $d\not\equiv 1 \pmod 4$ ise a ve b rasyonel tamsayılar olmak üzere $p=a+b\sqrt{d}$ şeklindedir. Buradan $p^2=a^2-db^2$ olur.

Böylece $a^2 \equiv db^2 \pmod{p}$ elde edilir. Böylece $\left(\frac{d}{p}\right) = +1$ bulunur. Bu ise kabulümüz ile çelişir. Dolayısıyla p bir asaldır.

b) p bir rasyonel asal olmak üzere $(p, 2d) = 1$ ve $\left(\frac{d}{p}\right) = +1$ olsun. p nin asal olduğunu kabul edelim. $\left(\frac{d}{p}\right) = +1$ olduğundan $x^2 \equiv d \pmod{p}$ çözülebilirdir. Buradan $p \mid x^2 - d = \left(x - \sqrt{d}\right)\left(x + \sqrt{d}\right)$ olur. p bir asal olduğundan $p \mid \left(x - \sqrt{d}\right)$ veya $p \mid \left(x + \sqrt{d}\right)$ olmalıdır. Eğer $p \mid \left(x - \sqrt{d}\right)$ ise $\frac{x}{p} - \frac{1}{p}\sqrt{d} = \alpha$ olacak biçimde bir $\alpha \in Q\left(\sqrt{d}\right)$ tamsayısı vardır. Eğer $d \not\equiv 1 \pmod{4}$ ise a ve b rasyonel tamsayılar olmak üzere $\alpha = a + b\sqrt{d}$ biçimindedir. Bu durumda $\frac{x}{p} - \frac{1}{p}\sqrt{d} = a + b\sqrt{d}$ olduğundan $a = \frac{x}{p}$ ve $b = -\frac{1}{p}$ dir. p bir asal olduğundan $-\frac{1}{p} = b$ olması mümkün değildir. Eğer $d \equiv 1 \pmod{4}$ ise a ve b ler aynı anda tek veya aynı anda çift olmak üzere $\alpha = \frac{1}{2}\left(a + b\sqrt{d}\right)$ biçimindedir. Bu durumda $\frac{x}{p} - \frac{1}{p}\sqrt{d} = \frac{1}{2}\left(a + b\sqrt{d}\right)$ olduğundan $\frac{x}{p} = \frac{1}{2}a$, $-\frac{1}{p} = \frac{1}{2}b$ olur. Ancak $bp = -2$ ve $p > 2$ olduğundan bu bir çelişkidir. O halde Teorem 10.41 in (b) şıkkına göre p, $Q\left(\sqrt{d}\right)$ de farklı iki asalın çarpımı biçimindedir.

Teorem 4.3.22 : $p > 2$ bir rasyonel asal olsun. $p = x^2 + 2y^2$ olacak biçimde x ve y tamsayıları vardır $\Leftrightarrow$ $p \equiv 1, 3 \pmod{8}$ dir.

İspat : $(\Rightarrow:)$ $p=x^2+2y^2$ olan x ve y tamsayıları varsa x tektir. Dolayısıyla $x^2\equiv 1(\mathrm{mod}\,8)$ olur. Diğer yandan $2y^2\equiv 0(\mathrm{mod}\,8)$ veya $2y^2\equiv 2(\mathrm{mod}\,8)$ olduğu açıktır. Buradan $x^2+2y^2\equiv 1(\mathrm{mod}\,8)$ veya $x^2+2y^2\equiv 3(\mathrm{mod}\,8)$ bulunur.

$(\Leftarrow:)$ $p\equiv 1(\mathrm{mod}\,8)$ veya $p\equiv 3(\mathrm{mod}\,8)$ ise $\left(-\frac{2}{p}\right)=\left(-\frac{1}{p}\right)\left(\frac{2}{p}\right)=(-1)^{\frac{p-1}{2}}(-1)^{\frac{p^2-1}{8}}$ olduğundan $\left(-\frac{2}{p}\right)=1$ olduğu görülür. Yani $x^2\equiv -2(\mathrm{mod}\,p)$ olan bir x tamsayısı vardır. Bu ise $p\mid x^2+2$ yani $p\mid\left(x-\sqrt{2}i\right)\left(x+\sqrt{2}i\right)$ olduğunu gösterir. $Q\left(\sqrt{2}i\right)$ tek türlü parçalanmalı bölgedir. Eğer p, $Q\left(\sqrt{2}i\right)$ de asal ise $p\mid x-\sqrt{2}i$ veya $p\mid x+\sqrt{2}i$ olmalıdır. Bunun olamayacağını görmek kolaydır. Şu halde p asal değildir. Dolayısıyla $Q\left(\sqrt{2}i\right)$ de birim olmayan α, β tamsyıları $p=\alpha\beta$ olacak biçimde vardır. Buradan $p^2=N(\alpha\beta)=N(\alpha)N(\beta)$ elde edilir. Bu nedenle $N(\alpha)=p$ olur. Eğer $\alpha=a+b\sqrt{2}i$ alınırsa $p=N(\alpha)=a^2+2b^2$ bulunur.

Örnek 4.3.23: $x^2+2=y^3$ denkleminin çözümlerinin $x=5,y=3$ ve $x=-5,y=3$ olduğunu gösteriniz.

Çözüm: $x^2+2=y^3$ ise

$$\left(x+\sqrt{2}i\right)\left(x-\sqrt{2}i\right)=y^3$$

tür. Şimdi $x+\sqrt{2}i$ ve $x-\sqrt{2}i$ nin bir ortak böleni γ olsun. $\gamma\mid x+\sqrt{2}i$ ve $\gamma\mid x-\sqrt{2}i$ olduğundan $\gamma\mid 2\sqrt{2}i$ olur. $x^2+2=y^3$ olduğundan x tek olmalıdır. Aksine x çift ise $x^2+2\equiv 2(\mathrm{mod}\,4)$, yani $y^3\equiv 2(\mathrm{mod}\,4)$ olur. Halbuki $a\in\mathbb{Z}$ ise $a^3=0,1,3(\mathrm{mod}\,4)$ olduğu açıktır. Dolayısıyla x tektir. $\gamma\mid 2\sqrt{2}i$ ise $N(\gamma)\mid 8$ dir. Eğer $N(\gamma)>1$ ise $N(\gamma)$ çift olur. $\gamma\mid x+\sqrt{2}i$ ise $N(\gamma)\mid x^2+2$ olur. Bu ise N(γ)

çift ve x^2+2 tek olduğundan mümkün değildir. Şu halde $N(\gamma)=1$ dir. Yani, γ birimdir. Böylece $x+\sqrt{2}i$ ve $x-\sqrt{2}i$ nin birimden başka ortak böleni yoktur. Teorem 4.3.6 ya göre $x+\sqrt{2}i=\varepsilon\lambda^3$ olacak biçimde ε birimi ve $\lambda\in Q(\sqrt{2}i)$ vardır. $Q(\sqrt{2}i)$ nin birimleri ∓ 1 ve $(-1)^3=-1$ olduğundan, $x+\sqrt{2}i=(a+b\sqrt{2}i)^3$ olarak yazılabilir. Buradan $x+\sqrt{2}i=(a+b\sqrt{2}i)^3=a^3+3a^2b\sqrt{2}i-6ab^2-2b^3\sqrt{2}i$ elde edilir. Burada reel ve sanal kısımları eşitlersek, $x=a(a^2-6ab^2)$ buluruz. $1=b(3a^2-2b^2)$ ve $a,b\in Z$ olduğundan $b=\pm 1$ dir. Eğer $b=1$ ise $3a^2-2=1$ dir. Buradan $a=\pm 1$ olur. Böylece $x=\mp 5$ bulunur. Burada $y^3=x^2+2$ olduğundan $y=3$ tür. Eğer $b=-1$ ise $3a^2-2=-1$ bulunur. Buradan da $a^2=\frac{1}{3}$ bulunur. Fakat $a\in\mathbb{Z}$ olduğundan çözüm yoktur. Sonuç olarak, $(x,y)=(\mp 5,3)$ bulunur.

Örnek 4.3.24: $x^2+1=y^3$ denklemini çözünüz.

Çözüm: $x^2+1=y^3$ olsun. $(x+i)(x-i)=y^3$ tür. $x^2\equiv 0,1(\mathrm{mod}\,4)$ olduğundan, $x^2+1\equiv 1,2(\mathrm{mod}\,4)$ olur. Herhangi bir y tamsayısı için, $y^3\equiv 0,1,3(\mathrm{mod}\,4)$ olduğundan $y^3\equiv 1(\mathrm{mod}\,4)$ olmalıdır. Bu ise $y\equiv 1(\mathrm{mod}\,4)$ olduğunu gösterir. Dolayısıyla y tektir. Şimdi π sayısı $x+i$ ve $x-i$ nin ortak asal böleni olsun. $\pi\,|\,x+i$ ve $\pi\,|\,x-i$ olduğundan $\pi\,|\,2i$ olur. Şu halde $\pi\,|2$ dir. $\pi\,|2$ ise π sayısı asal ve $2=(1+i)(1-i)$ olduğundan $\pi\,|\,1+i$ veya $\pi\,|\,1-i$ olmalıdır. Her iki durumda da $N(\pi)=2$ olduğu görülür. $\pi\,|\,x+i$ olduğundan $N(\pi)\,|\,N(x+i)$ dir. $2\,|\,x^2+1$ olur. Bu ise $2\,|\,y^3$, yani $2\,|\,y$ olmasını gerektirir. Bu olamaz. Şu halde $x+i$ ve $x-i$ nin birimden başka ortak böleni yoktur. Teorem 4.3.6 ya göre, $x+i=\varepsilon(c+di)^3$ olacak biçimde ε birimi ve $(c+di)\in Q(i)$ vardır. $Q(i)$ nin birimleri ∓ 1 ve $\mp$i dir. $(-1)^3=-1, i^3=-i$ ve $(-i)^3=i$ olduğundan $x+i=(a+bi)^3$ olarak yazılabilir. Buradan,

$$x+i=(a+bi)^3=a^3+3a^2(bi)+3a(bi)^2+(bi)^3=(a^3-3ab^2)+(3a^2b-b^3)i$$

elde edilir. Reel ve sanal kısımları eşitlersek, $x=a(a^2-3b^2)$ ve $1=b(3a^2-b^2)$ olur. İkinci eşitlikten $b=1$ ve $3a^2-b^2=1$ bulunur. Fakat $3a^2=2$ olamaz. Dolayısıyla çözüm yoktur. $b=-1$ ve $3a^2-b^2=-1$ ise $3a^2=0$ olur. Öyleyse $a=0$ elde edilir. Buradan, $(x,y)=(0,1)$ bulunur.

Örnek 4.3.25: $x^2+11=y^3$ denkleminin çözümünü bulunuz.

Çözüm: $x^2+11=y^3$ ise x çifttir. x sayısını tek kabul edelim. Bu durumda, $x^2+11\equiv 4(\mathrm{mod}\,8)$ dir. Herhangi bir y rasyonel tamsayısı için $y^3\not\equiv 4(\mathrm{mod}\,8)$ olduğundan bu bir çelişkidir. Şu halde x çifttir. $11\mid x$ ise $11\mid y$ olur ve $11^2\mid y^3-x^2$ bulunur. Bu ise $y^3-x^2=11$ olması ile çelişir. Öyleyse $11\nmid x$ olur. $m\equiv 1(\mathrm{mod}\,4)$ ise $Q(\sqrt{d})$ nin tamsayıları $a+b\left(\frac{1+\sqrt{d}}{2}\right)$ biçimindedir. $-11\equiv 1(\mathrm{mod}\,4)$ tür. x çift olsun. Bu durumda,

$$x+\sqrt{11}i=x-1+2\left(\frac{1+\sqrt{11}i}{2}\right)$$

ve

$$x-\sqrt{11}i=x-1+(-2)\left(\frac{1+\sqrt{11}i}{2}\right)$$

olarak yazılabilir. Dolayısıyla, $x+\sqrt{11}i, x-\sqrt{11}i\in Q(\sqrt{11}i)$ nin tamsayılarıdır. Buradan $(x+\sqrt{11}i)(x-\sqrt{11}i)=x^2+11=y^3$ olur.

$x+\sqrt{11}i$ ile $x-\sqrt{11}i$ in ortak asal böleni α olsun. Bu durumda, $\alpha\mid x+\sqrt{11}i$ ve $\alpha\mid x-\sqrt{11}i$ dir. Böylece $\alpha\mid 2\sqrt{11}i$ ve 2 ile $\sqrt{11}i$ asal olduğundan $\alpha=\pm 2$ veya $\alpha=\pm\sqrt{11}i$ olmalıdır. Fakat x çift ve $2\nmid\sqrt{11}i$ olduğundan $\alpha=\pm 2$ olamaz.

$\alpha = \pm\sqrt{11}i$ ise $\alpha \mid x$ dir. Buradan $11 \mid x$ elde edilir. Bu ise mümkün değildir. Bu durumda $x+\sqrt{11}i$ ve $x-\sqrt{11}i$ tamsayılarının birimden başka ortak böleni yoktur. Öyleyse Teorem 4.3.6 ya göre $x+\sqrt{11}i=\varepsilon\lambda^3$ olacak biçimde ε birimiyle $\lambda \in Q\left(\sqrt{11}i\right)$ vardır. $Q\left(\sqrt{11}i\right)$ in birimleri ∓ 1 ve $(\mp 1)^3 = \mp 1$ olduğundan $x+\sqrt{11}i=\lambda^3$ olur. Öyleyse,

$$x+\sqrt{11}i=\left[a+b(\frac{1+\sqrt{11}i}{2})\right]^3=\frac{(2a+b+b\sqrt{11}i)^3}{8}$$

$$=\frac{15}{2}ab^2+\frac{3}{2}a^2b)+(\frac{3}{2}a^2b+\frac{3}{2}ab^2-b^3)\sqrt{11}i$$

dir. Buradan $x=a^3-4b^3-\frac{15}{2}ab^2+\frac{3}{2}a^2b$ ve $1=(\frac{3}{2}a^2b+\frac{3}{2}ab^2-b^3)$ elde edilir. İkinci eşitlikten, $2=b\left(3a^2+3ab-2b^2\right)$ bulunur. Dolayısıyla $b \mid 2$ dir. Böylece $b=\pm 1$ veya $b=\pm 2$ olur. Eğer $b=1$ ise $2=3a^2+3a-2$ dir. Öyleyse, $4=3a(a+1)$ dir. $3 \nmid 4$ olduğundan bu olamaz. Eğer $b=-1$ ise $2=-3a^2+3a+2$ ve böylece $0=3a(1-a)$ bulunur. Buradan $a=0$ veya $a=1$ dir. Buradaki çözümler $a=0$ ise $x=4$ ve $a=1$ ise $x=-4$ tür. Eğer $b=2$ ise $2=6a^2+12a-16$ ve böylece $a^2+2a-3=0$ olur. Öyleyse $a=-3$ veya $a=1$ bulunur. Buradaki çözümler $a=-3$ ise $x=58$ ve $a=1$ ise $x=-58$ dir. Eğer $b=-2$ ise $2=6a^2+12a-16$ ve $-7=3a(2-a)$ olur. Fakat $3 \nmid 7$ olduğundan çözüm yoktur. Bulunan x değerleri için tüm çözümler; $x=\pm 4$ için $y^3=x^2+11=27$ ise $y=3$ ve $x=\pm 58$ için $y^3=3375$ ise $y=15$ olarak bulunur.

Örnek 4.3.26: $x^2+49=y^3$ ün tamsayılardaki tüm çözümlerini bulunuz.

Çözüm: $x^2+49=y^3$ olacak biçimde x ve y tamsayılarının var olduğunu kabul edelim. $x^2+49=(x+7i).(x-7i)$ olarak yazılabilir.

Önce $x+7i$ ve $x-7i$ sayılarının aralarında asal olduklarını, yani birimden başka ortak bölenlerinin olmadığını gösterelim. Aksini kabul edelim. Birimden farklı bir d elemanı $d \mid x+7i$ ve $d \mid x-7i$ olacak biçimde bulunsun. O zaman $N(d) \neq \mp 1$ dir.

$d \mid x+7i-(x-7i) \Rightarrow d \mid 14i$ dir. Buradan $N(d) \mid N(14i)$ yani $N(d) \mid 14^2$ olur. Dolayısıyla $N(d)$ nin bir p asal çarpanını alırsak, $p \mid 14^2$ bulunur. Bu durumda $p=2$ veya $p=7$ olabilir. Ayrıca $d \mid x+7i$ olduğundan, $N(d) \mid N(x+7i)=x^2+49=y^3$ tür. Yani $p \mid y^3$ tür. Böylece y, 2 veya 7 ile bölünebilir. $2 \mid y$ olsun. O zaman $8 \mid y^3$ yani $8 \mid x^2+49$ dur. Bu durumda x tek olmalıdır. $49 \equiv 1 \pmod 8$, $x^2 \equiv 1 \pmod 8$ ve $y^3 \equiv 0 \pmod 8$ ve $x^2+49=y^3$ olduğundan, $1+1 \equiv 0 \pmod 8$ bulunur. Bu bir çelişkidir.

$7 \mid y$ olsun. $x^2+49=y^3$ olduğundan $7 \mid x$ elde edilir. $s,t \in \mathbb{Z}$ olmak üzere $x=7s$ ve $y=7t$ alırsak $s^2+1=7t^3$ bulunur.

$s^2 \equiv -1 \pmod 7$ dir. Fakat, $0^2 \equiv 0 \pmod 7$, $(\mp 1)^2 \equiv 1 \pmod 7$, $(\mp 2)^2 \equiv 4 \pmod 7$ ve $(\mp 3)^2 \equiv 9 \equiv 2 \pmod 7$ olduğundan $s^2 \equiv -1 \pmod 7$ olan bir s tamsayısı yoktur. Bu bir çelişkidir. Dolayısıyla $x+7i$ ve $x-7i$ aralarında asaldır.

Tek türlü parçalanmalı bölge tanımından, $r \in Q(i)$ ve ε $Q(i)$ de bir birim olmak üzere, $x+7i=\varepsilon r^3$ şeklindedir.

Fakat Q (i) nin birimleri ∓ 1 ve $\mp i$ olduğundan, $x+7i=r^3$ olarak alabiliriz. $a,b \in \mathbb{Z}$ için $r=a+bi$ alırsak, $x+7i=(a+bi)^3=a^3+3ab^2bi-3ab^2-b^3i$ olur. Sanal kısımların eşitliğinden, $7=(3a^2-b^2)b$ bulunur. Yani $b \mid 7$ dir. O zaman $b \mp 1$ veya $b=\mp 7$ dir. $7 \equiv 1 \pmod 3$ ve $(3a^2-b^2)b \equiv -b^3 \pmod 3$ olduğundan, $b^3 \equiv -1 \pmod 3$ tür. Yani $b \equiv -1 \pmod 3$ tür. Buradan da $b \neq 7$ ve $b \neq 1$ olduğu görülür. Eğer $b=-1$ ise $-7=3a^2-b^2=3a^2-1 \Rightarrow 3a^2=-6 \Rightarrow a^2=-2$ olur. Bu ise olamaz. Eğer $b=-7$ ise $-b^2=3a^2-49$ ise $3a^2=48$ yani $a^2=16$ bulunur.

O halde $a=\mp 4$ olur. Dolayısıyla, $x^2+49=y^3$ denkleminin çözümleri sadece, $a=\mp 4$ ve $b=7$ için vardır. Böylece $y^3=N(r^3)=a^2+b^2=(\pm 4)^2+7^2=16+49=65$ ve $x^2+49=y^3$ olduğundan $x^2=y^3-49=65^3-49=274625-49=274576$ yani $x=\mp 524$ bulunur. O halde $(x,y)=(\mp 524,65)$ tir.

Örnek 4.3.27 : $x^2+44=y^3$ denkleminin tüm çözümlerini bulunuz.

Çözüm: $x^2+44=y^3$ denklemini sağlayan x ve y tamsayıları varolsun. O zaman,

$$x^2+44=(x+2\sqrt{11}i)(x-2\sqrt{11}i)$$

olarak yazabiliriz. $x+2\sqrt{11}i$ ve $x-2\sqrt{11}i$ sayılarının $Q(\sqrt{11}i)$ kuadratik cisminde aralarında asal olduklarını gösterelim. $Q(\sqrt{11}i)$ de birimden farklı bir d tamsayısı bu sayıların her ikisini de bölsün. O zaman, $d \mid x+2\sqrt{11}i-\left(x-2\sqrt{11}i\right)$ ise $d \mid 4\sqrt{11}i$ dir. Böylece ,

$$N(d) \mid N(4\sqrt{11}i)=N(4)N(\sqrt{11}i)=16.11$$

olur. $d, Q(\sqrt{11}i)$ de birim olmadığından $N(d)\neq \mp 1$ dir. $N(d)$ nin bir p asal bölenini alırsak, $p \mid 16.11$ olur. Yani $p=2$ veya $p=11$ dir. Ayrıca, $d \mid x+2\sqrt{11}i$ olduğundan

$$N(d) \mid N(x+2\sqrt{11}i)=x^2+44=y^3$$

tür. Dolayısıyla $p \mid y^3$ ise $2 \mid y$ veya $11 \mid y$ bulunur. $2 \mid y$ olduğunu kabul edelim. $x^2+44=y^3$ olduğundan, $2 \mid x$ dir. s ve t rasyonel tamsayılar olmak üzere, $x=2s$ ve $y=2t$ alırsak, $s^2+11=2t^3$ olur. Bu durumda s tektir. O halde $s^2 \equiv 1 \pmod 4$ ve $2t^3 \equiv s^2+11 \equiv 1+3 \equiv 0 \pmod 4$ bulunur.. Sonuç olarak $4 \mid 2t^3$ olur. Yani t çifttir. u bir tamsayı olmak üzere $t=2u$ alalım. Böylece,

$s^2+11=16u^3$ olur. $s^2\equiv 1\pmod 8$ dir. Çünkü s tektir. O halde $0\equiv 16u^3\equiv 2t^3\equiv s^2+11\equiv 1+3\equiv 4 \pmod 8$ olur. Bu ise olamaz. $11\mid y$ olsun. Ayrıca $x^2+44=y^3$ olduğundan $11\mid x$ dir. Burada $11^2\mid x^2$ ve $11^2\mid y^3$ tür. Fakat $11^2 \nmid 44$ olduğundan bu bir çelişkidir. Dolayısıyla $x+2\sqrt{11}i$ ve $x-2\sqrt{11}i$, $Q(\sqrt{11}i)$ de aralarında asaldır. $Q(\sqrt{11}i)$ tek türlü parçalanma özelliğine sahip olduğundan, $r\in Q(\sqrt{11}i)$ ve ε, $Q(\sqrt{11}i)$ de bir birim olmak üzere, $x+2\sqrt{11}i=\varepsilon r^3$ alınabilir. $Q(\sqrt{11}i)$ nin birimleri ∓ 1 olduğundan $\varepsilon=1$ alabiliriz. O zaman $x+2\sqrt{11}i=r^3$ olur. a ve b rasyonel tamsayılar olmak üzere $r=a+bi$ alırsak,

$$x+2\sqrt{11}i=(a+bi)^3=a^3-33ab^2-b^3i+3a^2b\sqrt{11}i$$

olur. Burada $a+b$ çifttir. Sanal kısımların eşitliğinden, $2=\dfrac{(3a^2-11b^2)b}{8}$ bulunur. Yani $16=(3a^2-11b^2)b$ dir.

Durum 1: a,b çift olsun. s,t rasyonel tamsayılar olmak üzere, $a=2s$ ve $b=2t$ alalım. $2=\left|3s^2-11t^2\right|t$ olur. $-1\equiv t^3\pmod 3$ ise $t\equiv -1\pmod 3$ bulunur. Yani, $t\mid 2$ ve $t\equiv -1\pmod 3$ olduğundan $t=2$ veya $t=-1$ dir. Eğer $t=2$ ise $2=\left(3s^2-11.2^2\right).2$ yani $3s^2-44=1$ olur. Böylece $3s^2=45$ yani $s^2=15$ bulunur. Bu ise olamaz. Eğer $t=-1$ ise $-2=3s^2-11$ yani $3s^2=9$ böylece $s^2=3$ bulunur. Bu ise olamaz.

Durum 2: a ve b tek olsun. O zaman b, 16 nın tek çarpanıdır. O halde $b=\pm 1$ olabilir. Eğer $b=1$ ise $16=\left(3a^2-11b^2\right)b$ olduğundan $16=3a^2-11$ yani $a=\pm 3$ bulunur. Eğer $b=-1$ ise $-16=3a^2-11$ yani $3a^2=-5$ bulunur. Bu ise olamaz. Dolayısıyla $16=\left(3a^2-11b^2\right)b$ nin çözümleri sadece $b=1$ ve $a=\pm 3$ olduğunda vardır. Bu ise

$$y=N(r)=\frac{a^2+11b^2}{4}=\frac{(\mp 3)^2+11.1^2}{4}=5$$

olmasını gerektirir. $x^2 = y^3 - 44 = 125 - 44 = 81$ ise $x = \pm 9$ bulunur. Çözümler $(x,y) = (\pm 9, 5)$ tir.

Örnek 4.3.28: $x^2 + 4 = y^3$ denkleminin tüm çözümlerini bulunuz.

Çözüm: x çift olsun. O halde y de çift olur. $y^3 \equiv 0 \pmod 8$ dir. $x \equiv 0 \pmod 4$ veya $x \equiv 2 \pmod 4$ olabilir. Eğer $x \equiv 0 \pmod 4$ ise, o zaman $x^2 + 4 \equiv 4 \pmod 8$ olur. Bu $y^3 \equiv 4 \pmod 8$ olmasını gerektirir. Halbuki $y^3 \equiv 0 \pmod 8$ dir. X tek olmak üzere $x = 2X$ ve $y = 2Y$ olsun. O zaman, $4X^2 + 4 = 8Y^3$ bulunur. Dolayısıyla, $X^2 + 1 = 2Y^3$ olur. Bu denklemi,

$$(X+i)(X-i) = 2Y^3 = (1+i)(1-i)Y^3$$

olarak yazabiliriz.

$X^2 + 1 \equiv 2 \pmod 4$ ve Y^3 ün tek olduğuna dikkat edelim. Böylece

$$Y^3 = \frac{(X+i)(X-i)}{(1+i)(1-i)} = \left(\frac{1+X}{2} + \frac{1-X}{2}i\right)\left(\frac{1+X}{2} - \frac{1-X}{2}i\right) = \left(\frac{1+X}{2}\right)^2 - \left(\frac{1-X}{2}\right)^2$$

olur. $\frac{1+X}{2} = a, \frac{1-X}{2} = b$ diyelim. X tek olduğundan a ve b rasyonel tamsayılardır. Bu durumda $Y^3 = a^2 + b^2$ olur. Burada $a + b = 1$, olduğundan $(a,b) = 1$ dir. Şimdi de $a+bi$ ve $a-bi$ nin aralarında asal olduğunu gösterelim. Birimden farklı bir d tamsayısının $d \mid a+bi$ ve $d \mid a-bi$ olacak biçimde var olduğunu kabul edelim. O zaman, $d \mid a+bi+a-bi$ den $d \mid 2a$ ve $d \mid a+bi-a+bi$ den $d \mid 2bi$ bulunur. $(a,b) = 1$ olduğundan, $d \mid 2$ olup d nin normu çift olmalıdır. $N(a+bi) = a^2 + b^2 = Y^3$ ve Y^3 tek olduğundan $d \mid a+bi$ olamaz. O halde $a+bi$ ve $a-bi$ aralarında asal ve $Q(i)$ tek türlü parçalanmalı bölge olduğundan, bu sayılar birer küptür.

$$a+bi=(s+ti)^3=s^3-3st^2+(3s^2t-t^3)i$$

alırsak,

$$a=s^3-3st^2 \text{ ve } b=3s^2t-t^3$$

bulunur.

$$a+b=s^3-3st^2+3s^2t-t^3 \text{ ve } a+b=1$$

olduğundan,

$$1=s^3-3st^2+3s^2t-t^3=(s-t)(s^2+4st+t^2)$$

olur.Yani, $s,t\in\mathbb{Z}$ olmak üzere $s-t=\pm1$ ve $s^2+4st+t^2=\pm1$ dir.

$(s-t)^2-(s^2+4st+t^2)=-6st$ olup $s-t=\pm1$, $s^2+4st+t^2=\pm1$ olduğu dikkate alınırsa $-6st=0$ veya $-6st=2$ olduğu görülür. $-6st=2$ olamayacağından $-6st=0$ dır. Dolayısıyla $s=0$ veya $t=0$ olmalıdır. Böylece $a=1$, $b=0$ veya $a=0$, $b=1$ bulunur. Bu durumda $X=\pm1$ olur. $\mathbb{Z}$ deki çözümler x çift olduğunda sadece $y=\pm2, x=2$ dir. x tek olsun. $y^3=(x+2i)(x-2i)$ yazalım. $d\mid x+2i$ ve $d\mid x-2i$ ise $d\mid x+2i-(x-2i)$ yani $d\mid 4i$ olur. Böylece $N(d)$ çift olur. Fakat X tek olduğundan $X+2i$ nin normu tektir. Dolayısıyla $d\nmid x+2i$ olur. Yani $x+2i$ ve $x-2i$ aralarında asaldır. O zaman $x+2i$ bir küptür.

$$x+2i=(q+ri)^3=q^3-3qr^2+(3q^2r-r^3)i$$

alalım. $2=3q^2r-r^3$ ise $r\mid 2$ ve $r=\pm1, r=\pm2$ olur. Böylece (q,r) nin mümkün değerleri sadece $(1,1),(-1,1),(1,-2),(-1,-2)$ olarak elde edilir. Buradan $x=\pm11$ bulunur. $y^3=x^2+4$ olduğundan $y=5$ tir. Sonuç olarak, $(x,y)=(\pm11,5)$ bulunur.

BÖLÜM 5. SONUÇLAR VE ÖNERİLER

Diophant denklemlerinin çözümüm sayılar teorisinin önemli konularından biridir. $x^3 + y^3 = z^3$ denkleminin çözümünün olmadığını göstermek oldukça zordur. Ancak tek türlü parçalanmalı bölgeler kullanılarak bazı Diophant denklemleri kolayca çözülebilir. Cebirsel sayılar teorisinin Diophant denklemlerinin çözümünde de önemli rol oynayacağı açıktır. Bu tez, daha ileri seviyede Diophant denklemlerinin çözümleri ile ilgilenmek isteyenler için bir başlangıç görevi görebilir. Bu konuyla detaylı bir şekilde ilgilenmek isteyenlere [4] numaralı kaynak tavsiye edilebilir.

KAYNAKLAR

[1] DAVID M. BURTON, Elemantary Number Theory Fourthod., McGrav-Hill. Companies, Inc, 1998.

[2] DON REDMO, Number Theory, an İntroduction. Marcel Dekker, 1996.

[3] H. STARK, An Introduction to Number Theory, M.I.T. Press, 1979.

[4] PAULO RIBENBOIM, Fermat' s Last Theorem for Amateurs, Springer Verlog, 1999.

[5] NIVEN, I., ZUCKERMAN, S., MONTGEMORY, H. L., An Introduction to the Theory of Numbers, fifty ed., John Willey, 1991.

ÖZGEÇMİŞ

Sündüz KELEŞ, 06.02.1979' da Sakarya' da doğdu. İlk, orta ve lise eğitimini Adapazarı' nda tamamladı.1996 yılında Kocaeli Üniversitesi Fen-Edebiyat Fakültesi Matematik Bölümü' nde lisans öğrenimine başladı. 2001 yılında bölümünden mezun oldu. Aynı yıl Adapazarı' nda öğretmenlik görevine başladı. Halen aynı okulda öğretmenlik yapmaktadır.