T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BAZI ÖZEL DİYOFANT DENKLEMLERİ VE ÇÖZÜMLERİ

YÜKSEK LİSANS TEZİ

Hilal Başak ÖZDEMİR

Enstitü Anabilim Dalı	**:**	**MATEMATİK**
Enstitü Bilim Dalı	**:**	**CEBİR VE SAYILAR TEORİSİ**
Tez Danışmanı	**:**	**Prof. Dr. Refik KESKİN**

Haziran 2015

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BAZI ÖZEL DİYOFANT DENKLEMLERİ VE ÇÖZÜMLERİ

YÜKSEK LİSANS TEZİ

Hilal Başak ÖZDEMİR

Enstitü Anabilim Dalı	:	MATEMATİK
Enstitü Bilim Dalı	:	CEBİR VE SAYILAR TEORİSİ

Bu tez 04/ 06 /2015 tarihinde aşağıdaki jüri tarafından oybirliği ile kabul edilmiştir.

Prof. Dr. Refik KESKİN	Prof. Dr. İbrahim OKUR	Doç. Dr. Yücel TÜRKER ULUTAŞ
Jüri Başkanı	Üye	Üye

BEYAN

Tez içindeki tüm verilerin akademik kurallar çerçevesinde tarafımdan elde edildiğini, görsel ve yazılı tüm bilgi ve sonuçların akademik ve etik kurallara uygun şekilde sunulduğunu, kullanılan verilerde herhangi bir tahrifat yapılmadığını, başkalarının eserlerinden yararlanılması durumunda bilimsel normlara uygun olarak atıfta bulunulduğunu, tezde yer alan verilerin bu üniversite veya başka bir üniversitede herhangi bir tez çalışmasında kullanılmadığını beyan ederim.

Hilal Başak ÖZDEMİR

04/06/2015

ÖNSÖZ

Tez çalışmamız boyunca üstün bilgi ve birikimleriyle beni yönlendiren, destek veren, yardımlarını ve zamanını esirgemeyen çok değerli danışman hocam Sayın Prof. Dr. Refik KESKİN'e sonsuz teşekkürlerimi sunarım. Hayatım boyunca desteğini hiç bir zaman esirgemeyen en değerli varlığım sevgili anneme; zor anlarımı paylaşan, bana daima güvenen ve inanan, beni bugünlere getiren aileme çok teşekkür ederim.

İÇİNDEKİLER

SİMGELER VE KISALTMALAR LİSTESİ

$a \mid b$	: a , b yi böler
$\Leftrightarrow$	: Ancak ve ancak
$>$	: Büyüktür
$\geq$	: Büyük eşittir
$\mathbb{Z}$	: Tam sayılar kümesi
$=$	: Eşittir
$\neq$	: Eşit değildir
$\Leftarrow, \Rightarrow$	: İse
$\equiv$	: Denktir.
$<$	: Küçüktür
$\leq$	: Küçük eşittir
$\lvert \; \rvert$	: Mutlak Değer
$\left(\frac{m}{p} \right)$	: Legendre sembolü
$a \nmid b$	: a , b yi bölmez
$\forall$	: Her
$\mathbb{R}$	: Reel sayılar kümesi
$a \approx b$	: a ilgili b
$a \not\approx b$	: a ilgili değil b

ÖZET

Anahtar Kelimeler :Diyofant Denklemleri, Tek türlü çarpanlara ayrılabilen bölge, Pisagor üçlüleri, Genelleştirilmiş Fibonacci ve Lucas Dizileri

Bu tez temel olarak altı bölümden ve bu bölümler de kendi içerisinde alt bölümlerden oluşmuştur. Birinci bölümde; sayılar teorisi ile ilgili temel tanımlar ve teoremler verildi.

İkinci bölümde; Kuadratik cisimler, Kuadratik tamsayılar, Kuadratik cisimlerde birimler ve asallarla ilgili tanımlar ve teoremler verildi. Ayrıca, tek türlü çarpanlara ayrılabilen bölge hakkında bilgi verildi. Tek türlü çarpanlara ayrılabilen bölge yardımıyla bazı Diyofant denklemleri çözüldü.

Üçüncü bölümde; Pisagor üçlüleri ile ilgili tanımlar ve teoremler verildi. Ayrıca, bazı özel Diyofant denklemlerinin çözümleri araştırıldı.

Dördüncü bölümde; Mordell denklemleri ile ilgili bazı tanımlar ve teoremler verildi.

Beşinci bölümde; Genelleştirilmiş Fibonacci ve Lucas dizileri yardımı ile bazı Diyofant denklemleri çözüldü.

Son olarak altıncı bölümde; Fibonacci ve Lucas dizileri yardımı ile bazı özel Diyofant denklemleri çözüldü.

SOME SPECIAL DIOPHANTINE EQUATIONS AND SOLUTIONS

SUMMARY

Keywords: Diophantine Equations, Unique factorization domain, Pytheporian triples, Generalized Fibonacci and Lucas Sequences

This thesis consist of fundamentally six chapters and these chapters consist of subchapters in itself. In the first chapter, fundamental definitions and theorems concerning number theory are given.

In the second chapter, quadratic fields, quadratic integers, definitions and theorems concerning units and primes in quadratic fields are given. Moreover, the information about unique factorization domain is given. Some Diophantine equations are solved with the help of unique factorization domain.

In the third chapter, definitions and theorems concerning Pytheporian triples are given. Moreover, solutions of some special Diophantine equations are investigated.

In the fourth chapter, definitions and theorems concerning Mordell equations are given.

In the fifth chapter, some Diophantine equations are solved with the help of Generalized Fibonacci and Lucas Sequences

Finally, in the sixth chapter, some special Diophantine equations are solved with the help of Fibonacci and Lucas Sequences.

BÖLÜM 1. GİRİŞ

1.1. Temel Tanım ve Teoremler

Tanım 1.1.1. $a,b \in \mathbb{Z}$ ve $a \neq 0$ olsun. Eğer $b = ac$ olacak şekilde $c \in \mathbb{Z}$ bulunabilirse a tamsayısı b tamsayısını böler denir ve bu $a \mid b$ ile gösterilir.

Önerme 1.1.2. (i) $\forall a \in \mathbb{Z}$ için $a \mid a$'dır.

(ii) $\forall a \in \mathbb{Z}$ için $a \mid 0$'dır.

(iii) $a \in \mathbb{Z}$ ve $\forall b \in \mathbb{Z}$ için $a \mid b \Leftrightarrow a = \pm 1$'dir.

(iv) $a,b \in \mathbb{Z}$ için $a \mid b$ ve $b \mid a \Leftrightarrow a = \pm b$'dir.

(v) $a,b,c \in \mathbb{Z}$ için $a \mid b$ ve $b \mid c \Rightarrow a \mid c$'dir.

(vi) $a,b,c \in \mathbb{Z}$ için $c \mid a$ ve $c \mid b \Rightarrow \forall x, y \in \mathbb{Z}$ için $c \mid ax + by$'dir [9].

Tanım 1.1.3. m,n sıfırdan farklı bir tamsayı olsun.

(i) $d \mid m$ ve $d \mid n$ olacak şekilde $d > 0$ tamsayısı varsa d'ye m ile n'nin bir ortak böleni denir.

(ii) d, m ile n'nin bir ortak böleni olsun. Eğer m ile n'nin her e ortak böleni için $e \mid d$ ise e'ye m ile n tamsayılarının en büyük ortak böleni denir ve bu $(m,n) = d$ ile gösterilir.

Teorem 1.1.4. Sıfırdan farklı herhangi iki sayının en büyük ortak böleni vardır ve $d = (m,n)$ ise $d = xm + yn$ olacak şekilde $x, y \in \mathbb{Z}$ bulunabilir. Özel olarak, $1 = (m,n)$ olduğunda $1 = xm + yn$ olacak şekilde $x, y \in \mathbb{Z}$ vardır [9].

Örnek 1.1.5. $a,b \in \mathbb{Z}$ için $xa + yb = 1$ olacak şekilde $x,y \in \mathbb{Z}$ bulunabilirse $(a,b) = 1$'dir.

Çözüm: $(a,b) = d$ olsun. Tanım 1.1.3 gereği $d \mid a$ ve $d \mid b$ olur. Buradan $x,y \in \mathbb{Z}$ için, $d \mid xa$ ve $d \mid yb$ yazılabilir. Böylece $d \mid xa + yb$ olur. O halde $xa + yb = 1$ olup $d > 0$ olduğundan $d \mid 1$ iken $d = 1$ bulunur.

Teorem 1.1.6. m ve n sıfırdan farklı iki tamsayı ve c herhangi bir tamsayı olsun.

$$(m,n) = 1 \text{ ve } m \mid nc \Rightarrow m \mid c$$

dir [9].

İspat: $(m,n) = 1$ olduğundan $1 = xm + yn$ olacak şekilde $\exists x, y \in \mathbb{Z}$ vardır. Son eşitliğin her iki yanı c ile çarpılırsa, $c = x(mc) + y(nc)$ bulunur. Böylece $m \mid mc$ ve $m \mid nc$ olup $m \mid x(mc) + y(nc)$ bulunur. Şu halde $c = x(mc) + y(nc)$ olduğundan $m \mid c$ elde edilir.

Teorem 1.1.7. (1). $(a,m) = (b,m) = 1$ ise $(ab,m) = 1$ ve en genelde $(a_1,m) = (a_2,m) = ... = (a_n,m) = 1$ ise $(a_1.a_2...a_n,m) = 1$ olur.

(2). $(b,c) = 1$ ise $(b^n,c^n) = 1$ ve $(b,c)^n = (b^n,c^n)$ dir. Ayrıca $(b,c) = 1$ ise n,m doğal sayılar olmak üzere $(b^n,c^m) = 1$'dir [9].

İspat: (1). $(a,m) = (b,m) = 1$ ise $1 = ax + my = br + ms$ olacak biçimde x,y,r,s tamsayıları vardır. Buradan $1 = (ax + my)(br + ms) = ab(xr) + m(bry + axs + mys)$ ve böylece $(ab,m) = 1$ elde edilir.

$(a_1,m) = (a_2,m) = ... = (a_n,m) = 1$ ise $(a_1.a_2...a_n,m) = 1$ olduğu tümevarımla gösterilir.

(2). $(b,c)=1$ ise (1)'den $(b^n,c)=1$'dir. Yine (1)'den $(b^n,c^n)=1$'dir. $g=(b,c)$ olsun. Dolayısıyla $\left(\left(\frac{b}{g}\right)^n,\left(\frac{c}{g}\right)^n\right)=1$ olduğu görülür. Burada $(b^n,c^n)=\left(g^n\left(\frac{b}{g}\right)^n,g^n\left(\frac{c}{g}\right)^n\right)=g^n\left(\left(\frac{b}{g}\right)^n,\left(\frac{c}{g}\right)^n\right)=g^n=(b,c)^n$ elde edilir.

Teorem 1.1.8. n ve m doğal sayılar olmak üzere $\left(a^n,b^m\right)=1$ ise $\left(a,b\right)=1$'dir [6].

Teorem 1.1.9. $a,b\in\mathbb{Z}$ olmak üzere $\left(a,mn\right)=1\Leftrightarrow\left(a,m\right)=\left(a,n\right)=1$'dir [9].

İspat: $\Rightarrow$:) $\left(a,mn\right)=1$ ve $\left(a,m\right)=d$ olsun. Buradan $d\mid a$, $d\mid m$ olur. Böylece $d\mid a$ ve $d\mid mn$ olup $d\mid\left(a,mn\right)$ bulunur. Öyleyse $\left(a,mn\right)=1$ olduğundan $d\mid 1$ olup $d=1$ dir. Benzer şekilde $\left(a,n\right)=1$ olduğu görülür.

$\Leftarrow$:) $\left(a,m\right)=\left(a,n\right)=1$ olsun. $\left(a,mn\right)=1$ olduğu kolayca görülebilir.

Teorem 1.1.10. n bir doğal sayı olmak üzere $a^n\mid b^n$ ise $a\mid b$'dir [6].

Teorem 1.1.11. a,b tamsayılar olmak üzere n sayısı a^2+b^2 biçiminde yazılabilir $\Leftrightarrow n$ sayısının asal çarpanlara ayrılışında (varsa) $4k+3$ biçimindeki asal bölenlerinin üsleri çifttir [5].

Teorem 1.1.12. $p>2$ asal sayı olmak üzere $p\equiv 3\left(\mathrm{mod}\,4\right)$ olsun. Eğer $p\mid a^2+b^2$ ise $p\mid a$ ve $p\mid b$'dir [5].

Tanım 1.1.13. $a,m\in\mathbb{Z}$ ve $(a,m)=1$ olmak üzere, $x^2\equiv a\left(\mathrm{mod}\,m\right)$ kongrüansının çözümü varsa a tamsayısına m moduna göre bir kuadratik rezidü denir. Eğer

$x^2 \equiv a \pmod{m}$ kongrüansının çözümü yoksa, a tamsayısına m moduna göre bir kuadratik nonrezidü denir.

Tanım 1.1.14(Legendre Sembolü). p tek asal sayı olsun. a bir kuadratik rezidü ise $\left(\frac{a}{p}\right)=1$, eğer bir kuadratik nonrezidü ise $\left(\frac{a}{p}\right)=-1$, eğer $p \mid a$ ise $\left(\frac{a}{p}\right)=0$ şeklinde gösterilir ve buna Legendre sembolü denir.

Teorem 1.1.15. p tek asal sayı olsun. Bu takdirde

1. $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$
2. $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$,
3. $a \equiv b \pmod{p}$ ise $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$,
4. $(a, p)=1$ ise $\left(\frac{a^2}{p}\right)=1, \left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$,
5. $\left(\frac{1}{p}\right)=1$, $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$
6. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

dir [7].

Sonuç 1.1.16. p tek asal sayı olmak üzere

1. $p \equiv \pm 1 \pmod{8}$ ise $\left(\frac{2}{p}\right)=1$'dir.
2. $p \equiv \pm 3 \pmod{8}$ ise $\left(\frac{2}{p}\right)=-1$'dir [8].

Sonuç 1.1.17. p tek asal sayı olmak üzere

1. $p \equiv 1,3 \pmod 8$ ise $\left(\frac{-2}{p}\right) = 1$ ’dir.
2. $p \equiv 5,7 \pmod 8$ ise $\left(\frac{-2}{p}\right) = -1$ ’dir [8].

Teorem 1.1.18(Fermat teoremi). p asal sayı olmak üzere $a \in \mathbb{Z}$ için $p \nmid a$ ise $a^{p-1} \equiv 1 \pmod p$ ’dir [9].

Teorem 1.1.19. a, b, m, n pozitif tamsayılar ve $(m,n) = 1$ olmak üzere $a^m = b^n$ ise $a = t^n$, $b = t^m$ olacak şekilde t pozitif tamsayısı vardır [6].

Teorem 1.1.20. n bir doğal sayı ise $1^3 + 2^3 + ... + n^3 = \left(\frac{n(n+1)}{2}\right)^2$ dir [8].

Teorem 1.1.21(Binom Açılımı). n bir doğal sayı olmak üzere, x, y reel sayılarsa $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$ ’dır [8].

Tanım 1.1.22. Ardışık iki terimi arasındaki farkın sabit olduğu dizilere aritmetik dizi denir.

Tanım 1.1.23. Farklı asalların çarpımı biçiminde yazılabilen sayılara karesiz sayı denir.

BÖLÜM 2. KUADRATİK CİSİMLER VE DENKLEM ÇÖZÜMLERİ

2.1. Kuadratik Cisimler ve Kuadratik Tamsayılar

Tanım 2.1.1. d tamkare olmayan sabit bir rasyonel sayı olsun. a,b herhangi rasyonel sayılar olmak üzere $a+b\sqrt{d}$ biçimindeki sayıların kümesi $Q\left(\sqrt{d}\right)$ ile gösterilir ve $Q\left(\sqrt{d}\right)$ kuadratik cisim olarak adlandırılır. Eğer $d>0$ ise, $Q\left(\sqrt{d}\right)$ cismine reel kuadratik cisim, eğer $d<0$ ise $Q\left(\sqrt{d}\right)$ cismine kompleks(sanal) kuadratik cisim denir. Kısaca,

$$Q\left(\sqrt{d}\right)=\left\{a+b\sqrt{d} : a \text{ ve } b \text{ rasyonel sayılar}\right\}$$

olarak tanımlanır.

Eğer $d<0$ ise $a+b\sqrt{d} = a+b\sqrt{-d}i$ olur.

Teorem 2.1.2. $a+b\sqrt{d} = c+e\sqrt{d} \Leftrightarrow a=c$ ve $b=e$ dir. Ayrıca, $a+b\sqrt{d} = 0 \Leftrightarrow a=b=0$ ’dır [2].

Teorem 2.1.3. α ve β, $Q\left(\sqrt{d}\right)$ cisminin elemanları ise; $\alpha+\beta$, $\alpha-\beta$, $\alpha\beta$ ve $\beta \neq 0$ olduğunda $\frac{\alpha}{\beta}$ elemanları da $Q\left(\sqrt{d}\right)$ cisminin elemanlarıdır [2].

Tanım 2.1.4. $\alpha = a+b\sqrt{d}$ olsun. $\bar{\alpha} = a-b\sqrt{d}$ ’ye α ’nın eşleniği denir.

Teorem 2.1.5. α ve β sayıları $Q\left(\sqrt{d}\right)$ cisminin iki elemanı ise, $\left(\overline{\overline{\alpha}}\right)=\alpha$, $\overline{\alpha+\beta}=\overline{\alpha}+\overline{\beta}$, $\overline{\alpha-\beta}=\overline{\alpha}-\overline{\beta}$, $\overline{\alpha\beta}=\overline{\alpha}\,\overline{\beta}$'dir. $\beta\neq 0$ ise $\overline{\beta}\neq 0$'dır ve $\overline{\left(\dfrac{\alpha}{\beta}\right)}=\dfrac{\overline{\alpha}}{\overline{\beta}}$'dir. Ayrıca $\alpha=\overline{\alpha}\Leftrightarrow\alpha$ bir rasyonel sayıdır [2].

Tanım 2.1.6. $\alpha\in Q\left(\sqrt{d}\right)$ bir irrasyonel sayı olsun. Ayrıca a,b,c tamsayılar ve $a>0$ olmak üzere, $(a,b,c)=1$ olsun. Bu durumda α , $ax^2+bx+c=0$ denklemini sağlıyorsa bu denkleme α sayısının tanımlayıcı denklemi denir.

Örnek 2.1.7. $\dfrac{3+\sqrt{17}}{4}$ sayısı $8x^2+12x-4=0$, $-10x^2+15x+5=0$, $-2x^2+3x+1=0$ denklemlerini sağlar. $\dfrac{3+\sqrt{17}}{4}$ sayısının tanımlayıcı denklemi $2x^2-3x-1=0$'dır.

Tanım 2.1.8. $\alpha\in Q\left(\sqrt{d}\right)$ olsun. α sayısının normu $N(\alpha)=\alpha\overline{\alpha}$ olarak tanımlanır.

Teorem 2.1.9. (i) $a\in Q$, $\alpha=a$ ise $N\left(a\right)=a^2$'dir.

(ii) Eğer $\alpha\in Q\left(\sqrt{d}\right)$ ise $N\left(\alpha\right)$ rasyoneldir.

(iii) $N\left(\alpha\right)=0\Leftrightarrow\alpha=0$'dır.

(iv) $\alpha\in Q\left(\sqrt{d}\right)$ ve $d<0$ ise $N\left(\alpha\right)\geq 0$'dır.

(v) Eğer $\alpha,\beta\in Q\left(\sqrt{d}\right)$ ise $N\left(\alpha\beta\right)=N\left(\alpha\right)N\left(\beta\right)$'dır. $\beta\neq 0$ ise $N\left(\dfrac{\alpha}{\beta}\right)=\dfrac{N\left(\alpha\right)}{N\left(\beta\right)}$'dır [2].

Tanım 2.1.10. $\alpha\in Q\left(\sqrt{d}\right)$ 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.

Bundan sonra $\mathbb{Z}$ 'nin elemanlarına rasyonel tamsayılar diyeceğiz.

Teorem 2.1.11. Eğer $d \equiv 2,3 \pmod 4$ ise $Q\left(\sqrt{d}\right)$ cisminin tamsayıları a,b rasyonel tamsayılar olmak üzere $a+b\sqrt{d}$ biçimindeki sayılardır. Eğer $d \equiv 1 \pmod 4$ ise $Q\left(\sqrt{d}\right)$ cisminin tamsayıları a ve b rasyonel tamsayılarının ikisi de çift veya ikisi de tek olmak üzere $\dfrac{a+b\sqrt{d}}{2}$ biçimindeki sayılardır [2].

Sonuç 2.1.12. $d \equiv 1 \pmod 4$ ise $Q\left(\sqrt{d}\right)$ cisminin bir α elemanı tamsayıdır $\Leftrightarrow$ a ve b rasyonel tamsayılar olmak üzere $\alpha = a + b\left(\dfrac{1+\sqrt{d}}{2}\right)$ olarak yazılabilir [2].

Örnek 2.1.13. $Q(i)$ cisminin tamsayılarını belirleyiniz.

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

Tanım 2.1.14. $\mathbb{Z}[i] = \{a+bi : a,b \in \mathbb{Z}\}$ kümesine Gauss Tamsayılar Halkası denir.

Örnek 2.1.15. $Q\left(\sqrt{7}i\right)$ cisminin tamsayılarını belirleyiniz.

Çözüm: $\sqrt{7}i = \sqrt{7i^2} = \sqrt{-7}$ olduğundan $d=-7\equiv 1 \pmod 4$ olduğundan $Q\left(\sqrt{7}i\right)$ cisminin tamsayılarının kümesi $\left\{a+b\left(\dfrac{1+\sqrt{7}i}{2}\right) : a,b \in \mathbb{Z}\right\}$ dir.

Teorem 2.1.16. α ve β $Q\left(\sqrt{d}\right)$ cisminde tamsayılar olsun. Bu takdirde $\alpha+\beta$, $\alpha-\beta$, $\alpha\beta$ da $Q\left(\sqrt{d}\right)$ cisminde tamsayılardır [2].

Tanım 2.1.17. α, $Q\left(\sqrt{d}\right)$ cisminde bir tamsayı olsun. Bu takdirde $N(\alpha)$ bir rasyonel tamsayıdır.

2.2. Kuadratik Cisimlerde Birimler ve Asallar

Tanım 2.2.1. $\alpha \neq 0$ ve $\alpha, \beta \in Q\left(\sqrt{d}\right)$ tamsayılar olmak üzere $\beta = \alpha\lambda$ olacak biçimde $Q\left(\sqrt{d}\right)$ cisminde bir λ 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.

$\alpha \mid \beta$ olduğunda $\alpha \neq 0$ olmak üzere α, β'nın $Q\left(\sqrt{d}\right)$ cisminde tamsayılar olduğunu kabul edeceğiz.

Teorem 2.2.2. $\alpha \mid \beta$ ve $\alpha \mid \lambda$ ise $\overline{\alpha} \mid \overline{\beta}$ ve ε, δ $Q\left(\sqrt{d}\right)$ cisminde herhangi tamsayılar olmak üzere $\alpha \mid (\beta\delta + \lambda\varepsilon)$ dur. Özel olarak, $\varepsilon = \delta = 1$ alınırsa $\alpha \mid \beta + \lambda$; $\delta = 1$, $\varepsilon = -1$ alınırsa $\alpha \mid \beta - \lambda$; $\varepsilon = 0$ alınırsa, $\alpha \mid \beta\delta$ dır. Eğer $\alpha \mid \beta$ ve $\beta \mid \lambda$ ise o zaman $\alpha \mid \gamma$ dır [2].

Tanım 2.2.3. $Q\left(\sqrt{d}\right)$ cisminde $\varepsilon \mid 1$ özelliğindeki bir ε tamsayısına birim denir. Özellikle 1 ve -1 $Q\left(\sqrt{d}\right)$ cisminde her zaman birimdirler**.**

Uyarı: ε sayısını bir tamsayı olarak sınırlandırmak gereklidir. Örneğin, $N\left(\frac{5}{13} + \frac{12}{13}\sqrt{-1}\right) = N\left(\frac{5}{13} + \frac{12}{13}i\right) = 1$ dir. Fakat $\frac{5}{13} + \frac{12}{13}i$, Teorem 2.1.11'e göre

$Q(i)$ cisminde bir tamsayı değildir. Dolayısıyla birim değildir.

Teorem 2.2.4. $Q\left(\sqrt{d}\right)$ cisminde ε birimdir $\Leftrightarrow N(\varepsilon) = \pm 1$'dir [2].

Teorem 2.2.5. $d<0$, $d\neq -1$, $d\neq -3$ ise $Q\left(\sqrt{d}\right)$ cisminin birimleri ± 1 olmak üzere iki tanedir. Ayrıca $Q(i)$ cisminin birimleri ± 1, $\pm\sqrt{-1}$ olmak üzere dört tane; $Q(\sqrt{3}i)$ cisminin ± 1, $\pm\left(-1+\sqrt{3}i\right)/2$, $\pm\left(-1-\sqrt{3}i\right)/2$ olmak üzere altı tane birimi vardır. Eğer $d>0$ ise $Q\left(\sqrt{d}\right)$ cismi sonsuz çoklukta birime sahiptir [2].

Tanım 2.2.6. ε, $Q\left(\sqrt{d}\right)$ cisminde bir birim olsun. $Q\left(\sqrt{d}\right)$ cisminde α ve β tamsayıları $\alpha=\beta\varepsilon$ olacak biçimde varsa, α ’ya β nın ilgilisidir veya α ile β ilgilidir denir. Bu durum $\alpha\approx\beta$ ile gösterilir. Eğer α ile β ilgili değil ise bu durum $\alpha\not\approx\beta$ ile gösterilir.

α , β ’nın ilgilisidir $\Leftrightarrow$ α/β bir birimdir.

Tanım 2.2.7. $\alpha,\beta,\gamma\in Q\left(\sqrt{d}\right)$ cisminde tamsayılar olsun. $\alpha\neq 0$ olsun ve α birim olmasın. Eğer $\alpha=\beta\gamma$ iken β ya da γ elemanlarından biri birim oluyorsa α ’ya indirgenemez eleman denir.

Tanım 2.2.8. $\alpha,\beta,\lambda\in Q\left(\sqrt{d}\right)$ cisminde tamsayılar olsun. $\alpha\neq 0$ olsun ve α birim olmasın. Eğer $\alpha\mid\lambda\beta$ iken $\alpha\mid\lambda$ veya $\alpha\mid\beta$ ise α ’ya asal eleman denir.

Bundan sonra $\mathbb{Z}$ ’nin asallarına rasyonel asal diyeceğiz.

2.3. Tek Türlü Çarpanlara Ayrılabilen Bölgeler

Tanım 2.3.1. $Q\left(\sqrt{d}\right)$ cismi aşağıdaki özellikleri sağlıyorsa, $Q\left(\sqrt{d}\right)$ cismine tek türlü çarpanlara ayrılabilen bölge veya tek çarpanlama bölgesi denir.

1) α sıfırdan farklı birim olmayan bir tamsayı ise $\alpha=\alpha_1\alpha_2...\alpha_r$ olacak biçimde indirgenemez $\alpha_1,\alpha_2,...,\alpha_r$ tamsayıları vardır.

2) $1 \le i \le r$ için $\alpha_i \in Q\left(\sqrt{d}\right)$, $1 \le j \le s$ için $\beta_j \in Q\left(\sqrt{d}\right)$ olmak üzere α_i ve β_j ler indirgenemez elemanlar olsun. Ayrıca ε birim olmak üzere, $\alpha_1\alpha_2...\alpha_r = \varepsilon\beta_1\beta_2...\beta_s$ olsun. Bu durumda $r = s$ dir ve $\sigma:\{1,...,r\} \to \{1,...,r\}$ bir permütasyon (birebir örten dönüşüm) olmak üzere, α_i tamsayısı $\beta_{\sigma(i)}$ tamsayısı ile ilgilidir.

Örnek 2.3.2. $Q\left(\sqrt{5}i\right)$ cismi tek türlü çarpanlara ayrılabilen bölge değildir.

Çözüm: $\sqrt{5}i = \sqrt{5i^2} = \sqrt{-5}$ olduğundan $-5 \equiv 3\left(\bmod 4\right)$ olur. Böylece Teorem 2.1.11'e göre $Q\left(\sqrt{5}i\right)$ cisminin tamsayıları a,b rasyonel tamsayılar olmak üzere $a+b\sqrt{5}i$ biçimindedir. O halde $2+\sqrt{5}i, 2-\sqrt{5}i \in Q\left(\sqrt{5}i\right)$ tamsayıları için $\left(2+\sqrt{5}i\right)\left(2-\sqrt{5}i\right) = 9 = 3.3$ dür. $2-\sqrt{5}i$ indirgenemez olmasın. O halde $2-\sqrt{5}i = \left(a+b\sqrt{5}i\right)\left(c+e\sqrt{5}i\right)$ olacak biçimde birimden farklı $\left(a+b\sqrt{5}i\right),\left(c+e\sqrt{5}i\right) \in Q\left(\sqrt{5}i\right)$ tamsayıları vardır.

$2-\sqrt{5}i = \left(a+b\sqrt{5}i\right)\left(c+e\sqrt{5}i\right)$ eşitliğinin her iki tarafının normu alınırsa, $9 = \left(a^2+5b^2\right)\left(c^2+5e^2\right)$ olur. $a+b\sqrt{5}i, c+e\sqrt{5}i$ birimden farklı olduklarından $a^2+5b^2 = 3, c^2+5e^2 = 3$ olmalıdır. Fakat iki eşitliğinde çözümü yoktur. Gerçekten, $a^2+5b^2 = 3$ olsun. $a^2 \equiv 3\left(\bmod 5\right)$ olur ki bu denkliği sağlayacak şekilde $a \in \mathbb{Z}$ yoktur. Öyleyse $2-\sqrt{5}i$ indirgenemezdir. Benzer şekilde $2+\sqrt{5}i$ de indirgenemezdir.

Kabul edelim ki 3 indirgenemez olmasın. O halde $3 = \left(a+b\sqrt{5}i\right)\left(c+e\sqrt{5}i\right)$ olacak biçimde birimden farklı $\left(a+b\sqrt{5}i\right),\left(c+e\sqrt{5}i\right) \in Q\left(\sqrt{5}i\right)$ tamsayıları vardır. Her iki tarafın normunu alırsak $9 = \left(a^2+5b^2\right)\left(c^2+5e^2\right)$ olur. O halde yukarıdakine benzer şekilde 3 de indirgenemezdir.

Sonuç olarak, $2+\sqrt{5}i, 2-\sqrt{5}i, 3$ indirgenemez elemanlardır.

Şimdi kabul edelim ki $3 \approx 2+\sqrt{5}i$ olsun. Bu durumda $3 \mid 2+\sqrt{5}i$ olur. Buradan Tanım 2.2.1'den $2+\sqrt{5}i = 3\left(a+b\sqrt{5}i\right)$ olacak şekilde $a+b\sqrt{5}i$ tamsayısı vardır. Böylece Teorem 2.1.2'ye göre $2=3a, 1=3b$ elde edilir. Bu ise $a,b \in \mathbb{Z}$ olması ile çelişir. Dolayısıyla $3 \not\approx 2+\sqrt{5}i$ dir. Öyleyse $Q\left(\sqrt{5}i\right)$ tek türlü çarpanlara ayrılabilen bölge değildir.

Tanım 2.3.3. (i) α, β sıfırdan farklı $Q\left(\sqrt{d}\right)$ cisminin tamsayıları olsun. $\lambda \neq 0$, $\lambda \mid \alpha$, $\lambda \mid \beta$ olacak şekilde $\lambda \in Q\left(\sqrt{d}\right)$ mevcut ise bu λ elemanına α ile β'nın bir ortak böleni denir.

(ii) λ, α ile β'nın ortak böleni olsun. Eğer α ile β'nın her γ ortak böleni için $\gamma \mid \lambda$ ise λ'ya α ile β tamsayılarının bir en büyük ortak böleni denir ve bu $(\alpha, \beta) = \lambda$ ile gösterilir.

Tanım 2.3.4. α ve $\beta \in Q\left(\sqrt{d}\right)$ olsun. α ile β sayılarının birimden başka ortak böleni yoksa α ile β aralarında asaldır denir. Bu durum $(\alpha, \beta) = 1$ ile gösterilir.

Teorem 2.3.5. $Q\left(\sqrt{d}\right)$ tek türlü çarpanlara ayrılabilen bölgedir $\Leftrightarrow$ $Q\left(\sqrt{d}\right)$ cisminin indirgenemez her elemanı asal elemandır [6] .

Teorem 2.3.6. $Q\left(\sqrt{d}\right)$ tek türlü çarpanlara ayrılabilen bölge olsun. α, β $Q\left(\sqrt{d}\right)$ cisminin tamsayıları olmak üzere α ve β tamsayılarının birimden başka ortak böleni olmasın. Eğer n pozitif tamsayısı için $\alpha\beta = \varepsilon\lambda^n$ eşitliğini sağlayan bir $\lambda \in Q\left(\sqrt{d}\right)$ tamsayısı varsa, $\alpha = \varepsilon_1\lambda_1^{\,n}$, $\beta = \varepsilon_2\lambda_2^{\,n}$ olacak biçimde $\varepsilon_1, \varepsilon_2$ birimleri ve $\lambda_1, \lambda_2 \in Q\left(\sqrt{d}\right)$ tamsayıları vardır [6].

Tanım 2.3.7. $K = Q\left(\sqrt{d}\right)$ kuadratik cisminin tamsayılarının halkası A_k 'ya, "$A_k^* = A_k - \{0\}$ olmak üzere her $(a,b) \in A_k \times A_k^*$ için $a = bq + r$ ve $|N(r)| < |N(b)|$ şartını sağlayan $(q,r) \in A_k^2 = A_k \times A_k$ vardır." özelliğini sağlıyorsa bir Öklid bölgesi denir.

Teorem 2.3.8. A_k bir öklid bölgesi ise bir tek türlü çarpanlara ayrılabilen bölgedir [4].

Teorem 2.3.9. $K = Q\left(\sqrt{d}\right)$ cisminin tamsayılarının halkası A_k $d = -11, -7, -3, -2, -1, 2, 3, 5$ ve 13 için bir Öklid bölgesidir [4].

2.4. Tek Türlü Çarpanlara Ayrılabilen Bölgeler Yardımıyla Denklem Çözümleri

Örnek 2.4.1. $x^5 - y^2 = 1$ denklemini çözünüz.

Çözüm: $x^5 - y^2 = 1$ olacak biçimde x ve y tamsayıları mevcut olsun. $y^2 \equiv 0,1 \pmod 4$ olduğundan $x^5 \equiv 1 \pmod 4$ ya da $x^5 \equiv 2 \pmod 4$ olur. Dolayısıyla x tektir. Gerçekten , x çift olsaydı $x^5 \equiv 0 \pmod 4$ olup çelişki elde edilirdi.

Denklemi $\mathbb{Z}[i]$ Gauss tamsayılar halkasında çarpanlara ayırırsak, $x^5 = (y+i)(y-i)$ olarak yazabiliriz. Burada $(y+i, y-i) = 1$ dir. Gerçekten, $\alpha \mid y+i$, $\alpha \mid y-i$ olsun. Bu durumda $\alpha \mid 2i$ ve böylece $N(\alpha) \mid 4$ olur. $\alpha \mid y+i$ olduğundan $N(\alpha) \mid (y+i)(y-i)$, yani $N(\alpha) \mid x^5$ 'dir. $N(\alpha) \mid 4$ ve $N(\alpha) \mid x^5$ olduğundan $N(\alpha) \mid \left(4, x^5\right)$ olur. x tek olduğundan $\left(4, x^5\right) = 1$ dir. Böylece $N(\alpha) \mid 1$ olup $N(\alpha) = 1$ dir. Teorem 2.2.4'e göre α birimdir.

$Q(i)$ cisminin tamsayılar halkası $\mathbb{Z}[i]$, Teorem 2.3.8 ve Teorem 2.3.9'a göre tek türlü çarpanlara ayrılabilen bölgedir. O halde Teorem 2.3.6'ya göre $y + i = \varepsilon u^5$

olacak şekilde $\varepsilon \in \mathbb{Z}[i]$ birimi ve $u \in \mathbb{Z}[i]$ vardır. Fakat, $\mathbb{Z}[i]$'nin birimleri $\pm 1, \pm i$ olup $(-1) = (-1)^5, 1 = 1^5, i = i^5, -i = (-i)^5$ olduğundan $(y+i) = (a+ib)^5, a, b \in \mathbb{Z}$ olarak yazabiliriz. Buradan Teorem 1.1.21'e göre

$$(a+ib)^5 = \binom{5}{0} a^0 (ib)^5 + \binom{5}{1} a^1 (ib)^4 + \binom{5}{2} a^2 (ib)^3 + \binom{5}{3} a^3 (ib)^2 + \binom{5}{4} a^4 (ib)^1 + \binom{5}{5} a^5 (ib)^0$$

$$= ib^5 + 5ab^4 - 10a^2b^3 i - 10a^3b^2 + 5a^4bi + a^5 = \left(a^5 - 10a^3b^2 + 5ab^4\right) + i\left(b^5 - 10a^2b^3 + 5a^4b\right)$$

elde edilir. Bu durumda $y + i = \left(a^5 - 10a^3b^2 + 5ab^4\right) + i\left(b^5 - 10a^2b^3 + 5a^4b\right)$ olur. Reel ve sanal kısımları eşitlersek $y = a^5 - 10a^3b^2 + 5ab^4$, $1 = b^5 - 10a^2b^3 + 5a^4b$ yazılır. $1 = b\left(b^4 - 10a^2b^2 + 5a^4\right)$ olduğundan $b \mid 1$ olup $b = \pm 1$'dir.

$b = 1$ için $5a^4 - 10a^2 + 1 = 1$ olur. Buradan $a^2 = 0$ olduğu görülür. O halde $a = 0$'dır. Böylece $y = 0$ bulunur. Burada $x^5 - y^2 = 1$ olduğundan $x = 1$ dir. $b = -1$ için $-1 + 10a^2 - 5a^4 = 1$ olur. Buradan $5a^2\left(2 - a^2\right) = 2$ olur. Fakat, bu eşitliği sağlayan $a \in \mathbb{Z}$ olmadığından çözüm yoktur. Sonuç olarak, $(x, y) = (1, 0)$'dır.

Örnek 2.4.2. $y^2 = x^3 - 1$ denklemini çözünüz.

Çözüm: $y^2 = x^3 - 1$ olacak biçimde x ve y tamsayıları mevcut olsun. x tektir. Aksi takdirde yani x çift olursa $x^3 \equiv 0 \pmod 4$ olur. Bu ise $y^2 = x^3 - 1$ olduğundan $y^2 \equiv 3 \pmod 4$ olmasını gerektirir. Halbuki $y^2 \equiv 0, 1 \pmod 4$ olduğu açıktır. Denklemi $\mathbb{Z}[i]$ Gauss tamsayılar halkasında çarpanlarına ayırırsak $(y+i)(y-i) = x^3$ olur. Burada $(y+i, y-i) = 1$'dir. Gerçekten, kabul edelim ki bir p asalı $\mathbb{Z}[i]$'de $y+i$ ve $y-i$ sayılarını bölsün. Yani, p asal olmak üzere $p \mid y+i$ ve $p \mid y-i$ olsun. Buradan $p \mid y+i-(y-i)$ olup $p \mid 2i$ dir. Bu ise $N(p) \mid 4$ olmasını gerektirir. p birim olamayacağından $N(p) = 2$ ya da $N(p) = 4$'tür. $p \mid y+i$ olduğundan

$N(p) \mid N(y+i)$, yani $N(p) \mid y^2+1$ ve böylece $N(p) \mid x^3$ olur. Fakat, bu x tek olduğundan $N(p)=2$ ya da $N(p)=4$ olması ile çelişir. Bu nedenle $y+i$ ve $y-i$ aralarında asaldır. Yani, $(y+i, y-i)=1$ olur.

$Q(i)$ cisminin tamsayılar halkası $\mathbb{Z}[i]$ Teorem 2.3.8 ve Teorem 2.3.9'a göre tek türlü çarpanlara ayrılabilen bölgedir. O halde Teorem 2.3.6'ya göre $(y+i)=\varepsilon(u+iv)^3$ olacak şekilde ε birimi ve $u+iv \in \mathbb{Z}[i]$ vardır. Ancak, $\mathbb{Z}[i]$'nin birimleri ± 1, $\pm i$ olup $1=1^3, -1=(-1)^3, i=(-i)^3, -i=i^3$ olduğundan $y+i=(a+bi)^3, a,b \in \mathbb{Z}$ olarak yazabiliriz. Böylece Teorem 1.1.21'e göre

$$
\begin{aligned}
(a+bi)^3 &= \binom{3}{0} a^0 (bi)^3 + \binom{3}{1} a^1 (bi)^2 + \binom{3}{2} a^2 (bi)^1 + \binom{3}{3} a^3 (bi)^0 \\
&= a^3 - 3ab^2 + i\left(3a^2b - b^3\right)
\end{aligned}
$$

elde edilir. Bu durumda $y+i = a^3-3ab^2 + i\left(3a^2b-b^3\right)$ olur. Reel ve sanal kısımları eşitlersek $y=a^3-3ab^2$ ve $1=3a^2b-b^3$ yazılır. $1=b\left(3a^2-b^2\right)$ olduğundan $b \mid 1$ olup $b=\pm 1$ dir. $b=1$ için $1=3a^2-1$ dir. Buradan $2=3a^2$ olur. Fakat, bu eşitliği sağlayan $a \in \mathbb{Z}$ yoktur. $b=-1$ için $-1=3a^2-1$ dir. Buradan $0=3a^2$ olup $a=0$'dır. Böylece $y=0$ bulunur. Burada $y^2=x^3-1$ olduğundan $x=1$ dir. Sonuç olarak, $(x,y)=(1,0)$ bulunur.

Örnek 2.4.3. $y^2=x^3-11$ denklemini çözünüz.

Çözüm: $y^2=x^3-11$ olacak biçimde x ve y tamsayıları mevcut olsun. x tektir. Aksi takdirde x çift olursa, $x^3 \equiv 0 \pmod 8$ olur. Bu ise $y^2=x^3-11$ olduğundan $y^2 \equiv 5 \pmod 8$ olmasını gerektirir. Halbuki $y^2 \equiv 0,1,4 \pmod 8$ olduğu açıktır. Denklemi $\left(y+i\sqrt{11}\right)\left(y-i\sqrt{11}\right)=x^3$ olarak yazabiliriz. Burada $\left(y+i\sqrt{11}, y-i\sqrt{11}\right)=1$'dir. Gerçekten, $d \mid y+i\sqrt{11}$ ve $d \mid y-i\sqrt{11}$ olsun. Buradan,

$d \mid y+i\sqrt{11}-\left(y-i\sqrt{11}\right)=2i\sqrt{11}$ olup $N\left(d\right)\mid 44$ olur. $d \mid y+i\sqrt{11}$ olduğundan $N\left(d\right)\mid\left(y+i\sqrt{11}\right)\left(y-i\sqrt{11}\right)=x^3$ olur. Ayrıca $11 \nmid x$ dir. Aksi takdirde $11 \mid x$ olursa $y^2 = x^3 - 11$ olduğundan $11 \mid y$ olur. Bu ise $11^2 \mid x^3 - y^2$ olmasını gerektirir. Böylece $x^3 - y^2 = 11$ olduğundan $11^2 \mid 11$ bulunur. Bu ise mümkün değildir.

$N\left(d\right)\mid 44$ ve $N\left(d\right)\mid x^3$ olduğundan $N\left(d\right)\mid\left(44, x^3\right)$, yani $N\left(d\right)\mid\left(4.11, x^3\right)$ elde edilir. $11 \nmid x$ ve x tek olduğundan $\left(44, x^3\right)=1$'dir. Bu ise $N(d)\mid 1$ olmasını gerektirir. Yani $N\left(d\right)=1$ olup d birimdir.

$Q\left(\sqrt{-11}\right)$ cisminin tamsayılarının halkası $A_k = \mathbb{Z}\left(\frac{1}{2}\left(1+i\sqrt{11}\right)\right)$, Teorem 2.3.8 ve Teorem 2.3.9'a göre tek türlü çarpanlara ayrılabilen bölgedir. O halde Teorem 2.3.6'ya göre $y+i\sqrt{11}=\varepsilon\left(\frac{a+ib\sqrt{11}}{2}\right)^3$ olacak şekilde aynı türden a ve b tamsayıları , ε birimi vardır. Teorem 2.2.5'e göre $Q\left(\sqrt{-11}\right)$ cisminin birimleri ± 1 dir. $1=1^3, -1=\left(-1\right)^3$ olduğundan $y+i\sqrt{11}=\left(\frac{c+ie\sqrt{11}}{2}\right)^3$, c ve d aynı türden tamsayılar olmak üzere yazılabilir. Buradan Teorem 1.1.21 kullanılarak $y+i\sqrt{11}=\frac{c^3-33cd^2}{8}+i\left(\frac{3c^2d-11d^3}{8}\right)$ elde edilir. Reel ve sanal kısımları eşitlersek $8y = c^3 - 33cd^2$ ve $8 = 3c^2d - 11d^3$ olur. Böylece $8 = d\left(3c^2 - 11d^2\right)$ olduğundan $d \mid 8$ elde edilir. Bu ise $d = \pm 1, \pm 2, \pm 4, \pm 8$ olmasını gerektirir.

$d = 1$ ise $8 = 3c^2 - 11$ olup $19 = 3c^2$ olur. Fakat, bu eşitliği sağlayan $c \in \mathbb{Z}$ yoktur. $d = -1$ ise $-8 = 3c^2 - 11$ olur. Buradan $c^2 = 1$ olup $c = \pm 1$ elde edilir. $d = 2$ için $8 = 6c^2 - 88$ olur. Buradan $c^2 = 16$ olup $c = \pm 4$ elde edilir. $d = -2$ için $8 = -6c^2 + 88$ olup $-80 = -6c^2$ dir. Fakat, bu eşitliği sağlayan $c \in \mathbb{Z}$ yoktur. $d = 4$ için $8 = 12c^2 - 704$ olup $712 = 12c^2$ dir. Fakat, bu eşitliği sağlayan $c \in \mathbb{Z}$ yoktur.

$d=-4$ için $8=-12c^2+704$ olup $696=12c^2$ dir. Fakat, bu eşitliği sağlayan $c\in\mathbb{Z}$ yoktur. $d=8$ için $8=24c^2-5632$ olup $705=3c^2$ dir. Fakat, bu eşitliği sağlayan $c\in\mathbb{Z}$ yoktur. $d=-8$ için $8=-24c^2+5632$ olup $703=3c^2$ olur. Ancak, bu eşitliği sağlayan $c\in\mathbb{Z}$ yoktur.

$d=-1, c=1$ için $8y=c\left(c^2-33d^2\right)$ olduğundan $8y=1(1-33)$'dir. Buradan $8y=-32$ olduğundan $y=-4$ olur. Böylece $y^2=x^3-11$ olduğundan $x=3$ bulunur. $d=-1, c=-1$ için $8y=-1(1-33)$ olduğundan $8y=32$ dir. Buradan $y=4$ olur. Böylece $y^2=x^3-11$ olduğundan $x=3$ bulunur. $d=2, c=4$ için $2y=16-132$ olup $y=-58$ dir. Böylece $y^2=x^3-11$ olduğundan $x=15$ bulunur. $d=2, c=-4$ için $-2y=-116$ olup $y=58$ dir. Böylece $y^2=x^3-11$ olduğundan $x=15$ dir. Sonuç olarak, çözümler $(3,4),(3,-4),(15,-58),(15,58)$ olarak bulunur.

Örnek 2.4.4. $y^2=x^3-2$ denklemini çözünüz.

Çözüm: $y^2=x^3-2$ olacak biçimde x ve y tamsayıları mevcut olsun. x tektir. Aksi takdirde x çift olursa, $x^3\equiv 0 \pmod 4$ olur. Buradan $y^2=x^3-2$ olduğundan $y^2\equiv 2 \pmod 4$ olur. Halbuki $y^2\equiv 0,1 \pmod 4$ olduğu açıktır. Denklemi $\left(y+i\sqrt{2}\right)\left(y-i\sqrt{2}\right)=x^3$ olarak yazabiliriz. Burada $\left(y+i\sqrt{2}, y-i\sqrt{2}\right)=1$ dir. Gerçekten, $d \mid y+i\sqrt{2}$ ve $d \mid y-i\sqrt{2}$ olsun. Buradan $d \mid y+i\sqrt{2}-\left(y-i\sqrt{2}\right)=2i\sqrt{2}$ olur. Bu ise $N(d)|8$ olmasını gerektirir. $N(d)\neq 1$ ise $N(d)$ çift olur. Fakat, $d \mid x^3$ olduğundan $N(d) \mid x^6$ olur. Bu durum x'in tek olması ile çelişir. O halde $N(d)=1$ dir. Yani d birimdir.

$Q\left(\sqrt{-2}\right)$ cisminin tamsayılarının halkası $\mathbb{Z}\left[i\sqrt{2}\right]=\mathbb{Z}\left[\sqrt{-2}\right]$ Teorem 2.3.8 ve Teorem 2.3.9'a göre tek türlü çarpanlara ayrılabilen bölgedir. O halde Teorem 2.3.6'ya göre $y+i\sqrt{2}=\varepsilon\left(u+iv\sqrt{2}\right)^3$ olacak şekilde ε birimi ve

$u+iv\sqrt{2}\in\mathbb{Z}\left[i\sqrt{2}\right]$ vardır. Teorem 2.2.5'e göre $\mathbb{Z}\left[i\sqrt{2}\right]$ halkasının birimleri ± 1 dir. $1=1^3,-1=(-1)^3$ olduğundan $a,b\in\mathbb{Z}$ olmak üzere $y+i\sqrt{2}=\left(a+ib\sqrt{2}\right)^3$ olarak yazabiliriz. Teorem 1.1.21 kullanılarak $y+i\sqrt{2}=a^3-6ab^2+\left(3a^2b-2b^3\right)i\sqrt{2}$ elde edilir. Reel ve sanal kısımları eşitlersek $y=a^3-6ab^2$ ve $1=3a^2b-2b^3$ bulunur. $1=b\left(3a^2-2b^2\right)$ olduğundan $b\,|\,1$'dir. Yani $b=\pm 1$'dir. $b=1$ için $1=3a^2-2$ olur. Böylece $a^2=1$ olup $a=\pm 1$ dir. $b=-1$ için $1=-3a^2+2$ olur. Buradan $-1=-3a^2$ bulunur. Fakat, bu eşitliği sağlayan $a\in\mathbb{Z}$ yoktur. $b=1,a=1$ için $y=a^3-6ab^2$ olduğundan $y=-5$'dir. Böylece $y^2=x^3-2$ olduğundan $x=3$ bulunur. $b=1,a=-1$ için $y=a^3-6ab^2$ olduğundan $y=5$ bulunur. Böylece $y^2=x^3-2$ olduğundan $x=3$ bulunur. Sonuç olarak, $(x,y)=(3,\pm 5)$ elde edilir.

Örnek 2.4.5. $x^2+x+2=y^3$ denklemini çözünüz.

Çözüm: $x^2+x+2=y^3$ olan x ve y tamsayıları mevcut olsun. Denklemi $\frac{(2x+1)+\sqrt{-7}}{2}.\frac{(2x+1)-\sqrt{-7}}{2}=y^3$ olarak yazabiliriz. Burada $\left(\frac{2x+1+\sqrt{-7}}{2},\frac{2x+1-\sqrt{-7}}{2}\right)=1$'dir. Gerçekten, $d\,|\,\frac{2x+1+\sqrt{-7}}{2},d\,|\,\frac{2x+1-\sqrt{-7}}{2}$ olsun. Buradan $d\,|\,\frac{2x+1+\sqrt{-7}}{2}-\left(\frac{2x+1-\sqrt{-7}}{2}\right)=\sqrt{-7}$ olur. Böylece $N(d)\,|\,N\left(\sqrt{-7}\right)$ olup $d^2\,|\,7$'dir. Şu halde $d^2=1$ olup $d=\pm 1$'dir. Yani d birimdir.

$Q\left(\sqrt{d}\right)$ cisminin tamsayılarının halkası $\mathrm{A}_k=\mathbb{Z}\left(\frac{1}{2}\left(1+i\sqrt{7}\right)\right)$ Teorem 2.3.8 ve Teorem 2.3.9'a göre tek türlü çarpanlara ayrılabilen bölgedir. O halde Teorem 2.3.6'ya göre $\frac{2x+1+\sqrt{-7}}{2}=\varepsilon\left(\frac{a+b\sqrt{-7}}{2}\right)^3$ olacak şekilde aynı türden a ve b

tamsayıları vardır. Teorem 2.2.5'e göre $Q\left(\sqrt{-7}\right)$ cisminin birimleri ± 1'dir. $1=1^3, -1=\left(-1\right)^3$ olduğundan $\dfrac{2x+1+\sqrt{-7}}{2}=\left(\dfrac{c+d\sqrt{-7}}{2}\right)^3$ olacak şekilde aynı türden c ve d tamsayıları vardır. Bu eşitliğin her iki tarafının normunu alırsak $y^3=\left(\dfrac{2x+1+\sqrt{-7}}{2}\right)\left(\dfrac{2x+1-\sqrt{-7}}{2}\right)=\left(\dfrac{c^2+7d^2}{4}\right)^3$ olur. Buradan $y=\dfrac{c^2+7d^2}{4}$ olduğu görülür. $\dfrac{2x+1+\sqrt{-7}}{2}=\left(\dfrac{c+e\sqrt{-7}}{2}\right)^3$ eşitliğinde Teorem 1.1.21 kullanılarak $\dfrac{2x+1+\sqrt{-7}}{2}=\dfrac{a^3+21ab^2+\left(3a^2b-7b^3\right)\sqrt{-7}}{8}$ bulunur. Böylece $4=3a^2b-7b^3$ olur. $b\left(3a^2-7b^2\right)=4$ olduğundan $b\,|\,4$ olup $b=\pm 1,\pm 2,\pm 4$' tür. $b=1$ için $3a^2-7=4$ olur. Buradan $3a^2=11$ bulunur. Fakat, bu eşitliği sağlayan $a\in\mathbb{Z}$ yoktur. $b=-1$ için $-3a^2+7=4$ olur. Buradan $a^2=1$ olup $a=\pm 1$'dir. $b=2$ için $6a^2-56=4$ olur. Böylece $6a^2=60$ eşitliği elde edilir. Ancak, bu eşitliği sağlayan $a\in\mathbb{Z}$ yoktur. $b=-2$ için $-6a^2+56=4$ olup $-6a^2=-52$'dir. Fakat, bu eşitliği sağlayan $a\in\mathbb{Z}$ yoktur. $b=4$ için $12a^2-448=4$ olur. Buradan $12a^2=452$ bulunur. Ancak bu eşitliği sağlayan $a\in\mathbb{Z}$ yoktur. $b=-4$ için $-12a^2+448=4$ olduğundan $-12a^2=-442$'dir. Fakat bu eşitliği sağlayan $a\in\mathbb{Z}$ yoktur. $b=-1$ ise $4=-3a^2+7$ ve böylece $a=\pm 1$ bulunur. Dolayısıyla $y=\dfrac{a^2+7b^2}{4}=2$ olur. Böylece $x^2+x+2=y^3$ olduğundan $x=-3$ ve $x=2$ bulunur. Sonuç olarak, $\left(-3,2\right),\left(2,2\right)$ istenen çözümlerdir.

BÖLÜM 3. BAZI DİYOFANT DENKLEMLERİNİN ÇÖZÜMLERİ

Tanım 3.1.1. x, y, z pozitif tamsayılar olsun. Eğer $x^2 + y^2 = z^2$ ise (x, y, z) üçlüsüne bir pisagor üçlüsü denir. Ayrıca $x^2 + y^2 = z^2$ ve $(x, y) = 1$ (veya $(x, y, z) = 1$) ise (x, y, z) üçlüsüne bir primitif pisagor üçlüsü denir.

Örnek 3.1.2. Yukarıdaki tanıma göre $(5,12,13)$ bir primitif pisagor üçlüsüdür. $(10, 24, 26)$ üçlüsü bir pisagor üçlüsüdür. Fakat, $(10, 24, 26)$ üçlüsü bir primitif pisagor üçlüsü değildir.

Teorem 3.1.3. (1) a, b pozitif tamsayılar, $(a, b) = 1$ ve $ab = c^n$ ise $a = u^n, b = v^n$ olacak biçimde u, v pozitif tamsayıları vardır.

(2) a, b pozitif tamsayılar, $(a, b) = 1$ ve $ab = rc^n$ ise $a = uy^n$, $b = vz^n$ ve $r = uv$ olacak biçimde u, v, y, z pozitif tamsayıları vardır.

(3) a, b pozitif tamsayılar, $(a, b) = 1$ ve $ab = 2c^n$ ise $a = y^n, b = 2z^n$ veya $a = 2y^n, b = z^n$ olacak biçimde u, v, y, z pozitif tamsayıları vardır.

Önerme 3.1.4. (a, b, c) bir pisagor üçlüsüdür $\Leftrightarrow a = kx, b = ky, c = kz$ olacak biçimde bir (x, y, z) primitif pisagor üçlüsü vardır.

Teorem 3.1.5. $x^2 + y^2 = z^2$ denkleminin tüm primitif çözümleri, $m > n$, m ve n aralarında asal , m ve n biri tek biri çift pozitif tamsayılar olmak üzere $x = m^2 - n^2$, $y = 2mn$, $z = m^2 + n^2$ formülüyle verilir [1].

İspat: Kabul edelim ki (x,y,z) $x^2+y^2=z^2$ denkleminin bir primitif çözümü olsun. Bu durumda x,y sayılarından biri çift diğeri tektir. Gerçekten, aksini kabul edersek, yani x,y sayılarının her ikisi de çift ya da her ikisi de tek olsun. x,y sayılarının her ikisi de çift olduğunda $x^2+y^2=z^2$ olduğundan z sayısı da çift olacaktır. Bu ise x,y,z sayılarının 2 ortak bölenine sahip olmasını gerektirir. Fakat, bu durum x,y,z sayılarının primitif çözüm olması ile çelişir. Eğer x,y sayılarının her ikisi de tek olursa, $x^2\equiv 1(\bmod 4)$, $y^2\equiv 1(\bmod 4)$ olur. Bu durumda $x^2+y^2=z^2$ olduğundan $z^2\equiv 2(\bmod 4)$ olacaktır. Halbuki $x^2+y^2=z^2$ ve x,y tek olduğundan z çift olup $z^2\equiv 0(\bmod 4)$'tür.

Kabul edelim ki y çift, x tek olsun. x ve y sayıları yer değiştirerek kalan çözümler elde edilir.

(x,y,z), $x^2+y^2=z^2$ denkleminin bir çözümü ve y çift, x tek olduğundan z tektir. $x^2+y^2=z^2$ denklemini $y^2=(z+x)(z-x)$ olarak yazabiliriz. $z+x$ ve $z-x$ sırasıyla iki tek sayının toplamı ve farkı olduğundan ikisi de çifttir. Sonuç olarak, $z+x=2a, z-x=2b$ olacak şekilde a,b pozitif tamsayıları vardır. Bu nedenle $z=a+b, x=a-b$ 'dir.

Burada a ve b aralarında asal olmalıdır. Gerçekten, aksi takdirde $\delta>1$ için $\delta\,|a$, $\delta\,|\,b$ olsun. Böylece $\delta\,|\,a+b$ ve $\delta|a-b$'dir. Yani $\delta\,|\,z, \delta\,|\,x$ olup $z=k\delta, x=\ell\delta$ olacak şekilde k,ℓ pozitif tamsayıları vardır. $y^2=z^2-x^2$ ve $x=\ell\delta$, $z=k\delta$ olduğundan $y^2=k^2\delta^2-\ell^2\delta^2$ olur. Şu halde $y^2=\left(k^2-\ell^2\right)\delta^2$ olup $\delta^2\,|\,y^2$'dir. O halde Teorem 1.1.10'a göre $\delta\,|\,y$'dir. Dolayısıyla $\delta>1$, x,y,z tamsayılarının bir ortak böleni olur. Bu ise (x,y,z)'nin bir primitif çözüm olması ile çelişir.

Kabulümüz gereği y çift olduğundan $y=2c$ olacak biçimde c pozitif tamsayısı vardır. Böylece $y^2=(z+x)(z-x)$ olduğundan $4c^2=(z+x)(z-x)$ olur. Dolayısıyla

$z+x=2a$, $z-x=2b$ olduğundan $c^2=ab$ bulunur. $(a,b)=1$ olduğundan Teorem 3.1.3'e göre $a=m^2, b=n^2$ olacak şekilde m,n pozitif tamsayıları vardır. Buradan $(a,b)=(m^2,n^2)=1$ olduğundan Teorem 1.1.8'e göre $(m,n)=1$ dir. $a=m^2, b=n^2$ ve $z=a+b$, $x=a-b$ olduğundan $z=m^2+n^2$, $x=m^2-n^2$ bulunur. Ayrıca $c^2=ab=m^2n^2$ ve $y=2c$ olduğundan $y=2mn$ olur. O halde ispat ettik ki (x,y,z) $x^2+y^2=z^2$ denkleminin bir primitif çözümü ve y çift olduğunda, $x=m^2-n^2$, $y=2mn$, $z=m^2+n^2$ elde edilir. Burada m,n pozitif tamsayılar, $(m,n)=1$ ve $m>n$'dir. Gerçekten, x bir pozitif tamsayı olduğundan $x=m^2-n^2>0$ olup $m^2>n^2$'dir. Yani $m>n$ olur. Ayrıca m,n sayılarından biri tek biri çifttir. Gerçekten, eğer her ikisi de çift olursa bu $(m,n)=1$ olması ile çelişir. Eğer her ikisi de tek olursa $x=m^2-n^2$, $y=2mn$, $z=m^2+n^2$ olduğundan x,y,z tamsayıları çift olur. Bu ise $(x,y,z)=1$ olması ile çelişir.

Tersine, m,n aralarında asal pozitif tamsayılar, $m>n$ ve m,n pozitif tamsayılarından biri tek biri çift olmak üzere $x=m^2-n^2$, $y=2mn$, $z=m^2+n^2$ olacak biçimde mevcut olsun. Bu durumda,

$$\begin{aligned} x^2+y^2 &= \left(m^2-n^2\right)^2+\left(2mn\right)^2 \\ &= m^4+n^4-2m^2n^2+4m^2n^2 \\ &= m^4+n^4+2m^2n^2=\left(m^2+n^2\right)^2=z^2 \end{aligned}$$

olup $x^2+y^2=z^2$ denkleminin sağlandığı açıktır.

Şimdi m ve n pozitif tamsayılarının aralarında asal olduğunu kullanarak $(x,y,z)=1$ olduğunu gösterelim. Aksine kabul edelim ki $(x,y,z)\neq 1$ olsun. O zaman x, y, z sayılarının $\delta>1$ olan bir ortak böleni vardır. Yani $\delta>1$olmak üzere $\delta \mid x$, $\delta \mid y$, $\delta \mid z$'dir. Burada δ çift olamaz. Çünkü, $z=m^2+n^2, m$ ve n biri tek biri çift pozitif tamsayı olduğundan z tektir. $x=m^2-n^2$, $y=2mn$, $z=m^2+n^2$ olduğundan dolayı $2m^2=x+z$, $2n^2=z-x$ olur. Burada $\delta \mid x$, $\delta \mid z$ olduğundan

$\delta \mid 2m^2$, $\delta \mid 2n^2$ bulunur. δ çift olmadığından $\delta \mid m^2$ ve $\delta \mid n^2$ yazabiliriz. Bu ise $\delta \mid \left(m^2, n^2\right)$ olmasını gerektirir. Halbuki $\left(m,n\right)=1$ olduğundan Teorem 1.1.7'e göre $\left(m^2, n^2\right)=1$'dir. O halde $\delta \mid 1$ olur. Bu ise $\delta > 1$ olması ile çelişir. Kabulümüz yanlıştır. Yani $\left(x,y,z\right)=1$'dir.

Sonuç 3.1.6. x,y,z pozitif tamsayıları $x^2+y^2=z^2$ denkleminin çözümüdür $\Leftrightarrow$ $m>n$, m, n, d pozitif tamsayılar , $\left(m,n\right)=1$, m, n biri çift biri tek pozitif tamsayılar olmak üzere

$$x=\left(m^2-n^2\right)d \quad , \; y=2mnd \; , \; z=\left(m^2+n^2\right)d$$

dir.

İspat: $\Leftarrow$:) $x=\left(m^2-n^2\right)d$, $y=2mnd$, $z=\left(m^2+n^2\right)d$ olsun. Bu durumda,

$$\begin{aligned} x^2+y^2 &= \left(\left(m^2-n^2\right)d\right)^2+\left(2mnd\right)^2 \\ &= m^4d^2+n^4d^2-2m^2n^2d^2+4m^2n^2d^2 \\ &= m^4d^2+n^4d^2+2m^2n^2d^2 \\ &= d^2\left(m^4+n^4+2m^2n^2\right) \\ &= d^2\left(m^2+n^2\right)^2=z^2 \end{aligned}$$

olup x,y,z tamsayıları $x^2+y^2=z^2$ denklemini sağlar.

$\Rightarrow$:) Önerme 3.1.4'e göre $x=da$, $y=db$, $z=dc$ olacak şekilde bir primitif $\left(a,b,c\right)$ üçlüsü vardır. Teorem 3.1.5'e göre $a=m^2-n^2$, $b=2mn$, $c=m^2+n^2$ olacak şekilde pozitif m ve n tamsayıları vardır. Buradan istenen elde edilir.

Teorem 3.1.5 ve Sonuç 3.1.6 'da x'in çift y'nin tek olduğu çözümler de mevcuttur. Bu çözümler x ve y ler yer değiştirerek elde edilir.

Örnek 3.1.7. (x, y, z) bir primitif pisagor üçlüsü ve $z - y = 2$ olsun. Bu takdirde $x = 2t$, $y = t^2 - 1$, $z = t^2 + 1$ olacak biçimde bir t pozitif tamsayısı vardır.

Çözüm: (x, y, z) bir primitif pisagor üçlüsü olduğundan $(x, y, z) = 1$ ve $x^2 + y^2 = z^2$'dir. Buradan $x^2 = z^2 - y^2 = (z + y)(z - y)$ yazarız. Hipotezden $z - y = 2$ olduğundan $x^2 = 2(z + y)$ elde edilir.

Teorem 3.1.5'e göre $x = 2uv$, $y = u^2 - v^2$, $z = u^2 + v^2$ olacak şekilde $u > v$, $(u, v) = 1$, biri tek biri çift olan u ve v pozitif tamsayıları vardır. Bu eşitlikler $x^2 = 2(z + y)$ eşitliğinde yerine yazılırsa,

$$4u^2v^2 = 2\left(u^2 + v^2 + u^2 - v^2\right)$$

$$4u^2v^2 = 2\left(2u^2\right)$$

$$4u^2v^2 = 4u^2$$

olup u pozitif tamsayı olduğundan $v^2 = 1$ elde edilir. Buradan v pozitif tamsayı olduğundan $v = 1$ olur. O halde $x = 2uv$, $y = u^2 - v^2$, $z = u^2 + v^2$ ve $v = 1$ olduğundan $x = 2u$, $y = u^2 - 1$, $z = u^2 + 1$ bulunur.

Teorem 3.1.8. $x^4 + y^4 = z^2$ denkleminin pozitif tamsayılarda çözümü yoktur [1].

İspat: Kabul edelim ki (x, y, z) $x^4 + y^4 = z^2$ denkleminin pozitif tamsayılarda bir çözümü olsun ve z bu özellikteki en küçük tamsayı olsun. Burada $(x, y) = 1$ olur. Gerçekten, aksini kabul edelim. $(x, y) = d > 1$ olsun. Bu takdirde $d \mid x$ ve $d \mid y$ olur. Buradan $x = dx_1$, $y = dy_1$ olacak şekilde x_1, y_1 pozitif tamsayıları vardır. Denklemde bu eşitlikleri yerine yazarsak,

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

olur. Böylece $d^4 \mid z^2$ olup Teorem 1.1.10' a göre $d^2 \mid z$ bulunur. Şu halde $z = d^2 z_1$ olacak şekilde z_1 pozitif tamsayısı vardır. Bulunan $x = dx_1$, $y = dy_1$, $z = d^2 z_1$

eşitliklerini $x^4+y^4=z^2$ denkleminde yerine yazarsak $d^4\left(x_1^{\,4}+y_1^{\,4}\right)=d^4z_1^{\,2}$ elde edilir. Bu ise $x_1^{\,4}+y_1^{\,4}=z_1^{\,2}<z^2$ olduğunu gösterir. Fakat bu z 'nin en küçük olması ile çelişir.

$(x,y)=1$ olduğundan Teorem 1.1.7'e göre $\left(x^2,y^2\right)=1$'dir. Buradan $\left(x^2,y^2,z\right)$ $\left(x^2\right)^2+\left(y^2\right)^2=z^2$ pisagor denkleminin bir primitif çözümüdür. Teorem 3.1.5'e göre x^2, y^2 sayılarından biri çift biri tektir. Kabul edelim ki y^2 çift olsun. O halde $x^2=m^2-n^2$, $y^2=2mn$, $z=m^2+n^2$ olacak şekilde $(m,n)=1$, $m>n$, biri tek biri çift olan m ve n pozitif tamsayıları vardır. Burada eğer m çift ve n tek olursa, $x^2+n^2=m^2$ olduğundan x de tektir. Fakat, bu mümkün değildir. Gerçekten, x tek olduğundan $x^2\equiv 1(\bmod 8)$, n tek olduğundan $n^2\equiv 1(\bmod 8)$ olup buradan $m^2=x^2+n^2\equiv 2(\bmod 8)$ bulunur. Halbuki m çift olduğundan $m^2\equiv 0,4(\bmod 8)$ olduğu açıktır. Yani bu bir çelişkidir. O halde m tektir, n çifttir. Şu halde $n=2k$ olacak şekilde k pozitif tamsayısı vardır. $(m,n)=1$ ve m tek olduğundan $(m,k)=1$ dir. $y=2mn$ ve $n=2k$ olduğundan $y^2=2^2mk$ yazılır. y çift olduğundan $y=2\ell$ olacak şekilde ℓ pozitif tamsayısı vardır. $y^2=2^2mk$ ve $y=2\ell$ olduğundan $4\ell^2=4mk$ olup buradan $\ell^2=mk$ elde edilir. $(m,k)=1$ olduğundan Teorem 3.1.3'e göre $m=a^2$, $k=b^2$ olacak şekilde a,b pozitif tamsayıları vardır. $n=2k$ ve $k=b^2$ olduğunda $n=2b^2$ olur. $x^2+n^2=m^2$ ve $(m,n)=1$ olduğundan $(x,n)=1$'dir. Gerçekten, $(x,n)=\delta$ olsun. Buradan $\delta\,|\,x$ ve $\delta\,|\,n$ olur. Bu ise $\delta\,|\,x^2$ ve $\delta\,|\,n^2$ olmasını gerektirir. Şu halde $\delta\,|\,x^2+n^2=m^2$ olur. Yani $\delta\,|\,m^2$, $\delta\,|\,n^2$ olup buradan $\delta\,|\left(m^2,n^2\right)$ bulunur. $(m,n)=1$ olduğundan Teorem 1.1.7'e göre $\left(m^2,n^2\right)=1$'dir. Sonuç olarak, $\delta\,|\,1$ olup $\delta=1$ elde edilir.

$(x,n)=1$ ve $x^2+n^2=m^2$ olduğundan (x,n,m), $x^2+y^2=z^2$ denkleminin bir primitif çözümüdür. O halde Teorem 3.1.5'e göre $x=m_1^{\,2}-n_1^{\,2}$, $n=2m_1n_1$, $m=m_1^{\,2}+n_1^{\,2}$ olacak şekilde $m_1>n_1$, $(m_1,n_1)=1$, biri tek biri çift olan m_1,n_1 pozitif tamsayıları vardır. $n = 2b^2$ ve $n = 2m_1n_1$ olduğundan $b^2 = m_1n_1$ olur. Burada $(m_1, n_1) = 1$ olduğundan Teorem 3.1.3'e göre $m_1 = a_1^2$, $n_1 = b_1^2$ olacak şekilde a_1 ve b_1 pozitif tamsayıları vardır. $m = m_1^2 + n_1^2$ ve $m = a^2$ olduğundan $a^2 = m_1^2 + n_1^2$ yazılır. Buradan $m_1 = a_1^2$, $n_1 = b_1^2$ olduğundan $a^2 = a_1^4 + b_1^4$ bulunur. Fakat, $a \le a^2 = m < m^2 + n^2 = z$ olup $a < z$ olur. Bu ise z 'nin en küçük olması ile çelişir. Sonuç olarak, kabulumüz yanlıştır. $x^4 + y^4 = z^2$ denkleminin pozitif tamsayılarda çözümü yoktur.

Örnek 3.1.9. $x^4 + y^4 = 4z^2$ denkleminin pozitif tamsayılarda çözümü yoktur.

Çözüm: Verilen denklem $x^4 + y^4 = (2z)^2$ olarak yazılırsa Teorem 3.1.8'den pozitif tamsayılarda çözümü olmadığı görülür.

Örnek 3.1.10. $x^4 - 4y^4 = z^2$ denklemini sağlayan pozitif x, y, z tamsayıları yoktur.

Çözüm: $x^4 - 4y^4 = z^2$ denkleminin her iki tarafının karesi alınırsa $z^4 = \left(x^4 - 4y^4\right)^2$ olur. Bulunan bu eşitliğin her iki tarafına $(2xy)^4$ eklersek $z^4 + (2xy)^4 = \left(x^4 - 4y^4\right)^2 + (2xy)^4$ elde edilir. Buradan

$$\begin{aligned} z^4 + (2xy)^4 &= x^8 - 8x^4y^4 + 16y^8 + 16x^4y^4 \\ &= x^8 + 8x^4y^4 + 16y^8 \\ &= \left(x^4 + 4y^4\right)^2 \end{aligned}$$

bulunur. Fakat, bu Teorem 3.1.8'e göre mümkün değildir.

Örnek 3.1.11. $y \neq 0$ ise $x^4 - 2y^2 = 1$ denkleminin pozitif tamsayılarda çözümü yoktur.

Çözüm: $x^4 - 2y^2 = 1$ olduğundan $x^4 = 1 + 2y^2$ olur. Eşitliğin her iki tarafına y^4 eklersek $x^4 + y^4 = 1 + 2y^2 + y^4 = \left(y^2 + 1\right)^2$ bulunur. Fakat, bu Teorem 3.1.8'e göre mümkün değildir.

Teorem 3.1.12. $a^2 - b^2 = x^2$ ve $a^2 + b^2 = y^2$ olacak şekilde a, b, x, y pozitif tamsayıları yoktur [5].

Örnek 3.1.13. $x^4 + y^4 = 2z^2$ denkleminin pozitif tamsayılarda çözümlerini bulalım:

Çözüm: Herhangi bir x pozitif tamsayısı için $x = y$, $z = x^2$ olmak üzere $\left(x, x, x^2\right)$ denkleminin çözümleridir.

$x \neq y$ için denklemin çözümü yoktur. Gerçekten, aksine genelliği bozmadan $x > y$ kabul edelim. Ayrıca kabul edelim ki x, y, z pozitif tamsayılar olmak üzere $\left(x, y, z\right)$ denklemin çözümü olsun. O halde $x^4 + y^4 = 2z^2$ olduğundan x ve y sayılarının ikisi de çift yada ikisi de tektir. Bu durumda $x^2 - y^2$ ve $x^2 + y^2$ sayıları da çift olacaktır. Sonuç olarak , $a = \frac{1}{2}\left(x^2 - y^2\right)$ ve $b = \frac{1}{2}\left(x^2 + y^2\right)$ pozitif tamsayılar olacaktır. Buradan bu eşitlikleri taraf tarafa toplar ve çıkarırsak sırasıyla, $x^2 = a + b$, $y^2 = a - b$ elde edilir. $2z^2 = x^4 + y^4$ denkleminde $x^2 = a + b$, $y^2 = a - b$ eşitliklerini yerine yazarsak $2z^2 = \left(a + b\right)^2 + \left(a - b\right)^2 = 2\left(a^2 + b^2\right)$ bulunur. Sonuç olarak, buradan $z^2 = a^2 + b^2$ elde edilir. $x^2 = a + b$, $y^2 = a - b$ olduğundan bu eşitlikleri taraf tarafa çarparsak $x^2 y^2 = a^2 - b^2$ bulunur. Buradan $a^2 - b^2 = \left(xy\right)^2$ olur.

$z^2 = a^2 + b^2$, $a^2 - b^2 = \left(xy\right)^2$ olur. Fakat, bu Teorem 3.1.12' ye göre mümkün değildir. O halde kabulümüz yanlıştır. Yani, $x \neq y$ için çözüm yoktur.

Teorem 3.1.14. $x^4 + y^4 = 5z^2$ denkleminin pozitif tamsayılarda çözümü yoktur [1].

İspat: 1. durum: $5 \nmid x$ olsun. O zaman $x^4 + y^4 = 5z^2$ olduğundan $5 \nmid y$ olur. Böylece buradan $x^4 \equiv 1(\text{mod}\, 5)$ ve $y^4 \equiv 1(\text{mod}\, 5)$ bulunur. O halde $x^4 + y^4 \equiv 2(\text{mod}\, 5)$ dir. Halbuki $x^4 + y^4 = 5z^2$ olduğundan $x^4 + y^4 \equiv 0(\text{mod}\, 5)$ olduğu açıktır. O halde bu durumda denklemin bir çözümü yoktur.

2. durum: $5 \mid x$ olsun. O zaman $x^4 + y^4 = 5z^2$ olduğundan $5 \mid y$ olur. Buradan $x = 5^r a$, $5 \nmid a$ ve $y = 5^s b$, $5 \nmid b$ olacak şekilde a, b, r, s pozitif tamsayıları vardır. $x^4 + y^4 = 5z^2$ denkleminde $x = 5^r a$, $y = 5^s b$ eşitlikleri yerine yazılırsa,

$$5^{4r} a^4 + 5^{4s} b^4 = 5z^2$$
$$5^{4r-1} a^4 + 5^{4s-1} b^4 = z^2$$

olup buradan $5 \mid z^2$ olur. Şu halde 5 asal olduğundan $5 \mid z$'dir. O halde $z = 5^t c$, $5 \nmid c$ olacak şekilde c ve t pozitif tamsayıları vardır. $5^{4r-1} a^4 + 5^{4s-1} b^4 = z^2$ denkleminde $z = 5^t c$ eşitliğini yerine yazarsak ve her iki tarafı 5 ile çarparsak,

$$5^{4r} a^4 + 5^{4s} b^4 = 5^{2t+1} c^2$$

elde edilir.

$r = s$ ise $5^{4r}\left(a^4 + b^4\right) = 5^{2t+1} c^2$ olur. Buradan $a^4 + b^4 = 5\left(5^{t-2r} c\right)^2$ bulunur. $w = 5^{t-2r} c$ dersek, $a^4 + b^4 = 5w^2$ elde edilir. $5 \nmid a$ ve $5 \nmid b$ olduğundan 1. durumdan buradan çözüm elde edilemez.

$r > s$ ise $5^{4s}\left(5^{4r-4s} a^4 + b^4\right) = 5^{2t+1} c^2$ olur. Bu ise $5 \mid b$ olmasını gerektirir. Halbuki $5 \nmid b$ dir. O halde buradan da çözüm elde edilemez.

Teorem 3.1.15. $x^4 + y^4 = 3z^2$ denkleminin pozitif tamsayılarda çözümü yoktur [1].

İspat: Kabul edelim ki (x, y, z), $x^4 + y^4 = 3z^2$ denkleminin bir çözümü olsun ve x en küçük olsun. Şu halde $3 \mid x^4 + y^4$ olur. Yani $3 \mid \left(x^2\right)^2 + \left(y^2\right)^2$ elde edilir. O halde Teorem 1.1.12'ye göre $3 \mid x^2$ ve $3 \mid y^2$ olur. Buradan 3 asal olduğundan $3 \mid x$ ve

$3 \mid y$'dir. Böylece $x = 3a$, $y = 3b$ olacak şekide a, b pozitif tamsayıları vardır. $x = 3a$, $y = 3b$ eşitlikleri $x^4 + y^4 = 3z^2$ denkleminde yerine yazılırsa,

$$81a^4 + 81b^4 = 3z^2$$
$$9\left(3a^4 + 3b^4\right) = z^2$$

olur. Buradan $9 \mid z^2$ olup $3^2 \mid z^2$ bulunur. Böylece Teorem 1.1.10'a göre $3 \mid z$'dir. Şu halde $z = 3t$ olacak şekilde t pozitif tamsayısı vardır. $9\left(3a^4 + 3b^4\right) = z^2$ denkleminde $z = 3t$ eşitliğini yerine yazarsak,

$$9\left(3a^4 + 3b^4\right) = 9t^2$$
$$3a^4 + 3b^4 = t^2$$

olur. Bu ise $3 \mid t^2$ olmasını gerektirir. Böylece 3 asal olduğundan $3 \mid t$'dir. O halde $t = 3t_1$ olacak şekilde t_1 pozitif tamsayısı vardır. $t = 3t_1$ eşitliğini $3a^4 + 3b^4 = t^2$ denkleminde yerine yazarsak $a^4 + b^4 = 3t_1^2$ elde edilir. $x = 3a$ olduğundan $a < x$ dir. Bu ise x'in en küçük olması ile çelişir. O zaman kabulümüz yanlıştır. $x^4 + y^4 = 3z^2$ denkleminin pozitif tamsayılarda çözümü yoktur.

Teorem 3.1.16. $x^4 + y^4 = 13z^2$ denkleminin pozitif tamsayılarda çözümü yoktur [1].

İspat: 1. durum: $13 \nmid x$ olsun. Buradan $x^4 + y^4 = 13z^2$ olduğundan $13 \nmid y$ olur. $13 \nmid x$ ve 13 asal sayı olduğundan Teorem 1.1.18'e göre $x^{12} \equiv 1 \pmod{13}$, $y^{12} \equiv 1 \pmod{13}$ bulunur. $x^4 + y^4 = 13z^2$ olduğundan $x^4 + y^4 \equiv 0 \pmod{13}$ elde edilir. Buradan $x^4 \equiv -y^4 \pmod{13}$ olur. Her iki tarafın küpü alınırsa $x^{12} \equiv -y^{12} \pmod{13}$ bulunur. Şu halde $x^{12} \equiv 1 \pmod{13}$, $y^{12} \equiv 1 \pmod{13}$ olduğundan $1 \equiv -1 \pmod{13}$ çelişkisi elde edilir. O halde bu durumda çözüm elde edilemez.

2. durum: $13 \mid x$ olsun. O zaman $x^4 + y^4 = 13z^2$ olduğundan $13 \mid y$ olur. Burada kabul edelim ki x en küçük olsun. $13 \mid x$, $13 \mid y$ olduğundan $x = 13a$, $y = 13b$

olacak biçimde a ve b pozitif tamsayıları vardır. $x=13a$ ve $y=13b$ eşitliklerini $x^4+y^4=13z^2$ denkleminde yerine yazarsak,

$$13^4a^4+13^4b^4=13z^2$$

$$13^3a^4+13^3b^4=z^2$$

olup buradan $13\,|\,z^2$ elde edilir. 13 asal olduğundan $13\,|\,z$ 'dir. O halde $z=13t$ olacak şekilde t pozitif tamsayısı vardır. $13^3a^4+13^3b^4=z^2$ denkleminde $z=13t$ eşitliği yerine yazılırsa,

$$13^3a^4+13^3b^4=13^2t^2$$

$$13\left(a^4+b^4\right)=t^2$$

olup buradan $13\,|\,t^2$ olur. 13 asal olduğundan $13\,|\,t$ 'dir. O zaman $t=13k$ olacak şekilde k pozitif tamsayısı vardır. $13\left(a^4+b^4\right)=t^2$ eşitliğinde $t=13k$ yerine yazılırsa,

$$13\left(a^4+b^4\right)=13^2k^2$$

$$\left(a^4+b^4\right)=13k^2$$

olur. $x=13a$ olduğundan $a<x$ 'dir. Fakat, bu x 'in en küçük olması ile çelişir. O halde bu durumda da çözüm elde edilemez.

Teorem 3.1.17. $x^2+y^2+z^2=t^2$ denkleminin y,z çift olduğunda pozitif tamsayılardaki tüm çözümleri, $x=\dfrac{\ell^2+m^2-n^2}{n}$, $y=2\ell$, $z=2m$, $t=\dfrac{\ell^2+m^2+n^2}{n}$ şeklindedir. Burada ℓ, m pozitif tamsayılar ve ℓ^2+m^2 'nin bölenleri olan n pozitif tamsayıları $\sqrt{\ell^2+m^2}$ ' den küçüktür [1].

İspat: Kabul edelim ki (x,y,z,t), $x^2+y^2+z^2=t^2$ denkleminin pozitif tamsayılarda bir çözümü olsun. Burada x, y, z sayılarının en az ikisi çift olmalıdır. Gerçekten, aksine kabul edelim ki x, y, z sayılarının üçü de tek olsun. Buradan $x^2\equiv 1(\text{mod}\,8)$, $y^2\equiv 1(\text{mod}\,8)$, $z^2\equiv 1(\text{mod}\,8)$ olur. O zaman $x^2+y^2+z^2=t^2$

olduğundan $t^2 \equiv 3 \pmod 8$ bulunur. Halbuki $t^2 \equiv 0,1,4 \pmod 8$ olduğu açıktır. O halde kabülümüz yanlıştır. x, y, z sayılarının üçü de tek olamaz. Şimdi kabul edelim ki x, y, z sayılarının sadece biri çift olsun. Ayrıca genelliği bozmadan kabul edelim ki bu çift sayı z olsun. O zaman $x^2 \equiv 1 \pmod 4$, $y^2 \equiv 1 \pmod 4$, $z^2 \equiv 0 \pmod 4$ olur. Buradan $x^2 + y^2 + z^2 = t^2$ olduğundan $t^2 \equiv 2 \pmod 4$ bulunur. Halbuki $t^2 \equiv 0,1 \pmod 4$ olduğu açıktır. O halde kabülümüz yanlıştır. x, y, z sayılarının sadece biri çift olamaz.

Şimdi kabul edelim ki x, y, z sayılarından çift olanlar y ve z olsun. Böylece $y = 2\ell$, $z = 2m$ olacak şekilde ℓ, m pozitif tamsayıları vardır. $x^2 + y^2 + z^2 = t^2$ olduğundan $t > x$ olduğu açıktır. O halde $t - x = u$ dersek u bir pozitif tamsayıdır. $t - x = u$, $y = 2\ell$, $z = 2m$ eşitlikleri $x^2 + y^2 + z^2 = t^2$ denkleminde yerine yazılırsa,

$$(x+u)^2 = x^2 + (2\ell)^2 + (2m)^2 = x^2 + 4\ell^2 + 4m^2$$

ve böylece

$$x^2 + 2xu + u^2 = x^2 + 4\ell^2 + 4m^2$$

elde edilir. Buradan

$$2xu + u^2 = 4\ell^2 + 4m^2$$

bulunur. Şu halde

$$u^2 = 4\ell^2 + 4m^2 - 2xu$$

elde edilir.

$u^2 = 4\ell^2 + 4m^2 - 2xu$ eşitliğinin sağ tarafı çift sayıların bir cebirsel toplamı olduğundan çifttir. Bu nedenle u^2 de çift olur. O halde u da çift olur. Dolayısıyla $u = 2n$ olacak şekilde n pozitif tamsayısı vardır. $u^2 = 4\ell^2 + 4m^2 - 2xu$ eşitliğinde $u = 2n$'i yerine yazarsak,

$$4n^2 = 4\ell^2 + 4m^2 - 4xn$$

$$n^2 = \ell^2 + m^2 - xn$$
$$xn = \ell^2 + m^2 - n^2$$

ve böylece

$$x = \frac{\ell^2 + m^2 - n^2}{n}$$

bulunur.

$t - x = u$ olduğundan $t = x + u$ olur. Böylece $x = \dfrac{\ell^2 + m^2 - n^2}{n}$, $u = 2n$ eşitlikleri $t = x + u$'da yerine yazılırsa,

$$t = \frac{\ell^2 + m^2 - n^2}{n} + 2n$$
$$= \frac{\ell^2 + m^2 + n^2}{n}$$

bulunur. Burada t pozitif tamsayı olduğundan $n \mid \ell^2 + m^2 + n^2$ olur. O halde $n \mid n^2$ olduğundan $n \mid \ell^2 + m^2$ dir. $n^2 = \ell^2 + m^2 - xn$ ve xn pozitif tamsayı olduğundan $n^2 < \ell^2 + m^2$ olur. Şu halde $n < \sqrt{\ell^2 + m^2}$ bulunur. Sonuç olarak, $x^2 + y^2 + z^2 = t^2$ denkleminin çözümleri için, $x = \dfrac{\ell^2 + m^2 - n^2}{n}$, $y = 2\ell$, $z = 2m$, $t = \dfrac{\ell^2 + m^2 + n^2}{n}$ elde edilir. Burada $n \mid \ell^2 + m^2$, $n < \sqrt{\ell^2 + m^2}$, ℓ, m, n pozitif tamsayılardır.

Tersine, $x = \dfrac{\ell^2 + m^2 - n^2}{n}$, $y = 2\ell$, $z = 2m$, $t = \dfrac{\ell^2 + m^2 + n^2}{n}$ sayılarının $x^2 + y^2 + z^2 = t^2$ denklemini sağladığını gösterelim. $x^2 + y^2 + z^2 = t^2$ denkleminde, $x = \dfrac{\ell^2 + m^2 - n^2}{n}$, $y = 2\ell$, $z = 2m$, $t = \dfrac{\ell^2 + m^2 + n^2}{n}$ eşitliklerini yerine yazarsak,

$$\left(\frac{\ell^2 + m^2 - n^2}{n}\right)^2 + (2\ell)^2 + (2m)^2 = \frac{\ell^4 + m^4 + n^4 - 2\ell^2 n^2 - 2m^2 n^2 + 2\ell^2 m^2}{n^2} + 4\ell^2 + 4m^2$$

$$= \frac{\ell^4 + m^4 + n^4 - 2\ell^2 n^2 - 2m^2 n^2 + 2\ell^2 m^2 + 4n^2\ell^2 + 4n^2 m^2}{n^2}$$

$$= \frac{\ell^4 + m^4 + n^4 + 2\ell^2 n^2 + 2n^2 m^2 + 2\ell^2 m^2}{n^2}$$

$$= \left(\frac{\ell^2 + m^2 + n^2}{n} \right)^2$$

olup istenen elde edilir.

Sonuç olarak, y, z çift olmak üzere $x^2 + y^2 + z^2 = t^2$ denkleminin her bir çözümü $x = \frac{\ell^2 + m^2 - n^2}{n}$, $y = 2\ell$, $z = 2m$, $t = \frac{\ell^2 + m^2 + n^2}{n}$ eşitliklerinden elde edilir. Bu eşitliklerden $\ell = \frac{y}{2}$, $m = \frac{z}{2}$, $n = \frac{t - x}{2}$ olup ℓ, m, n sayıları x, y, z, t tarafından tek türlü olarak tanımlıdır.

Teorem 3.1.18. $xy = zt$ denkleminin pozitif tamsayılardaki tüm çözümleri a, b, c, d herhangi pozitif tamsayılar ve $(c, d) = 1$ olmak üzere $x = ac$, $y = bd$, $z = ad$, $t = bc$ şeklinde verilir [1].

İspat: Kabul edelim ki (x, y, z, t), pozitif tamsayılarda $xy = zt$ denkleminin bir çözümü olsun ve $(x, z) = a$ olsun. Şu halde $x = ac$, $z = ad$ olacak şekilde c, d pozitif tamsayıları vardır ve $(c, d) = 1$'dir. $x = ac$, $z = ad$ eşitliklerini $xy = zt$ denkleminde yerine yazarsak, $acy = adt$ olup buradan $cy = dt$ bulunur. Bu ise $d \mid cy$ olmasını gerektirir. $(c, d) = 1$ olduğundan Teorem 1.1.6'ya göre $d \mid y$ olur. O zaman $y = bd$ olacak şekilde b pozitif tamsayısı vardır. $cy = dt$ ve $y = bd$ olduğundan $cbd = dt$ olup buradan $cb = t$ elde edilir. Sonuç olarak, $(c, d) = 1$ olmak üzere $x = ac$, $y = bd$, $z = ad$, $t = bc$ bulunur.

Tersine, açıktır ki a, b, c, d pozitif tamsayılar olmak üzere $x = ac$, $y = bd$, $z = ad$, $t = bc$ eşitlikleri ile verilen x, y, z, t sayıları $xy = zt$ denklemini sağlar.

Teorem 3.1.19. $x^4 - x^2y^2 + y^4 = z^2$ denkleminin pozitif tamsayılarda $x = y$, $z = x^2$ aşikar çözümünden başka çözümü yoktur [1].

İspat: x herhangi bir pozitif tamsayı olmak üzere $x^4 - x^2y^2 + y^4 = z^2$ denklemi pozitif tamsayılarda $x = y$, $z = x^2$ olan aşikar çözümlere sahiptir.

Kabul edelim ki $x \neq y$ olmak üzere (x, y, z), pozitif tamsayılarda $x^4 - x^2y^2 + y^4 = z^2$ denkleminin bir çözümü olsun. Burada $(x, y) = 1$ kabul edebiliriz. Gerçekten, kabul edelim ki $(x, y) = d > 1$ olsun. O zaman $x = dx_1, y = dy_1$, $(x_1, y_1) = 1$ olacak şekilde x_1, y_1 pozitif tamsayıları vardır. $x = dx_1$, $y = dy_1$ eşitlikleri $x^4 - x^2y^2 + y^4 = z^2$ denkleminde yerine yazılırsa,

$$d^4x_1^4 + d^4y_1^4 - d^4x_1^2y_1^2 = z^2$$

$$d^4\left(x_1^4 + y_1^4 - x_1^2y_1^2\right) = z^2$$

ve buradan $d^4 \mid z^2$ elde edilir. Şu halde Teorem 1.1.10'a göre $d^2 \mid z$'dir. Böylece $z = d^2z_1$ olacak şekilde z_1 pozitif tamsayısı vardır. $z = d^2z_1$ eşitliğini $d^4\left(x_1^4 + y_1^4 - x_1^2y_1^2\right) = z^2$ denkleminde yerine yazarsak,

$$d^4\left(x_1^4 + y_1^4 - x_1^2y_1^2\right) = d^4z_1^2$$

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

elde edilir. Burada $(x_1, y_1) = 1$'dir.

O halde $(x, y) = 1$ ve $x \neq y$ olmak üzere (x, y, z), pozitif tamsayılarda $x^4 - x^2y^2 + y^4 = z^2$ denkleminin bir çözümü ve ayrıca kabul edelim ki burada xy en küçük olsun.

1. durum: Kabul edelim ki x, y sayılarından biri örneğin y çift olsun. $(x, y) = 1$ olduğundan x tek olmalıdır. $x^4 - x^2y^2 + y^4 = z^2$ denklemi $\left(x^2 - y^2\right)^2 + (xy)^2 = z^2$ olarak yazılabilir. Burada $x \neq y$ olduğundan $x^2 - y^2 \neq 0$ olur. $(x, y) = 1$ olduğundan

$\left(x^2-y^2,xy\right)=1$ dir. Gerçekten, kabul edelim ki x^2-y^2 ve xy sayılarının bir ortak p asal böleni olsun. Yani $p\,|\,x^2-y^2$ ve $p\,|\,xy$ olsun. Burada $p\,|\,xy$ ve p asal olduğundan $p\,|\,x$ veya $p\,|\,y$ dir. Kabul edelim ki $p\,|\,x$ olsun. Dolayısıyla $x=pk$ olacak şekilde k pozitif tamsayısı vardır. $p\,|\,x^2-y^2$ ve $x=pk$ olduğundan $p\,|\,p^2k^2-y^2$ olur. Şu halde $p\,|\,y^2$ olup p asal olduğundan $p\,|\,y$ dir. Böylece $p\,|\,x$ ve $p\,|\,y$ ve dolayısıyla $p\,|\,(x,y)$ olur. Şu halde $(x,y)=1$ olduğundan $p\,|\,1$ elde edilir. Bu ise p sayısının asal olması ile çelişir. O halde kabülümüz yanlıştır. x^2-y^2 ve xy sayılarının bir ortak p asal böleni yoktur. Sonuç olarak, $\left(x^2-y^2,xy\right)=1$ dir. x tek ve y çift olduğundan xy çifttir. $\left(x^2-y^2,xy\right)=1$ ve $\left(x^2-y^2\right)^2+(xy)^2=z^2$ olduğundan Teorem 3.1.5'e göre $(m,n)=1$, $m>n$, $m+n$ tek olmak üzere $x^2-y^2=m^2-n^2$, $xy=2mn$ olacak şekilde m, n pozitif tamsayıları vardır. x tek olduğundan $x^2\equiv 1(\mathrm{mod}\,4)$, y çift olduğundan $y^2\equiv 0(\mathrm{mod}\,4)$ olup buradan $x^2-y^2\equiv 1(\mathrm{mod}\,4)$ olur. Yani x^2-y^2 sayısı ve $x^2-y^2=m^2-n^2$ olduğundan m^2-n^2 sayısı $4k+1$ formundadır. Bu durum m'nin çift , n'nin tek olamayacağını gösterir. Gerçekten, eğer m çift , n tek olursa $m^2\equiv 0(\mathrm{mod}\,4)$, $n^2\equiv 1(\mathrm{mod}\,4)$ olacağından $m^2-n^2\equiv 0-1\equiv 3(\mathrm{mod}\,4)$ olur. O halde n çift m tek olmalıdır. y çift olduğundan $y=2y_0$ olacak şekilde y_0 pozitif tamsayısı vardır. $xy=2mn$ eşitliğinde $y=2y_0$ sayısını yerine yazarsak $x2y_0=2mn$ olur. Buradan $xy_0=mn$ dir. $(x,y)=1$ ve $y=2y_0$ olduğundan $(x,2y_0)=1$ bulunur. Burada x tek olduğundan $(x,y_0)=1$ dir. Sonuç olarak, $(x,y_0)=(m,n)=1$ dir. $xy_0=mn$ olduğundan Teorem 3.1.18'e göre $x=ac$, $y_0=bd$, $m=ad$, $n=bc$, $(c,d)=1$ olacak şekilde a,b,c,d pozitif tamsayıları vardır. Burada $(x,y_0)=(m,n)=1$ olduğundan açıktır ki a,b,c,d sayılarının herhangi ikisi aralarında asaldır. Yine burada x,m tek sayılar olduğundan a,c,d tek sayılardır. Bundan dolayı n çift olduğundan b çifttir.

$x = ac$, $y = 2y_0 = 2bd$, $m = ad$, $n = bc$ eşitlikleri $x^2 - y^2 = m^2 - n^2$ eşitliğinde yerine yazılırsa,

$$a^2c^2 - 4b^2d^2 = a^2d^2 - b^2c^2$$

ve böylece

$$a^2c^2 + b^2c^2 = a^2d^2 + 4b^2d^2$$

ve buradan da

$$\left(a^2 + b^2\right)c^2 = \left(a^2 + 4b^2\right)d^2$$

elde edilir. Şimdi burada $\left(a^2 + b^2, a^2 + 4b^2\right) = 1$ olduğunu gösterelim. Kabul edelim ki $\left(a^2 + b^2, a^2 + 4b^2\right) = \delta$ olsun. O zaman $\delta \mid a^2 + b^2$ ve $\delta \mid a^2 + 4b^2$ olur. Bu ise $\delta \mid a^2 + 4b^2 - \left(a^2 + b^2\right) = 3b^2$ ve $\delta \mid 4\left(a^2 + b^2\right) - \left(a^2 + 4b^2\right) = 3a^2$ olmasını gerektirir. Buradan $\delta \mid \left(3a^2, 3b^2\right)$ dir. Yani $\delta \mid 3\left(a^2, b^2\right)$ olur. $(a,b) = 1$'dir. Gerçekten, $m = ad$, $n = bc$ ve $(m,n) = 1$ olduğundan $(ad, bc) = 1$ olur. Böylece $(c,d) = 1$ olduğundan $(a,b) = 1$ dir. O halde Teorem 1.1.7'e göre $\left(a^2, b^2\right) = 1$'dir. Dolayısıyla $\delta \mid 3\left(a^2, b^2\right)$ ve $\left(a^2, b^2\right) = 1$ olduğundan $\delta \mid 3$ bulunur. Fakat, 3 sayısı $a^2 + b^2$ sayısının bir böleni değildir. Gerçekten, $a^2 \equiv 0,1 \pmod 3$ ve $b^2 \equiv 0,1 \pmod 3$ dür. Eğer $a^2 + b^2 \equiv 0 \pmod 3$ olursa 3 hem a yı hem de b yi böler. Bu ise $(a,b) = 1$ olmasıyla çelişir. O halde $a^2 + b^2 \equiv 1,2 \pmod 3$ olur. Sonuç olarak $3 \nmid a^2 + b^2$ dir. O zaman $\delta \mid a^2 + b^2$, $\delta \mid 3$, $3 \nmid a^2 + b^2$ olduğundan $\delta = 1$ bulunur. Yani $\left(a^2 + b^2, a^2 + 4b^2\right) = 1$ dir. Burada $\left(a^2 + b^2\right)c^2 = \left(a^2 + 4b^2\right)d^2$ olduğundan Teorem 1.1.6'ya göre $a^2 + b^2 \mid d^2$ ve $a^2 + 4b^2 \mid c^2$ olur. Diğer taraftan $(c,d) = 1$ olduğundan Teorem 1.1.7'ye göre $\left(c^2, d^2\right) = 1$ olup $\left(a^2 + b^2\right)c^2 = \left(a^2 + 4b^2\right)d^2$ ve Teorem 1.1.6'ya göre $c^2 \mid a^2 + 4b^2$ ve $d^2 \mid a^2 + b^2$ olur. O halde $a^2 + b^2 \mid d^2$ ve $d^2 \mid a^2 + b^2$ olduğundan $a^2 + b^2 = d^2$, ayrıca $a^2 + 4b^2 \mid c^2$ ve $c^2 \mid a^2 + 4b^2$ olduğundan $a^2 + 4b^2 = a^2 + (2b)^2 = c^2$ bulunur. $(a,b) = 1$ ve a tek olduğundan $(a, 2b) = 1$ olur. $a^2 + (2b)^2 = c^2$ ve $(a, 2b) = 1$

olduğundan Teorem 3.1.5'e göre $(x_1, y_1)=1$, x_1+y_1 tek , $x_1>y_1$ olmak üzere $a=x_1^2-y_1^2$, $b=x_1y_1$ olacak şekilde x_1, y_1 pozitif tamsayıları vardır. Bu eşitlikler $a^2+b^2=d^2$ eşitliğinde yerine yazılırsa,

$$\left(x_1^2-y_1^2\right)^2+\left(x_1y_1\right)^2=d^2$$

ve böylece

$$x_1^4-x_1^2y_1^2+y_1^4=d^2$$

olur. Burada $x_1y_1=b<2bd=y\le xy$ olduğundan $x_1y_1<xy$ olur. Bu ise xy'nin en küçük olması ile çelişir.

2. durum: Eğer x, y sayılarının her ikisi de çift olursa bu $(x, y)=1$ olması ile çelişir.

3. durum: x, y sayılarının her ikisi de tek olsun. $x\neq y$ olduğundan $x>y$ kabul edebiliriz. $x^4-x^2y^2+y^4=z^2$ denklemi $\left(x^2-y^2\right)^2+(xy)^2=z^2$ olarak yazılabilir ve burada $x>y$ olduğundan $x^2-y^2>0$ dır. Aynı zamanda x, y tek olduğundan x^2-y^2 çifttir. $\left(x^2-y^2, xy\right)=1$ olduğundan Teorem 3.1.5'e göre $2\,|\,mn$, $m>n$, $(m, n)=1$olmak üzere $x^2-y^2=2mn$, $xy=m^2-n^2$ olacak şekilde m, n pozitif tamsayıları vardır. Sonuç olarak,

$$\begin{aligned}m^4-m^2n^2+n^4&=\left(m^2-n^2\right)^2+m^2n^2\\&=(xy)^2+\left(\frac{x^2-y^2}{2}\right)^2\\&=\left(\frac{x^2+y^2}{2}\right)^2\end{aligned}$$

olur. Burada $(m, n)=1$, ayrıca m ve n sayılarının biri tek biri çift olduğundan 1.durum'da gösterdiğimiz gibi bu mümkün değildir.

Sonuç olarak, $x\neq y$ olduğunda çözüm elde edilmez.

Teorem 3.1.20. Aritmetik dizi formunda dört farklı tamkare sayı yoktur [1].

İspat: $y^2 - x^2 = z^2 - y^2 = w^2 - z^2$ olacak biçimde x, y, z, w pozitif tamsayıları mevcut olsun. Buradan $2y^2 = x^2 + z^2$, $2z^2 = y^2 + w^2$ olur. Şu halde $2y^2 = x^2 + z^2$ eşitliğinin her iki tarafını w^2 ile çarparsak $2y^2w^2 = x^2w^2 + z^2w^2$ elde edilir. Ayrıca, $2z^2 = y^2 + w^2$ eşitliğinin her iki tarafını x^2 ile çarparsak $2x^2z^2 = x^2y^2 + x^2w^2$ bulunur. Bulunan $2y^2w^2 = x^2w^2 + z^2w^2$, $2x^2z^2 = x^2y^2 + x^2w^2$ eşitliklerini taraf tarafa çıkarırsak , $2x^2z^2 - 2y^2w^2 = x^2y^2 - z^2w^2$ olur. Buradan görüldüğü gibi $x^2y^2 - z^2w^2$ çifttir. Bu nedenle xy ve zw sayılarının ya ikisi de çifttir ya da ikisi de tektir.

$u = xz$, $v = yw$, $r = \dfrac{xy + zw}{2}$, $s = \dfrac{xy - zw}{2}$ olsun. Burada u, v, r, s tamsayılardır. Kolayca gösterilebilir ki $u^2 - v^2 = 2rs$, $uv = r^2 - s^2$ dir. Böylece $u^2 - v^2 = 2rs$ eşitliğin her iki tarafının karesi alınırsa,

$$\left(u^2 - v^2\right)^2 = 4r^2s^2$$

ve böylece

$$u^4 - 2u^2v^2 + v^4 = 4r^2s^2$$

ve buradan da

$$u^4 - u^2v^2 + v^4 = 4r^2s^2 + u^2v^2$$

elde edilir. Burada $uv = r^2 - s^2$ değeri yerine yazılırsa,

$$u^4 - u^2v^2 + v^4 = 4r^2s^2 + r^4 - 2r^2s^2 + s^4$$

ve buradan da

$$u^4 - u^2v^2 + v^4 = r^4 + 2r^2s^2 + s^4$$

elde edilir. Bu ise

$$u^4 - u^2v^2 + v^4 = \left(r^2 + s^2\right)^2$$

olduğunu gösterir. Şu halde Teorem 3.1.19'a göre $u = v$ olmalıdır. x^2, y^2, z^2, w^2 hepsi farklı olan aritmetik dizinin terimleri olduğundan $x < y < z < w$ varsayabiliriz. Buradan $xz < yw$ olup $u < v$ dir. Bu ise $u = v$ olması ile çelişir.

Teorem 3.1.21. $x^4+9x^2y^2+27y^4=z^2$ denkleminin pozitif tamsayılarda çözümü yoktur [1].

İspat: Kabul edelim ki $x^4+9x^2y^2+27y^4=z^2$ denklemi pozitif tamsayılarda çözülebilir olsun. Ayrıca , kabul edelim ki z en küçük olmak üzere (x,y,z) denklemin bir çözümü olsun.

Eğer $(x,y)=d>1$ olursa $x=dx_1$, $y=dy_1$ olacak şekilde x_1, y_1 pozitif tamsayıları vardır. Bu eşitlikler $x^4+9x^2y^2+27y^4=z^2$ denkleminde yerine yazılırsa,

$$d^4x_1^{\ 4}+9d^2x_1^{\ 2}d^2y_1^{\ 2}+27d^4y_1^{\ 4}=z^2$$

ve buradan

$$d^4\left(x_1^{\ 4}+9x_1^{\ 2}y_1^{\ 2}+27y_1^{\ 4}\right)=z^2$$

olur. Bu ise $d^4\mid z^2$ olmasını gerektirir. O halde $\left(d^2\right)^2\mid z^2$ olduğundan Teorem 1.1.10'a göre $d^2\mid z$ olur. Böylece $z=d^2z_1$ olacak şekilde z_1 pozitif tamsayısı vardır. $z=d^2z_1$ eşitliği $d^4\left(x_1^{\ 4}+9x_1^{\ 2}y_1^{\ 2}+27y_1^{\ 4}\right)=z^2$ denkleminde yerine yazılırsa, $d^4\left(x_1^{\ 4}+9x_1^{\ 2}y_1^{\ 2}+27y_1^{\ 4}\right)=d^4z_1^{\ 2}$ bulunur. Bu eşitliğin her iki tarafı d^4 ile bölünürse $x_1^{\ 4}+9x_1^{\ 2}y_1^{\ 2}+27y_1^{\ 4}=z_1^{\ 2}$ elde edilir. Burada $z=d^2z_1$ olduğundan $z_1<z$ olur. Bu ise z sayısının en küçük olması ile çelişir. O halde kabulümüz yanlıştır. Yani $(x,y)=1$'dir.

Eğer $2\mid x$ ise $x^4+9x^2y^2+27y^4=z^2$ denkleminden $4\mid 27y^4-z^2$ dir. Bu ise $27y^4-z^2\equiv 0\pmod 4$ olmasını gerektirir. Buradan $27y^4\equiv z^2\pmod 4$ elde edilir. $27\equiv -1\pmod 4$ olduğundan $-y^4\equiv z^2\pmod 4$ bulunur. Eğer y tek olursa $y^4\equiv 1\pmod 4$ olduğundan $-1\equiv z^2\pmod 4$ olur. Halbuki $z^2\equiv 0,1\pmod 4$ olduğu açıktır. O halde y çifttir. Bu ise $2\mid y$ olmasını gerektirir. Sonuç olarak, $2\mid x$, $2\mid y$ elde edilir. Bu ise $(x,y)=1$ olması ile çelişir. Şu halde kabülümüz yanlıştır. Yani $2\nmid x$ olur. O halde x tektir. Aynı zamanda y sayısı da tek olursa, buradan

$x^2 \equiv 1(\text{mod}\,8)$, $y^2 \equiv 1(\text{mod}\,8)$ olur. Bu denklikler $x^4 + 9x^2y^2 + 27y^4 = z^2$ denkleminde yerine yazılırsa, $z^2 \equiv 1+9+27 \equiv 37 \equiv 5(\text{mod}\,8)$ olur. Halbuki $z^2 \equiv 0,1,4(\text{mod}\,8)$ olduğu açıktır. O halde x tek, y çifttir.

Eğer $3 \mid x$ olursa, $27 \mid x^4 + 9x^2y^2 + 27y^4 = z^2$ bulunur. Buradan $27 \mid z^3$ yazılabilir. $27 = 3^3$ olduğundan $3^3 \mid z^3$ olup buradan Teorem 1.1.10'a göre $3 \mid z$ dir. $27 \mid z^2$ olduğundan $3.9 \mid z.z$ olur. Bu ise $3 \mid z$ olduğundan $9 \mid z$ olmasını gerektirir. Bu nedenle $9^2 \mid z^2$ yazabiliriz. Yani $81 \mid z^2 = x^4 + 9x^2y^2 + 27y^4$ olur. $3 \mid x$ olduğundan $3^4 \mid x^4 + 9x^2y^2$ olup buradan $81 \mid 27y^4$ bulunur. Şu halde $27.3 \mid 27y^4$ olduğundan $3 \mid y^4$ elde edilir. Böylece 3 asal olduğundan $3 \mid y$ yazılır. Sonuç olarak, $3 \mid x$ ve $3 \mid y$ olur. Bu ise $(x,y) = 1$ olması ile çelişir. O halde kabülümüz yanlıştır. $3 \nmid x$ dir. Buradan 3 asal olduğundan $(x,3) = 1$ yazılır. Aynı zamanda $(x,z) = 1$'dir. Gerçekten, $(x,z) = d$ olsun. O halde $d \mid x$ ve $d \mid z$ olur. $d \mid z$ olduğundan $d \mid z^2$, yani $d \mid x^4 + 9x^2y^2 + 27y^4$ bulunur. $d \mid x$ olduğundan $d \mid x^4$ ve $d \mid 9x^2y^2$ olup $d \mid x^4 + 9x^2y^2$ dir. $d \mid z^2, d \mid x^4 + 9x^2y^2$ olduğundan $d \mid z^2 - \left(x^4 + 9x^2y^2\right)$ olur. Buradan $x^4 + 9x^2y^2 + 27y^4 = z^2$ olduğundan $d \mid 27y^4$ yazılır. $(x,y) = 1$ ve $3 \nmid x$ olduğundan $(x,3y) = 1$ olur. Böylece $\left(x,3^3y^4\right) = 1$ elde edilir. Yani $\left(x,27y^4\right) = 1$ dir. O halde $d \mid x$ ve $d \mid 27y^4$ olduğundan $d \mid \left(x,27y^4\right)$ olup $d \mid 1$'dir. Bu ise $d = 1$ olmasını gerektirir.

y çift olduğundan $y = 2y_1$ olacak şekilde y_1 pozitif tamsayısı vardır. $y = 2y_1$ eşitliğini $x^4 + 9x^2y^2 + 27y^4 = z^2$ denkleminde yerine yazarsak,

$$x^4 + 36x^2y_1^2 + 432y_1^4 = z^2$$

ve böylece

$$432y_1^4 = z^2 - x^4 - 36x^2y_1^2$$

olur. Buradan $108y_1^4 + 324y_1^4 = z^2 - x^4 - 36x^2y_1^2$ yazılır. Böylece

$$108y_1^4 = z^2 - \left(x^4 + 36x^2y_1^2 + 324y_1^4\right),$$

yani

$$108y_1^4 = z^2 - \left(x^2 + 18y_1^2\right)^2$$

ve buradan

$$108y_1^4 = \left(z - \left(x^2 + 18y_1^2\right)\right)\left(z + \left(x^2 + 18y_1^2\right)\right)$$

elde edilir. $108y_1^4 = \left(z - \left(x^2 + 18y_1^2\right)\right)\left(z + \left(x^2 + 18y_1^2\right)\right)$ eşitliğinin her iki tarafı 4 ile bölünürse,

$$\begin{aligned} 27y_1^4 &= \frac{\left(z - \left(x^2 + 18y_1^2\right)\right)\left(z + \left(x^2 + 18y_1^2\right)\right)}{4} \\ &= \frac{\left(z - \left(x^2 + 18y_1^2\right)\right)}{2}\frac{\left(z + \left(x^2 + 18y_1^2\right)\right)}{2} \\ &= \left(\frac{z + x^2}{2} + 9y_1^2\right)\left(\frac{z - x^2}{2} - 9y_1^2\right) \end{aligned}$$

elde edilir. Bu eşitlikte sağ taraftaki öğeler pozitiftir. d_1, $\left(\frac{z + x^2}{2} + 9y_1^2\right)$ ve $\left(\frac{z - x^2}{2} - 9y_1^2\right)$ sayılarının en büyük ortak böleni olsun. Dolayısıyla $d_1 \mid \frac{z + x^2}{2} + 9y_1^2$ ve $d_1 \mid \frac{z - x^2}{2} - 9y_1^2$ olur. $27y_1^4 = \left(\frac{z + x^2}{2} + 9y_1^2\right)\left(\frac{z - x^2}{2} - 9y_1^2\right)$ olduğundan $d_1^2 \mid 27y_1^4$ bulunur. Buradan $d_1^2 \mid 81y_1^4$ olacağından $d_1^2 \mid \left(9y_1^2\right)^2$ elde edilir. Böylece Teorem 1.1.10'a göre $d_1 \mid 9y_1^2$ bulunur. $d_1 \mid \frac{z - x^2}{2} - 9y_1^2$ ve $d_1 \mid \frac{z + x^2}{2} + 9y_1^2$ olduğundan $d_1 \mid \left(\frac{z + x^2}{2} + 9y_1^2\right) - \left(\frac{z - x^2}{2} - 9y_1^2\right)$ olup $d_1 \mid x^2 + 18y_1^2$ olduğu görülür. $d_1 \mid 9y_1^2$ ve $d_1 \mid x^2 + 18y_1^2$ olduğundan buradan $d_1 \mid x^2$ elde edilir. Aynı zamanda $d_1 \mid \frac{z - x^2}{2} - 9y_1^2$ ve $d_1 \mid \frac{z + x^2}{2} + 9y_1^2$ olduğundan $d_1 \mid \frac{z + x^2}{2} + 9y_1^2 + \frac{z - x^2}{2} - 9y_1^2$ olup $d_1 \mid z$ olur. Böylece $d_1 \mid x^2$ ve $d_1 \mid z$ ve böylece $d_1 \mid \left(x^2, z\right)$ dir. Şu halde $\left(x, z\right) = 1$ olduğundan Teorem 1.1.7'ye göre $\left(x^2, z\right) = 1$ olur. O halde $d_1 \mid 1$, ve buradan $d_1 = 1$ bulunur.

$27y_1^{\,4} = \left(\frac{z + x^2}{2} + 9y_1^{\,2}\right)\left(\frac{z - x^2}{2} - 9y_1^{\,2}\right)$ ve $\left(\frac{z + x^2}{2} + 9y_1^{\,2}, \frac{z - x^2}{2} - 9y_1^{\,2}\right) = 1$

olduğundan Teorem 3.1.3'e göre , $\frac{z + x^2}{2} + 9y_1^{\,2} = ua^4$, $\frac{z - x^2}{2} - 9y_1^{\,2} = vb^4$, $uv = 27$, $y_1 = ab$ olacak şekilde u, v, a, b pozitif tamsayıları vardır. Burada $uv = 27$ ve $\left(\frac{z + x^2}{2} + 9y_1^{\,2}, \frac{z - x^2}{2} - 9y_1^{\,2}\right) = 1$ olduğundan $u = 3, v = 9$ ve $u = 9, v = 3$ olamaz. Yani burada ya $u = 1, v = 27$ ya da $u = 27, v = 1$ olabilir. O halde ya $\frac{z + x^2}{2} + 9y_1^{\,2} = 27a^4$, $\frac{z - x^2}{2} - 9y_1^{\,2} = b^4$ ya da $\frac{z + x^2}{2} + 9y_1^{\,2} = a^4$, $\frac{z - x^2}{2} - 9y_1^{\,2} = 27b^4$ olacaktır. Burada $\left(\frac{z + x^2}{2} + 9y_1^{\,2}, \frac{z - x^2}{2} - 9y_1^{\,2}\right) = 1$ olduğundan $\left(a^4, b^4\right) = 1$ olup Teorem 1.1.8'e göre $\left(a, b\right) = 1$ dir. $\frac{z + x^2}{2} + 9y_1^{\,2} = 27a^4$, $\frac{z - x^2}{2} - 9y_1^{\,2} = b^4$ eşitliklerini taraf tarafa çıkarırsak ve $y_1 = ab$ yazarsak,

$$x^2 + 18a^2b^2 = 27a^4 - b^4$$

ve böylece

$$x^2 + b^4 = 27a^4 - 18a^2b^2$$

elde edilir. Ayrıca buradan $x^2 + b^4 = 3\left(9a^4 - 6a^2b^2\right)$ elde edilir. O halde $3 \mid x^2 + b^4$, yani $x^2 + b^4 \equiv 0 \pmod 3$ olur. Halbuki $b^4 \equiv 0, 1 \pmod 3$ ve $3 \nmid x$ olduğundan $x^2 \equiv 1 \pmod 3$ olup $x^2 + b^4 \equiv 1, 2 \pmod 3$ olduğu açıktır. $\frac{z + x^2}{2} + 9y_1^{\,2} = a^4$ ve $\frac{z - x^2}{2} - 9y_1^{\,2} = 27b^4$ eşitlliklerini taraf tarafa toplarsak ve $y_1 = ab$ yazarsak,

$$x^2 + 18a^2b^2 = a^4 - 27b^4$$

elde edilir. x tek olduğundan denklemin sol tarafı tektir. Bu yüzden sağ tarafta tek olmalıdır. Bu ise a ve b sayılarının birinin tek birinin çift olmasını gerektirir. Eğer a çift olursa, $18a^2b^2 \equiv 0 (\bmod 8)$, x tek olduğundan $x^2 \equiv 1 (\bmod 8)$, b tek olduğundan $27b^4 \equiv 3 (\bmod 8)$ olup $a^4 = x^2 + 18a^2b^2 + 27b^4$ olduğundan $a^4 \equiv 4 (\bmod 8)$ olur. Halbuki a çift olduğundan $a^4 \equiv 0 (\bmod 8)$ olduğu açıktır. O halde b çifttir. b çift ve $a^4 = x^2 + 18a^2b^2 + 27b^4$ olduğundan $108b^4 = a^4 - x^2 - 18a^2b^2 + 81b^4$ yazılır. Böylece $108b^4 = \left(a^2 - 9b^2\right)^2 - x^2$, yani $108b^4 = \left(a^2 - 9b^2 - x\right)\left(a^2 - 9b^2 + x\right)$ olur. $108b^4 = \left(a^2 - 9b^2 - x\right)\left(a^2 - 9b^2 + x\right)$ eşitliğinin her iki tarafını 4 ile bölersek,

$$
\begin{aligned}
27b^4 &= \frac{\left(a^2 - 9b^2 - x\right)\left(a^2 - 9b^2 + x\right)}{4} \\
&= \left(\frac{a^2 + x}{2} - \frac{9b^2}{2}\right)\left(\frac{a^2 - x}{2} - \frac{9b^2}{2}\right)
\end{aligned}
$$

elde edilir. $d_2 = \left(\frac{a^2 + x}{2} - \frac{9b^2}{2}, \frac{a^2 - x}{2} - \frac{9b^2}{2}\right)$ olsun. Böylece $d_2 \mid \frac{a^2 + x}{2} - \frac{9b^2}{2}$, $d_2 \mid \frac{a^2 - x}{2} - \frac{9b^2}{2}$ olur. Bu ise $d_2^{\,2} \mid \left(\frac{a^2 + x}{2} - \frac{9b^2}{2}\right)\left(\frac{a^2 - x}{2} - \frac{9b^2}{2}\right) = 27b^4$ olmasını gerektirir. Şu halde $d_2^{\,2} \mid 81b^4$ ve böylece $d_2 \mid 9b^2$ bulunur. $d_2 \mid \frac{a^2 + x}{2} - \frac{9b^2}{2}$, $d_2 \mid \frac{a^2 - x}{2} - \frac{9b^2}{2}$ olduğundan $d_2 \mid \left(\frac{a^2 + x}{2} - \frac{9b^2}{2}\right) - \left(\frac{a^2 - x}{2} - \frac{9b^2}{2}\right)$, yani $d_2 \mid x$ olur.

$y_1 = ab$, $y = 2y_1$ olduğundan $y = 2ab$ ve buradan da $9y^2 = 9.4a^2b^2$ olur. Bu ise $d_2 \mid 9b^2$ olduğundan $d_2 \mid 9y^2$ olmasını gerektirir. O halde $d_2 \mid x$ ve $d_2 \mid 9y^2$ olup $d_2 \mid \left(9y^2, x\right)$ olur. $(3y, x) = 1$ olduğundan Teorem 1.1.7'ye göre $\left((3y)^2, x\right) = 1$, yani $\left(9y^2, x\right) = 1$ dir. Yani $d_2 \mid 1$ olup $d_2 = 1$'dir.

$27b^4 = \left(\frac{a^2 + x}{2} - \frac{9b^2}{2}\right)\left(\frac{a^2 - x}{2} - \frac{9b^2}{2}\right)$ eşitliğinin sol tarafının pozitif bir tamsayıya eşit olduğu açıktır. Bu nedenle $\frac{a^2 \pm x}{2} - \frac{9b^2}{2}$ sayıları aynı işaretlidir. Eğer $\frac{a^2 \pm x}{2} - \frac{9b^2}{2}$ sayılarının ikisi de negatif olursa, $a^2 \pm x - 9b^2 < 0$ olur. Buradan $a^2 \pm x < 9b^2$ eşitsizliklerini taraf tarafa toplarsak $a^2 < 9b^2$ bulunur. $x^2 + 18a^2b^2 = a^4 - 27b^4$ olduğundan $a^4 - 27b^4 > 0$ olup buradan $a^4 > 27b^4$ elde edilir. Böylece $a^2 > 3\sqrt{3}b^2$ olur. Bu ise $a^2 < 9b^2$ olması ile çelişir. O halde $\frac{a^2 + x}{2} - \frac{9b^2}{2}$ ve $\frac{a^2 - x}{2} - \frac{9b^2}{2}$ sayıları aralarında asal pozitif tamsayılardır. Böylece Teorem 3.1.3'e göre $\frac{a^2 \pm x}{2} - \frac{9b^2}{2} = m^4$, $\frac{a^2 \pm x}{2} - \frac{9b^2}{2} = 27n^4$, $b = mn$ olacak şekilde m, n pozitif tamsayıları vardır. Bu eşitlikleri taraf tarafa toplarsak, $a^2 = m^4 + 9m^2n^2 + 27n^4$ ve $a \le y_1 < y < z$ olur. Bu ise z sayısının en küçük olması ile çelişir. Sonuç olarak, kabülümüz yanlıştır. $x^4 + 9x^2y^2 + 27y^4 = z^2$ denkleminin pozitif tamsayılarda çözümü yoktur.

Lemma 3.1.22. $a, b \in \mathbb{Z}$ olsun. $a^3 \mid 2b^3$ ise $a \mid b$'dir.

İspat: $a^3 \mid 2b^3$ olsun. a, b tamsayılarını $a = 2^r x$, x tek ve $b = 2^s y$, y tek olarak yazabiliriz. O halde $a^3 \mid 2b^3$ olduğundan buradan $2^{3r} x^3 \mid 2.2^{3s} y^3$ olup $2^{3r} x^3 \mid 2^{3s+1} y^3$ elde edilir. Böylece $2^{3r} \mid 2^{3s+1} y^3$ olur. y tek olduğundan $\left(2^{3r}, y^3\right) = 1$ dir. Şu halde Teorem 1.1.6'ya göre $2^{3r} \mid 2^{3s+1}$ bulunur. Buradan $3r < 3s + 1$ olup $r \le s$ dir. Gerçekten, $r > s$ olursa $3r > 3s$ olup $3r \ge 3s + 1$ çelişkisi elde edilir. $r \le s$ olduğundan $2^r \mid 2^s$ dir. $2^{3r} x^3 \mid 2^{3s+1} y^3$ olduğundan $x^3 \mid 2^{3s+1} y^3$ olur. x tek olduğundan $\left(x^3, 2^{3s+1}\right) = 1$ dir. O halde Teorem 1.1.6'ya göre $x^3 \mid y^3$ olur. Buradan Teorem 1.1.10'a göre $x \mid y$ dir. $2^r \mid 2^s$ ve $x \mid y$ olduğundan $2^r x \mid 2^s y$ olup $a \mid b$ bulunur.

Teorem 3.1.23. $x^3 + y^3 = 2z^3$ denkleminin $x \ne y$ ve $z \ne 0$ şartını sağlayan (x, y, z) tamsayı çözümü yoktur [1] .

İspat: Kabul edelim ki $x^3+y^3=2z^3$ denklemi tamsayılarda (x,y,z) çözümüne sahip olsun ve $x \neq y$, $z \neq 0$ olsun.

$(x,y)=1$ kabul edebiliriz. Gerçekten, $(x,y)=d>1$ olduğunda $x=dx_1$, $y=dy_1$, $(x_1,y_1)=1$ olacak şekilde x_1,y_1 tamsayıları vardır. $x=dx_1$, $y=dy_1$ eşitliklerini $x^3+y^3=2z^3$ denkleminde yerine yazarsak $d^3x_1^3+d^3y_1^3=2z^3$ olur. Buradan $d^3\left(x_1^3+y_1^3\right)=2z^3$ bulunur. Bu ise $d^3 \mid 2z^3$ olmasını gerektirir. Böylece Lemma 3.1.22' e göre $d \mid z$'dir. Sonuç olarak, $z=dz_1$ olacak şekilde z_1 tamsayısı vardır. $x=dx_1$, $y=dy_1$, $z=dz_1$ eşitliklerini $x^3+y^3=2z^3$ denkleminde yerine yazarsak $x_1^3+y_1^3=2z_1^3$ elde edilir. Yani $(x_1,y_1)=1$ olmak üzere $x_1^3+y_1^3=2z_1^3$ olur.

$x^3+y^3=2z^3$ denkleminden dolayı x ve y sayılarının ya ikisi de çifttir ya da ikisi de tektir. O halde $x+y$ ve $x-y$ çifttir. Şu halde $u=\dfrac{x+y}{2}$ ve $v=\dfrac{x-y}{2}$ tamsayılardır. Bu eşitlikleri taraf tarafa toplar ve çıkarırsak sırasıyla $x=u+v$, $y=u-v$ olur. $(x,y)=1$ olduğundan $(u+v,u-v)=1$ olup buradan $(u,v)=1$ olduğu görülür. $x=u+v$, $y=u-v$ değerleri $x^3+y^3=2z^3$ denkleminde yerine yazılırsa ,

$$\begin{aligned} 2z^3 &= (u+v)^3+(u-v)^3 \\ &= 2u^3+6uv^2 \end{aligned}$$

ve böylece

$$z^3=u\left(u^2+3v^2\right)$$

elde edilir. $x \neq y$, $z \neq 0$ ve $u=\dfrac{x+y}{2}, v=\dfrac{x-y}{2}$ olduğundan $uvz=\dfrac{1}{4}\left(x^2-y^2\right)z \neq 0$ bulunur.

1. durum: Eğer $(u,3)=1$ ise $(u,v)=1$ olduğundan $(u,3v^2+u^2)=1$ dir. $u(u^2+3v^2)=z^3$ ve $(u,3v^2+u^2)=1$ olduğundan Teorem 3.1.3'e göre $u=z_1^3$, $u^2+3v^2=z_2^3$ olacak şekilde z_1, z_2 tamsayıları vardır. Buradan

$$z_2^3-z_1^6=z_2^3-\left(z_1^3\right)^2=u^2+3v^2-u^2=3v^2$$

olduğu görülür.

$$z_2^3-z_1^6=\left(z_2^3-\left(z_1^2\right)^3\right)=\left(z_2-z_1^2\right)\left(z_2^2+z_2z_1^2+z_1^4\right)=\left(z_2-z_1^2\right)\left(\left(z_2-z_1\right)^2+3z_2z_1^2\right)$$

olduğundan $\left(z_2-z_1^2\right)\left(\left(z_2-z_1^2\right)^2+3z_2z_1^2\right)=3v^2$'dir. Burada $t=z_2-z_1^2$ diyelim. $(u,3v^2+u^2)=1$ ve $u=z_1^3$, $u^2+3v^2=z_2^3$ olduğundan $\left(z_1^3,z_2^3\right)=1$ olur. O halde Teorem 1.1.8'e göre $(z_1,z_2)=1$ bulunur. Aynı zamanda $(t,z_1)=1$ dir. Gerçekten $t=z_2-z_1^2$ oludğundan $(t,z_1)=\lambda$ ise $\lambda\,|\,z_2-z_1^2$ ve $\lambda\,|\,z_1$ olur. Buradan $\lambda\,|\,z_2$ olduğu görülür. $\lambda\,|\,z_1$ ve $\lambda\,|\,z_2$ olduğundan $\lambda\,|\,(z_1,z_2)$ bulunur. Böylece $(z_1,z_2)=1$ olduğundan $\lambda\,|\,1$ ve dolayısıyla $\lambda=1$ dir. $\left(z_2-z_1^2\right)\left(\left(z_2-z_1^2\right)^2+3z_2z_1^2\right)=3v^2$ eşitliğinde $t=z_2-z_1^2$ değerini yerine yazarsak $t\left(t^2+3\left(t+z_1^2\right)z_1^2\right)=3v^2$ ve böylece $t\left(t^2+3tz_1^2+3z_1^4\right)=3v^2$ bulunur. Buradan $3\,|\,t$ elde edilir. O halde $t=3t_1$ olacak şekilde t_1 tamsayısı vardır. $t\left(t^2+3tz_1^2+3z_1^4\right)=3v^2$ eşitliğinde $t=3t_1$ değeri yerine yazılırsa,

$$3t_1\left(9t_1^2+9t_1z_1^2+3z_1^4\right)=3v^2$$

ve böylece

$$3t_1\left(3t_1^2+3t_1z_1^2+z_1^4\right)=v^2$$

elde edilir. Buradan $3\,|\,v^2$ olduğu ve 3 asal olduğundan $3\,|\,v$ olduğu görülür. Şu halde $v=3v_1$ olacak şekilde v_1 tamsayısı vardır. Ayrıca $3\,|\,v$ olduğundan $9\,|\,v^2$ dir. $u=z_1^3$ ve $(u,3)=1$ olduğundan $\left(z_1^3,3\right)=1$'dir. Teorem 1.1.8'e göre $(z_1,3)=1$ olur. Böylece $3\nmid z_1$ dir. Buradan $9\nmid 9t_1^2+9t_1z_1^2+3z_1^4$ olduğu görülür. $9\,|\,v^2$ ve $t_1\left(9t_1^2+9t_1z_1^2+3z_1^4\right)=v^2$ olduğundan $9\,|\,t_1\left(9t_1^2+9t_1z_1^2+3z_1^4\right)$ olur. $9=3.3$, $3\,|\,9t_1^2+9t_1z_1^2+3z_1^4$ ve $9\nmid 9t_1^2+9t_1z_1^2+3z_1^4$ olduğundan $3\,|\,t_1$ bulunur. O halde

$t_1 = 3t_2$ olacak şekilde t_2 tamsayısı vardır. $t_1\left(9t_1^2 + 9t_1 z_1^2 + 3z_1^4\right) = v^2$ eşitliğinde $t_1 = 3t_2$ ve $v = 3v_1$ değerlerini yerine yazarsak,

$$9v_1^2 = 3t_2\left(81t_2^2 + 27t_2 z_1^2 + 3z_1^4\right)$$
$$= 9t_2\left(27t_2^2 + 9t_2 z_1^2 + z_1^4\right)$$

ve böylece

$$v_1^2 = t_2\left(27t_2^2 + 9t_2 z_1^2 + z_1^4\right)$$

elde edilir. $t = 3t_1$ ve $t_1 = 3t_2$ olduğundan $t = 9t_2$ bulunur. O halde $(t, z_1) = 1$ olduğundan $(9t_2, z_1) = 1$ dir. Yani $(3^2 t_2, z_1) = 1$ dir. $(3, z_1) = 1$ olduğundan Teorem 1.1.7'ye göre $(3^2, z_1) = 1$ olur. Böylece $(t_2, z_1) = 1$ bulunur. Şu halde $\left(t_2, 27t_2^2 + 9t_2 z_1^2 + z_1^4\right) = 1$ elde edilir. $t_2\left(27t_2^2 + 9t_2 z_1^2 + z_1^4\right) = v_1^2$ ve $\left(t_2, 27t_2^2 + 9t_2 z_1^2 + z_1^4\right) = 1$ olduğundan Teorem 3.1.3'e göre $t_2 = b^2$, $27t_2^2 + 9t_2 z_1^2 + z_1^4 = c^2$ olacak şekilde b, c pozitif tamsayıları vardır. Burada $t_2 = b^2$ değerini $27t_2^2 + 9t_2 z_1^2 + z_1^4 = c^2$ denkleminde yerine yazarsak $27b^4 + 9b^2 z_1^2 + z_1^4 = c^2$ elde edilir. Halbuki Teorem 3.1.21'e göre $27b^4 + 9b^2 z_1^2 + z_1^4 = c^2$ denkleminin pozitif tamsayılarda çözümü yoktur. Denklemdeki kuvvetler çift olduğundan negatif tamsayılarda da çözümü yoktur. Burada $b = 0$ veya $z_1 = 0$ olduğundaki durumu incelememiz yeterli olacaktır. $b = 0$ ise $t_2 = b^2$ olduğundan $t_2 = 0$ dır. Dolayısıyla $t = 9t_2$ olduğundan $t = 0$ olur. Şu halde $t = z_2 - z_1^2 = 0$ olup $z_2 = z_1^2$ bulunur. $(z_1, z_2) = 1$ olduğundan $z_2 = 1$, $z_1 = \pm 1$'dir. Böylece $t_2 = 0$, $z_1 = \pm 1$ ve $t_2\left(27t_2^2 + 9t_2 z_1^2 + z_1^4\right) = v_1^2$ olduğundan $v_1 = 0$ elde edilir. $v = 3v_1$ olduğundan $v = 0$ 'dır. O halde $x = u + v$ ve $y = u - v$ olduğundan $x = y$ bulunur. Bu ise kabülümüz ile çelişir. Diğer taraftan $z_1 = 0$ ise $(3, z_1) = 1$ olması ile çelişir. Sonuç olarak, bu durumdan çözüm elde edilemez.

2. durum: Eğer $3 \mid u$ ise $(u, v) = 1$ olduğundan $3 \nmid v$ 'dir. Yani $(v, 3) = 1$'dir. $3 \mid u$ olduğundan $u = 3u_1$ olacak şekilde u_1 tamsayısı vardır. $u\left(u^2 + 3v^2\right) = z^3$ ve $3 \mid u$

olduğundan $3|z^3$ bulunur. Böylece 3 asal olduğundan $3|z$'dir. O halde $z=3z_1$ olacak şekilde z_1 tamsayısı vardır. $u=3u_1$ ve $z=3z_1$ değerleri $u\left(u^2+3v^2\right)=z^3$ eşitliğinde yerine yazılırsa,

$$3u_1\left(9u_1^{\ 2}+3v^2\right)=27z_1^{\ 3}$$

ve buradan

$$u_1\left(3u_1^{\ 2}+v^2\right)=3z_1^{\ 3}$$

elde edilir. O halde $3|u_1\left(3u_1^{\ 2}+v^2\right)$ olduğu görülür. Yani $3|3u_1^{\ 3}+u_1v^2$ olur. Ayrıca $(v,3)=1$ olduğundan $3|u_1$ dir. Böylece $u_1=3u_2$ olacak şekilde u_2 tamsayısı vardır. $u_1=3u_2$ değeri $u_1\left(3u_1^{\ 2}+v^2\right)=3z_1^{\ 3}$ eşitliğinde yerine yazılırsa,

$$u_2\left(27u_2^{\ 2}+v^2\right)=z_1^{\ 3}$$

elde edilir. $u=3u_1$ ve $u_1=3u_2$ olduğundan $u=9u_2$ olur. Böylece $(u,v)=1$ olduğu dikkate alınırsa $(9u_2,v)=1$ olduğu görülür. Yani $\left(3^2u_2,v\right)=1$ olur. $(v,3)=1$ olduğundan Teorem 1.1.7'ye göre $\left(v,3^2\right)=1$ dir. Şu halde $(u_2,v)=1$ bulunur. Buradan $\left(u_2,27u_2^{\ 2}+v^2\right)=1$ elde edilir. $u_2\left(27u_2^{\ 2}+v^2\right)=z_1^{\ 3}$ ve $\left(u_2,27u_2^{\ 2}+v^2\right)=1$ olduğundan Teorem 3.1.3'e göre $u_2=a^3$, $27u_2^{\ 2}+v^2=b^3$ olacak şekilde a,b tamsayıları vardır. Böylece $\left(a^3,b^3\right)=1$ olup Teorem 1.1.8'e göre $(a,b)=1$ dir. $(v,3)=1$ olduğundan $3\nmid 27u^2+v^2$ ve böylece $27u_2^{\ 2}+v^{\ 2}=b$ olduğu dikkate alınırsa $3\nmid b^3$ olduğu görülür. Yani $\left(b^3,3\right)=1$ olur. Buradan Teroem 1.1.8'e göre $(b,3)=1$ ve böylece $k=b-3a^2$ dersek $(k,3)=1$ bulunur. $u_2=a^3$ değerini $27u_2^{\ 2}+v^2=b^3$ eşitliğinde yerine yazarsak,

$$\begin{aligned}v^2&=b^3-27a^6\\&=b^3-\left(3a^2\right)^3\\&=\left(b-3a^2\right)\left(b^2+3a^2b+9a^4\right)\end{aligned}$$

ve böylece

$$v^2=\left(b-3a^2\right)\left(\left(b-3a^2\right)^2+9a^2\left(b-3a^2\right)+27a^4\right)$$

elde edilir. $k=b-3a^2$ değeri yerine yazılırsa $v^2=k\left(k^2+9a^2k+27a^4\right)$ bulunur. $(a,b)=1$ ve $k=b-3a^2$ olduğundan $(a,k)=1$ ve buradan da $(k,3)=1$ olduğu dikkate alınırsa $\left(k,k^2+9a^2k+27a^4\right)=1$ olduğu görülür. $v^2=k\left(k^2+9a^2k+27a^4\right)$ ve $\left(k,k^2+9a^2k+27a^4\right)=1$ olduğundan Teorem 3.1.3'e göre $k=a_1^{\,2}$, $k^2+9a^2k+27a^4=b_1^2$ olacak şekilde a_1,b_1 pozitif tamsayıları vardır. $k=a_1^2$ değerini $k^2+9a^2k+27a^4=b_1^2$ denkleminde yerine yazarsak $a_1^{\,4}+9a^2a_1^{\,2}+27a^4=b_1^2$ olur. Halbuki Teorem 3.1.21'e göre $a_1^{\,4}+9a^2a_1^{\,2}+27a^4=b_1^2$ denkleminin pozitif tamsayılarda çözümü yoktur. Denklemdeki kuvvetler çift olduğundan negatif tamsayılarda da çözüm yoktur. Burada $a=0$ veya $a_1=0$ olduğundaki durumları incelememiz yeterli olacaktır.

$a_1=0$ ise $k=a_1^2$ ve böylece $k=0$ olur. Bu ise $(k,3)=1$ olması ile çelişir. $a=0$ ise $u_2=a^3$ olduğundan $u_2=0$'dır. Ayrıca $u=3u_1$, $u_1=3u_2$ olduğu dikkate alınırsa $u=9u_2$ olur. Buradan $u_2=0$ olduğu için $u=0$ bulunur. Böylece $u\left(u^2+3v^2\right)=z^3$ olduğundan $z=0$ olur. Bu ise $z\neq 0$ olması ile çelişir. Sonuç olarak, bu durumdan da çözüm elde edilemez.

Tanım 3.1.24. $m\geq 1$ olmak üzere m bir tamsayı olsun. $\dfrac{m(m+1)}{2}$ formundaki sayılara üçgensel sayı denir.

Sonuç 3.1.25. Bir doğal sayının küpü olan 1'den büyük üçgensel sayı yoktur [1].

İspat: Kabul edelim ki bir doğal sayının küpü olan 1'den büyük bir üçgensel sayı var olsun. O zaman $m(m+1)=2n^3$ olacak biçimde $m>1$ olan m ve n doğal sayıları vardır. m çift ise, $m=2k$ olacak şekilde k doğal sayısı vardır. $m=2k$ değeri $m(m+1)=2n^3$ eşitliğinde yerine yazılırsa, $2k(2k+1)=2n^3$ ve buradan $k(2k+1)=n^3$ elde edilir. Burada $(k,2k+1)=1$ dir. $(k,2k+1)=1$ ve $k(2k+1)=n^3$

olduğundan Teorem 3.1.3'e göre $k = z^3$, $2k+1 = x^3$ olacak şekilde z, x pozitif tamsayıları vardır. Buradan $x^3 - 2z^3 = 2k+1-2k = 1$ olur. Bu ise Teorem 3.1.23'e göre mümkün değildir.

m tek ise $m = 2k-1$ olacak şekilde k pozitif tamsayısı vardır. $m > 1$ olduğundan $k > 1$'dir. $m(m+1) = 2n^3$ ve $m = 2k-1$ olduğundan $(2k-1)k = n^3$ elde edilir. Burada $(k, 2k-1) = 1$ dir. $(2k-1)k = n^3$ ve $(k, 2k-1) = 1$ olduğu kullanılırsa Teorem 3.1.3'e göre $2k-1 = x^3$, $k = z^3$ olacak şekilde x, z pozitif tamsayılarının mevcut olduğu görülür. Böylece $x^3 - 2z^3 = 2k-1-2k = -1$ bulunur. Yani $x^3 + 1 = 2z^3$ olur. Bu ise Teorem 3.1.23'e göre mümkün değildir.

Sonuç 3.1.26. $x^2 - y^3 = 1$ denkleminin pozitif tamsayılarda çözümü sadece $(x, y) = (3, 2)$'dir [1].

İspat: Kabul edelim ki $x \neq 3$ olmak üzere (x, y), $x^2 - y^3 = 1$ denkleminin pozitif tamsayılarda bir çözümü olsun. x çift ise $x = 2k$ olacak şekilde k pozitif tamsayısı vardır. Dolayısıyla $(x-1, x+1) = 1$'dir.

$x^2 - y^3 = 1$ olduğundan $x^2 - 1 = y^3$ olup buradan $(x+1)(x-1) = y^3$ yazılır. Böylece $(x-1, x+1) = 1$ olduğundan Teorem 3.1.3'e göre $x-1 = a^3$, $x+1 = b^3$ olacak şekilde a, b pozitif tamsayıları vardır. O halde $b^3 - a^3 = x+1-(x-1) = 2$ bulunur. Buradan $b^3 - a^3 = (b-a)(b^2+ab+a^2) = 2$ olur. Bu ise $b^2+ab+a^2 \mid 2$ olmasını gerektirir. Halbuki a, b pozitif tamsayılar olduğundan $b^2+ab+a^2 > 2$ olup bu bir çelişkidir. x tek ise $x = 2k+1$ olacak şekilde k pozitif tamsayısı vardır. Ayrıca burada $x \neq 3$ olduğundan $k > 1$ olmalıdır. $x^2 - 1 = y^3$ ve x tek olduğundan y çifttir. O halde $y = 2n$ olacak şekilde n pozitif tamsayısı vardır. $x = 2k+1$, $y = 2n$ değerleri $x^2 - 1 = y^3$ denkleminde yerine yazılırsa,

$$(2k+1)^2 - 1 = (2n)^3$$

ve buradan

$$4k^2+4k+1-1=8n^3$$

yani

$$k(k+1)=2n^3$$

elde edilir. Böylece $k>1$ olmak üzere $k(k+1)=2n^3$ olur. Bu ise Sonuç 3.1.25'e göre mümkün değildir.

Sonuç 3.1.27. $n,\ n>1$ olan bir doğal sayı ise $1^3+2^3+...+n^3$ sayısı bir doğal sayının küpü değildir [1] .

İspat: Teorem 1.1.20 'ye göre $1^3+2^3+...+n^3=\left(\frac{n(n+1)}{2}\right)^2$ dir. $\frac{n(n+1)}{2}=t_n$ diyelim. O zaman $1^3+2^3+...+n^3=\left(\frac{n(n+1)}{2}\right)^2=t_n^{\ 2}$ olur. Burada kabul edelim ki $t_n^{\ 2}$ bir doğal sayının küpü olsun. O halde $t_n^{\ 2}=a^3$ olacak şekilde a doğal sayısı vardır. Böylece Teorem 1.1.19'a göre $t_n=k^3,\ a=k^2$ olacak şekilde k doğal sayısı vardır. Buradan $\frac{n(n+1)}{2}=t_n$ olduğundan $\frac{n(n+1)}{2}=k^3$ elde edilir. Bu ise Sonuç 3.1.25 ile çelişir. O halde kabulümüz yanlıştır.

BÖLÜM 4. MORDELL DENKLEMLERİ

Tanım 4.1.1. k bir tamsayı olmak üzere $x^2+k=y^3$ denklemine Mordell denklemi denir.

Teorem 4.1.2. a bir tek tamsayı , b , 3 ile bölünmeyen bir çift tamsayı olmak üzere ve a ile b tamsayılarının $4t+3$ formunda bir ortak böleni olmasın. Bu durumda $k=b^2-a^3$ ve k , $8t-1$ formunda değil ise $x^2+k=y^3$ denklemi tamsayılarda çözüme sahip değildir [1].

İspat: (x,y) tamsayı ikilisinin $x^2+k=y^3$ denkleminin bir çözümü olduğunu kabul edelim. b çift ve a tek olduğundan $k=b^2-a^3$ sayısı tektir. O halde y çift olursa $x^2+k=y^3$ olduğundan x tek olur. Böylece $y^3\equiv 0(\bmod 8)$ ve $x^2\equiv 1(\bmod 8)$'dir. Bu denkliklerden $8\,|\,y^3$ ve $8\,|\,x^2-1$ elde edilir. $x^2+k=y^3$ olduğundan $k=y^3-x^2$ dir. Buradan $k+1=y^3-(x^2-1)$ yazılırsa $8\,|\,y^3$ ve $8\,|\,x^2-1$ olduğundan $8\,|\,k+1$ bulunur. O halde $k+1=8t$ olacak şekilde t tamsayısı vardır. Böylece $k=8t-1$ olur. Bu ise Teoremin hipotezi ile çelişir. O halde y tek olmalıdır. O halde $x^2+k=y^3$ olduğundan x çift olup $x=2u$ olacak şekilde u tamsayısı vardır. b de çift tamsayı olduğundan $b=2c$ olacak şekilde c tamsayısı vardır. $x^2+k=y^3$ denkleminde $k=b^2-a^3$ değeri yerine yazılırsa $x^2+b^2=y^3+a^3$ bulunur. $x=2u$ ve $b=2c$ olduğundan $x^2+b^2=4u^2+4c^2=4(u^2+c^2)$'dir. O halde buradan $4(u^2+c^2)=y^3+a^3=(y+a)(y^2-ay+a^2)$ olur. Böylece $4\,|\,(y+a)(y^2-ay+a^2)$ bulunur. y ve a tek olduğundan $y-a$ çifttir. Bu ise $y^2-ay+a^2=(y-a)y+a^2$ sayısının tek olmasını gerektirir. O zaman y^2-ay+a^2 tek olduğundan

$\left(4, y^2 - ay + a^2\right) = 1$ olur. Teorem 1.1.6'ya göre $4 \mid y + a$ bulunur. Öyleyse $y + a = 4v$ olacak şekilde v tamsayısı vardır. Buradan $y = 4v - a$ yazılır . Ayrıca $y + a - 2a = 4v - 2a$ olup $y - a = 4v - 2a$ bulunur. O halde $(y-a)y = (4v-2a)(4v-a) = 16v^2 - 12av + 2a^2 = 4\left(4v^2 - 3av\right) + 2a^2$ elde edilir. $w = 4v^2 - 3av$ alınırsa $y^2 - ay = (y-a)y = 4w + 2a^2$ olur. Böylece $y^2 - ay + a^2 = 4w + 3a^2$'dir. a tek olduğundan $a^2 \equiv 1 \pmod 4$ olup $4w + 3a^2 \equiv 3 \pmod 4$ bulunur. O zaman $y^2 - ay + a^2 = 4w + 3a^2$ eşitliğinin sağ tarafı $4t + 3$ formundadır. Bu ise $4w + 3a^2$ sayısının $4t + 3$ formunda bir p asal bölenine sahip olmasını gerektirir. $4w + 3a^2$ sayısı c, d tamsayılar olmak üzere $c^2 + d^2$ formunda yazılamaz. Gerçekten, aksine kabul edelim ki $4w + 3a^2 = c^2 + d^2$ olarak yazılsın. Burada c, d sayılarını her ikisi çift ise $c^2 \equiv 0 \pmod 4$, $d^2 \equiv 0 \pmod 4$ olup $c^2 + d^2 \equiv 0 \pmod 4$ bulunur. Bu ise $4w + 3a^2 \equiv 3 \pmod 4$ olması ile çelişir. c, d sayılarının her ikisi de tek ise $c^2 \equiv 1 \pmod 4$, $d^2 \equiv 1 \pmod 4$ olup $c^2 + d^2 \equiv 2 \pmod 4$ olur. Bu ise $4w + 3a^2 \equiv 3 \pmod 4$ olması ile çelişir. c, d sayılarının biri tek diğeri çift olsun. Kabul edelim ki c çift olsun. O halde $c^2 \equiv 0 \pmod 4$, $d^2 \equiv 1 \pmod 4$ olup $c^2 + d^2 \equiv 1 \pmod 4$ bulunur. Bu da $4w + 3a^2 \equiv 3 \pmod 4$ olması ile çelişir. $4w + 3a^2$ sayısı $c^2 + d^2$ formunda yazılamadığından Teorem 1.1.11'e göre $4w + 3a^2$ sayısının $4t + 3$ formundaki asal böleninin maksimum üssü tek olur. Yani , p asal sayı olmak üzere $p^s \mid 4w + 3a^2$ şartını sağlayan maksimum s tektir. O halde $s = 2\alpha - 1$ olacak şekilde bir α tamsayısı vardır. O halde $p^{2\alpha-1} \mid 4w + 3a^2$ dir. Böylece $y^2 - ay + a^2 = 4w + 3a^2$ olduğundan $p^{2\alpha-1} \mid y^2 - ay + a^2$ yazılır. Ayrıca $x^2 + b^2 = (y+a)\left(y^2 - ay + a^2\right)$ olduğundan $y^2 - ay + a^2 \mid x^2 + b^2$ olur. Geçişme özelliğinden $p^{2\alpha-1} \mid x^2 + b^2$ bulunur. Burada $d = (x, b)$ olsun. O halde $x = dx_1$, $b = db_1$, $(x_1, b_1) = 1$ olacak şekilde x_1, b_1 tamsayıları vardır. Bu değerleri yerine yazarsak $p^{2\alpha-1} \mid d^2\left(x_1^2 + b_1^2\right)$ bulunur. Bu ise $p \mid d^2\left(x_1^2 + b_1^2\right)$ olmasını gerektirir. Burada eğer $p \mid x_1^2 + b_1^2$ ise p asalı $4t + 3$

formunda olduğundan Teorem 1.1.12'ye göre $p \mid x_1$ ve $p \mid b_1$ olur. Bu $(x_1, b_1) = 1$ olması ile çelişir. O halde $p \nmid x_1^2 + b_1^2$ dir. Böylece p asal olduğundan $\left(p, x_1^2 + b_1^2\right) = 1$ olur. O halde Teorem 1.1.6'ya göre $p \mid d^2$ dir. Bu ise p asal olduğundan $p \mid d$ olmasını gerektirir. Şu halde $d = p^t.a,\ p \nmid a$ olacak şekilde bir a tamsayısı vardır. $\left(p, x_1^2 + b_1^2\right) = 1$ olduğundan Teorem 1.1.7'ye göre $\left(p^{2\alpha-1}, x_1^2 + b_1^2\right) = 1$'dir. Buradan ayrıca $p^{2\alpha-1} \mid d^2\left(x_1^2 + b_1^2\right)$ olduğundan Teorem 1.1.6'ya göre $p^{2\alpha-1} \mid d^2$ bulunur. Böylece $p^{2\alpha-1} \mid d^2$ olduğundan $p^{2\alpha-1} \mid p^{2t}a^2$ yazılır. $p \nmid a$ ve p asal olduğundan $(p, a) = 1$'dir. Teorem 1.1.7'ye göre $\left(p^{2\alpha-1}, a^2\right) = 1$'dir. O halde Teorem 1.1.6'ya göre $p^{2\alpha-1} \mid p^{2t}$ elde edilir. Bu ise $2\alpha - 1 < 2t$ olmasını gerektirir. Şu halde $2\alpha \le 2t$ olur. Öyleyse $p^{2\alpha} \mid p^{2t}$ ve dolayısıyla $p^{2\alpha} \mid p^{2t}a^2$ olur. $d^2 = p^{2t}a^2$ olduğundan $p^{2\alpha} \mid d^2$'dir. O zaman Teorem 1.1.10'a göre $p^{\alpha} \mid d$'dir. Sonuç olarak, $x = dx_1$, $b = db_1$ olduğundan $p^{\alpha} \mid x$ ve $p^{\alpha} \mid b$ olur. Şu halde $p^{2\alpha} \mid x^2$ ve $p^{2\alpha} \mid b^2$ olup buradan $p^{2\alpha} \mid x^2 + b^2$ bulunur. $x^2 + b^2 = (y + a)\left(y^2 - ay + a^2\right)$ olduğundan $p^{2\alpha} \mid (y + a)\left(y^2 - ay + a^2\right)$'dir. Yani $p^{2\alpha-1}p \mid (y + a)\left(y^2 - ay + a^2\right)$'dir. $y^2 - ay + a^2$ yi bölen p^s ler için en büyük üs $s = 2\alpha - 1$ olduğundan $p \mid y + a$ olur. Aynı zamanda $p^{2\alpha-1} \mid y^2 - ay + a^2$ olduğu dikkate alınırsa $p \mid y^2 - ay + a^2$ bulunur. Böylece $y^2 - ay + a^2 = (y + a)(y - 2a) + 3a^2$ olduğundan $p \mid 3a^2$ dir. Ayrıca $p^{\alpha} \mid b$ ve p asal olduğundan $p \mid b$ elde edilir. $p \mid 3a^2$ ve $p \mid b$ olması $p \mid \left(3a^2, b\right)$ olmasını gerektirir. b, 3 tarafından bölünemediğinden $p \mid \left(a^2, b\right)$ yazılır. Böylece $p \mid a^2$ ve $p \mid b$ olup $p \mid a$ ve $p \mid b$'dir. Bu ise a ve b sayılarının $4t + 3$ formunda ortak böleni olmaması ile çelişir.

Örnek 4.1.3. $k = 3, 5, 17, -11, -13$ için $x^2 + k = y^3$ denklemi tamsayılarda bir çözüme sahip değildir.

Çözüm: $3=2^2-1^3$, $5=2^2-(-1)^3$, $-11=4^2-3^3$, $17=4^2-(-1)^3$, $-13=70^2-17^3$ olduğundan Teorem 4.1.2'e göre $k=3,5,17,-11,-13$ için $x^2+k=y^3$ denkleminin çözümü yoktur.

Teorem 4.1.4. a, $4t+2$ formunda bir tamsayı ve b, 3 ile bölünmeyen tek tamsayı olsun. Ayrıca a ile b sayıları $4t+3$ formunda bir ortak bölene sahip olmasın. Eğer $k=b^2-a^3$ ise $x^2+k=y^3$ denklemi tamsayılarda çözüme sahip değildir [1].

İspat: (x,y), $x^2+k=y^3$ denkleminin tamsayılarda bir çözümü olsun. a çift, b tek olduğundan $a^3\equiv 0(\mathrm{mod}\,8)$, $b^2\equiv 1(\mathrm{mod}\,8)$ olur. $k=b^2-a^3$ olduğundan $k=1(\mathrm{mod}\,8)$ elde edilir. O halde k sayısı $8t+1$ formundadır. Eğer y çift ise $y^3\equiv 0(\mathrm{mod}\,8)$ olur. Buradan $x^2+k=y^3$ olduğundan $x^2=y^3-k$ ve böylece $x^2\equiv -1\equiv 7(\mathrm{mod}\,8)$ bulunur. Halbuki k tek, y çift olduğundan x tek olup $x^2\equiv 1(\mathrm{mod}\,8)$ olduğu açıktır. O halde y tektir. k tek, y tek olduğundan x çift olur.

Eğer y, $4t+1$ formunda ise $y+a=4t+1+4t+2=4(2t)+3$ olur. $2t=w$ dersek $y+a=4w+3$ bulunur. O halde $y+a$ sayısı $4t+3$ formunda bir p asal bölenine sahiptir. $y+a$ sayısı c^2+d^2 formunda yazılamaz. Gerçekten, $y+a=c^2+d^2$ olduğunu kabul edelim. $c^2+d^2\equiv 0,1,2(\mathrm{mod}\,4)$ olur ki bu $y+a\equiv 3(\mathrm{mod}\,4)$ olması ile çelişir. O halde Teorem 1.1.11'e göre $y+a$ sayısını bölen $4t+3$ formundaki asal bölenlerin maksimum üssü tektir. Yani , p asal sayı olmak üzere $p^\mu \mid y+a$ şartını sağlayan maksimum μ tektir. O halde $\mu=2\alpha-1$ olacak şekilde α tamsayısı vardır.

$k=b^2-a^3$ ve $x^2+k=y^3$ olduğundan $x^2+b^2=y^3+a^3=(y+a)(y^2-ay+a^2)$ olur. O halde $p^{2\alpha-1}\mid y+a$ olduğundan $p^{2\alpha-1}\mid x^2+b^2$ bulunur. Burada Teorem 4.1.3'ün ispatında olduğu gibi $p^\alpha \mid b$, $p^\alpha \mid x$ ve $p\mid 3a^2$ olduğu görülür. Böylece p asal sayı olduğundan $p\mid b$ olup b sayısı 3 tarafından bölünemediğinden $p\neq 3$ olur. Şu halde

$(p,3)=1$ dir. O halde $p\,|\,3a^2$ olduğu dikkate alınırsa Teorem 1.1.6'ya göre $p\,|\,a^2$ olduğu görülür. p asal sayı olduğundan $p\,|\,a$ olur. $p\,|\,a$ ve $p\,|\,b$ olması $p\,|\,(a,b)$ olmasını gerektirir. Bu ise a ile b sayısının $4t+3$ formunda ortak böleni olmaması ile çelişir. $y=4t+3$ formunda ise $y-a=4t+3-(4t-2)=1$ olduğundan $y-a\equiv 1(\mathrm{mod}\,4)$ elde edilir. Yani $y-a$, $4t+1$ formundadır. $y^2-ay=y(y-a)\equiv 3(\mathrm{mod}\,4)$ olur. a çift olduğundan $a^2\equiv 0(\mathrm{mod}\,4)$ olup $y^2-ay+a^2\equiv 3(\mathrm{mod}\,4)$ olur. Yani y^2-ay+a^2 $4t+3$ formundadır. O halde y^2-ay+a^2 sayısının aynı formda bir p asal böleni vardır. y^2-ay+a^2 sayısı iki kare toplamı şeklinde yazılamaz. Gerçekten, $y^2-ay+a^2=c^2+d^2$ olacak şekilde c,d tamsayılarının var olduğunu kabul edelim. Burada $c^2+d^2\equiv 0,1,2(\mathrm{mod}\,4)$ olur. Bu ise $y^2-ay+a^2\equiv 3(\mathrm{mod}\,4)$ olması ile çelişir. O halde Teorem 1.1.12'ye göre y^2-ay+a^2 sayısının $4t+3$ formundaki asal bölenlerinin üssü tektir. Yani, p asal sayı olmak üzere $p^s\,|\,y^2-ay+a^2$ olan en büyük s sayısı bir tek tamsayıdır. O halde $s=2\beta-1$ olacak şekilde β tamsayısı vardır. $x^2+b^2=y^3+a^3=(y+a)(y^2-ay+a^2)$ olduğundan $y^2-ay+a^2\,|\,x^2+b^2$ dir. Aynı zamanda $p^{2\beta-1}\,|\,y^2-ay+a^2$ olduğu dikkate alınırsa $p^{2\beta-1}\,|\,x^2+b^2$ olduğu görülür. $d=(x,b)$ olsun. Böylece $x=dx_1$, $b=db_1$, $(x_1,b_1)=1$ olacak şekilde x_1,b_1 tamsayıları vardır. Bu değerleri yerine yazarsak $p^{2\beta-1}\,|\,d^2\left(x_1^2+b_1^2\right)$ ve buradan $p\,|\,d^2\left(x_1^2+b_1^2\right)$ bulunur. $p\,|\,x_1^2+b_1^2$ ise Teorem 1.1.12'ye göre $p\,|\,x_1$ ve $p\,|\,b_1$ olur. Bu ise $(x_1,b_1)=1$ olması ile çelişir. O halde $p\nmid x_1^2+b_1^2$ dir ve p asal olduğundan $\left(p,x_1^2+b_1^2\right)=1$ olur. O halde Teorem 1.1.6'ya göre $p\,|\,d^2$ dir. Bu ise p asal olduğundan $p\,|\,d$ olmasını gerektirir. Şu halde $d=p^t\alpha$, $p\nmid\alpha$ olacak şekilde α tamsayısı vardır. $\left(p,x_1^2+b_1^2\right)=1$ olduğundan Teorem 1.1.7'ye göre $\left(p^{2\beta-1},x_1^2+b_1^2\right)=1$ dir. Dolayısıyla $p^{2\beta-1}\,|\,d^2\left(x_1^2+b_1^2\right)$ olduğundan Teorem 1.1.6'ya göre $p^{2\beta-1}\,|\,d^2$ bulunur. Dolayısıyla $p^{2\beta-1}\,|\,d^2$ olduğu kullanırsa

$p^{2\beta-1} \mid p^{2t}a^2$ bulunur. $p \nmid a$ ve p asal olduğundan $(p,a)=1$ olup Teorem 1.1.7'ye göre $\left(p^{2\beta-1},a^2\right)=1$ dir. Dolayısıyla Teorem 1.1.6'ya göre $p^{2\beta-1} \mid p^{2t}$ olur. Bu ise $2\beta-1<2t$ olmasını gerektirir. Böylece $2\beta \le 2t$ bulunur. Şu halde $p^{2\beta} \mid p^{2t}$ olup $p^{2\beta} \mid p^{2t}a^2$ yazılır. $d^2=p^{2t}a^2$ olduğundan $p^{2\beta} \mid d^2$ elde edilir. Bu ise $p^{\beta} \mid d$ olmasını gerektirir. Sonuç olarak, $x=dx_1$, $b=db_1$ olduğundan $p^{\beta} \mid x$ ve $p^{\beta} \mid b$ olup buradan $p^{2\beta} \mid x^2$, $p^{2\beta} \mid b^2$ elde edilir. Böylece $p^{2\beta} \mid x^2+b^2$ olur. $x^2+b^2=y^3+a^3=(y+a)\left(y^2-ay+a^2\right)$ olduğundan $p^{2\beta} \mid (y+a)\left(y^2-ay+a^2\right)$ olur. Yani $p^{2\beta-1}p \mid (y+a)\left(y^2-ay+a^2\right)$ dir. y^2-ay+a^2 sayısını bölen asal sayının en büyük üssü $2\beta-1$ olduğundan $p \mid y+a$ dır. $p^{2\beta-1} \mid \left(y^2-ay+a^2\right)$ ve p asal olduğu kullanılırsa $p \mid y^2-ay+a^2$ elde edilir. O halde $y^2-ay+a^2=(y+a)(y-2a)+3a^2$ olduğundan $p \mid 3a^2$ bulunur. $p^{\beta} \mid b$ ve p asal olduğu için $p \mid b$ dir. Bu ise $p \mid \left(3a^2,b\right)$ olmasını gerektirir. b, 3 ile bölünemediğinden $p \mid \left(a^2,b\right)$ yazılır. Buradan $p \mid a^2$, $p \mid b$ olup p asal olduğundan $p \mid a$, $p \mid b$ elde edilir. Bu ise a ve b sayılarının $4t+3$ formunda ortak böleni olmaması ile çelişir.

Örnek 4.1.5. $k=9$ ve $k=-7$ için $x^2+k=y^3$ denkleminin çözümü yoktur.

Çözüm: $9=1^2-(-2)^3$, $-7=1^2-2^3$ olduğundan Teorem 4.1.4'e göre $k=9$ ve $k=-7$ için $x^2+k=y^3$ denkleminin tamsayılarda çözümü yoktur.

Teorem 4.1.6. $x^2+12=y^3$ denklemi tamsayılarda çözüme sahip değildir [1].

İspat: (x,y), $x^2+12=y^3$ denkleminin tamsayılarda bir çözümü olsun. Eğer x çift ise $x=2x_1$ olacak şekilde x_1 tamsayısı vardır. $x^2+12=y^3$ ve x çift olduğundan y sayısı da aynı zamanda çifttir. O halde $y=2y_1$ olacak şekilde y_1 tamsayısı vardır.

$x=2x_1$, $y=2y_1$ eşitliklerini $x^2+12=y^3$ denkleminde yerine yazarsak, $4x_1^2+12=8y_1^3$ olup buradan $x_1^2+3=2y_1^3$ bulunur. Böylece x_1 sayısının tek olduğu görülür. Sonuç olarak, $x_1^2\equiv 1(\bmod 8)$ olur. Diğer bir deyişle x_1 sayısı $8t+1$ formundadır. O halde $2y_1^3=x_1^2+3=8t+4$ olup $2y_1^3\equiv 4(\bmod 8)$ olur. Aynı zamanda $y_1^3=4t+2$ olduğundan y_1^3 çift olur. Bu ise y_1 sayısının çift olmasını gerektirir. Böylece $y_1^3\equiv 0(\bmod 8)$ olup $2y_1^3\equiv 0(\bmod 8)$ elde edilir. Bu ise $2y_1^3\equiv 4(\bmod 8)$ olması ile çelişir. Sonuç olarak, x ve y tek olmalıdır.

$x^2+12=y^3$ olduğu kullanılırsa $x^2+4=y^3-8=(y-2)(y^2+2y+4)$ bulunur. y tek olduğundan $y^2\equiv 1(\bmod 4)$, $2y\equiv 2(\bmod 4)$ olur. O halde $y^2+2y+4\equiv 3(\bmod 4)$ elde edilir. Diğer bir deyişle y^2+2y+4 sayısı $4t+3$ formundadır. $x^2+2^2=y^3-8=(y-2)(y^2+2y+4)$ olduğundan $y^2+2y+4 \mid x^2+2^2$ olup x^2+2^2 sayısı $4t+3$ formunda bir bölene sahiptir. O halde x^2+2^2 sayısı $4t+3$ formunda bir p asal bölene de sahiptir. O halde Teorem 1.1.12'ye göre $p\mid x$ ve $p\mid 2$ olur. Bu ise 2 sayısı $4t+3$ formunda bir asal sayı tarafından bölünemeyeceğinden bir çelişkidir.

Teorem 4.1.7. $x^2+16=y^3$ denklemi tamsayılarda çözüme sahip değildir [1].

İspat: Eğer x çift ise $x^2+16=y^3$ olduğundan y sayısı da çifttir. Böylece $x=2x_1$, $y=2y_1$ olacak şekilde x_1, y_1 tamsayıları vardır. Bu eşitlikleri $x^2+16=y^3$ denkleminde yerine yazarsak $4x_1^2+16=8y_1^3$ olup $x_1^2+4=2y_1^3$ bulunur. Şu halde x_1 sayısının çift olduğu görülür. Öyleyse $x_1=2x_2$ olacak şekilde x_2 tamsayısı vardır. $x_1=2x_2$ değeri $x_1^2+4=2y_1^3$ denkleminde yerine yazılırsa $4x_2^2+4=2y_1^3$ ve buradan $2x_2^2+2=y_1^3$ bulunur. Böylece y_1^3 sayısının çift olduğu görülür. Bu ise y_1 sayısının çift olmasını gerektirir. O halde $y_1=2y_2$ olacak şekilde y_2 tamsayısı vardır. $y_1=2y_2$ değeri $2x_2^2+2=y_1^3$ denkleminde yerine yazılırsa $2x_2^2+2=8y_2^3$

yani $x_2^{\,2}+1=4y_2^{\,3}$ elde edilir. Bu ise $x_2^{\,2}=-1\equiv 3\pmod 4$ olmasını gerektirir. Halbuki $x_2^{\,2}\equiv 0,1\pmod 4$ olduğu açıktır. O halde x tektir. x tek olduğundan $x^2\equiv 1\pmod 8$ olur. Böylece $16\equiv 0\pmod 8$ olduğundan $x^2+16\equiv 1\pmod 8$ bulunur. Şu halde $x^2+16=y^3$ olduğundan $y^3\equiv 1\pmod 8$ olur. Diğer bir ifadeyle y^3 sayısı $8t+1$ formundadır. Bu y sayının da $8t+1$ formunda olmasını gerektirir. Sonuç olarak , $y-2=8t+1-2$, yani $y-2$ sayısı $8t-1$ formundadır. $y^3-8=(y-2)\left(y^2+2y+4\right)$ olduğundan $y-2\,|\,y^3-8$ olur. $x^2+16=y^3$ olduğundan $y^3-8=x^2+8$ olup $y-2\,|\,x^2+8$ bulunur. O halde x^2+8 sayısı $8t-1$ formunda bir bölene sahiptir. Böylece x^2+8 sayısı ya $8t+5$ ya da $8t+7$ formunda bir p asal bölenine sahiptir. Bu ise bir çelişkidir. Gerçekten, kabul edelim ki p asal sayı olmak üzere $p\,|\,x^2+8$ olsun. Buradan $x^2\equiv -8\pmod p$ olur. Tanım 1.1.13 ve Tanım 1.1.14'e göre $\left(\frac{-8}{p}\right)=1$ olur. Böylece Teorem 1.1.15'den $\left(\frac{-8}{p}\right)=\left(\frac{-2}{p}\right)\left(\frac{4}{p}\right)$ ve $\left(\frac{4}{p}\right)=\left(\frac{2^2}{p}\right)=1$ olup $\left(\frac{-8}{p}\right)=\left(\frac{-2}{p}\right)\left(\frac{4}{p}\right)=\left(\frac{-2}{p}\right)=1$ bulunur. Bu ise Sonuç 1.1.17'ye göre $p\equiv 1,3\pmod 8$ olmasını gerektirir. Yani p asalı $8t+1$ ya da $8t+3$ formundadır.

Teorem 4.1.8. $x^2-16=y^3$ denkleminin tamsayılarda $(x,y)=(\pm 4,0)$ çözümünden başka çözümü yoktur [1].

İspat: (x,y), $x^2-16=y^3$ denkleminin bir çözümü olsun. Eğer x sayısı tek ise $(x+4,x-4)=1$ olur. Gerçekten, $(x+4,x-4)=\delta$ olsun. Tanım gereği $\delta\,|\,x+4$, $\delta\,|\,x-4$ olur. Buradan $\delta\,|\,(x+4)+(x-4)$ ve $\delta\,|\,(x+4)-(x-4)$ olup $\delta\,|\,2x$ ve $\delta\,|\,8$ bulunur. Bu ise $\delta\,|\,(2x,8)$ olmasını gerektirir. Şu halde $\delta\,|\,2(x,4)$ olur. x tek olduğundan $(x,4)=1$ olup $\delta\,|\,2$ elde edilir. Yine x tek olduğundan $x+4$ ve $x-4$ tek olup δ bu sayıları böldüğünden $\delta\neq 2$ olmalıdır. O halde $\delta=1$'dir.

$x^2 - 16 = y^3$ denklemini $(x-4)(x+4) = y^3$ olarak yazabiliriz. O halde Teorem 3.1.3'e göre $x+4 = a^3$, $x-4 = b^3$ olacak şekilde a,b tamsayıları vardır. Burada $x+4$ ve $x-4$ tek olduğundan a, b sayıları da tektir. Buradan $a^3 - b^3 = 8$ bulunur. a, b tek tamsayı olduklarından $a = 2k+1$, $b = 2t+1$ olacak şekilde k, t pozitif tamsayıları vardır. O halde $a^3 = 8k^3 + 12k^2 + 6k + 1$, $b^3 = 8t^3 + 12t^2 + 6t + 1$ bulunur. $a^3 - b^3 = 8(k^3 - t^3) + 12(k^2 - t^2) + 6(k-t)$ eşitliği 8'e eşit olamaz. Gerçekten, burada $k = t$ olursa $a^3 - b^3 = 0$ olur. Ayrıca genelliği bozmadan $k > t$ kabul edelim. Bu takdirde k ve t pozitif tamsayılar olduğundan $k^3 - t^3 \geq 1$, $k^2 - t^2 \geq 1$, $k - t \geq 1$ olur. Böylece

$$a^3 - b^3 = 8(k^3 - t^3) + 12(k^2 - t^2) + 6(k-t) \geq 8 + 12 + 6 = 26$$

elde edilir. Bu ise $a^3 - b^3 = 8$ olması ile çelişir. O halde x çifttir. Şu halde $x = 2x_1$ olacak şekilde x_1 tamsayısı vardır. $x^2 - 16 = y^3$ ve x çift olduğundan y de çifttir. O zaman $y = 2y_1$ olacak şekilde y_1 tamsayısı vardır. $x = 2x_1$, $y = 2y_1$ eşitlikleri $x^2 - 16 = y^3$ denkleminde yerine yazılırsa $4x_1^2 - 16 = 8y_1^3$ ve böylece $x_1^2 - 4 = 2y_1^3$ bulunur. O halde x_1 çifttir. Dolayısıyla $x_1 = 2x_2$ oalcak şekilde x_2 tamsayısı vardır. Bu eşitliği $x_1^2 - 4 = 2y_1^3$ denkleminde yerine yazarsak $4x_2^2 - 4 = 2y_1^3$ ve buradan $2x_2^2 - 2 = y_1^3$ elde edilir. Dolayısıyla y_1 çifttir. O halde $y_1 = 2y_2$ olacak şekilde y_2 tamsayısı vardır. Bu eşitliği $2x_2^2 - 2 = y_1^3$ denkleminde yerine yazarsak $2x_2^2 - 2 = 8y_2^3$, yani $x_2^2 - 1 = 4y_2^3$ olur. Buradan x_2 sayısının tek olduğu görülür. Öyleyse $x_2 = 2x_3 + 1$ olacak şekilde x_3 tamsayısı vardır. $x_2 = 2x_3 + 1$ değeri $x_2^2 - 1 = 4y_2^3$ denkleminde yerine yazılırsa $4x_3^2 + 4x_3 + 1 - 1 = 4y_2^3$ ve buradan $x_3^2 + x_3 = y_2^3$ elde edilir. O halde $x_3(x_3 + 1) = y_2^3$ olur. x_3 ve $x_3 + 1$ ardışık sayılar olduğundan $(x_3, x_3 + 1) = 1$'dir. O halde Teorem 3.1.3'e göre $x_3 = a^3$, $x_3 + 1 = b^3$ olacak şekilde a,b tamsayıları vardır. Fakat iki ardışık tamsayı sadece ya -1 ve 0 ya da 0 ve 1 olduğu durumda tamsayıların küpüdür. Şu halde $x_3 = -1$, $x_3 + 1 = 0$ olduğunda $x_3(x_3 + 1) = -1.0 = 0$ olduğundan $y_2^3 = 0$, yani $y_2 = 0$ dır. Diğer yandan

$x_3 = 0$, $x_3 + 1 = 1$ olduğunda da $x_3(x_3+1) = 0.1 = 0$ olduğundan $y_2{}^3 = 0$ olup yine $y_2 = 0$ elde edilir. O halde $y = 2y_1$, $y_1 = 2y_2$ olduğu kullanılırsa $y = 0$ bulunur. Dolayısıyla $x^2 - 16 = y^3$ olduğundan $x^2 = 16$ ve buradan $x = \pm 4$ bulunur. Sonuç olarak, denklemin çözümü $(x, y) = (\pm 4, 0)$'dır.

BÖLÜM 5. GENELLEŞTİRİLMİŞ FİBONACCİ VE LUCAS DİZİLERİ YARDIMI İLE DENKLEM ÇÖZÜMLERİ

Tanım 5.1.1. $F_0 = 0$, $F_1 = 1$ ve $n \geq 2$ olmak üzere $F_n = F_{n-1} + F_{n-2}$ tekrarlama bağıntısı ile tanımlanan $\{F_n\}$ dizisine Fibonacci dizisi denir ve F_n sayısına n. Fibonacci sayısı denir.

Tanım 5.1.2. $L_0 = 2$, $L_1 = 1$ ve $n \geq 2$ olmak üzere $L_n = L_{n-1} + L_{n-2}$ tekrarlama bağıntısı ile tanımlanan $\{L_n\}$ dizisine Lucas dizisi denir ve L_n sayısına n. Lucas sayısı denir.

Tanım 5.1.3. k ve s sıfırdan farklı tamsayılar ve $k^2 + 4s > 0$ olsun. $U_0(k,s) = 0$, $U_1(k,s) = 1$, $n \geq 2$ için $U_n(k,s) = kU_{n-1}(k,s) + sU_{n-2}(k,s)$, $V_0(k,s) = 2$, $V_1(k,s) = k$, $n \geq 2$ için $V_n(k,s) = kV_{n-1}(k,s) + sV_{n-2}(k,s)$ biçiminde tanımlanan $\{U_n\}$ ve $\{V_n\}$ dizilerine sırasıyla Genelleştirilmiş Fibonacci ve Lucas dizileri denir.

Genelleştirilmiş Fibonacci ve Lucas sayıları negatif indisler için $n \geq 1$ olmak üzere $U_{-n}(k,s) = \dfrac{-U_n(k,s)}{(-s)^n}$, $V_{-n}(k,s) = \dfrac{V_n(k,s)}{(-s)^n}$ olarak tanımlanır.

$k = s = 1$ için $\{U_n\}$ ve $\{V_n\}$ dizileri sırasıyla Fibonacci ve Lucas dizilerini temsil eder. $\{U_n\}$ ve $\{V_n\}$ dizilerinin karakteristik denklemi $x^2 - kx - s = 0$ dır. Bu denklemin kökleri $\alpha = \dfrac{k + \sqrt{k^2 + 4s}}{2}$ ve $\beta = \dfrac{k - \sqrt{k^2 + 4s}}{2}$ olmak üzere $U_n(k,s) = \dfrac{\alpha^n - \beta^n}{\alpha - \beta}$, $V_n(k,s) = \alpha^n + \beta^n$ dir. Bu formüllere Binet Formülleri denir.

Ayrıca $n \geq 1$ için $\alpha + \beta = k$, $\alpha\beta = -s$ ’dir.

Özel olarak, eğer $k \geq 1$, $\alpha = \dfrac{k+\sqrt{k^2+4}}{2}$, $\beta = \dfrac{k-\sqrt{k^2+4}}{2}$ ise

$U_n(k,1) = \dfrac{\alpha^n - \beta^n}{\alpha - \beta}$ ve $V_n(k,1) = \alpha^n + \beta^n$

dir. Eğer $k \geq 3$, $\alpha = \dfrac{k+\sqrt{k^2-4}}{2}$, $\beta = \dfrac{k-\sqrt{k^2-4}}{2}$ ise

$U_n(k,-1) = \dfrac{\alpha^n - \beta^n}{\alpha - \beta}$ ve $V_n(k,-1) = \alpha^n + \beta^n$

dir. Eğer $\alpha = \dfrac{1+\sqrt{5}}{2}$, $\beta = \dfrac{1-\sqrt{5}}{2}$ ise

$F_n = \dfrac{\alpha^n - \beta^n}{\alpha - \beta}$, $L_n = \alpha^n + \beta^n$

dir.

Teorem 5.1.4. k, s sıfırdan farklı tamsayılar olsun. Her $n \in \mathbb{Z}$ için $V_n = U_{n+1} + sU_{n-1} = kU_n + 2sU_{n-1}$ ve $\left(k^2+4s\right)U_n = V_{n+1} + sV_{n-1}$’dir.

İspat: Binet formüllerinden $U_n = \dfrac{\alpha^n - \beta^n}{\alpha - \beta}$, $V_n = \alpha^n + \beta^n$ olduğunu kullanırsak,

$$\begin{aligned} U_{n-1} + sU_{n-1} &= \frac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta} + s\frac{\alpha^{n-1} - \beta^{n-1}}{\alpha - \beta} \\ &= \frac{\alpha^n\left(\alpha + s\alpha^{-1}\right) - \beta^n\left(\beta + s\beta^{-1}\right)}{\alpha - \beta} \end{aligned}$$

bulunur. $\alpha\beta = -s$ olduğundan $\dfrac{1}{\alpha} = \alpha^{-1} = -\dfrac{\beta}{s}$, $\dfrac{1}{\beta} = \beta^{-1} = -\dfrac{\alpha}{s}$ olur. Bu ise $s\alpha^{-1} = -\beta$ ve $s\beta^{-1} = -\alpha$ olmasını gerektirir. O halde

$$\begin{aligned} U_{n+1} + sU_{n-1} &= \frac{\alpha^n\left(\alpha - \beta\right) - \beta^n\left(\beta - \alpha\right)}{\alpha - \beta} \\ &= \frac{\alpha^n\left(\alpha - \beta\right) + \beta^n\left(\alpha - \beta\right)}{\alpha - \beta} \end{aligned}$$

$$= \frac{(\alpha-\beta)\left(\alpha^n+\beta^n\right)}{\alpha-\beta}$$

$$= \alpha^n+\beta^n = V_n$$

elde edilir. Ayrıca, $U_{n+1} = kU_n + sU_{n-1}$ olduğundan

$$V_n = U_{n+1} + sU_{n-1} = kU_n + sU_{n-1} + sU_{n-1} = kU_n + 2sU_{n-1}$$

bulunur.

Şimdi Binet formüllerinden yararlanarak $V_{n+1} + sV_{n-1} = \left(k^2+4s\right)U_n$ olduğunu gösterelim.

$$V_{n+1} + sV_{n-1} = \alpha^{n+1} + \beta^{n+1} + s\left(\alpha^{n-1} + \beta^{n-1}\right)$$

$$= \alpha^n\left(\alpha + s\alpha^{-1}\right) + \beta^n\left(\beta + s\beta^{-1}\right)$$

olup $s\alpha^{-1} = -\beta$ ve $s\beta^{-1} = -\alpha$ olduğundan

$$V_{n+1} + sV_{n-1} = \alpha^n(\alpha-\beta) + \beta^n(\beta-\alpha)$$

$$= \alpha^n(\alpha-\beta) - \beta^n(\alpha-\beta)$$

$$= \left(\alpha^n-\beta^n\right)(\alpha-\beta)$$

$$= \left(\alpha^n-\beta^n\right)(\alpha-\beta)\frac{(\alpha-\beta)}{\alpha-\beta}$$

$$= \left(\frac{\alpha^n-\beta^n}{\alpha-\beta}\right)(\alpha-\beta)^2$$

bulunur. Burada $\alpha-\beta = \sqrt{k^2+4s}$ olduğundan $(\alpha-\beta)^2 = k^2+4s$ olduğu kullanılırsa

$$V_{n+1} + sV_{n-1} = \left(\frac{\alpha^n-\beta^n}{\alpha-\beta}\right)\left(k^2+4s\right)$$

$$= U_n\left(k^2+4s\right)$$

elde edilir.

Bundan sonra özel olarak $\{U_n(k,1)\}$, $\{V_n(k,1)\}$, $\{U_n(k,-1)\}$, $\{V_n(k,-1)\}$ dizilerini kullanacağız. Aynı zamanda $\{U_n(k,1)\}$, $\{V_n(k,1)\}$ dizilerini sırasıyla $\{U_n\}$ ve $\{V_n\}$ ile $\{U_n(k,-1)\}$, $\{V_n(k,-1)\}$ dizilerini de sırasıyla $\{u_n\}$ ve $\{v_n\}$ ile göstereceğiz.

Teorem 5.1.5. $k \geq 1$ bir tamsayı, k^2+4 tamkare olmayan bir tamsayı olmak üzere $\alpha = \dfrac{k+\sqrt{k^2+4}}{2}$ olsun. Bu takdirde $\mathbb{Z}[\alpha] = \{a\alpha + b \mid a,b \in \mathbb{Z}\}$, $Q\left(\sqrt{k^2+4}\right)$ reel kuadratik cisminin bir alt halkasıdır. Ayrıca $\mathbb{Z}[\alpha]$, $Q\left(\sqrt{k^2+4}\right)$ reel kuadratik cisminin tamsayılarının bir alt halkasıdır [3].

Tanım 5.1.6. $a\alpha + b \in \mathbb{Z}[\alpha]$ olsun. $a\alpha + b$ sayısının eşleniği $\overline{\alpha} = \beta$ olmak üzere $\overline{a\alpha + b} = a\beta + b$ olarak tanımlanır.

Teorem 5.1.7. $k \geq 1$ bir tamsayı, $\alpha = \dfrac{k+\sqrt{k^2+4}}{2}$, $\overline{\alpha} = \beta$ olmak üzere $\alpha x + y \in \mathbb{Z}[\alpha]$ birimdir $\Leftrightarrow (\alpha x + y)(\beta x + y) = \pm 1 \Leftrightarrow -x^2 + kxy + y^2 = \pm 1$ dir [3].

Teorem 5.1.8. $k \geq 1$ ve $\alpha = \dfrac{k+\sqrt{k^2+4}}{2}$ olmak üzere $\mathbb{Z}[\alpha] = \{a\alpha + b \mid a,b \in \mathbb{Z}\}$ halkasının birimlerinin kümesi $\{\pm\alpha^n \mid n \in \mathbb{Z}\}$ 'dir [3].

İspat: $n \in \mathbb{Z}$ olmak üzere $\pm\alpha^n$ ler birimdir. Gerçekten, $n \geq 0$ ise $\pm\alpha^n = \pm\left(\dfrac{1}{\alpha^{-n}}\right) = \pm\left(\dfrac{1}{\alpha}\right)^{-n}$ olup $\alpha\overline{\alpha} = -1$ olduğundan $\pm\alpha^n = \pm\left(-\overline{\alpha}\right)^{-n}$ olur. $-\overline{\alpha}$ birim olduğundan $\pm\left(-\overline{\alpha}\right)^{-n}$ de birimdir. Dolayısıyla $\pm\alpha^n$ ler birimdir. $k \geq 1$ olduğundan $\alpha = \dfrac{k+\sqrt{k^2+4}}{2} \geq \dfrac{1+\sqrt{5}}{2} > 1$'dir. İlk olarak $1 < w < \alpha$ şartını sağlayan w biriminin olmadığını gösterelim. Aksine kabul edelim ki $w = \alpha x + y \in \mathbb{Z}[\alpha]$ birimi $1 < w < \alpha$ olmak üzere var olsun. O zaman $\alpha x + y$ birim olduğundan Teorem

5.1.7'ye göre $-x^2+kxy+y^2=(\alpha x+y)(\overline{\alpha}x+y)=\pm 1$'dir. Böylece $\left|(\alpha x+y)(\overline{\alpha}x+y)\right|=|\pm 1|=1$, yani $|(\alpha x+y)||\overline{\alpha}x+y|=1$ olur. Buradan $\alpha x+y>1$ olduğundan $1=|(\alpha x+y)||\overline{\alpha}x+y|>|\overline{\alpha}x+y|$ olup $\left|(\overline{\alpha}x+y)\right|<1$ bulunur. Bu ise $-1<\overline{\alpha}x+y<1$ olmasını gerektirir. Şu halde $-1<\overline{\alpha}x+y$ ve $1<\alpha x+y$ olduğundan bu eşitsizlikleri taraf tarafa toplarsak $0<(\alpha+\overline{\alpha})x+2y$ olur. Böylece $\alpha+\overline{\alpha}=k$ olduğu dikkate alınırsa $kx+2y>0$ elde edilir. Ayrıca $-1<\overline{\alpha}x+y<1$ olduğundan $-1<-\overline{\alpha}x-y<1$ olur. Böylece $-1<-\overline{\alpha}x-y$ ve $1<\alpha x+y$ olduğundan bu eşitsizlikleri taraf tarafa toplarsak $0<(\alpha-\overline{\alpha})x$ bulunur. Şu halde $\alpha-\overline{\alpha}=\sqrt{k^2+4}$ olduğu dikkate alınırsa $0<\left(\sqrt{k^2+4}\right)x$ olur. Bu ise $\sqrt{k^2+4}$ daima pozitif olduğundan $x>0$ olmasını gerektirir. Yani $x\geq 1$'dir. $1<\alpha x+y<\alpha$ ve $x\geq 1$ olduğundan $y<\alpha-\alpha x=\alpha(1-x)\leq 0$ olur. Yani $y<0$'dır. Ayrıca, $-x^2+kxy+y^2=\pm 1$ ve $x\geq 1$ olduğundan $kxy+y^2=\pm 1+x^2\geq 0$ olup $y(kx+y)\geq 0$ bulunur. Bu ise $y<0$ olduğundan $kx+y\leq 0$ olmasını gerektirir. Buradan

$$0<kx+2y=kx+y+y<kx+y\leq 0$$

çelişkisi elde edilir.

Şimdi $w>1$, $w\neq\alpha$ olmak üzere w'nın birim olduğunu kabul edelim. Ayrıca her $n\geq 2$ için $w\neq\alpha^n$ olsun. Şu halde $\alpha^m<w<\alpha^{m+1}$ olacak şekilde $m\geq 1$ şartını sağlayan m doğal sayısı vardır. $\alpha^m<w<\alpha^{m+1}$ eşitsizliğini α^m ile bölersek $1<\dfrac{w}{\alpha^m}<\alpha$ bulunur. w ve α^m birim olduğundan $\dfrac{w}{\alpha^m}$ de birimdir. Fakat $1<\dfrac{w}{\alpha^m}<\alpha$ olduğundan bu mümkün değildir. O halde $w\neq\alpha$, $w>1$şartını sağlayan bir birim ise $w=\alpha^n$ olacak şekilde $n\geq 2$ vardır. Sonuç olarak $w\geq 1$ ise $w=\alpha^n$ olan $n\geq 0$ vardır.

Şimdi $0<w<1$ ve w birim olsun. O zaman $\frac{1}{w}>1$ ve $\frac{1}{w}$ birim olduğundan $\frac{1}{w}=\alpha^n$ olacak şekilde $n\geq 1$ vardır. Dolayısıyla $w=\frac{1}{\alpha^n}=\alpha^{-n}$ olur. O halde $w>0$ birim ise $w=\alpha^n$ olacak şekilde $n\in\mathbb{Z}$ vardır.

Şimdi de $w<0$ ve w birim olsun. O zaman $-w>0$ ve $-w$ birim olduğundan $-w=\alpha^n$ olacak şekilde $n\in\mathbb{Z}$ vardır. Şu halde $w=-\alpha^n$ olan $n\in\mathbb{Z}$ vardır.

Teorem 5.1.9. Her $n\in\mathbb{Z}$ için $U_n^{\,2}-kU_nU_{n-1}-U_{n-1}^{\,2}=(-1)^{n+1}$'dir.

İspat: Binet Formüllerinden $U_n=\frac{\alpha^n-\beta^n}{\alpha-\beta}$, $V_n=\alpha^n+\beta^n$ olduğundan

$$U_n^{\,2}-kU_nU_{n-1}-U_{n-1}^{\,2}=\left(\frac{\alpha^n-\beta^n}{\alpha-\beta}\right)^2-k\left(\frac{\alpha^n-\beta^n}{\alpha-\beta}\right)\left(\frac{\alpha^{n-1}-\beta^{n-1}}{\alpha-\beta}\right)-\left(\frac{\alpha^{n-1}-\beta^{n-1}}{\alpha-\beta}\right)^2$$

$$=\frac{\alpha^{2n}-2(\alpha\beta)^n+\beta^{2n}-k\left(\alpha^{2n-1}+\beta^{2n-1}-(\alpha\beta)^n\left(\beta^{-1}+\alpha^{-1}\right)\right)-\left(\alpha^{2n-2}+\beta^{2n-2}-2(\alpha\beta)^{n-1}\right)}{(\alpha-\beta)^2}$$

$$=\frac{V_{2n}-kV_{2n-1}-2(\alpha\beta)^n+k(\alpha\beta)^n\left(\alpha^{-1}+\beta^{-1}\right)-V_{2n-2}+2(\alpha\beta)^{n-1}}{(\alpha-\beta)^2}$$ bulunur. Böylece

$\alpha\beta=-1$ olduğundan $\frac{1}{\alpha}=\alpha^{-1}=-\beta$, $\frac{1}{\beta}=\beta^{-1}=-\alpha$ dir. Buradan

$$U_n^{\,2}-kU_nU_{n-1}-U_{n-1}^{\,2}=\frac{V_{2n}-kV_{2n-1}-V_{2n-2}-2(-1)^n+k(-1)^n(-\alpha-\beta)+2(-1)^{n-1}}{(\alpha-\beta)^2}$$

$$=\frac{V_{2n}-kV_{2n-1}-V_{2n-2}-2(-1)^n-k(-1)^n(\alpha+\beta)-2(-1)^n}{(\alpha-\beta)^2}$$

elde edilir.. Ayrıca $\alpha+\beta=k$ olduğundan

$$U_n^{\,2}-kU_nU_{n-1}-U_{n-1}^{\,2}=\frac{V_{2n}-kV_{2n-1}-V_{2n-2}-4(-1)^n-k(-1)^n k}{(\alpha-\beta)^2}$$ olur. Böylece

$V_{2n}=kV_{2n-1}+V_{2n-2}$ olduğu kullanılırsa

$$U_n^{\ 2} - kU_nU_{n-1} - U_{n-1}^{\ 2} = \frac{V_{2n} - V_{2n} - 4(-1)^n - k(-1)^n k}{(\alpha-\beta)^2} = \frac{-(-1)^n(k^2+4)}{(\alpha-\beta)^2}$$ bulunur.

Böylece $\alpha - \beta = \sqrt{k^2+4}$ olduğundan $(\alpha-\beta)^2 = k^2+4$ ve buradan

$$U_n^{\ 2} - kU_nU_{n-1} - U_{n-1}^{\ 2} = \frac{-(-1)^n(\alpha-\beta)^2}{(\alpha-\beta)^2} = -(-1)^n = (-1)^{n+1}$$ elde edilir.

Aşağıda vereceğimiz teorem tümevarımla kolay bir şekilde gösterilebilir.

Teorem 5.1.10. $k \geq 1$ bir tamsayı ve $\alpha = \dfrac{k+\sqrt{k^2+4}}{2}$, $\beta = \dfrac{k-\sqrt{k^2+4}}{2}$ olsun. O zaman her $n \in \mathbb{Z}$ için $\alpha^n = \alpha U_n + U_{n-1}$, $\beta^n = \beta U_n + U_{n-1}$'dir.

Uyarı: $\alpha = \dfrac{k+\sqrt{k^2+4}}{2}$ irrasyonel sayıdır. Çünkü, k^2+4 kök dışına çıkmaz. Yani, $k^2+4=t^2$ olan t tamsayısı yoktur. Gerçekten, aksini kabul edelim. Yani, $k^2+4=t^2$ olacak biçimde t tamsayısı mevcut olsun. Buradan $t^2-k^2=4$ olup $(t-k)(t+k)=4$ elde edilir. Bu ise $t-k=1$, $t+k=4$ veya $t-k=2$, $t+k=2$ olmasını gerektirir. Eğer $t-k=1, t+k=4$ olursa $t=\dfrac{5}{2}$ olur. Fakat $\dfrac{5}{2} \notin \mathbb{Z}$ dir. Eğer $t-k=2, t+k=2$ olursa $k=0$ bulunur. Fakat $k \geq 1$ olduğundan bu mümkün değildir.

Teorem 5.1.11. $x^2 - kxy - y^2 = \pm 1$ denkleminin pozitif tamsayılarda çözümleri $n \geq 2$ olmak üzere $(x,y) = (U_n, U_{n-1})$ biçimindedir.

İspat: $(x,y) = (U_n, U_{n-1})$ ise Teorem 5.1.9'a göre $x^2 - kxy - y^2 = U_n^{\ 2} - kU_nU_{n-1} - U_{n-1}^{\ 2} = \pm 1$'dir. Şimdi $x^2 - kxy - y^2 = \pm 1$ denklemini sağlayan x, y pozitif tamsayılarının var olduğunu kabul edelim. O halde Teorem 5.1.7'ye göre $\alpha x + y$, $\mathbb{Z}[\alpha]$ halkasının birimidir ve $\alpha x + y > 1$ dir. Şu halde Teorem 5.1.10'a göre $\alpha x + y = \alpha^n$ olacak şekilde $n \geq 2$ olan n tamsayısı vardır. Böylece Teorem 5.1.10'a göre $\alpha x + y = \alpha^n = \alpha U_n + U_{n-1}$ olur. Bu ise α irrasyonel olduğundan $x = U_n$, $y = U_{n-1}$ olmasını gerektirir.

Sonuç 5.1.12. $x^2 - kxy - y^2 = 1$ denkleminin tüm pozitif tamsayı çözümleri , $n \geq 1$ olmak üzere $(x, y) = (U_{2n+1}, U_{2n})$ biçimindedir .

Sonuç 5.1.13. $x^2 - kxy - y^2 = -1$ denkleminin tüm pozitif tamsayı çözümleri , $n \geq 1$ olmak üzere $(x, y) = (U_{2n}, U_{2n-1})$ biçimindedir .

Teorem 5.1.14. Her $n \in \mathbb{Z}$ için $V_n^2 - (k^2 + 4)U_n^2 = 4(-1)^n$'dir.

İspat: Binet formüllerinden $V_n = \alpha^n + \beta^n$, $U_n = \dfrac{\alpha^n - \beta^n}{\alpha - \beta}$ olduğundan

$$V_n^2 - (k^2 + 4)U_n^2 = (\alpha^n + \beta^n)^2 - (k^2 + 4)\left(\frac{\alpha^n - \beta^n}{\alpha - \beta}\right)^2$$

$$= (\alpha^n + \beta^n)^2 - (k^2 + 4)\frac{(\alpha^n - \beta^n)^2}{(\alpha - \beta)^2}$$

yazılır. $\alpha - \beta = \sqrt{k^2 + 4}$ olduğundan $(\alpha - \beta)^2 = k^2 + 4$ olur. Böylece

$$V_n^2 - (k^2 + 4)U_n^2 = (\alpha^n + \beta^n)^2 - (k^2 + 4)\frac{(\alpha^n - \beta^n)}{k^2 + 4}$$

$$= (\alpha^n + \beta^n)^2 - (\alpha^n - \beta^n)^2$$

$$= \alpha^{2n} + \beta^{2n} + 2(\alpha\beta)^n - \left(\alpha^{2n} + \beta^{2n} - 2(\alpha\beta)^n\right)$$

$$= \alpha^{2n} + \beta^{2n} + 2(\alpha\beta)^n - \alpha^{2n} - \beta^{2n} + 2(\alpha\beta)^n$$

$$= 4(\alpha\beta)^n$$

bulunur. O halde $\alpha\beta = -1$ olduğundan $V_n^2 - (k^2 + 4)U_n^2 = 4(-1)^n$ elde edilir.

Teorem 5.1.15. $x^2-\left(k^2+4\right)y^2=4$ denkleminin tüm pozitif tamsayı çözümleri $n\geq 1$ olmak üzere $\left(x,y\right)=\left(V_{2n},U_{2n}\right)$ biçimindedir.

İspat: $\left(x,y\right)=\left(V_{2n},U_{2n}\right)$ ise $x=V_{2n}$, $y=U_{2n}$ olur. O halde Teorem 5.1.14'e göre $x^2-\left(k^2+4\right)y^2=V_{2n}{}^2-\left(k^2+4\right)U_{2n}{}^2=4\left(-1\right)^{2n}=4$ bulunur. $x^2-\left(k^2+4\right)y^2=4$ olacak şekilde x,y pozitif tamsayılarının var olduğunu kabul edelim. Buradan $x^2-k^2y^2=4+4y^2$ olup $x^2-k^2y^2$ çifttir. Dolayısıyla x ve ky tamsayılarının her ikisi çifttir ya da her ikisi de tektir. $u=\dfrac{x+ky}{2}$, $v=y$ alınırsa u,v pozitif tamsayılar olur. Ayrıca $u^2-kuv-v^2=1$ dir. Gerçekten,

$$\begin{aligned}
u^2-kuv-v^2 &= \frac{x^2+2kxy+k^2y^2}{4}-k\left(\frac{x+ky}{2}\right)y-y^2\\
&=\frac{x^2+2kxy+k^2y^2}{4}-\frac{2kxy+2k^2y^2}{4}-\frac{4y^2}{4}\\
&=\frac{x^2+2kxy+k^2y^2-2kxy-2k^2y^2-4y^2}{4}\\
&=\frac{x^2-k^2y^2-4y^2}{4}
\end{aligned}$$

elde edilir. O halde $x^2-\left(k^2+4\right)y^2=4$ olduğundan $x^2-4y^2=4+k^2y^2$ olup yerine yazılırsa,

$$u^2-kuv-v^2=\frac{4+k^2y^2-k^2y^2}{4}=\frac{4}{4}=1$$

bulunur. O halde Sonuç 5.1.12'ye göre $\left(u,v\right)=\left(U_{2n+1},U_{2n}\right)$ olan $n\geq 1$ vardır. Yani $u=U_{2n+1}$, $v=U_{2n}$ 'dir. Sonuç olarak, $y=v$ olduğundan $y=U_{2n}$ olur. Ayrıca $u=\dfrac{x+ky}{2}$ olduğundan

$$x=2u-ky=2U_{2n+1}-kU_{2n}=U_{2n+1}+U_{2n+1}-kU_{2n}$$

olur. Böylece $U_{2n+1}=kU_{2n}+U_{2n-1}$ olduğundan

$$x=kU_{2n}+U_{2n-1}+U_{2n+1}-kU_{2n}=U_{2n+1}+U_{2n-1}$$

bulunur. Şu halde Teorem 5.1.4'e göre $U_{2n+1}+U_{2n-1}=V_{2n}$ olduğundan $x=V_{2n}$ olur.

Sonuç olarak, $n \geq 1$ olmak üzere $(x, y) = (V_{2n}, U_{2n})$ elde edilir.

Aşağıdaki teoremlerin ispatı benzer biçimde yapılabilir.

Teorem 5.1.16. $x^2 - (k^2+4)y^2 = -4$ denkleminin tüm pozitif tamsayı çözümleri $n \geq 0$ olmak üzere $(x, y) = (V_{2n+1}, U_{2n+1})$ biçimindedir [10] .

Teorem 5.1.17. $x^2 - (k^2+4)y^2 = \pm 4$ denkleminin tüm pozitif tamsayı çözümleri $n \geq 1$ olmak üzere $(x, y) = (V_n, U_n)$ biçimindedir [10] .

Teorem 5.1.18. Her $n \in \mathbb{Z}$ için $V_n^2 - kV_nV_{n-1} - V_{n-1}^2 = (-1)^n (k^2+4)$ ' tür.

İspat: Binet formülleri kullanılarak,

$$V_n^2 - kV_nV_{n-1} - V_{n-1}^2 = (\alpha^n + \beta^n)^2 - k(\alpha^n + \beta^n)(\alpha^{n-1} + \beta^{n-1}) - (\alpha^{n-1} + \beta^{n-1})^2$$

$$= \alpha^{2n} + \beta^{2n} + 2(\alpha\beta)^n - k\left(\alpha^{2n-1} + \beta^{2n-1} + (\alpha\beta)^n (\alpha^{-1} + \beta^{-1})\right) - \left(\alpha^{2n-2} + \beta^{2n-2} + 2(\alpha\beta)^{n-1}\right)$$

$= V_{2n} + 2(\alpha\beta)^n - kV_{2n-1} - k(\alpha\beta)^n (\alpha^{-1} + \beta^{-1}) - V_{2n-2} - 2(\alpha\beta)^{n-1}$ olur. $\alpha\beta = -1$ olduğundan $\dfrac{1}{\alpha} = \alpha^{-1} = -\beta$ ve $\dfrac{1}{\beta} = \beta^{-1} = -\alpha$ dır. O halde

$$\begin{aligned} V_n^2 - kV_nV_{n-1} - V_{n-1}^2 &= V_{2n} + 2(-1)^n - kV_{2n-1} - k(-1)^n(-\alpha - \beta) - V_{2n-2} - 2(-1)^{n-1} \\ &= V_{2n} + 2(-1)^n - kV_{2n-1} + k(-1)^n(\alpha + \beta) - V_{2n-2} + 2(-1)^n \end{aligned}$$

bulunur. Böylece $\alpha + \beta = k$ olduğundan

$$\begin{aligned} V_n^2 - kV_nV_{n-1} - V_{n-1}^2 &= V_{2n} - kV_{2n-1} - V_{2n-2} + 4(-1)^n + k^2(-1)^n \\ &= V_{2n} - kV_{2n-1} - V_{2n-2} + (-1)^n (k^2+4) \end{aligned}$$

elde edilir. Ayrıca, $V_{2n} = kV_{2n-1} + V_{2n-2}$ olduğundan

$$V_n^2 - kV_nV_{n-1} - V_{n-1}^2 = V_{2n} - V_{2n} + (-1)^n (k^2+4)$$

$$= (-1)^n \left(k^2+4\right)$$

olur.

Teorem 5.1.19. $k \geq 1$ ve k^2+4 karesiz olsun. Bu takdirde, $x^2-kxy-y^2 = \pm\left(k^2+4\right)$ denkleminin tüm pozitif tamsayı çözümleri $n \geq 1$ olmak üzere $(x,y) = (V_n, V_{n-1})$ biçimindedir.

İspat: $n \geq 1$ olmak üzere $(x,y) = (V_n, V_{n-1})$ olsun. O zaman $x = V_n$, $y = V_{n-1}$ olacağından Teorem 5.1.18'e göre ,

$$x^2-kxy-y^2 = V_n^{\,2} - kV_nV_{n-1} - V_{n-1}^{\,2} = (-1)^n\left(k^2+4\right) = \pm\left(k^2+4\right)$$

olur.

$x^2-kxy-y^2 = \pm\left(k^2+4\right)$ denklemini sağlayan x ve y pozitif tamsayılarının var olduğunu kabul edelim. O halde $x^2-kxy-y^2 = \pm\left(k^2+4\right)$ denkleminin her iki tarafını 4 ile çarparsak $4x^2-4kxy-4y^2 = \pm 4\left(k^2+4\right)$ olur. Dolayısıyla buradan $(2x-ky)^2 - \left(k^2+4\right)y^2 = \pm 4\left(k^2+4\right)$ yazılır. Bu ise $k^2+4 \mid (2x-ky)^2$ olmasını gerektirir. Böylece k^2+4 karesiz tamsayı olduğundan $k^2+4 \mid 2x-ky$ dir. O halde $2x-ky = \left(k^2+4\right)a$ olacak şekilde a tamsayısı vardır. $2x-ky = \left(k^2+4\right)a$ eşitliğini $(2x-ky)^2 - \left(k^2+4\right)y^2 = \pm 4\left(k^2+4\right)$ denkleminde yerine yazarsak,

$$\left(k^2+4\right)^2 a^2 - \left(k^2+4\right)y^2 = \pm 4\left(k^2+4\right)$$

ve buradan

$$\left(k^2+4\right)\left(\left(k^2+4\right)a^2 - y^2\right) = \pm 4\left(k^2+4\right)$$

bulunur. Bu eşitliğin her iki tarafı k^2+4 ile bölünürse $\left(k^2+4\right)a^2 - y^2 = \pm 4$ olur. Yani $y^2 - \left(k^2+4\right)a^2 = \pm 4$ bulunur.

1. durum: $a<0$ olsun. $y^2-\left(k^2+4\right)a^2=\pm 4$ olarak yazılabileceğinden ayrıca $y>0$ ve $-a>0$ olduğundan Teorem 5.1.17'ye göre $y=V_n$,$-a=U_n$ olan $n\geq 1$ vardır. Bu durumda $2x-ky=\left(k^2+4\right)a$ olduğundan $2x=\left(k^2+4\right)a+ky$ olur. $y=V_n$, $-a=U_n$ eşitlikleri $2x=\left(k^2+4\right)a+ky$ denkleminde yerine yazılırsa,

$$2x=\left(k^2+4\right)\left(-U_n\right)+kV_n$$

bulunur. Yani $x=\dfrac{-\left(k^2+4\right)U_n+kV_n}{2}$ dir. Böylece Teorem 5.1.4'e göre $\left(k^2+4\right)U_n=V_{n+1}+V_{n-1}$ olduğundan $x=\dfrac{-\left(V_{n+1}+V_{n-1}\right)+kV_n}{2}$ bulunur. Ayrıca, $V_{n+1}=kV_n+V_{n-1}$ olduğundan $x=\dfrac{-\left(kV_n+V_{n-1}+V_{n-1}\right)+kV_n}{2}=\dfrac{-2V_{n-1}}{2}=-V_{n-1}<0$ olur.Yani $x<0$ dır. Halbuki x pozitif tamsayı olduğundan bu mümkün değildir. O halde $a\geq 0$ dır.

2. durum: $a>0$ olsun. O zaman $y^2-\left(k^2+4\right)a^2=\pm 4$ olduğundan Teorem 5.1.17'ye göre $y=V_n$, $a=U_n$ olan $n\geq 1$ vardır. Böylece $2x-ky=\left(k^2+4\right)a$ olduğundan $y=V_n$, $a=U_n$ eşitliklerini yerine yazarsak $2x=kV_n+\left(k^2+4\right)U_n$ olup buradan $x=\dfrac{\left(k^2+4\right)U_n+kV_n}{2}$ olur. Şu halde Teorem 5.1.4'e göre $\left(k^2+4\right)U_n=V_{n+1}+V_{n-1}$ olduğundan $x=\dfrac{V_{n+1}+V_{n-1}+kV_n}{2}$ bulunur. Ayrıca $V_{n+1}=kV_n+V_{n-1}$ olduğundan $x=\dfrac{V_{n+1}+V_{n+1}}{2}=\dfrac{2V_{n+1}}{2}=V_{n+1}$ elde edilir. Sonuç olarak, $x=V_{n+1}$, $y=V_n$ olan $n\geq 1$ vardır.

3. durum: $a=0$ olsun. Bu durumda $y^2-\left(k^2+4\right)a^2=\pm 4$ olduğundan $y^2=\pm 4$ olur. Dolayısıyla $y^2=4$ olup y pozitif olduğundan $y=2$'dir. Böylece $2x-ky=\left(k^2+4\right)a$ olduğundan $a=0$ ve $y=2$ değerleri yerine yazılırsa,

$2x-2k=0$ olup $x=k$ bulunur. Şu halde $V_1=k$ olduğundan $x=k=V_1$, $V_0=2$ olduğundan $y=2=V_0$ olur.

Sonuç olarak, $n\geq 1$ olmak üzere $(x,y)=(V_n,V_{n-1})$ elde edilir.

Sonuç 5.1.20. $k\geq 1$ ve k^2+4 karesiz tamsayı olsun. Bu durumda $x^2-kxy-y^2=k^2+4$ denkleminin tüm pozitif tamsayı çözümleri $n\geq 1$ olmak üzere $(x,y)=(V_{2n},V_{2n-1})$ biçimindedir [10].

Sonuç 5.1.21. $k\geq 1$ ve k^2+4 karesiz olsun. Bu durumda, $x^2-kxy-y^2=-\left(k^2+4\right)$ denkleminin tüm pozitif tamsayı çözümleri $n\geq 1$ olmak üzere $(x,y)=(V_{2n+1},V_{2n})$ biçimindedir [10].

Teorem 5.1.22. $k\geq 3$ bir tamsayı , k^2-4 tamkare olmayan bir tamsayı olmak üzere $\alpha=\dfrac{k+\sqrt{k^2-4}}{2}$ olsun. $\mathbb{Z}[\alpha]=\{a\alpha+b \mid a,b\in\mathbb{Z}\}$, $Q\left(\sqrt{k^2-4}\right)$ reel kuadratik cisminin bir alt halkasıdır. Ayrıca $\mathbb{Z}[\alpha]$, $Q\left(\sqrt{k^2-4}\right)$ reel kuadratik cisminin tamsayılarının bir alt halkasıdır [3].

Teorem 5.1.23. $k\geq 3$ bir tamsayı, $\alpha=\dfrac{k+\sqrt{k^2-4}}{2}$, $\overline{\alpha}=\beta$ olsun. Aşağıdaki ifadeler denktir.

(i) $\alpha x+y\in\mathbb{Z}[\alpha]$ birimdir.

(ii) $(\alpha x+y)(\beta x+y)=\pm 1$

(iii) $x^2+kxy+y^2=\pm 1$ 'dir [3].

Teorem 5.1.24. Her $n\in\mathbb{Z}$ için $u_n{}^2-ku_nu_{n-1}+u_{n-1}{}^2=1$'dir.

İspat: Binet formülleri kullanılarak

$$u_n^2 - ku_n u_{n-1} + u_{n-1}^2 = \left(\frac{\alpha^n - \beta^n}{\alpha - \beta}\right)^2 - k\left(\frac{\alpha^n - \beta^n}{\alpha - \beta}\right)\left(\frac{\alpha^{n-1} - \beta^{n-1}}{\alpha - \beta}\right) + \left(\frac{\alpha^{n-1} - \beta^{n-1}}{\alpha - \beta}\right)^2$$

$$= \frac{\alpha^{2n} + \beta^{2n} - 2(\alpha\beta)^n}{(\alpha-\beta)^2} - k\left(\frac{\alpha^{2n-1} + \beta^{2n-1} - (\alpha\beta)^n\left(\alpha^{-1} + \beta^{-1}\right)}{(\alpha-\beta)^2}\right) + \frac{\alpha^{2n-2} + \beta^{2n-2} - 2(\alpha\beta)^{n-1}}{(\alpha-\beta)^2}$$

$$= \frac{v_n - 2(\alpha\beta)^n - kv_{2n-1} + k(\alpha\beta)^n\left(\alpha^{-1} + \beta^{-1}\right) + v_{2n-2} - 2(\alpha\beta)^{n-1}}{(\alpha-\beta)^2}$$

bulunur. $\alpha\beta = 1$ olduğundan $\frac{1}{\alpha} = \alpha^{-1} = \beta$, $\frac{1}{\beta} = \beta^{-1} = \alpha$ olur. O halde

$$u_n^2 - ku_n u_{n-1} + u_{n-1}^2 = \frac{v_{2n} - 2 - kv_{2n-1} + k(\beta + \alpha) + v_{2n-2} - 2}{(\alpha-\beta)^2}$$

olur. Burada $\alpha + \beta = k$ dır. Ayrıca $\alpha - \beta = \sqrt{k^2 - 4}$ olduğundan $(\alpha - \beta)^2 = k^2 - 4$ olur. Şu halde

$$u_n^2 - ku_n u_{n-1} + u_{n-1}^2 = \frac{v_{2n} - kv_{2n-1} + k^2 + v_{2n-2} - 4}{k^2 - 4}$$

bulunur. Ayrıca , $v_{2n} = kv_{2n-1} - v_{2n-2}$ olduğundan

$$u_n^2 - ku_n u_{n-1} + u_{n-1}^2 = \frac{v_{2n} - v_{2n} + k^2 - 4}{k^2 - 4}$$

$$= \frac{k^2 - 4}{k^2 - 4} = 1$$

elde edilir.

Aşağıda vereceğimiz teoremin ispatı tümevarımla kolay bir şekilde yapılabilir.

Teorem 5.1.25. $k \geq 3$ bir tamsayı ve $\alpha = \frac{k + \sqrt{k^2 - 4}}{2}$, $\beta = \frac{k - \sqrt{k^2 - 4}}{2}$ olsun. O zaman her $n \in \mathbb{Z}$ için $\alpha^n = \alpha U_n - U_{n-1}$, $\beta^n = \beta U_n - U_{n-1}$ 'dir.

Uyarı: $k \geq 3$ olmak üzere $\alpha = \frac{k + \sqrt{k^2 - 4}}{2}$ irrasyonel sayıdır. Çünkü, $k^2 - 4$ kök dışına çıkmaz. Yani, $k^2 - 4 = t^2$ olan t tamsayısı yoktur. $k^2 - 4 = t^2$ olacak biçimde

t tamsayısının var olduğunu kabul edelim. Buradan $k^2 - t^2 = 4$ olup $(k-t)(k+t) = 4$ elde edilir. Bu ise $k - t = 1, k + t = 4$ veya $k - t = 2$, $k + t = 2$ olmasını gerektirir. Eğer $k - t = 1, k + t = 4$ olursa $k = \frac{5}{2}$ olur. Fakat k tamsayı olduğundan bu mümkün değildir. Eğer $k - t = 2$, $k + t = 2$ olursa $k = 0$ bulunur. Yine $k \geq 3$ olduğundan bu mümkün değildir.

Teorem 5.1.26. $k > 3$ ve $\alpha = \dfrac{k + \sqrt{k^2 - 4}}{2}$ olsun. Bu takdirde $\mathbb{Z}[\alpha] = \{a\alpha + b \mid a, b \in \mathbb{Z}\}$ halkasının birimlerinin kümesi $\{\pm\alpha^n \mid n \in \mathbb{Z}\}$'dir [3].

İspat: İlk olarak $1 < w < \alpha$ şartını sağlayan w biriminin olmadığını gösterelim. $w = \alpha x + y$, $1 < \alpha x + y < \alpha$ olacak şekilde bir birimi olsun. x bu şartı sağlayan en küçük tamsayı olsun. $\alpha x + y$ birim olduğundan $x^2 + kxy + y^2 = (\alpha x + y)(\overline{\alpha} x + y) = \pm 1$'dir. Buradan

$$\left|(\alpha x + y)(\overline{\alpha} x + y)\right| = |\alpha x + y|\left|\overline{\alpha} x + y\right| = 1$$

yazılır. Böylece $\alpha x + y > 1$ olduğundan $1 = |\alpha x + y|\left|\overline{\alpha} x + y\right| > \left|\overline{\alpha} x + y\right|$ olur. Yani $\left|\overline{\alpha} x + y\right| < 1$'dir. Buradan $-1 < \overline{\alpha} x + y < 1$ olur. $1 < \alpha x + y$ ve $-1 < \overline{\alpha} x + y$ olduğundan bu eşitsizlikleri taraf tarafa toplarsak $0 < (\alpha + \beta)x + 2y$ bulunur. $\alpha + \beta = k$ olduğundan $0 < kx + 2y$ olur. Ayrıca $-1 < \overline{\alpha} x + y < 1$ olduğundan $-1 < -\overline{\alpha} x - y < 1$'dir. O halde $-1 < -\overline{\alpha} x - y$ ve $1 < \alpha x + y$ olduğundan bu eşitsizlikleri taraf tarafa toplarsak $0 < \left(\alpha - \overline{\alpha}\right)x$ elde edilir. Böylece $\alpha - \overline{\alpha} = \sqrt{k^2 - 4}$ olduğundan $0 < \left(\sqrt{k^2 - 4}\right)x$ elde edilir. Burada $\sqrt{k^2 - 4}$ daima pozitif olduğundan $x > 0$ dır. O halde $1 < \alpha x + y < \alpha$ ve $x > 0$ olduğundan $y < \alpha - \alpha x = \alpha(1 - x) \leq 0$ olur. Yani $y < 0$'dır. $1 < \alpha x + y < \alpha$ eşitsizliğinin her iki tarafını $\overline{\alpha}$ ile çarparsak $\overline{\alpha} < \overline{\alpha}(\alpha x + y) < \alpha\overline{\alpha}$ olur. Yani $\overline{\alpha} < \alpha\overline{\alpha} x + \overline{\alpha} y < \alpha\overline{\alpha}$ dir. Ayrıca $\alpha\overline{\alpha} = 1$ olduğundan $\overline{\alpha} < x + \overline{\alpha} y < 1$' dir. $\overline{\alpha}$, $\alpha x + y$ birim ve

$x+\overline{\alpha}y=\overline{\alpha}\left(\alpha x+y\right)$ olduğundan $x+\overline{\alpha}y$ de birimdir. O halde $\dfrac{1}{x+\overline{\alpha}y}$ birimdir. $\overline{\alpha}<x+\overline{\alpha}y<1$ olduğundan $1<\dfrac{1}{x+\overline{\alpha}y}<\dfrac{1}{\overline{\alpha}}$ olur. Böylece $\alpha\overline{\alpha}=1$ olduğu kullanılırsa $\dfrac{1}{\overline{\alpha}}=\alpha$ ve böylece $1<\dfrac{1}{x+\overline{\alpha}y}<\alpha$ bulunur. $\varepsilon=\left(x+\overline{\alpha}y\right)\left(x+\alpha y\right)$ olsun. $x+\overline{\alpha}y$ birim olduğundan Teorem 5.1.23'e göre $\varepsilon=\pm 1$'dir.

1. durum: $\varepsilon=1$ olsun. O zaman $1<\dfrac{1}{x+\overline{\alpha}}<\alpha$ ve $1=\left(x+\overline{\alpha}y\right)\left(x+\alpha y\right)$ olduğundan $1<x+\alpha y<\alpha$ olur. Bu şartı sağlayan en küçük x olduğundan $x\leq y$ dir. O halde $y<0$ olduğundan $x<0$ olur. Halbuki $x>0$'dır.

2. durum: $\varepsilon=-1$ olsun. Şu halde $-1=\left(x+\overline{\alpha}y\right)\left(x+\alpha y\right)$ olduğundan $\dfrac{1}{x+\overline{\alpha}y}=-x-\alpha y$ olur. Böylece $1<\dfrac{1}{\overline{\alpha}x+y}<\alpha$ olduğundan $1<-x-\alpha y<\alpha$ elde edilir. Yani $1<\left(-y\right)\alpha-x<\alpha$'dır. Bu şartı sağlayan en küçük x olduğundan $x\leq -y$ olur. Böylece $-x+\alpha x\leq -x+\alpha\left(-y\right)$ ve $-x+\alpha\left(-y\right)<\alpha$ olduğundan $-x+\alpha x\leq -x+\alpha\left(-y\right)<\alpha$ bulunur. Şu halde $x\left(\alpha-1\right)<\alpha$'dır. $k>3$ olduğundan $\alpha=\dfrac{k+\sqrt{k^2-4}}{2}>\dfrac{3+\sqrt{5}}{2}>2$'dir. Dolayısıyla $\dfrac{1}{\alpha-1}<1$'dir. $x<\dfrac{\alpha}{\alpha-1}$ olduğundan ve $\dfrac{\alpha}{\alpha-1}=1+\dfrac{1}{\alpha-1}$ olarak yazılabildiğinden $x<1+\dfrac{1}{\alpha-1}$ olur. O halde $\dfrac{1}{\alpha-1}<1$ olduğundan $x<1+1$ olup $x<2$ dir. O halde $x>0$ olduğundan $x=1$ bulunur. Diğer yandan $-1=\left(x+\overline{\alpha}y\right)\left(x+\alpha y\right)=x^2+kxy+y^2$ olduğundan $x=1$ değeri yerine yazılırsa $1+ky+y^2=-1$ olur. Buradan $y\left(k+y\right)=-2$ olur. Bu ise $y\,|\,-2$ olmasını gerektirir. O halde $y<0$ olduğundan $y=-1$ ya da $y=-2$'dir. Bu ise $y\left(k+y\right)=-2$ olduğundan $k=3$ olmasını gerektirir. Halbuki $k>3$'dür. İspatın bundan sonraki kısmı Teorem 5.1.8 ile aynıdır.

Teorem 5.1.27. $k>3$ olsun. $x^2-kxy+y^2=1$ denkleminin tüm pozitif tamsayı çözümleri $n\geq 1$ olmak üzere $(x,y)=(u_{n+1},u_n)$ biçimindedir.

İspat: $(x,y)=(u_{n+1},u_n)$ ise $x=u_{n+1}$, $y=u_n$ olacağından Teorem 5.1.24'e göre $x^2-kxy+y^2=u_{n+1}{}^2-ku_{n+1}u_n+u_n{}^2=1$'dir. Şimdi kabul edelim ki $x^2-kxy+y^2=1$ denklemini x ve y pozitif tamsayıları mevcut olsun. Bu durumda Teorem 5.1.23'e göre $\alpha x-y$ birimdir. Ayrıca $\alpha x-y>1$ veya $\alpha y-x>1$ dir. Gerçekten, aksine kabul edelim ki $\alpha x-y\leq 1$ ve $\alpha y-x\leq 1$ olsun. O zaman bu eşitsizlikleri taraf tarafa toplarsak $\alpha x-y+\alpha y-x\leq 2$ olur. Yani $\alpha(x+y)-(x+y)\leq 2$ dir. $x+y=a$ dersek, $\alpha a-a\leq 2$ bulunur. O halde $a(\alpha-1)\leq 2$ dir. $k>3$ olduğundan $\alpha=\dfrac{k+\sqrt{k^2+4}}{2}>\dfrac{3+\sqrt{5}}{2}>2$ olup $\alpha-1>1$ dir. O halde $a(\alpha-1)\leq 2$ olduğundan $a<2$ olur. Halbuki x ve y pozitif tamsayılar olduğundan $a=x+y\geq 1+1$ olup $a\geq 2$ dir. Şu halde x,y $x^2-kxy+y^2=1$ denklemine göre simetrik olduğundan $\alpha x-y>1$ kabul edebiliriz. Böylece Teorem 5.1.26'ya göre $\alpha x-y=\alpha^{n+1}$ olan $n\geq 1$ sayısı vardır. Burada $n=0$ almadık. Çünkü ,$n=0$ olursa $\alpha x-y=\alpha$ olur. Buradan α irrasyonel olduğundan $y=0$ bulunur. Bu ise y sayısının pozitif tamsayı olması ile çelişir.

$\alpha x-y=\alpha^{n+1}$ olduğundan Teorem 5.1.25'e göre $\alpha x-y=\alpha u_{n+1}-u_n$ olur. Böylece α irrasyonel olduğundan $x=u_{n+1}$, $y=u_n$ bulunur. Sonuç olarak, $n\geq 1$ olmak üzere $(x,y)=(u_{n+1},u_n)$'dir.

Teorem 5.1.28. $x^2-kxy+y^2=-1$ denkleminin tamsayılarda çözümü yoktur [3].

İspat: Aksine kabul edelim ki $x^2-kxy+y^2=-1$ denklemini sağlayan x ve y tamsayıları mevcut olsun. O halde Teorem 5.1.23'e göre $\alpha x-y$ birimdir. Böylece Teorem 5.1.26'ya göre $\alpha x-y=\pm\alpha^n$ olacak şekilde $n\in\mathbb{Z}$ vardır. Şu halde Teorem 5.1.25'e göre $\alpha x-y=\pm(\alpha u_n-u_{n-1})$ olur. Bu ise α irrasyonel olduğundan $x=\pm u_n$

$y=\pm u_{n-1}$ olmasını gerektirir. Buradan $-1=x^2-kxy+y^2=u_n{}^2-ku_nu_{n-1}+u_{n-1}{}^2$ bulunur. Halbuki Teorem 5.1.24'e göre $u_n{}^2-ku_nu_{n-1}+u_{n-1}{}^2=1$'dir. O halde bu bir çelişkidir. Sonuç olarak, $x^2-kxy+y^2=-1$ denkleminin tamsayılarda çözümü yoktur.

Teorem 5.1.29. Her $n\in\mathbb{Z}$ için $v_n{}^2-\left(k^2-4\right)u_n{}^2=4$'tür.

İspat: Binet formüllerinden yararlanılarak

$$v_n{}^2-\left(k^2-4\right)u_n{}^2=\left(\alpha^n+\beta^n\right)^2-\left(k^2-4\right)\left(\frac{\alpha^n-\beta^n}{\alpha-\beta}\right)^2$$

$$=\alpha^{2n}+\beta^{2n}+2\left(\alpha\beta\right)^n-\left(k^2-4\right)\frac{\left(\alpha^{2n}+\beta^{2n}-2\left(\alpha\beta\right)^n\right)}{\left(\alpha-\beta\right)^2}$$

yazılır. $\alpha-\beta=\sqrt{k^2-4}$ olduğundan $\left(\alpha-\beta\right)^2=k^2-4$ olur. Şu halde

$$v_n{}^2-\left(k^2-4\right)u_n{}^2=\alpha^{2n}+\beta^{2n}+2\left(\alpha\beta\right)^n-\left(k^2-4\right)\frac{\left(\alpha^{2n}+\beta^{2n}-2\left(\alpha\beta\right)^n\right)}{k^2-4}$$

$$=\alpha^{2n}+\beta^{2n}+2\left(\alpha\beta\right)^n-\alpha^{2n}-\beta^{2n}+2\left(\alpha\beta\right)^n$$

$$=4\left(\alpha\beta\right)^n$$

bulunur. Böylece $\alpha\beta=1$ olduğundan $v_n{}^2-\left(k^2-4\right)u_n{}^2=4$ elde edilir.

Teorem 5.1.30. $x^2-\left(k^2-4\right)y^2=4$ denkleminin tüm pozitif tamsayı çözümleri $n\geq 1$ olmak üzere $\left(x,y\right)=\left(v_n,u_n\right)$ ile verilir.

İspat: $\left(x,y\right)=\left(v_n,u_n\right)$ ise $x=v_n$, $y=u_n$ olacağından Teorem 5.1.29'a göre $x^2-\left(k^2-4\right)y^2=v_n{}^2-\left(k^2-4\right)u_n{}^2=4$ 'tür. Şimdi de kabul edelim ki $x^2-\left(k^2-4\right)y^2=4$ olan x ve y pozitif tamsayıları mevcut olsun. Buradan $x^2-k^2y^2=4+4y^2$ olduğundan $x^2-k^2y^2$ çifttir. Bu ise x ve ky sayılarının ya ikisinin de çift ya da ikisinin de tek olmasını gerektirir. O halde $u=\dfrac{x+ky}{2}, v=y$ alınırsa u ve v pozitif tamsayılar olur. Ayrıca $u^2-kuv+v^2=1$ dir. Gerçekten,

$$\begin{aligned}
u^2-kuv+v^2 &= \left(\frac{x+ky}{2}\right)^2-k\left(\frac{x+ky}{2}\right)y+y^2\\
&= \frac{(x+ky)^2}{4}-\frac{2k(x+ky)y}{4}+\frac{4y^2}{4}\\
&= \frac{x^2+2xky+k^2y^2-2kxy-2k^2y^2+4y^2}{4}\\
&= \frac{x^2-k^2y^2+4y^2}{4}\\
&= \frac{x^2-(k^2-4)y^2}{4}
\end{aligned}$$

bulunur. Şu halde $x^2-(k^2-4)y^2=4$ olduğundan $u^2-kuv+v^2=\dfrac{4}{4}=1$ elde edilir. Böylece Teorem 5.1.27'ye göre $u=u_{n+1}, v=u_n$ olan $n\geq 1$ vardır. Buradan $y=v$ olduğundan $y=u_n$ bulunur. Ayrıca $u=\dfrac{x+ky}{2}$ olduğundan $x=2u-ky$ olup buradan $x=2u_{n+1}-ku_n=u_{n+1}+u_{n+1}-ku_n$ olur. $u_{n+1}=ku_n-u_{n-1}$ olduğundan $x=ku_n-u_{n-1}+u_{n+1}-ku_n=u_{n+1}-u_{n-1}$ bulunur. Böylece Teorem 5.1.4'e göre $x=v_n$ elde edilir. Sonuç olarak, $n\geq 1$ olmak üzere $(x,y)=(v_n,u_n)$'dir.

Teorem 5.1.31. $x^2-(k^2-4)y^2=-4$ denkleminin tamsayılarda çözümü yoktur.

İspat: Aksine kabul edelim ki x ve y tamsayıları $x^2-(k^2-4)y^2=-4$ denklemini sağlasın. Buradan $x^2-k^2y^2=-4y^2-4$ bulunur. Bu ise x ve ky sayılarının her ikisinin de çift ya da her ikisinin de tek olmasını gerektirir. O halde $u=\dfrac{x+ky}{2}$, $v=y$ alınırsa u ve v tamsayılar olur. Ayrıca $u^2-kuv+v^2=-1$'dir. Gerçekten ,

$$u^2-kuv+v^2=\left(\frac{x+ky}{2}\right)^2-k\left(\frac{x+ky}{2}\right)y+y^2$$

$$=\frac{(x+ky)^2}{4}-\frac{2k(x+ky)y}{4}+\frac{4y^2}{4}$$

$$=\frac{x^2+2xky+k^2y^2-2kxy-2k^2y^2+4y^2}{4}$$

$$=\frac{x^2-k^2y^2+4y^2}{4}$$

$$=\frac{x^2-(k^2-4)y^2}{4}$$

bulunur. Şu halde $x^2-(k^2-4)y^2=-4$ olduğundan $u^2-kuv+v^2=\frac{-4}{4}=-1$'dir. Fakat Teorem 5.1.28'e göre $u^2-kuv+v^2=-1$ denklemini sağlayan u ve v tamsayısı yoktur. Sonuç olarak, $x^2-(k^2-4)y^2=-4$ denklemini sağlayan x ve y tamsayıları yoktur.

Teorem 5.1.32. $k>3$ ve k^2-4 karesiz olsun. $x^2-kxy+y^2=-(k^2-4)$ denkleminin pozitif tamsayılardaki tüm çözümleri $n\geq 0$ olmak üzere $(x,y)=(v_n,v_{n-1})$ biçimindedir [10].

Teorem 5.1.33. $k>3$ ve k^2-4 karesiz olsun. Bu takdirde $x^2-kxy+y^2=k^2-4$ denkleminin tamsayılarda çözümü yoktur [10].

BÖLÜM 6. FİBONACCİ VE LUCAS DİZİLERİ YARDIMI İLE BAZI ÖZEL DENKLEM ÇÖZÜMLERİ

Aşağıda vereceğimiz teoremler Binet formülleri yardımı ile kolaylıkla ispatlanabilir.

Teorem 6.1.1. $n \geq 1$ için $L_n^2 - 5F_n^2 = 4(-1)^n$ 'dir.

Teorem 6.1.2. $n \geq 1$ için $L_{n-1} + L_{n+1} = 5F_n$ 'dir.

Teorem 6.1.3. $n \geq 1$ için $L_{2n}^2 + 5F_{2n+1}^2 + 1 = 5L_{2n}^2 F_{2n+1}^2$ 'dir.

Teorem 6.1.4. $n \geq 1$ için $\left(L_{2n+2}^2 + 5F_{2n+1}^2 + 1\right)^2 = 25L_{2n+2}^2 F_{2n+1}^2$ 'dir.

Teorem 6.1.5. $n \geq 1$ için $\left(L_{2n+1}^2 + 5F_{2n} - 1\right)^2 = 25L_{2n+1}^2 F_{2n}^2$ 'dir.

Teorem 6.1.6. $n \geq 1$ için $\left(L_{2n-1}^2 + 5F_{2n} - 1\right)^2 = 25L_{2n-1}^2 F_{2n}^2$ 'dir.

Teorem 6.1.7. $n \geq 1$ için $\left(F_{2n+1}^2 + F_{2n+2}^2 + 1\right)^2 = F_{2n+1}^2\left(5F_{2n+2}^2 + 4\right)$ 'tür.

Teorem 6.1.8. $n \geq 1$ için $\left(F_{2n+1}^2 + F_{2n}^2 + 1\right)^2 = F_{2n+1}^2\left(5F_{2n}^2 + 4\right)$ 'tür.

Teorem 6.1.9. $n \geq 1$ için $\left(F_{2n}^2 + F_{2n+1}^2 - 1\right)^2 = F_{2n}^2\left(5F_{2n+1}^2 - 4\right)$ 'tür.

Teorem 6.1.10. $n \geq 1$ için $\left(F_{2n}^2 + F_{2n-1}^2 - 1\right)^2 = F_{2n}^2\left(5F_{2n-1}^2 - 4\right)$ 'tür.

Teorem 6.1.11. $n \geq 1$ için $3 \mid F_n \Leftrightarrow 4 \mid n$ 'dir.

Şimdi vereceğimiz Teorem 6.1.12 ve Teorem 6.1.13 ‘ün ispatları Teorem 5.1.15 ve Teorem 5.1.16’da $k=1$ alınarak kolaylıkla görülebilir.

Teorem 6.1.12. $x^2-5y^2=4$ denkleminin tüm pozitif tamsayı çözümleri $n\geq 1$ olmak üzere $(x,y)=(L_{2n},F_{2n})$ biçimindedir.

Teorem 6.1.13. $x^2-5y^2=-4$ denkleminin tüm pozitif tamsayı çözümleri $n\geq 1$ olmak üzere $(x,y)=(L_{2n+1},F_{2n+1})$ biçimindedir.

Teorem 6.1.14. $(x+y+1)^2=5xy$ denkleminin tüm pozitif tamsayı çözümleri $n\geq 1$ olmak üzere $(x,y)=(L_{2n}^2,5F_{2n+1}^2)$ veya $(L_{2n+2}^2,5F_{2n+1}^2)$ biçimindedir.

İspat: Kabul edelim ki x ve y pozitif tamsayıları $(x+y+1)^2=5xy$ denklemini sağlasın. Burada $(x,y)=1$ olduğunu görmek kolaydır. Gerçekten, aksine kabul edelim ki x ve y sayılarının bir ortak p asal böleni olsun. Yani p asal olmak üzere $p\,|\,x$ ve $p\,|\,y$ olsun. Bu takdirde $p\,|\,x+y$ ve $p\,|\,5xy$ yazılır. Bu ise $(x+y+1)^2=5xy$ olduğundan $p\,|\,(x+y+1)^2$ olmasını gerektirir. Dolayısıyla p asal olduğundan $p\,|\,x+y+1$ olur. Böylece $p\,|\,x+y$ olduğundan $p\,|\,1$ bulunur. Bu ise p sayısının asal olması ile çelişir. Şu halde genelliği bozmadan a ve b pozitif tamsayılar olmak üzere $x=a^2$ ve $y=5b^2$ kabul edebiliriz. Bu eşitlikleri $(x+y+1)^2=5xy$ denkleminde yerine yazarsak,

$$\left(a^2+5b^2+1\right)^2=25a^2b^2=(5ab)^2$$

bulunur. Bu ise $a^2+5b^2+1=5ab$ olmasını gerektirir. Dolayısıyla $a^2+5b^2-5ab=-1$ olur. $a^2+5b^2-5ab=-1$ denkleminin her iki tarafını 4 ile çarpıp tamkareye tamamlarsak,

$$(2a-5b)^2-5b^2=-4$$

elde edilir. Teorem 6.1.13'e göre $n \geq 1$ olmak üzere $|2a-5b| = L_{2n+1}$ ve $b = F_{2n+1}$ olur. Eğer $2a-5b = L_{2n+1}$ ise $a = \dfrac{(L_{2n+1}+5b)}{2} = \dfrac{(L_{2n+1}+5F_{2n+1})}{2}$ olur. Böylece Teorem 6.1.4'e göre $5F_{2n+1} = L_{2n} + L_{2n+2}$ olduğundan $a = \dfrac{(L_{2n}+L_{2n+2}+L_{2n+1})}{2}$ elde edilir. Aynı zamanda $L_{2n+2} = L_{2n} + L_{2n+1}$ olduğu kullanılırsa $a = \dfrac{2L_{2n+2}}{2} = L_{2n+2}$ bulunur. Benzer şekilde eğer $2a-5b = -L_{2n+1}$ ise $a = \dfrac{5b-L_{2n+1}}{2} = \dfrac{5F_{2n+1}-L_{2n+1}}{2}$ olur. Teorem 6.1.4'e göre $5F_{2n+1} = L_{2n} + L_{2n+2}$ olduğundan $a = \dfrac{L_{2n}+L_{2n+2}-L_{2n+1}}{2}$ bulunur. Böylece $L_{2n+2} = L_{2n} + L_{2n+1}$ olduğu kullanılırsa $a = \dfrac{L_{2n}+L_{2n}}{2} = \dfrac{2L_{2n}}{2} = L_{2n}$ elde edilir. Şu halde $x = a^2$ ve $y = 5b^2$ olduğundan $(x,y) = (L_{2n}^2, 5F_{2n+1}^2)$ veya $(x,y) = (L_{2n+2}^2, 5F_{2n+1}^2)$ bulunur. Tersine $(x,y) = (L_{2n}^2, 5F_{2n+1}^2)$ veya $(x,y) = (L_{2n+2}^2, 5F_{2n+1}^2)$ ise Teorem 6.1.5 veya Teorem 6.1.4'e göre $(x+y+1)^2 = 5xy$ olur.

Sonuç 6.1.15. $x^2 + y^2 - 3xy + x = 0$ denkleminin tüm pozitif tamsayı çözümleri $n \geq 1$ olmak üzere $(x,y) = (F_{2n+1}^2, F_{2n+2}^2 + 1)$ veya $(F_{2n+1}^2, F_{2n}^2 + 1)$ biçimindedir.

İspat: Kabul edelim ki x ve y tamsayıları $x^2 + y^2 - 3xy + x = 0$ denklemini sağlasın. Buradan $x^2 + y^2 + 2xy - 5xy + x = 0$ ve böylece $x^2 + y^2 + 2xy = 5xy - x$ yazılır. O halde $(x+y)^2 = x(5y-1)$ elde edilir. $(x+y)^2 = x(5y-1)$ denkleminin her iki tarafını 5^2 ile çarparsak

$$5^2(x+y)^2 = 5^2 x(5y-1)$$

ve böylece

$$(5x+5y-1+1)^2 = 5(5x(5y-1))$$

bulunur.

Teorem 6.1.1'e göre $5 \nmid L_n$ olduğundan Teorem 6.1.14'e göre $(5y-1,5x)=\left(L_{2n}^2,5F_{2n+1}^2\right)$ veya $(5y-1,5x)=\left(L_{2n+2}^2,5F_{2n+1}^2\right)$ olur. Eğer $(5y-1,5x)=\left(L_{2n}^2,5F_{2n+1}^2\right)$ olursa bu $5y-1=L_{2n}^2$ ve $x=F_{2n+1}^2$ olmasını gerektirir. Ayrıca $y=\dfrac{L_{2n}^2+1}{5}$ olup Teorem 6.1.3'e göre $L_{2n}^2=5F_{2n}^2+4(-1)^{2n}=5F_{2n}^2+4$ olduğundan $y=\dfrac{5F_{2n}^2+5}{5}=F_{2n}^2+1$ elde edilir. Şu halde $(x,y)=\left(F_{2n+1}^2,F_{2n}^2+1\right)$ bulunur. Eğer $(5y-1,5x)=\left(L_{2n+2}^2,5F_{2n+1}^2\right)$ olursa bu $5y-1=L_{2n+2}^2$ ve $x=F_{2n+1}^2$ olmasını gerektirir. O halde $y=\dfrac{L_{2n+2}^2+1}{5}$ olup Teorem 6.1.1'e göre $L_{2n+2}^2=5F_{2n+2}^2+4(-1)^{2n+2}=5F_{2n+2}^2+4$ olduğundan $y=\dfrac{5F_{2n+2}^2+5}{5}=F_{2n+2}^2+1$ bulunur. O halde $(x,y)=\left(F_{2n+1}^2,F_{2n+2}^2+1\right)$ dir. Tersine $(x,y)=\left(F_{2n+1}^2,F_{2n+2}^2+1\right)$ veya $(x,y)=\left(F_{2n+1}^2,F_{2n}^2+1\right)$ ise Teorem 6.1.7 ve Teorem 6.1.9'a göre $(x+y)^2=x(5y-1)$ olur.

Teorem 6.1.16. $(x+y-1)^2=5xy$ denkleminin tüm pozitif tamsayı çözümleri $n\geq 1$ olmak üzere $(x,y)=\left(L_{2n+1}^2,5F_{2n}^2\right)$ veya $\left(L_{2n-1}^2,5F_{2n}^2\right)$ ile verilir.

İspat: Kabul edelim ki x ve y pozitif tamsayıları $(x+y-1)^2=5xy$ denklemini sağlasın. Burada $(x,y)=1$ olduğunu görmek kolaydır. Gerçekten , aksine kabul edelim ki x ve y tamsayılarının bir ortak p asal böleni olsun. Yani p asal olmak üzere , $p\mid x$ ve $p\mid y$ olsun. Bu takdirde $p\mid x+y$ ve $p\mid 5xy$ yazılır. Böylece $(x+y-1)^2=5xy$ olduğundan $p\mid (x+y-1)^2$ bulunur. Şu halde p asal olduğundan $p\mid x+y-1$ dir. Bu ise $p\mid x+y$ olduğundan $p\mid 1$ olmasını gerektirir. Fakat, bu p sayısının asal olması ile çelişir. Şu halde genelliği bozmadan a ve b pozitif tamsayılar olmak üzere $x=a^2$ ve $y=5b^2$ kabul edebiliriz. Bu eşitlikleri $(x+y-1)^2=5xy$ denkleminde yerine yazarsak,

$$\left(a^2+5b^2-1\right)^2=25a^2b^2=(5ab)^2$$

bulunur. Bu ise $a^2+5b^2-1=5ab$ olmasını gerektirir. Yani $a^2+5b^2-5ab=1$ dir. $a^2+5b^2-5ab=1$ denkleminin her iki tarafını 4 ile çarpıp tamkareye tamamlarsak, $(2a-5b)^2-5b^2=4$ elde edilir. Böylece Teorem 6.1.12'ye göre $n\geq 1$ için $|2a-5b|=L_{2n}$ ve $b=F_{2n}$ olur. Yani $2a-5b=\pm L_{2n}$ ve $b=F_{2n}$ dir. Eğer $2a-5b=L_{2n}$ ise $a=\dfrac{L_{2n}+5b}{2}=\dfrac{L_{2n}+5F_{2n}}{2}$ elde edilir. Şu halde Teorem 6.1.2'ye göre $5F_{2n}=L_{2n+1}+L_{2n-1}$ olduğu kullanılırsa $a=\dfrac{L_{2n}+L_{2n-1}+L_{2n+1}}{2}$ olur. Aynı zamanda $L_{2n+1}=L_{2n}+L_{2n-1}$ olduğundan $a=\dfrac{L_{2n+1}+L_{2n+1}}{2}=\dfrac{2L_{2n+1}}{2}=L_{2n+1}$ dir. Benzer şekilde eğer $2a-5b=-L_{2n}$ ise $a=\dfrac{-L_{2n}+5b}{2}=\dfrac{-L_{2n}+5F_{2n}}{2}$ olur. Teorem 6.1.2'ye göre $5F_{2n}=L_{2n-1}+L_{2n+1}$ olduğu kullanılırsa $a=\dfrac{-L_{2n}+L_{2n-1}+L_{2n+1}}{2}$ bulunur. Ayrıca $L_{2n+1}=L_{2n}+L_{2n-1}$ olduğundan $a=\dfrac{L_{2n-1}+L_{2n-1}}{2}=\dfrac{2L_{2n-1}}{2}=L_{2n-1}$ dir. Sonuç olarak, $x=a^2$ ve $y=5b^2$ olduğu kullanılırsa $(x,y)=\left(L_{2n+1}^2,5F_{2n}^2\right)$ veya $(x,y)=\left(L_{2n-1}^2,5F_{2n}^2\right)$ elde edilir. Tersine $(x,y)=\left(L_{2n+1}^2,5F_{2n}^2\right)$ veya $(x,y)=\left(L_{2n-1}^2,5F_{2n}^2\right)$ ise Teorem 6.1.7 ve Teorem 6.1.6'e göre $(x+y-1)^2=5xy$ denklemi sağlanır.

Teorem 6.1.16 , Teorem 6.1.9, Teorem 6.1.10 kullanılarak aşağıdaki sonuç kolaylıkla ispatlanır.

Sonuç 6.1.17. $x^2+y^2-3xy-x=0$ denkleminin tüm pozitif tamsayı çözümleri $n\geq 1$ olmak üzere $(x,y)=\left(F_{2n}^2,F_{2n+1}^2-1\right)$ veya $\left(F_{2n}^2,F_{2n-1}^2-1\right)$ biçimindedir.

Aşağıdaki teoremlerin ve sonuçların ispatları Teorem 6.1.11 kullanılarak benzer şekilde yapılır.

Teorem 6.1.18. $(x-y+1)^2 = 5xy$ denkleminin tüm pozitif tamsayı çözümleri $n \geq 1$ olmak üzere $(x,y) = \left(5F_{4n}^2/9, L_{4n+2}^2/9\right)$ veya $\left(5F_{4n}^2/9, L_{4n-2}^2/9\right)$ biçimindedir.

Sonuç 6.1.19. $x^2+y^2-7xy-x=0$ denkleminin tüm pozitif tamsayı çözümleri $n \geq 1$ olmak üzere $(x,y) = \left(F_{4n}^2/9, \left(F_{4n+2}^2-1\right)/9\right)$ veya $\left(F_{4n}^2/9, \left(F_{4n-2}^2-1\right)/9\right)$ biçimindedir.

Sonuç 6.1.20. $x^2+y^2-7xy+x=0$ denklemi pozitif tamsayılarda çözüme sahip değildir.

İspat: Aksine kabul edelim ki x ve y pozitif tamsayıları $x^2+y^2-7xy+x=0$ denklemini sağlasın. Buradan $x^2+y^2-2xy-5xy+x=0$ ve böylece $(y-x)^2 = x(5y-1)$ bulunur. Bu denklemin her iki tarafını 5^2 ile çarparsak,

$$5^2(y-x)^2 = 5^2x(5y-1)$$

ve buradan da

$$(5y-1-5x+1)^2 = 5\left(5x(5y-1)\right)$$

elde edilir. Böylece Teorem 6.1.18'e göre $n \geq 1$ için $5y-1 = 5F_{4n}^2/9$, yani $5y = 5F_{4n}^2/9+1$ elde edilir. O halde $45y = 5F_{4n}^2+9$ olur. $45y \equiv 0 \pmod 5$ ve $5F_{4n}^2+9 \equiv 4 \pmod 5$ olduğundan $0 \equiv 4 \pmod 5$ çelişkisi elde edilir.

BÖLÜM 7. SONUÇLAR VE ÖNERİLER

Bu tezin ikinci bölümünde tek türlü çarpanlara ayrılabilen bölgelerde verilen bir teorem kullanılarak $x^5 - y^2 = 1$, $y^2 + 2 = x^3$, $y^2 + 1 = x^3$, $y^2 + 11 = x^3$, $x^2 + x + 2 = y^3$ Diyofant denklemleri çözüldü. Daha genel olarak $n \geq 4$ olmak üzere $x^2 + 2 = y^n$, $x^2 + 1 = y^n$ gibi Diyofant denklemlerinin çözümlerinin olup olmadığı araştırılabilir. Son bölümde bazı Diyofant denklemlerinin çözümleri Fibonacci ve Lucas dizilerinin terimleri cinsinden ifade edilmiştir. Burada incelenen denklemlerden başka $(x + y + 1)^2 = 10xy$, $(x + y - 1)^2 = 10xy$ Diyofant denklemleri incelenerek çözümlerinin olup olmadığı araştırılabilir. Ayrıca $(x + y + 1)^2 = 6xy$ ve $(x + y - 1)^2 = 6xy$ denklemlerinin çözümleri araştırılabilir.

KAYNAKLAR

[1] SIERPINSKI, W., Elemantary Theory of Numbers: Second English Edition (edited by A. Schinzel). Elsevier, 1988.

[2] REDMOND, D., Number Theory: An Introduction, Markel Dekker. Inc, Newyork, 1996.

[3] KESKİN, R., Solutions of Some Quadratic Diophantine Equations, Computers and Mathematics with applications, 60, 2225-2230, 2010.

[4] Duverney, D., Number Theory, An Elemantary Introduction Through Diophantine Problems, World Scientific Publishing Company, September 9, 2010.

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

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

[7] ANDREESCU, T.; ANDRICA, D.; CUCUREZEANU, I., An Introduction to Diophantine Equations: a problem-based approach. Springer Science & Business Media, 2010.

[8] NAGELL, T., Introduction to Number Theory, Chelsea Publishing Company, New York, 1981.

[9] ÇALLIALP, F., Soyut Cebir, Birsen Yayınevi, İstanbul 2011.

[10] KESKİN, R. ; DEMİRTÜRK , B., Solutions of some Diophantine equations using generalized Fibonacci and Lucas sequences, Ars Combinatoria, 2013, 111:161-179.

[11] KELEŞ, S., Diophant Denklemleri, Yüksek Lisans Tezi, Sakarya Üniversitesi Fen Bilimleri Enstitüsü, 2007.

ÖZGEÇMİŞ

Hilal Başak Özdemir, 14.09.1990'da Samsun'da doğdu. İlk, orta ve lise eğitimini Samsun'da tamamladı. 2008 yılında Milli Piyango Anadolu Lisesi'nden mezun oldu. 2008 yılında başladığı Ondokuz Mayıs Üniversitesi Fen Edebiyat Fakültesi Matematik bölümünü 2012 yılında birincilikle bitirdi. 2010-2012 yılları arasında Ondokuz Mayıs Üniversitesi'nde Formasyon eğitimi aldı. 2012 yılında Sakarya Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim dalında yüksek lisans eğitimine başladı. 2013-2014 eğitim öğretim yılları arasında Kandıra Mefkure Dershanesi'nde matematik öğretmeni olarak görev yaptı.