T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

KONGRUENT SAYILAR VE ELİPTİK EĞRİLER

YÜKSEK LİSANS TEZİ

Ümmügülsüm ÖĞÜT

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

Ocak 2014

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

KONGRUENT SAYILAR VE ELİPTİK EĞRİLER

YÜKSEK LİSANS TEZİ

Ümmügülsüm ÖĞÜT

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

Bu tez 02/01/2014 tarihinde aşağıdaki jüri tarafından Oybirliği ile kabul edilmiştir.

Prof. Dr. Refik KESKİN Jüri Başkanı	Prof. Dr. Halim ÖZDEMİR Üye	Doç. Dr. Gökhan SOYDAN Üye

ÖNSÖZ

Tez çalışmamın her aşamasında engin bilgi ve tecrübeleriyle beni yönlendiren, yardımlarını ve zamanını hiçbir zaman esirgemeyen saygı değer danışman hocam Prof. Dr. Refik KESKİN' e teşekkürlerimi sunarım.

Bugüne kadar bana daima güvenip beni destekleyen ve hiçbir fedakarlıktan kaçınmayan çok sevdiğim aileme tüm içtenlikle teşekkür ederim.

Ayrıca, yüksek lisans eğitimim boyunca sağladığı finansal destekten dolayı TÜBİTAK'a teşekkür ederim.

İÇİNDEKİLER

SİMGELER VE KISALTMALAR LİSTESİ

$\mathbb{Q}$	: Rasyonel sayılar kümesi
$\mathbb{Z}$	: Tamsayılar kümesi
$\mathbb{Z}^+$	: Pozitif tamsayılar kümesi
$\mathbb{N}$	: Doğal sayılar kümesi
(a,b)	: a,b sayılarının ortak bölenlerinin en büyüğü
$E(\mathbb{Q})$	: E eliptik eğrisinin rasyonel noktalarının kümesi
$\lvert\cdot\rvert$	: Kardinalite
F_n	: n-inci Fibonacci sayısı
L_n	: n-inci Lucas sayısı
P_n	: n-inci Pell sayısı
Q_n	: n-inci Pell-Lucas sayısı
(V_n)	: Genelleştirilmiş Lucas dizisi
(U_n)	: Genelleştirilmiş Fibonacci dizisi
$\left(\frac{p}{q}\right)$	: Legendre Sembolü

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

ÖZET

Anahtar kelimeler: Kongruent Sayılar, Eliptik Eğriler, Genelleştirilmiş Fibonacci ve Lucas Dizileri, Pell Denklemleri

Bu tez temel olarak iki bölümden ve bu bölümlerde kendi içerisinde alt bölümlerden oluşmuştur.

Birinci bölümde kongruent sayılar hakkında temel bilgiler verildi. Daha sonra Pisagor üçlüleri yardımıyla bazı kongruent sayı aileleri oluşturuldu. Bu bölümde son olarak genelleştirilmiş Fibonacci ve Lucas dizilerinden elde edilen bazı kongruent sayılar belirlendi. Özellikle L_n, n. Lucas sayısı olmak üzere $5L_{2n-1}$ ve $10L_{2n}$ değerlerinin kongruent sayı olduğu belirlendi. Ayrıca Q_n, n. Pell-Lucas sayısını belirtmek üzere $Q_{2n-1}/2$ sayısının kongruent sayı olduğu gösterildi.

İkinci bölümde ise eliptik eğriler teorisi hakkında iyi bilinen temel kavramlar verildikten sonra kongruent sayılarla eliptik eğriler arasındaki ilişki ifade edildi. Ayrıca Birch ve Swinnerton-Dyer konjektürü verildi ve bu konjektürün $y^2 = x^3 - n^2 x$ eliptik eğrisi için doğru olması durumunda $n \equiv 5,6,7 \pmod 8$ şartını sağlayan karesiz pozitif tamsayıların kongruent sayı olduğu gösterildi.

CONGRUENT NUMBERS AND ELLIPTIC CURVES

SUMMARY

Key Words: Congruent Numbers, Elliptic Curves, Generalized Fibonacci and Lucas Sequences, Pell Equations

This thesis consists of fundamentally two chapters and these chapters consist of subchapters in itself.

In the first chapter, the congruent numbers are discussed and explained. After that, some families of congruent numbers are demonstrated by utilizing Pythagorean triple. The last part of the chapter is terminated with determination of congruent numbers that are derived from generalized Fibonacci and Lucas sequences. In particular, $5L_{2n-1}$ and $10L_{2n}$ are determined to be congruent number where L_n is the nth Lucas number. Moreover, it is shown that $Q_{2n-1}/2$ is congruent number where Q_n is the nth Pell-Lucas number.

In the second chapter, the addition of two points in an elliptic curve is given and the relation between congruent numbers and elliptic curves is seeked. By explaining Birch and Swinnerton-Dyer conjecture, it is demonstrated that if this conjecture is true for the elliptic curve $y^2 = x^3 - n^2 x$ then the squarefree positive integer n congruent to $5, 6$ or 7 modulo 8 is a congruent number.

BÖLÜM 1. KONGRUENT SAYILAR

1.1. Giriş

Bir dik üçgenin dik kenarları ve hipotenüsü rasyonel sayı ise bu dik üçgene rasyonel dik üçgen denir. Bir rasyonel dik üçgenin alanı da rasyoneldir. Fakat bütün pozitif rasyonel sayılar, bir dik üçgenin alanı olarak karşımıza çıkmaz. Örneğin, alanı 1 olan bir rasyonel dik üçgen yoktur. Eğer $\frac{r}{s}$ pozitif rasyonel sayı ise $m^2\frac{r}{s}$ doğal sayı olacak biçimde m rasyonel sayısı vardır. O halde $\frac{r}{s}$, kenarları x, y, z olan rasyonel dik üçgenin alanı ise $m^2\frac{r}{s}$ kenarları mx, my, mz olan rasyonel dik üçgenin alanıdır. Dolayısıyla hangi pozitif rasyonel sayıların rasyonel dik üçgenin alanı olacağını araştırmak yerine hangi doğal sayının rasyonel dik üçgenin alanı olacağını araştırmak yeterlidir. Eğer pozitif n tamsayısı bir rasyonel dik üçgenin alanı ise, bu n sayısına kongruent sayı denir. Kongruent sayı problemi sayılar teorisinin en eski problemlerinden biridir. Hangi sayıların kongruent sayı olduğu problemi, ilk olarak 10. yüzyıl Arap bilim adamları tarafından tartışılmıştır. 10. yüzyıldan sonra birçok bilinen matematikçi kongruent sayı problemi ile ilgilenmiştir. Örneğin, Euler $n=7$ nin bir kongruent sayı olduğunu göstermiştir. Bu kongruent sayı, kenarları $\frac{24}{5}, \frac{35}{12}$ ve $\frac{337}{60}$ olan dik üçgenin alanıdır. Leonardo Pisano (Fibonacci) $n=5$ in bir kongruent sayı olduğunu göstermiştir. Bu kongruent sayı kenarları $\frac{3}{2}$, $\frac{20}{3}$ ve $\frac{41}{6}$ olan rasyonel dik üçgenin alanıdır. Kongruent sayı tanımının dik üçgenin kenarlarının tamsayı olmasını gerektirmediğine dikkat edilmelidir. Gerçekten $n=6$ kenarları tamsayı olan dik üçgenin mümkün olan en küçük alanıdır. Bu dik üçgen $3-4-5$ dik üçgenidir. Fakat $n=5$ en küçük kongruent sayıdır. Alanı 5 olan rasyonel dik üçgenin kenarları

$\frac{3}{2}, \frac{20}{3}$ ve $\frac{41}{6}$ dır. Fibonacci, 1225 te kongruent sayı problemi ile ilgili genel bir değerlendirme yapmıştır. Fibonacci, eğer n tam kare ise n nin kongruent sayı olamayacağını ispatsız olarak belirtmiştir. Bu iddia Pierre de Fermat tarafından ispatlanmıştır. Fermat $n=1$ ve böylece tüm tam karelerin kongruent sayı olamayacağını sonsuz azalan yöntemiyle ispatlamıştır.

1.2. Kongruent Sayılar

Tanım 1.2.1. Pozitif n tamsayısı bir rasyonel dik üçgenin alanı ise bu n sayısına kongruent sayı denir.

Tanımdan da anlaşılacağı gibi dik üçgenin alanı tamsayı olsa bile, kenarları rasyonel sayı değilse kongruent sayı değildir. Örneğin, kenarları $1, 2, \sqrt{5}$ olan dik üçgen ele alındığında alanı 1 dir. Fakat 1 kongruent sayı değildir.

Ek' te 1000 den küçük kongruent sayılar verildi. Ayrıca 3000 e kadar hangi sayıların kongruent sayı olduğu ile ilgili [1] ve [2] kaynaklarına bakılabilir.

Tanım 1.2.2. x, y, z pozitif tamsayılar olsun. Eğer $x^2+y^2=z^2$ ise (x,y,z) üçlüsüne Pisagor üçlüsü denir. Ayrıca $(x,y,z)=1$ ise (x,y,z) üçlüsüne bir primitif Pisagor üçlüsü denir.

Lemma 1.2.3.

i) (x,y,z) bir primitif Pisagor üçlüsü olsun. Bu takdirde, $x=u^2-v^2$, $y=2uv$, $z=u^2+v^2$, $(u,v)=1$ ve $u+v$ tek olacak biçimde $u>v\geq 1$ tamsayıları mevcuttur.

ii) (x,y,z) bir Pisagor üçlüsüdür $\Leftrightarrow$ $x=k(u^2-v^2)$, $y=k(2uv)$, $z=k(u^2+v^2)$, $u>v\geq 1$, $(u,v)=1$ ve $u+v$ tek olacak biçimde u,v,k pozitif tamsayıları vardır.

Şimdi n kongruent sayı ise n nin tam kare olamayacağını gösterelim. Bunun için aşağıdaki lemmaya ihtiyaç vardır.

Lemma 1.2.4. $a^2-b^2=x^2$ ve $a^2+b^2=y^2$ olacak biçimde a,b,x,y pozitif tamsayıları yoktur.

İspat. $a^2-b^2=x^2$ ve $a^2+b^2=y^2$ denklemlerini sağlayan b tamsayılarının en küçüğünü ele alalım. O halde $(a,b,x)=(a,b,y)=1$ dir. $a^2-b^2=x^2$ ve $a^2+b^2=y^2$ ise $a^2=b^2+x^2$ ve $a^2+b^2=y^2$ olup (a,b,x) ve (a,b,y) birer primitif Pisagor üçlüsüdür. Dolayısıyla a tamsayısı tek ve böylece b tamsayısı çift olur. Diğer yandan $z=xy$ olmak üzere $a^4-b^4=\left(a^2-b^2\right)\left(a^2+b^2\right)=x^2y^2=(xy)^2=z^2$ yazılabilir. Yani $\left(a^2\right)^2=z^2+\left(b^2\right)^2$ dir. $(z,b^2,a^2)=1$ olduğu kolayca gösterilebilir. Dolayısıyla $b^2=2uv$, $z=u^2-v^2$, $a^2=u^2+v^2$ olacak biçimde aralarında asal olan u ve v tamsayıları vardır. $a^2=u^2+v^2$ ve u ve v tamsayılarının rolleri simetrik olduğundan v çift kabul edilebilir. Dolayısıyla Lemma 1.2.3 e göre $u=r^2-s^2$, $v=2rs$, $a=r^2+s^2$ olacak biçimde aralarında asal olan r ve s tamsayıları vardır. Buradan $b^2=2uv=2(r^2-s^2)(2rs)=4rs(r^2-s^2)$ yani $\left(\frac{b}{2}\right)^2=rs(r^2-s^2)$ yazılabilir. $(r,s)=1$ olduğundan $(rs,r^2-s^2)=1$ olduğunu görmek kolaydır. Şu halde rs ve r^2-s^2 birer tam karedir. Ayrıca r ve s tamsayılarından biri tek diğeri çift ve iki tamsayı aralarında asal olduğundan $(r-s,r+s)=1$ dir. Dolayısıyla $r^2-s^2=(r-s)(r+s)$ olduğu dikkate alınırsa $r-s$ ve $r+s$ tamsayıları birer tam karedir. Şu halde $r=t^2$, $s=k^2$, $r-s=c^2$ ve $r+s=d^2$ olacak biçimde t,k,c,d tamsayıları vardır. Buradan $t^2-k^2=c^2$ ve $t^2+k^2=d^2$ elde edilir. $v=2rs$, $b^2=2uv$ ve $s=k^2$ olduğu kullanılırsa $b^2=4urk^2$ elde edilir. Bu ise $k<b$ olmasını gerektirir. Bu durum b tamsayısının tanımıyla çelişir. Şu halde kabul yanlıştır.

Teorem 1.2.5. n kongruent sayı olsun. Bu takdirde n tam kare olamaz.

İspat. n bir kongruent sayı ve $k \in \mathbb{Z}$ için $n = k^2$ olsun. n kongruent sayı olduğundan $n = \frac{xy}{2}$ olan ve kenarları $x, y, z \in \mathbb{Q}$ olan bir dik üçgen vardır. Pozitif a, b, c, m tamsayıları için $x = \frac{a}{m}$, $y = \frac{b}{m}$, $z = \frac{c}{m}$ olsun. $x^2 + y^2 = z^2$ olduğu kullanılırsa, yukarıdaki değerler yerine yazılarak,

$$\left(\frac{a}{m}\right)^2 + \left(\frac{b}{m}\right)^2 = \left(\frac{c}{m}\right)^2$$

ve dolayısıyla $a^2 + b^2 = c^2$ bulunur. Böylece,

$$k^2 = n = \frac{xy}{2} = \frac{\left(\frac{a}{m}\right)\left(\frac{b}{m}\right)}{2} = \frac{ab}{2m^2}$$

olduğundan, $ab = 2m^2k^2 = 2(mk)^2$ olur. $a^2 + b^2 = c^2$ ve $ab = 2(mk)^2$ eşitlikleri kullanılarak,

$$(a+b)^2 = a^2 + b^2 + 2ab = c^2 + (2mk)^2,$$
$$(a-b)^2 = a^2 + b^2 - 2ab = c^2 - (2mk)^2$$

elde edilir. Bu ise Lemma 1.2.4 gereği imkansızdır. Böylece ispat tamamlanır.

Lemma 1.2.6. m karesiz pozitif bir tamsayı olmak üzere $n=s^2m$ olsun. O zaman n kongruent sayıdır $\Leftrightarrow$ m kongruent sayıdır.

İspat.

$\Rightarrow)$: n kongruent sayı olsun. Bu takdirde kenarları $x,y,z\in\mathbb{Q}$ olan rasyonel dik üçgen vardır. Bu durumda $n=\frac{xy}{2}$ dir. $n=s^2m$ olduğundan $m=\frac{n}{s^2}$ ve böylece $m=\frac{xy}{2s^2}=\frac{1}{2}\cdot\left(\frac{x}{s}\right)\left(\frac{y}{s}\right)$ dir. Dolayısıyla m, kenarları $\frac{x}{s},\frac{y}{s},\frac{z}{s}\in\mathbb{Q}$ olan rasyonel dik üçgenin alanıdır. O halde m kongruent sayıdır.

$\Leftarrow)$: m kongruent sayı olsun. Bu takdirde kenarları $x,y,z\in\mathbb{Q}$ olan rasyonel dik üçgen vardır ve $m=\frac{xy}{2}$ dir. $n=s^2m$ olduğundan $n=\frac{s^2xy}{2}=\frac{(sx)(sy)}{2}$ dir. Bu ise n nin kenarları $sx,sy,sz\in\mathbb{Q}$ olan rasyonel dik üçgenin alanı olduğunu gösterir. Böylece n kongruent sayıdır.

n pozitif tamsayısı, m karesiz bir tamsayı olmak üzere $n=s^2m$ biçiminde yazılabilir. Dolayısıyla Lemma 1.2.6 ya göre hangi karesiz sayıların kongruent sayı olduğunu araştırmak yeterlidir.

Teorem 1.2.7. n karesiz pozitif bir tamsayı olsun. Aşağıdaki ifadeler birbirine denktir [3].

i) $x^2+ny^2=z^2$ ve $x^2-ny^2=t^2$ olacak biçimde $x,y,z,t\in\mathbb{Z}^+$ vardır.

ii) $x^4-n^2y^4=w^2$ olacak biçimde $x,y,w\in\mathbb{Z}^+$ vardır.

iii) $Y^2=X^3-n^2X$ denkleminin $\mathbb{Q}$ da aşikar olmayan çözümleri vardır.

iv) Alanı n olan rasyonel dik üçgen vardır.

v) $nw^2=uv(u^2-v^2)$ olacak biçimde $u,v,w\in\mathbb{Z}^+$ vardır.

İspat.

$i \Rightarrow ii)$:

$$x^2 + ny^2 = z^2 \tag{1.1}$$

$$x^2 - ny^2 = t^2 \tag{1.2}$$

olacak biçimde $x, y, z, t \in \mathbb{Z}^+$ olsun. (1.1) ve (1.2) eşitlikleri taraf tarafa çarpılırsa $\left(x^2 + ny^2\right)\left(x^2 - ny^2\right) = z^2 t^2$, yani $x^4 - n^2 y^4 = (zt)^2$ elde edilir. Dolayısıyla $w = zt$ alınırsa, $x^4 - n^2 y^4 = w^2$ elde edilir.

$ii \Rightarrow iii)$: $x, y, z \in \mathbb{Z}^+$ olmak üzere $x^4 - n^2 y^4 = w^2$ olsun. O zaman,

$$x^4 - n^2 y^4 = w^2 \Rightarrow \frac{x^4}{y^4} - n^2 \frac{y^4}{y^4} = \frac{w^2}{y^4}$$

$$\Rightarrow \frac{x^4}{y^4} - n^2 \frac{y^4}{y^4} = \frac{w^2}{y^4}$$

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

$$\Rightarrow \frac{x^2}{y^2}\left[\left(\frac{x}{y}\right)^4 - n^2\right] = \frac{x^2}{y^2}\left[\left(\frac{w}{y^2}\right)^2\right]$$

$$\Rightarrow \left(\frac{x}{y}\right)^6 - n^2 \frac{x^2}{y^2} = \left(\frac{wx}{y^3}\right)^2$$

dir.

Şimdi $X = \frac{x^2}{y^2}$, $Y = \frac{wx}{y^3}$ alınırsa, $Y^2 = X^3 - n^2 X$ elde edilir. Burada X ve Y sıfırdan farklıdır ve bunlar denklemin aşikar olmayan çözümleridir.

$iii \Rightarrow iv)$: $Y \neq 0$ ve $X, Y \in \mathbb{Q}$ olmak üzere $Y^2 = X^3 - n^2 X$ olduğunu kabul edelim. Bu durumda $X \neq n$ dir. O halde $a = \frac{X^2 - n^2}{Y}$, $b = \frac{2nX}{Y}$ ve $c = \frac{X^2 + n^2}{Y}$ alınırsa $a^2 + b^2 = c^2$ olur. Böylece kenarları a, b, c olan rasyonel dik üçgen elde edilir. Bu dik üçgenin alanı $\frac{ab}{2} = \frac{\left(X^2 - n^2\right)(2nX)}{2Y^2} = n$ dir.

$iv \Rightarrow v)$: n pozitif bir tamsayı $a^2 + b^2 = c^2$ ve $n = \frac{ab}{2}$ olacak biçimde kenarları $a, b, c \in \mathbb{Q}$ olan rasyonel dik üçgen olduğunu kabul edelim. $f, g, h, m \in \mathbb{Z}^+$ olmak üzere $a = \frac{f}{m}$, $b = \frac{g}{m}$, $c = \frac{h}{m}$ olarak yazılabilir. $a^2 + b^2 = c^2$ olduğundan $f^2 + g^2 = h^2$ elde edilir. Bu dik üçgenin alanı $\frac{fg}{2} = \frac{ma \cdot mb}{2} = m^2 \frac{ab}{2} = m^2 n$ dir. Ayrıca Lemma 1.2.3. e göre $f = k\left(r^2 - s^2\right)$, $g = k(2rs)$, $h = k\left(r^2 + s^2\right)$, $(r, s) = 1$, $r > s$ ve $r - s$ tek olacak biçimde $k, r, s \in \mathbb{Z}^+$ vardır. Dolayısıyla,

$$nm^2 = \frac{k(2rs)\,k(r^2 - s^2)}{2} = k^2 rs(r^2 - s^2)$$

dir.

Böylece, $n(km)^2 = (kr)(ks)\left((kr)^2 - (ks)^2\right)$ dir. O halde $w = km$, $u = kr$, $v = ks$ alınırsa $nw^2 = uv\left(u^2 - v^2\right)$ elde edilir. Bu ise istenen sonuçtur.

$v \Rightarrow i)$: n pozitif karesiz tamsayı ve $nw^2 = uv(u^2 - v^2)$ olacak biçimde $u > v$, $u, v, n, w \in \mathbb{Z}^+$ olduğunu kabul edelim. $r = u^2 - v^2$, $s = 2uv$, $h = u^2 + v^2$ olsun. Bu durumda $(r + s)^2 = r^2 + s^2 + 2rs = h^2 + 4nw^2$ ve $(r - s)^2 = r^2 + s^2 - 2rs = h^2 - 4nw^2$ dir. Dolayısıyla

$$\left(\frac{r+s}{2}\right)^2 = \left(\frac{h}{2}\right)^2 + nw^2,$$

$$\left(\frac{r-s}{2}\right)^2=\left(\frac{h}{2}\right)^2-nw^2$$

dir. Ayrıca $x,z,t,m\in\mathbb{Z}^+$ olmak üzere $\frac{r-s}{2}=\frac{t}{m}$, $\frac{r+s}{2}=\frac{z}{m}$, $\frac{h}{2}=\frac{x}{m}$ olarak yazılabilir. Bu durumda $z^2=x^2+n(wm)^2$ ve $t^2=x^2-n(wm)^2$ olur. Dolayısıyla $y=wm$ alınırsa $y\in\mathbb{Z}^+$ dir ve buradan $x^2+ny^2=z^2$, $x^2-ny^2=t^2$ bulunur. Bu ise ispatı tamamlar.

Önerme 1.2.8. n pozitif bir tamsayı olsun. n kongruent sayıdır $\Leftrightarrow$ x^2+n ve x^2-n sayılarının her biri bir rasyonel sayının karesi olacak biçimde $x\in\mathbb{Q}$ vardır [4].

İspat.

$\Rightarrow$): n bir kongruent sayı olsun. O halde kenarları $a,b,c\in\mathbb{Q}$ olan bir dik üçgen vardır ve bu dik üçgenin alanı n dir. Dolayısıyla $a^2+b^2=c^2$ ve $n=\frac{ab}{2}$ dir.

$$\left(\frac{c}{2}\right)^2=\frac{c^2}{4}=\frac{a^2+b^2}{4}=\frac{a^2+2ab+b^2}{4}-\frac{ab}{2}=\left(\frac{a+b}{2}\right)^2-\frac{ab}{2},$$

$$\left(\frac{c}{2}\right)^2=\frac{c^2}{4}=\frac{a^2+b^2}{4}=\frac{a^2-2ab+b^2}{4}+\frac{ab}{2}=\left(\frac{a-b}{2}\right)^2+\frac{ab}{2}$$

olup $x=\frac{c}{2}$ alınırsa

$$x^2=\left(\frac{a+b}{2}\right)^2-n,$$

$$x^2=\left(\frac{a-b}{2}\right)^2+n$$

yani $x^2+n=\left(\frac{a+b}{2}\right)^2$ ve $x^2-n=\left(\frac{a-b}{2}\right)^2$ olur. Şu halde x^2+n ve x^2-n sayılarının her biri bir rasyonel sayının karesidir.

$\Leftarrow$): x^2+n ve x^2-n sayılarının her biri bir rasyonel sayının karesi olsun. O zaman $a=\sqrt{x^2+n}-\sqrt{x^2-n}$, $b=\sqrt{x^2+n}+\sqrt{x^2-n}$ ve $c=2x$ alınırsa $a^2+b^2=c^2$ ve $\frac{ab}{2}=\frac{\left(\sqrt{x^2+n}-\sqrt{x^2-n}\right)\left(\sqrt{x^2+n}+\sqrt{x^2-n}\right)}{2}=\frac{x^2+n-\left(x^2-n\right)}{2}=n$ elde edilir.

O halde n kongruent sayıdır .

Örnekler 1.2.9.

i) $5^2+24=7^2$ ve $5^2-24=1^2$ olduğundan 24 bir kongruent sayıdır.

ii) $10^2+96=14^2$ ve $10^2-96=2^2$ olduğundan 96 bir kongruent sayıdır. $96=16\cdot 6$ olduğundan 6 bir kongruent sayıdır.

iii) $\left(\frac{41}{12}\right)^2+5=\left(\frac{49}{12}\right)^2$ ve $\left(\frac{41}{12}\right)^2-5=\left(\frac{31}{12}\right)^2$ olduğundan 5 bir kongruent sayıdır.

iv) $\left(\frac{337}{120}\right)^2+7=\left(\frac{463}{120}\right)^2$ ve $\left(\frac{337}{120}\right)^2-7=\left(\frac{113}{120}\right)^2$ olduğundan 7 bir kongruent sayıdır.

İlerideki soru çözümlerinde ve ispatlarda aşağıdaki iki teoreme ihtiyaç vardır.

Teorem 1.2.10. $x,y,z\in\mathbb{Z}^+$ olmak üzere $x^4+y^4=z^2$ denkleminin $x>0$, $y>0$, $z>0$ şartını sağlayan tamsayı çözümleri yoktur.

İspat. Pozitif x,y,z tamsayıları $x^4+y^4=z^2$ denkleminin çözümü olsun. Bu çözüm z nin en küçük değerini aldığı çözüm olsun. Bu durumda $(x,y)=1$ kabul edilebilir. O zaman $\left(x^2\right)^2+\left(y^2\right)^2=z^2$, $\left(x^2,y^2\right)=1$ yazılabilir. Dolayısıyla $\left(x^2,y^2,z\right)$ bir primitif Pisagor üçlüsüdür. O halde Lemma 1.2.3 e göre $x^2=2rs$, $y^2=r^2-s^2$, $z=r^2+s^2$ olacak biçimde $(r,s)=1$ ve $r+s$ tek olan $r,s\in\mathbb{Z}^+$ vardır. O zaman $y^2+s^2=r^2$ olup y tek ve $(r,s)=1$ olduğundan (y,s,r)

bir primitif Pisagor üçlüsüdür. O halde $s=2ab,\ y=a^2-b^2,\ r=a^2+b^2$ olacak biçimde $(a,b)=1$ ve $a+b$ tek olan a,b pozitif tamsayıları vardır. Böylece $x^2=2rs=2\left(a^2+b^2\right)2ab=4ab\left(a^2+b^2\right)$ dir. $(a,b)=\left(a,a^2+b^2\right)=\left(b,a^2+b^2\right)=1$ olduğundan $a=u^2,\ b=v^2,\ a^2+b^2=w^2$ olacak biçimde u,v,w pozitif tamsayıları vardır. Böylece $u^4+v^4=a^2+b^2=w^2$ elde edilir. Yani $(u,v,w),\ x^4+y^4=z^2$ denkleminin başka bir çözümüdür. Burada $w\le w^2=a^2+b^2=r\le r^2+s^2=z$ dir. Bu ise z nin en küçük olmasıyla çelişir.

Teorem 1.2.11. $x^4-y^4=z^2$ denkleminin $x>0,\ y>0,\ z>0$ şartını sağlayan tamsayı çözümleri yoktur.

İspat. $x^4-y^4=z^2$ olan $x>0,\ y>0,\ z>0$ tamsayılarının mevcut olduğunu kabul edelim. $d=(x,y)$ olsun. O zaman $x=da,\ y=db,\ (a,b)=1$ olacak biçimde $a,b\in\mathbb{Z}^+$ vardır. Dolayısıyla $d^4\left(a^4-b^4\right)=z^2$ yani $a^4-b^4=\left(\frac{z}{d^2}\right)^2$ dir. Şu halde $x^4-y^4=z^2$ denkleminde $x>0,\ y>0,\ z>0$ tamsayıları için $(x,y)=1$ kabul edilebilir. O zaman $x^4-y^4=z^2$ olduğundan $\left(x^2-y^2\right)\left(x^2+y^2\right)=z^2$ dir.

$d=\left(x^2-y^2,x^2+y^2\right)$ olsun. $d=1$ veya $d=2$ olduğunu görmek kolaydır.

$\left(x^2-y^2,x^2+y^2\right)=1$ ise $x^2-y^2=a^2$ ve $x^2+y^2=b^2$ olacak biçimde $(a,b)=1$ olan $a,b\in\mathbb{Z}^+$ vardır. Fakat bu Lemma 1.2.4 gereği imkansızdır.

$\left(x^2-y^2,x^2+y^2\right)=2$ ise $x^2-y^2=2u^2$ ve $x^2+y^2=2v^2$ olacak biçimde $u,v\in\mathbb{Z}^+$ vardır. Buradan $x^2=v^2+u^2$ ve $y^2=v^2-u^2$ elde edilir. Bu ise Lemma 1.2.4. e göre mümkün değildir.

Sonuç olarak $x^4-y^4=z^2$ eşitliğinin $x>0,\ y>0,\ z>0$ olan tamsayı çözümü yoktur.

Örnek 1.2.12. $n=2$ bir kongruent sayı değildir [5].

Tersine olarak, 2 bir kongruent sayı olsun. O halde Teorem 1.2.7 ye göre $x^2+2y^2=z^2$ ve $x^2-2y^2=t^2$ olacak şekilde $x,y,z,t\in\mathbb{Z}^+$ vardır. Bu durumda $2x^2=z^2+t^2$, $4y^2=z^2-t^2$ dir. $2x^2=z^2+t^2$ olduğundan $4x^2=(z+t)^2+(z-t)^2$ olur. Dolayısıyla

$$\left[2x(z-t)\right]^2=4x^2(z-t)^2=(z-t)^2\left[(z+t)^2+(z-t)^2\right]=(z^2-t^2)^2+(z-t)^4$$

olur. $(2y)^2=z^2-t^2$ olduğundan $\left[2x(z-t)\right]^2=(2y)^4+(z-t)^4$ elde edilir. $y\neq 0$ olduğundan $z-t\neq 0$ olur. Dolayısıyla $a=\left[2x(z-t)\right]$, $b=2y$ ve $c=z-t$ alınırsa $a\neq 0$, $b\neq 0$, $c\neq 0$ dır. Ayrıca $b^4+c^4=a^2$ dır. Teorem 1.2.10 gereği bu denklemin sıfırdan farklı çözümü yoktur. O halde 2 bir kongruent sayı değildir.

[6] da Genocchi p asal ve $p\equiv 3\pmod 8$ ise p nin kongruent sayı olmadığını göstermiştir. [7] de bu lemmanın ispatı mevcuttur. Fakat ispat uzundur. Burada daha kısa bir ispat verilecektir.

Lemma 1.2.13. p asal ve $p\equiv 3\pmod 8$ olsun. Bu takdirde p kongruent sayı olamaz.

İspat. Aksini kabul edelim. p kongruent sayı olsun. p kongruent sayı ise Teorem 1.2.7 ye göre,

$$f^2+pg^2=h^2,$$
$$f^2-pg^2=k^2$$

olacak biçimde $f,g,h\in\mathbb{Z}^+$ vardır. g bu şartı sağlayan en küçük tamsayı olsun. Bu durumda $h^2-k^2=2pg^2$ ve böylece $h\equiv k\pmod 2$ dir. O halde $r=\frac{h+k}{2}$, $s=\frac{h-k}{2}$ birer tamsayıdır. Buradan $f^2=r^2+s^2$ elde edilir. Dolayısıyla (r,s,f) bir Pisagor üçlüsüdür.

Şu halde Lemma 1.2.3 e göre $f=k\left(u^2+v^2\right)$, $r=k\left(u^2-v^2\right)$, $s=k(2uv)$ veya $f=k\left(u^2+v^2\right)$, $r=k(2uv)$, $s=k\left(u^2-v^2\right)$ $(u,v)=1$, $u>v$, $u+v$ tek olacak biçimde $u,v\in\mathbb{Z}^+$ vardır.

Genelliği bozmadan $f=k\left(u^2+v^2\right), r=k\left(u^2-v^2\right), s=k(2uv)$ alınabilir. Ayrıca, $2pg^2=h^2-k^2=(h-k)(h+k)=2r\cdot 2s=4rs$ olduğundan $pg^2=2rs$ olur. r ve s değerleri yerine yazılırsa,

$$pg^2=2rs=4k^2uv(u^2-v^2) \tag{1.3}$$

elde edilir.

(1.3) kullanılarak $pw^2=uv(u^2-v^2)$ olacak biçimde $w\in\mathbb{Z}^+$ olduğu kolaylıkla gösterilebilir. $pw^2=uv(u^2-v^2)$ olması için için dört durum söz konusudur.

1. Durum: $u=f_1^2$, $v=pg_1^2$, $u+v=h_1^2$, $u-v=k_1^2$ olabilir.

Bu durumda $f_1^2+pg_1^2=h_1^2$ ve $f_1^2-pg_1^2=k_1^2$ elde edilir. u, v, $u+v$, $u-v$ değerleri (1.3) denkleminde yerine yazılırsa $pg^2=4k^2(f_1^2pg_1^2)(h_1^2k_1^2)$ ve böylece $pg^2>pg_1^2$, yani $g>g_1$ elde edilir. Bu ise g sayısının en küçük olmasıyla çelişir.

2. Durum: $u=f_1^2$, $v=g_1^2$, $u+v=ph_1^2$, $u-v=k_1^2$ olabilir.

Bu durumda $u+v+(u-v)=2u$ ve buradan $ph_1^2+k_1^2=2f_1^2$ olur. $p\nmid k_1$ ve $p\nmid f_1$ olduğu kolaylıkla gösterilebilir. O zaman $k_1^2\equiv 2f_1^2\pmod p$ ve böylece $\left(\frac{2}{p}\right)=1$ elde edilir. Bu ise $p\equiv 3\pmod 8$ olduğundan mümkün değildir.

3. Durum: $u=f_1^2,\ v=g_1^2,\ u+v=h_1^2,\ u-v=pk_1^2$ olabilir.

Bu durumda $u+v+(u-v)=2u \Rightarrow h_1^2+pk_1^2=2f_1^2$ olur. Kolaylıkla $p \nmid k_1$ ve $p \nmid f_1$ olduğu gösterilebilir. O zaman $h_1^2 \equiv 2f_1^2 \pmod{p}$ ve böylece $\left(\frac{2}{p}\right)=1$ elde edilir. Bu ise $p \equiv 3 \pmod{8}$ olduğundan mümkün değildir.

4. Durum: $u=pf_1^2,\ v=g_1^2,\ u+v=h_1^2,\ u-v=k_1^2$ olabilir.

O zaman $u+v+(u-v)=2u \Rightarrow h_1^2+k_1^2=2pf_1^2$ yani $2pf_1^2=h_1^2+k_1^2$ olur. $p \nmid k_1$ ve $p \nmid f_1$ olduğu kolaylıkla gösterilebilir. O zaman $h_1^2 \equiv -k_1^2 \pmod{p}$ ve böylece $\left(\frac{-1}{p}\right)=1$ elde edilir. $p \equiv 3 \pmod{8}$ olduğundan bu mümkün değildir.

Sonuç olarak $p \equiv 3 \pmod{8}$ ise p kongruent sayı olamaz.

Kongruent sayılarla ilgili bazı sonuçlar aşağıdaki tabloda verilmiştir.

p_i, q_i, r_i, s_i, $8k+i$, $k \in \mathbb{Z}$ biçiminde tanımlanan farklı asal sayılar olsun. Yani $p_i \equiv i \pmod 8$, $q_i \equiv i \pmod 8$, $r_i \equiv i \pmod 8$, $s_i \equiv i \pmod 8$ olsun. Bu takdirde aşağıdaki sayılar kongruent sayıdır [8].

Tablo 1.1. Bazı kongruent Sayılar

Heegner, 1952[9] Birch, 1968 [10]	$\rightarrow 2p_3$ ve $2p_7$
Stephens, 1978 [11]	$\rightarrow p_5$ ve p_7
Monsky, 1990 [12]	$\rightarrow p_3p_7$, p_3q_5, $2p_3q_5$ ve $2p_5q_7$ $\rightarrow \left(\frac{p_1}{q_5}\right) = -1$ olmak üzere p_1q_5 $\rightarrow \left(\frac{p_1}{q_7}\right) = -1$ olmak üzere p_1q_7 $\rightarrow \left(\frac{p_1}{q_3}\right) = -1$ olmak üzere $2p_1q_3$ $\rightarrow \left(\frac{p_1}{q_7}\right) = -1$ olmak üzere $2p_1q_7$
Serf, 1991 [1]	$\rightarrow p_3q_3r_5$, $p_3q_3r_7$, $2p_3q_3r_7$, $2p_3q_5r_5$ ve $2p_5q_5r_7$ $\rightarrow \left(\frac{p_7}{q_7}\right) = \left(\frac{q_7}{r_7}\right) = -\left(\frac{p_7}{q_7}\right)$ olmak üzere $p_7q_7r_7$ $\rightarrow \left(\frac{p_7}{q_7}\right) = \left(\frac{q_7}{r_7}\right) = -\left(\frac{p_7}{r_7}\right)$ olmak üzere $2p_7q_7r_7$ $\rightarrow \left.\begin{array}{l} \left(\frac{p_1}{q_3}\right) = \left(\frac{p_1}{r_3}\right) = \left(\frac{p_1}{s_5}\right) = 1 \\ \left(\frac{p_1}{s_5}\right) = -\left(\frac{p_1}{q_3}\right) = -\left(\frac{p_1}{r_3}\right) = 1, \ \left(\frac{q_3}{s_5}\right) = \left(\frac{r_3}{s_5}\right) \end{array}\right\}$ olmak üzere $p_1q_3r_3s_5$ $\rightarrow \left.\begin{array}{l} \left(\frac{p_1}{q_3}\right) = \left(\frac{p_1}{r_5}\right) = \left(\frac{p_1}{s_5}\right) = 1 \\ \left(\frac{p_1}{q_3}\right) = -\left(\frac{p_1}{r_5}\right) = -\left(\frac{p_1}{s_5}\right) = 1, \ \left(\frac{q_3}{r_5}\right) = \left(\frac{q_3}{s_5}\right) \end{array}\right\}$ olmak üzere $2p_1q_3r_5s_5$

Kongruent sayılarla ilgili bilinen en iyi sonuç Tunnel' e dayanır.

Teorem 1.2.14. (Tunnel) Kenarları rasyonel sayı olan bir dik üçgenin alanı n, yani n kongruent sayı olsun. Bu takdirde aşağıdakiler doğrudur [13] .

i) n karesiz tek tamsayı ise,

$$\left|\left\{(x,y,z)\in\mathbb{Z}^3 : n=2x^2+y^2+32z^2\right\}\right| = \frac{1}{2}\left|\left\{(x,y,z)\in\mathbb{Z}^3 : n=2x^2+y^2+8z^2\right\}\right|$$

dir.

ii) n karesiz çift tamsayı ise,

$$\left|\left\{(x,y,z)\in\mathbb{Z}^3 : \frac{n}{2}=4x^2+y^2+32z^2\right\}\right| = \frac{1}{2}\left|\left\{(x,y,z)\in\mathbb{Z}^3 : \frac{n}{2}=4x^2+y^2+8z^2\right\}\right|$$

dir.

Örnek 1.2.12 de $n=2$ nin kongruent sayı olmadığı gösterildi. Burada Tunnel teoreminden faydalanak daha basit bir şekilde $n=2$ nin kongruent sayı olmadığı gösterilecektir.

Örnek 1.2.15. $n=2$ nin kongruent sayı olmadığını Tunnel teoreminden faydalanarak bulalım.

$\frac{n}{2}=1=4x^2+y^2+32z^2$ olduğundan $1=4x^2+y^2+32z^2$ denkleminin çözümleri $x=z=0$ ve $y=\pm 1$, yani $(0,1,0)$, $(0,-1,0)$ dır. $\frac{n}{2}=1=4x^2+y^2+8z^2$ olduğundan $1=4x^2+y^2+8z^2$ denkleminin çözümleri $x=z=0$ ve $y=\pm 1$, yani $(0,1,0)$, $(0,-1,0)$ dır.

O halde,

$$\left|\left\{(x,y,z)\in\mathbb{Z}^3:\frac{n}{2}=4x^2+y^2+32z^2\right\}\right|=2,\ \ \frac{1}{2}\left|\left\{(x,y,z)\in\mathbb{Z}^3:\frac{n}{2}=4x^2+y^2+8z^2\right\}\right|=1$$

olup $2\neq 1$ olduğundan $n=2$ bir kongruent sayı değildir.

Örnek 1.2.16. $n=1$ in kongruent sayı olmadığını Tunnel teoreminden faydalanarak bulalım.

$n=1=2x^2+y^2+32z^2$ olduğundan $1=2x^2+y^2+32z^2$ denkleminin çözümleri $x=z=0$ ve $y=\pm 1$ yani $(0,1,0)$, $(0,-1,0)$ dır.

$n=1=2x^2+y^2+8z^2$ olduğundan $1=2x^2+y^2+8z^2$ denkleminin çözümleri $x=z=0$ ve $y=\pm 1$ yani $(0,1,0)$, $(0,-1,0)$ dır.

O halde,

$$\left|\left\{(x,y,z)\in\mathbb{Z}^3:n=2x^2+y^2+32z^2\right\}\right|=2,\ \frac{1}{2}\left(\left|\left\{(x,y,z)\in\mathbb{Z}^3:n=2x^2+y^2+8z^2\right\}\right|\right)=1$$

olup $2\neq 1$ olduğundan $n=1$ bir kongruent sayı değildir.

1.3. Kongruent Sayı Aileleri

Lemma 1.3.1. (a,b,c) bir Pisagor üçlüsü ve $b>a$ olsun. Bu takdirde, aşağıdakiler de Pisagor üçlüsüdür [14] :

i) $(2ac,b^2,a^2+c^2)$,

ii) $(2bc,a^2,b^2+c^2)$,

iii) $(2ab,b^2-a^2,c^2)$.

İspat. (a,b,c) bir Pisagor üçlüsü ise $a^2+b^2=c^2$ dir.

i) $(2ac)^2+(b^2)^2=4a^2c^2+(c^2-a^2)^2=a^4+2a^2c^2+c^4=(a^2+c^2)^2$ olur ve $(2ac,b^2,a^2+c^2)$ bir Pisagor üçlüsüdür.

ii) $(2bc)^2+\left(a^2\right)^2=4b^2c^2+\left(c^2-b^2\right)^2=b^4+2b^2c^2+c^4=\left(b^2+c^2\right)^2$ olup $\left(2bc,a^2,b^2+c^2\right)$ bir Pisagor üçlüsüdür.

iii) $(2ab)^2+\left(b^2-a^2\right)^2=4a^2b^2+b^4-2a^2b^2+a^4=\left(a^2+b^2\right)^2=\left(c^2\right)^2$ dir. Dolayısıyla $\left(2ab,b^2-a^2,c^2\right)$ bir Pisagor üçlüsüdür.

Sonuç 1.3.2. (a,b,c) bir Pisagor üçlüsü olsun. Bu durumda ac, bc, b^2+c^2, a^2+c^2 sayılarının her biri bir kongruent sayıdır. $b>a$ olması durumunda b^2-a^2 kongruent sayıdır [14].

İspat. (a,b,c) bir Pisagor üçlüsü ve $b>a$ olsun

i) $\left(2ac,b^2,a^2+c^2\right)$ Pisagor üçlüsü olduğundan $\frac{(2ac)b^2}{2}=(ac)b^2$ bir kongruent sayıdır. Lemma 1.2.6 gereği ac kongruent sayıdır.

ii) $\left(2bc,a^2,b^2+c^2\right)$ Pisagor üçlüsü olduğundan $\frac{(2bc)a^2}{2}=(bc)a^2$ bir kongruent sayıdır. Lemma 1.2.6 gereği bc kongruent sayıdır.

iii) $\left(2ab,b^2-a^2,c^2\right)$ Pisagor üçlüsüdür. *ii*) gereği $\left(b^2-a^2\right)c^2$ kongruent sayıdır. Lemma 1.2.6 gereği b^2-a^2 kongruent sayıdır.

iv) $\left(2ac,b^2,a^2+c^2\right)$ Pisagor üçlüsüdür. *ii*) gereği $b^2\left(a^2+c^2\right)$ kongruent sayıdır. Lemma 1.2.6 gereği a^2+c^2 kongruent sayıdır.

v) $\left(2bc,a^2,b^2+c^2\right)$ Pisagor üçlüsüdür. *ii*) gereği $a^2\left(b^2+c^2\right)$ kongruent sayıdır. Lemma 1.2.6 gereği b^2+c^2 kongruent sayıdır.

Sonuç 1.3.3. $s>t$ ve s, t pozitif tamsayılar olsun. O zaman aşağıdaki sayılar kongruent sayıdır [14].

i) $st(s^2-t^2)$,

ii) $\frac{st(s^2+t^2)}{2}$,

iii) s^4-t^4,

iv) $2s^4+2t^4$,

v) $s^4+t^4+6s^2t^2$,

vi) $6s^2t^2-s^4-t^4$.

İspat. $a=s^2-t^2$, $b=2st$, $c=s^2+t^2$ ise $a^2+b^2=c^2$ olduğu ve Sonuç 1.3.2 kullanılarak ispatlar yapılacaktır.

i) $\frac{ab}{2}$ kongruent sayı olduğundan $\frac{ab}{2}=\frac{(s^2-t^2)2st}{2}=st(s^2-t^2)$ kongruent sayıdır

ii) bc kongruent sayı olduğundan $2st(s^2+t^2)=4\left(\frac{st(s^2+t^2)}{2}\right)$, yani $\frac{st(s^2+t^2)}{2}$ bir kongruent sayıdır.

iii) ac kongruent sayı olduğundan $\left(s^2-t^2\right)\left(s^2+t^2\right)=s^4-t^4$ bir kongruent sayıdır.

iv) a^2+c^2 kongruent sayı olduğundan $\left(s^2-t^2\right)^2+\left(s^2+t^2\right)^2=2s^4+2t^4$ bir kongruent sayıdır.

v) b^2+c^2 kongruent sayı olduğundan $4s^2t^2+\left(s^2+t^2\right)^2=s^4+t^4+6s^2t^2$ bir kongruent sayıdır.

vi) b^2-a^2 kongruent sayı olduğundan $4s^2t^2-\left(s^2-t^2\right)^2=6s^2t^2-s^4-t^4$ bir kongruent sayıdır.

Teorem 1.3.4. Herhangi pozitif k tamsayısı için aşağıdaki sayıların tümü kongruent sayıdır [14]:

1) $k>1$ olmak üzere $\begin{cases} i)\ k\left(k^2-1\right) \\ ii)\ 2k\left(k^2+1\right) \\ iii)\ k^4-1 \end{cases}$,

2) $k\geq 1$ olmak üzere $\begin{cases} i)\ 2k(2k+1)(4k+1) \\ ii)\ 2k(2k+1)\left(8k^2+4k+1\right) \\ iii)\ (4k+1)\left(8k^2+4k+1\right) \end{cases}$,

3) $k\geq 0$ olmak üzere $\begin{cases} i)\ 2(k+1)(4k+3) \\ ii)\ (k+1)(2k+1)\left(8k^2+12k+5\right) \\ iii)\ (4k+3)\left(8k^2+12k+5\right) \end{cases}$.

İspat. İspatlar Sonuç 1.3.3 kullanılarak yapılacaktır.

1) $k>1$ ve $s=k+1$, $t=k-1$ olsun.

i) $st\left(s^2-t^2\right)=(k+1)(k-1)\left((k+1)^2-(k-1)^2\right)=4k\left(k^2-1\right)$ yani $k\left(k^2-1\right)$ kongruent sayıdır.

ii) $\dfrac{st(s^2+t^2)}{2}=\dfrac{(k+1)(k-1)\left((k+1)^2+(k-1)^2\right)}{2}=k^4-1$ kongruent sayıdır.

iii) $s^4-t^4=\left(s^2-t^2\right)\left(s^2+t^2\right)=\left((k+1)^2-(k-1)^2\right)\left((k+1)^2+(k-1)^2\right)=8k\left(k^2+1\right)$

yani $2k\left(k^2+1\right)$ kongruent sayıdır.

2) $k \geq 1$ ve $s = 2k+1$, $t = 2k$ olsun.

i) $st\left(s^2 - t^2\right) = (2k)(2k+1)\left((2k+1)^2 - (2k)^2\right) = 2k(2k+1)(4k+1)$ kongruent sayıdır.

ii) $\dfrac{st(s^2+t^2)}{2} = \dfrac{(2k+1)(2k)\left((2k+1)^2 + (2k)^2\right)}{2} = k(2k+1)\left(8k^2+4k+1\right)$ kongruent sayıdır.

iii) $s^4 - t^4 = \left((2k+1)^2 - (2k)^2\right)\left((2k+1)^2 + (2k)^2\right) = (4k+1)\left(8k^2+4k+1\right)$ kongruent sayıdır.

3) $k \geq 0$ ve $s = 2k+2$ ve $t = 2k+1$ olsun.

i) $st\left(s^2 - t^2\right) = (2k+2)(2k+1)\left((2k+2)^2 - (2k+1)^2\right) = 2(k+1)(2k+1)(4k+3)$ kongruent sayıdır.

ii) $\dfrac{st(s^2+t^2)}{2} = \dfrac{(2k+2)(2k+1)\left((2k+2)^2 + (2k+1)^2\right)}{2} = (k+1)(2k+1)\left(8k^2+12k+5\right)$ kongruent sayıdır.

iii) $s^4 - t^4 = \left((2k+2)^2 - (2k+1)^2\right)\left((2k+2)^2 + (2k+1)^2\right) = (4k+3)\left(8k^2+12k+5\right)$ kongruent sayıdır.

1.4. Genelleştirilmiş Fibonacci ve Lucas Dizileri ve Kongruent Sayılar

Tanım 1.4.1. k ve s sıfırdan farklı tamsayılar olmak üzere $U_0 = 0$, $U_1 = 1$, $n \geq 2$ için $U_n = kU_{n-1} + sU_{n-2}$ ve $V_0 = 2$, $V_1 = k$, $n \geq 2$ için $V_n = kV_{n-1} + sV_{n-2}$ biçiminde tanımlanan (U_n) ve (V_n) dizilerine sırasıyla genelleştirilmiş Fibonacci ve Lucas dizileri denir.

U_n ve V_n değerlerine sırasıyla *n.* Fibonacci ve *n.* Lucas sayıları denir. Bazen U_n yerine $U_n(k,s)$ ve V_n yerine $V_n(k,s)$ yazılır.

$k=1$, $s=1$ ise $U_n=F_n$ ve $V_n=L_n$ olur. (F_n), (L_n) dizilerine sırasıyla Fibonacci ve Lucas dizileri denir.

$k=2$, $s=1$ ise $U_n=P_n$ ve $V_n=Q_n$ olur. (P_n), (Q_n) dizilerine sırasıyla Pell ve Pell-Lucas dizileri denir.

[15] de aşağıdaki teoremlerin ispatları mevcuttur. Burada teoremler ispatsız verilecektir.

Teorem 1.4.2. k tamsayı ve $k>1$ olsun. $x^2-\left(k^2+4\right)y^2=1$ denkleminin tüm pozitif tamsayı çözümleri $n\geq 1$ olmak üzere k çift ise $(x,y)=\left(\frac{V_{2n}(k,1)}{2},\frac{U_{2n}(k,1)}{2}\right)$ ve k tek ise $(x,y)=\left(\frac{V_{6n}(k,1)}{2},\frac{U_{6n}(k,1)}{2}\right)$ biçimindedir [15].

Teorem 1.4.3. k tamsayı ve $k>1$ tek tamsayı olsun. Bu takdirde $x^2-\left(k^2+4\right)y^2=-1$ denkleminin tüm pozitif tamsayı çözümleri $n\geq 1$ olmak üzere $(x,y)=\left(\frac{V_{6n-3}(k,1)}{2},\frac{U_{6n-3}(k,1)}{2}\right)$ biçimindedir [15].

Teorem 1.4.4. k tamsayı ve $k>3$ olsun. Bu takdirde $x^2-\left(k^2-4\right)y^2=1$ denkleminin tüm pozitif tamsayı çözümleri $n\geq 1$ olmak üzere k çift ise $(x,y)=\left(\frac{V_{2n}(k,-1)}{2},\frac{U_{2n}(k,-1)}{2}\right)$ ve k tek ise $(x,y)=\left(\frac{V_{3n}(k,-1)}{2},\frac{U_{3n}(k,-1)}{2}\right)$ biçimindedir [15].

Teorem 1.4.5. k tamsayı ve $k>1$ olsun. Bu takdirde $x^2-\left(k^2+4\right)y^2=4$ denkleminin tüm pozitif tamsayı çözümleri $n\geq 1$ olmak üzere $(x,y)=\left(V_{2n}(k,1),U_{2n}(k,1)\right)$ biçimindedir [15].

Teorem 1.4.6. k tamsayı ve $k>1$ olsun. Bu takdirde $x^2-\left(k^2+4\right)y^2=-4$ denkleminin tüm pozitif tamsayı çözümleri $n\geq 1$ olmak üzere $(x,y)=\left(V_{2n-1}(k,1),U_{2n-1}(k,1)\right)$ biçimindedir [15].

Teorem 1.4.7. k tamsayı ve $k>3$ olsun. Bu takdirde $x^2-\left(k^2-4\right)y^2=4$ denkleminin tüm pozitif tamsayı çözümleri $n\geq 1$ olmak üzere $(x,y)=\left(V_n(k,-1),U_n(k,-1)\right)$ biçimindedir [15].

Teorem 1.4.8. k tamsayı ve $k\geq 1$ olsun. Bu takdirde $x^2-\left(k^2+1\right)y^2=1$ denkleminin tüm pozitif tamsayı çözümleri $n\geq 1$ olmak üzere $(x,y)=\left(\frac{V_{2n}(2k,1)}{2},U_{2n}(2k,1)\right)$ biçimindedir [15].

Teorem 1.4.9. k tamsayı ve $k\geq 1$ olsun. Bu takdirde $x^2-\left(k^2+1\right)y^2=-1$ denkleminin tüm pozitif tamsayı çözümleri $n\geq 1$ olmak üzere $(x,y)=\left(\frac{V_{2n-1}(2k,1)}{2},U_{2n-1}(2k,1)\right)$ biçimindedir [15].

Teorem 1.4.10. k tamsayı ve $k>1$ olsun. Bu takdirde $x^2-\left(k^2-1\right)y^2=1$ denkleminin tüm pozitif tamsayı çözümleri $n\geq 1$ olmak üzere $(x,y)=\left(\frac{V_n(2k,-1)}{2},U_n(2k,-1)\right)$ biçimindedir [15].

Teorem 1.4.11. k tamsayı ve $k\geq 1$, $k\neq 2$ olsun. Bu takdirde $x^2-\left(k^2+1\right)y^2=-4$ denkleminin tüm pozitif tamsayı çözümleri $n\geq 1$ olmak üzere $(x,y)=\left(V_{2n-1}(2k,1),2U_{2n-1}(2k,1)\right)$ biçimindedir [15].

Teorem 1.4.12. k tamsayı ve $k>1$ olsun. Bu takdirde $x^2-\left(k^2-1\right)y^2=4$ denkleminin tüm pozitif tamsayı çözümleri $n\geq 1$ olmak üzere $(x,y)=\left(V_n(2k,-1),2U_n(2k,-1)\right)$ biçimindedir [15].

Teorem 1.4.13. k tamsayı ve $k\geq 1$, $k\neq 2$ olsun. Bu takdirde $x^2-\left(k^2+1\right)y^2=4$ denkleminin tüm pozitif tamsayı çözümleri $n\geq 1$ olmak üzere $(x,y)=\left(V_{2n}(2k,1),2U_{2n}(2k,1)\right)$ biçimindedir [15].

[14] te $x^2-dy^2=1$ ve $x^2-dy^2=-1$ Pell denklemlerinin pozitif (x,y) çözümleri için sırasıyla xd ve $2xd$ sayılarının kongruent sayı olduğu gösterilmiştir. Burada, ayrıca $x^2-dy^2=4$ ve $x^2-dy^2=-4$ Pell denklemlerinin pozitif (x,y) çözümleri alınarak sırasıyla $2xd$ ve xd sayılarının kongruent sayı olduğu gösterilecektir.

Teorem 1.4.14. $x^2-dy^2=-1$ Pell denkleminin herhangi bir (x,y) pozitif çözümü verilsin. Bu takdirde $2xd$ bir kongruent sayıdır. Eğer x tam kare ise $2d$ bir kongruent sayıdır.

İspat. Çözümdeki herhangi bir x değeri için $\left(x^2-1,2x,x^2+1\right)$ üçlüsü bir Pisagor üçlüsü olduğundan Sonuç 1.3.2 ye göre $2x\left(x^2+1\right)$ sayısı kongruent sayıdır. x^2+1 yerine dy^2 yazılırsa $2xdy^2$ elde edilir. O halde $2xdy^2$ kongruent sayıdır. Lemma1.2.6 gereği $2xd$ bir kongruent sayıdır [14].

Teorem 1.4.15. $x^2 - dy^2 = 1$ Pell denkleminin herhangi bir (x, y) pozitif çözümü verilsin. Bu takdirde xd bir kongruent sayıdır. Eğer x tam kare ise d kongruent sayıdır.

İspat. Çözümdeki herhangi bir pozitif x değeri için $(x^2 - 1, 2x, x^2 + 1)$ bir Pisagor üçlüsüdür. Sonuç 1.3.2 ye göre $x(x^2 - 1)$ sayısı kongruent sayıdır. $x^2 - 1$ yerine dy^2 yazılırsa xdy^2 elde edilir. O halde xdy^2 bir kongruent sayıdır. Lemma 1.2.6 gereği xd bir kongruent sayıdır [14].

Teorem 1.4.16. $x^2 - dy^2 = 4$ Pell denkleminin $x > 2$ olmak üzere bir pozitif tamsayı çözümü (x, y) olsun. Bu takdirde $2xd$ bir kongruent sayıdır. Eğer x tam kare ise $2d$ kongruent sayıdır.

İspat. $x > 2$ ve $x^2 - dy^2 = 4$ olsun. $(x^2 - 4, 4x, x^2 + 4)$ üçlüsü bir Pisagor üçlüsü olduğundan Sonuç 1.3.2 ye göre $2x(x^2 - 4)$ bir kongruent sayıdır. $x^2 - 4$ yerine dy^2 yazılırsa $2xdy^2$ elde edilir. O halde $2xdy^2$ bir kongruent sayıdır. Lemma 1.2.6 gereği $2xd$ kongruent sayıdır.

Teorem 1.4.17. $x^2 - dy^2 = -4$ Pell denkleminin pozitif tamsayı çözümü (x, y) olsun. Bu takdirde xd bir kongruent sayıdır. Eğer x tam kare ise d kongruent sayıdır.

İspat. $x^2 - dy^2 = -4$ olsun. $(x^2 - 4, 4x, x^2 + 4)$ üçlüsü bir Pisagor üçlüsü olduğundan Sonuç 1.3.2 ye göre $4x(x^2 + 4)$ bir kongruent sayıdır. $x^2 + 4$ yerine dy^2 yazılırsa $4xdy^2$ elde edilir. O halde $4xdy^2$ bir kongruent sayıdır. Lemma 1.2.4 gereği xd kongruent sayıdır.

Yukarıda verilen teoremlerden aşağıdaki sonuçlar çıkarılabilir.

Sonuç 1.4.18. $k>1$ olsun. Her $n\in\mathbb{N}$ için k çift ise $\dfrac{(k^2+4)V_{2n}(k,1)}{2}$ ve k tek ise $\dfrac{(k^2+4)V_{6n}(k,1)}{2}$ kongruent sayıdır.

İspat. $k>1$ tamsayı ve $d=k^2+4$ olsun. Teorem 1.4.2 gereği $x^2-dy^2=1$ Pell denkleminin tüm pozitif tamsayı çözümleri $n\geq 1$ olmak üzere;

k çift ise $(x,y)=\left(\dfrac{V_{2n}(k,1)}{2},\dfrac{U_{2n}(k,1)}{2}\right)$ ve k tek ise $(x,y)=\left(\dfrac{V_{6n}(k,1)}{2},\dfrac{U_{6n}(k,1)}{2}\right)$ biçimindedir. O halde Teorem 1.4.15 gereği k çift ise $\dfrac{(k^2+4)V_{2n}(k,1)}{2}$ ve k tek ise $\dfrac{(k^2+4)V_{6n}(k,1)}{2}$ kongruent sayıdır.

Sonuç 1.4.19. $k>3$ tamsayı olsun. Her $n\in\mathbb{N}$ için k çift ise $\dfrac{(k^2-4)V_{2n}(k,-1)}{2}$ ve k tek ise $\dfrac{(k^2-4)V_{3n}(k,-1)}{2}$ kongruent sayıdır.

İspat. $k>3$ tamsayı ve $d=k^2-4$ olsun. Teorem 1.4.4 gereği $x^2-dy^2=1$ Pell denkleminin tüm pozitif tamsayı çözümleri $n\geq 1$ olmak üzere, k çift ise $(x,y)=\left(\dfrac{V_{2n}(k,-1)}{2},\dfrac{U_{2n}(k,-1)}{2}\right)$ ve k tek ise $(x,y)=\left(\dfrac{V_{3n}(k,-1)}{2},\dfrac{U_{3n}(k,-1)}{2}\right)$ biçimindedir. O halde Teorem 1.4.15 gereği k çift ise $\dfrac{(k^2-4)V_{2n}(k,-1)}{2}$ ve k tek ise $\dfrac{(k^2-4)V_{3n}(k,-1)}{2}$ kongruent sayıdır.

Sonuç 1.4.20. $k>1$ tamsayı olsun. Bu takdirde, her $n\in\mathbb{N}$ için $\dfrac{\left(k^2+1\right)V_{2n}\left(2k,1\right)}{2}$ bir kongruent sayıdır.

İspat. $k>1$ tamsayı ve $d=k^2+1$ olsun. Teorem 1.4.8 gereği $x^2-dy^2=1$ Pell denkleminin tüm pozitif tamsayı çözümleri $n\geq 1$ olmak üzere $(x,y)=\left(\dfrac{V_{2n}\left(2k,1\right)}{2},U_{2n}\left(2k,1\right)\right)$ biçimindedir. O halde Teorem 1.4.15 gereği $\dfrac{\left(k^2+1\right)V_{2n}\left(2k,1\right)}{2}$ bir kongruent sayıdır.

Teorem 1.4.10 ve Teorem 1.4.15 yardımıyla aşağıdaki sonuç elde edilir

Sonuç 1.4.21. k tamsayı ve $k>1$ olsun. Bu takdirde, her $n\in\mathbb{N}$ için $\dfrac{\left(k^2-1\right)V_n\left(2k,-1\right)}{2}$ bir kongruent sayıdır.

Sonuç 1.4.22. $k\geq 1$ tek tamsayı olsun. Bu takdirde, her $n\in\mathbb{N}$ için $\left(k^2+4\right)V_{6n-3}\left(k,1\right)$ bir kongruent sayıdır.

İspat. $k\geq 1$ tek tamsayı ve $d=k^2+4$ olsun. Teorem 1.4.3 gereği $x^2-dy^2=-1$ Pell denkleminin tüm pozitif tamsayı çözümleri $n\geq 1$ olmak üzere $(x,y)=\left(\dfrac{V_{6n-3}\left(k,1\right)}{2},\dfrac{U_{6n-3}\left(k,1\right)}{2}\right)$ biçimindedir. Teorem 1.4.14 gereği $\left(k^2+4\right)V_{6n-3}\left(k,1\right)$ bir kongruent sayıdır.

Teorem 1.4.9 ve Teorem 1.4.14 kullanılarak aşağıdaki sonuç elde edilir.

Sonuç 1.4.23. $k\geq 1$ tamsayı olsun. Bu takdirde, her $n\in\mathbb{N}$ için $\left(k^2+1\right)V_{2n-1}\left(2k,1\right)$ bir kongruent sayıdır.

Sonuç 1.4.24. $k \geq 1$ tamsayı olsun. Bu takdirde, her $n \in \mathbb{N}$ için $2\left(k^2+4\right)V_{2n}(k,1)$ bir kongruent sayıdır.

İspat. $k \geq 1$ tamsayı ve $d = k^2+4$ olsun. Teorem 1.4.5 gereği $x^2 - dy^2 = 4$ Pell denkleminin tüm pozitif tamsayı çözümleri $n \geq 1$ olmak üzere $(x,y) = \left(V_{2n}(k,1), U_{2n}(k,1)\right)$ biçimindedir. O halde Teorem 1.4.16 gereği $2\left(k^2+4\right)V_{2n}(k,1)$ bir kongruent sayıdır.

Yukarıdaki sonuçta $k=1$ alınırsa aşağıdaki sonuç elde edilir.

Sonuç 1.4.25. Her $n \in \mathbb{N}$ için $10L_{2n}$ kongruent sayıdır.

Örnek 1.4.26. Sonuç 1.4.25 te, $n=1$ için $10L_2 = 30$, $n=2$ için $10L_4 = 70$, $n=3$ için $10L_6 = 180$ ve $n=4$ için $10L_8 = 470$ olup, bu sayıların kongruent sayı olduğu Ek' te verilen tablodan kontrol edilebilir.

Teorem 1.4.7 ve Teorem 1.4.16 kullanılarak aşağıdaki sonuç elde edilir.

Sonuç 1.4.27. $k > 3$ tamsayı olsun. Bu takdirde her $n \in \mathbb{N}$ için $2\left(k^2-4\right)V_n(k,-1)$ bir kongruent sayıdır.

Sonuç 1.4.28. Her $n \in \mathbb{N}$ için $V_n(6,-1)$ bir kongruent sayıdır.

İspat. Sonuç 1.4.27 de $k=6$ alınırsa, $2\cdot\left(32V_n(k,-1)\right) = 64V_n(6,-1)$ kongruent sayıdır. Lemma 1.2.6 gereği $V_n(6,-1)$ kongruent sayıdır.

Örnek 1.4.29. Sonuç 1.4.28 de, $n=1$ için $V_1(6,-1)=6$, $n=2$ için $V_2(6,-1)=34$, $n=3$ için $V_3(6,-1)=84$, $n=4$ için $V_4(6,-1)=470$ ve $n=5$ için $V_5(6,-1)=856$ olur. Ek' teki tablodan bakıldığında 6, 34, 84, 470 ve 856 sayıları birer kongruent sayıdır.

Teorem 1.4.8 ve Teorem 1.4.15 yardımıyla aşağıdaki sonuç elde edilir.

Sonuç 1.4.30. k, $k\geq 1$ ve $k\neq 2$ olacak biçimde bir tamsayı olsun. Bu takdirde her $n\in\mathbb{N}$ için $2\left(k^2+1\right)V_{2n}(2k,1)$ kongruent sayıdır.

Teorem 1.4.10 ve Teorem 1.4.15 kullanılarak aşağıdaki sonuç elde edilir.

Sonuç 1.4.31. $k>1$ tamsayı olsun. Bu takdirde her $n\in\mathbb{N}$ için $\left(k^2-1\right)\dfrac{V_n(2k,-1)}{2}$ bir kongruent sayıdır.

Sonuç 1.4.32. $k\geq 1$ tamsayı olsun. Bu takdirde her $n\in\mathbb{N}$ için $\left(k^2+4\right)V_{2n-1}(k,1)$ kongruent sayıdır.

İspat. $k\geq 1$ tamsayı ve $d=k^2+4$ olsun. Teorem 1.4.6 gereği $x^2-dy^2=-4$ Pell denkleminin tüm pozitif tamsayı çözümleri $(x,y)=\left(V_{2n-1}(k,1),U_{2n-1}(k,1)\right)$ biçimindedir. Teorem 1.4.17 gereği her $n\geq 1$ için $\left(k^2+4\right)V_{2n-1}(k,1)$ bir kongruent sayıdır.

Sonuç 1.4.33. Her $n>1$ için $5L_{2n-1}$ bir kongruent sayıdır.

İspat. Sonuç 1.4.32 de $k=1$ alınırsa, $5V_{2n-1}(1,1)$ sayısının kongruent sayı olduğu görülür. $5V_{2n-1}(1,1)=5L_{2n-1}$ olduğundan $5L_{2n-1}$ kongruent sayıdır.

Örnek 1.4.34. Sonuç 1.4.32 de, $n=2$ için $5L_3=20$, $n=3$ için $5L_5=55$, $n=4$ için $5L_7=145$, $n=5$ için $5L_9=380$ ve $n=6$ için $5L_{11}=995$ olup, bu sayıların kongruent sayı olduğu Ek' te verilen tablodan kontrol edilebilir.

Sonuç 1.4.35. $n\in\mathbb{N}$ olmak üzere $k=1$ ise $n\geq 2$ için $2V_{2n-1}(2,1)$ ve $k>2$ ise $n\geq 1$ için $\left(k^2+1\right)V_{2n-1}(2k,1)$ bir kongruent sayıdır.

İspat. k, $k\geq 1$ ve $k\neq 2$ olacak biçimde bir tamsayı ve $d=k^2+1$ olsun. Bu takdirde Teorem 1.4.11 gereği $x^2-dy^2=-4$ Pell denkleminin tüm pozitif tamsayı çözümleri $n\geq 1$ olmak üzere $(x,y)=\left(V_{2n-1}(2k,1),2U_{2n-1}(2k,1)\right)$ biçimindedir. O halde Teorem1.4.17 gereği $k=1$ ise $n\geq 2$ için $2V_{2n-1}(2,1)$ ve $k>2$ ise $n\geq 1$ için $\left(k^2+1\right)V_{2n-1}(2k,1)$ bir kongruent sayıdır.

Sonuç 1.4.36. Her $n\geq 2$ için $\frac{Q_{2n-1}}{2}$ bir kongruent sayıdır.

İspat. Sonuç 1.4.35 te $k=1$ alınırsa $2V_{2n-1}(2,1)=2Q_{2n-1}$ in bir kongruent sayı olduğu görülür. $Q_{2n-1}=2t$, $t\in\mathbb{Z}$ denirse t kongruent sayıdır. Yani $\frac{Q_{2n-1}}{2}$ kongruent sayıdır.

Örnek 1.4.37. Yukarıdaki sonuçta, $n=2$ alınırsa $\frac{Q_3}{2}=\frac{14}{2}=7$, $n=3$ alınırsa $\frac{Q_5}{2}=\frac{82}{2}=41$ ve $n=4$ alınırsa $\frac{Q_7}{2}=\frac{478}{2}=239$ elde edilir. Ek' teki tablodan $7, 41$ ve 239 sayılarının birer kongruent sayı olduğu görülür

BÖLÜM 2. ELİPTİK EĞRİLER

2.1. Eliptik Eğriler

Bu bölümde $a,b \in \mathbb{Z}$ ve $x^3+ax+b=0$ kübik denkleminin kökleri farklı olmak üzere, $y^2=x^3+ax+b$ biçimindeki eliptik eğriler ele alınacaktır. Eliptik eğrilerle ilgili detaylı bilgi için [16], [17], [18], [19], [20] kaynaklarına bakılabilir.

Tanım 2.1.1. $E: y^2=x^3+ax+b$ bir eliptik eğri olsun. E üzerindeki rasyonel noktaların kümesi $E(\mathbb{Q})$ ile gösterilir ve

$$E(\mathbb{Q})=\{\infty\}\cup\left\{(x,y)\in\mathbb{Q}\times\mathbb{Q}\,\middle|\, y^2=x^3+ax+b\right\}$$

olarak tanımlanır.

Tanım 2.1.2. $a,b \in \mathbb{Z}$ olmak üzere $\mathbb{Q}$ da bir $f(x)=x^3+ax+b$ kübik polinomu olsun. $x^3+ax+b=0$ kübik denkleminin kökleri α,β,γ olmak üzere, bu kübik denklemin diskriminantı

$$\Delta=(\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2 \tag{2.1}$$

olarak tanımlanır.

$\Delta = -(4a^3 + 27b^2)$ olduğu kolaylıkla gösterilebilir. Gerçekten,

$$x^3 + ax + b = (x-\alpha)(x-\beta)(x-\gamma)$$

olduğundan,

$$\alpha + \beta + \gamma = 0 \qquad (2.2)$$

$$\alpha \cdot \beta \cdot \gamma = -b \qquad (2.3)$$

$$\alpha \cdot \beta + \beta \cdot \gamma + \alpha \cdot \gamma = a \qquad (2.4)$$

yazılabilir. (2.2), (2.3) ve (2.4) eşitlikleri (2.1) eşitliğinde yerlerine yazılırsa,

$$(\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2 = -(4a^3 + 27b^2)$$

elde edilir.

$\Delta = 0$ ise kübik polinomun katlı kökü vardır. Bu durumda $E: y^2 = x^3 + ax + b$ eğrisi bir eliptik eğri belirtmez.

$\Delta \neq 0$ ise kübik polinomun katlı kökü yoktur. Bu durumda $E: y^2 = x^3 + ax + b$ eğrisi bir eliptik eğri belirtir.

Örnekler 2.1.3.

i) $y^2 = x^3$ eğrisi bir eliptik eğri belirtmez. Çünkü $f(x) = x^3$ polinomunda $\Delta = 0$ olup $x = 0$ bir katlı köktür.

ii) $y^2 = x^3 + x^2$ eğrisi bir eliptik eğri değildir. Çünkü $f(x) = x^3 + x^2$ polinomunda $\Delta = 0$ olup $x = 0$ katlı köktür.

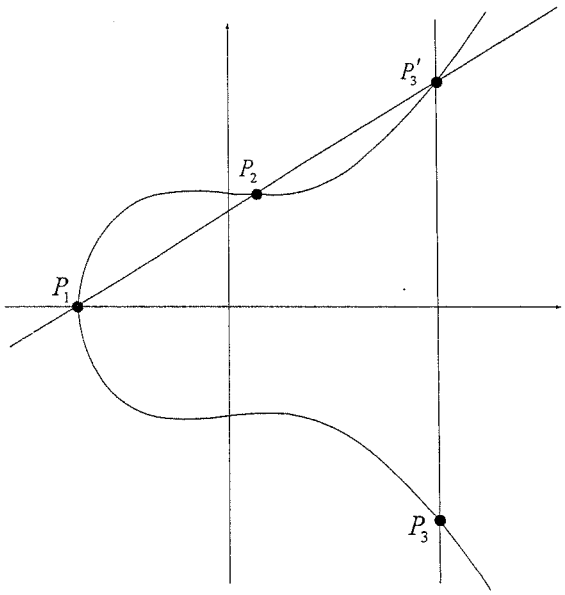
iii) $y^2 = x^3 - x$ eğrisi bir eliptik eğridir. Çünkü, $f(x) = x^3 - x$ polinomunda $\Delta = -4$ tür.

iv) $y^2 = x^3 - 3x + 3$ eğrisi bir eliptik eğridir. Çünkü $f(x) = x^3 - 3x + 3$ polinomunda $\Delta = -135$ tir.

v) $y^2 = x^3 + x$ eğrisi bir eliptik eğridir. Çünkü, $f(x) = x^3 + x$ polinomunda $\Delta = -4$ tür.

2.2. Eliptik Eğrilerde Toplama İşlemi

$E: y^2 = x^3 + ax + b$ bir eliptik eğri olsun. Bu eğri üzerinde $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ iki nokta olsun.



Şekil 2.1. Eliptik Eğrilerde Toplama İşlemi

P_1 ve P_2 noktalarından geçen ℓ doğrusu E eliptik eğrisini üçüncü bir P_3' noktasında keser. $P_1 + P_2 = P_3$ olarak tanımlanan P_3 noktası, P_3' noktasının x eksenine göre simetriğinin alınmasıyla bulunur.

İlk olarak $P_1 \neq P_2$ ve $P_1, P_2 \neq \infty$ olsun. P_1 ve P_2 noktalarından geçen doğru ℓ olsun.

ℓ nin eğimi $m = \dfrac{y_2 - y_1}{x_2 - x_1}$ dir.

Eğer $x_1 \neq x_2$ ise ℓ doğrusunun denklemi $y = m(x - x_1) + y_1$ dir. ℓ doğrusunun E eliptik eğrisi ile kesişimini bulmak için $y = m(x - x_1) + y_1$ ifadesi, $y^2 = x^3 + ax + b$ denkleminde yerine yazılır. Buradan, $(m(x - x_1) + y_1)^2 = x^3 + ax + b$ olduğundan $x^3 - m^2x^2 + (-2m^2x_1 - 2my_1 + a)x + (-x_1{}^2m^2 + 2mx_1y_1 - y_1{}^2 + b) = 0$ elde edilir. Bu kübik polinomun kökleri, ℓ ile E nin kesişim noktalarıdır. Bu köklerden ikisinin x_1 ve x_2 olduğu biliniyor. O halde üçüncü dereceden denklemin kökler toplamından $x_1 + x_2 + x_3 = m^2$ bulunur. Şu halde $x = x_3 = m^2 - x_1 - x_2$ dir. Bu x değeri doğru denkleminde yerine yazılarak $y = m(x - x_1) + y_1$ bulunur. Şimdi (x, y) noktasının x ekseninine göre simetrisi alınıp P_3 elde edilir. Böylece $x_3 = m^2 - x_1 - x_2$, $y_3 = m(x - x_1) - y_1$ elde edilir. Dolayısıyla,

$$P_1 + P_2 = P_3 = (m^2 - x_1 - x_2, m(x - x_1) - y_1)$$

dir.

$x_1 = x_2$ ve $y_1 \neq y_2$ durumu düşünüldüğünde P_1 ve P_2 noktalarından geçen doğru x eksenine dik doğrudur. Bu durumda

$$P_1 + P_2 = \infty$$

olarak tanımlanır.

Şimdi de $P_1 = P_2$ durumunu ele alalım. P_1 ve P_2 den geçen doğru, eğriye bu noktada teğet olan doğrudur. ℓ doğrusunun eğimi $2y\frac{dy}{dx} = 3x^2 + a$, yani $m = \frac{3x_1{}^2 + a}{2y_1}$ dir.

Eğer $y_1 = 0$ ise, bu noktadan geçen doğru x eksenine diktir. Bu durumda,

$$P_1 + P_2 = \infty$$

olarak tanımlanır.

$y_1 \neq 0$ olduğunu kabul edelim. ℓ doğrusunun denklemi $y = m(x - x_1) + y_1$ dir. Buradan ℓ doğrusu ile E eliptik eğrisinin kesişiminden $x^3 - m^2x^2 + (-2m^2x_1 - 2my_1 + a)x + (-x_1{}^2m^2 + 2mx_1y_1 - y_1{}^2 + b) = 0$ kübik denklemi elde edilir. Şu halde sadece x_1 kökü biliniyor. Fakat ℓ doğrusu E eliptik eğrisine P_1 noktasında teğet olduğundan x_1 çift katlı köktür. Önceki işlemler yapıldığında $x = m^2 - 2x_1$ ve $y = m(x - x_1) + y_1$ bulunur. Bu (x, y) noktasının x eksenine göre simetriği alınarak

$$P_1 + P_2 = (x_3, y_3) = (m^2 - 2x_1, m(x_1 - x_3) - y_1)$$

olarak bulunur.

Eğer $P_2 = \infty$ ise,

$$P_1 + P_2 = P_1 + \infty = P_1$$

olarak tanımlanır.

Ayrıca $\infty + \infty = \infty$ olarak tanımlanır.

Yukarıdaki bilgiler özetlenirse aşağıdaki yazılabilir.

$E: y^2 = x^3 + ax + b$ biçiminde bir eliptik eğri olsun. $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ noktaları E de ∞ dan farklı noktalar olsun. $P_1 + P_2 = P_3 = (x_3, y_3)$ aşağıdaki gibidir.

i) $x_1 \neq x_2$ ise $x_3 = m^2 - x_1 - x_2$, $y_3 = m(x - x_1) - y_1$ dir. Burada $m = \dfrac{y_2 - y_1}{x_2 - x_1}$ dir.

ii) $x_1 = x_2$ ve $y_1 \neq y_2$ ise $P_1 + P_2 = \infty$ dur.

iii) $P_1 = P_2$ ve $y_1 \neq 0$ ise $x_3 = m^2 - 2x_1$, $y_3 = m(x_1 - x_3) - y_1$ dir. Burada $m = \dfrac{3x_1{}^2 + a}{2y_1}$ dir.

iv) $P_1 = P_2$ ve $y_1 = 0$ ise $P_1 + P_2 = \infty$ dur.

Ayrıca eğri üzerindeki her P noktası için $P+\infty=P$ dir.

Örnek 2.2.1. $E: y^2=x^3+2$ eğrisi üzerinde $P=(-1,1)$ noktasının kendisi ile toplamını bulalım.

$2yy'=3x^2 \Rightarrow m=y'_{(-1,1)}=\frac{3}{2}$ ve böylece $P=(-1,1)$ noktasından geçen teğet doğrunun denklemi $(y-1)=\frac{3}{2}(x+1) \Rightarrow y=\frac{3x+5}{2}$ biçimindedir.

Doğru ile eğrinin kesişiminden $\left(\frac{3x+5}{2}\right)^2=x^3+2$ ise $x^3-\frac{9}{4}x^2-\frac{15}{2}x-\frac{13}{4}=0$ elde edilir. Bu eşitliğin iki kökü $x_1=x_2=-1$ olduğundan $(-1)+(-1)+x=\frac{9}{4} \Rightarrow x=\frac{17}{4}$ ve böylece $y=\frac{71}{8}$ olarak bulunur. Sonuç olarak $P'=\left(\frac{17}{4},\frac{71}{8}\right)$ ve bu noktanın x eksenine göre simetriği alınarak $P+P=2P=\left(\frac{17}{4},-\frac{71}{8}\right)$ bulunur.

Örnek 2.2.2. $E: y^2=x^3-2x$ eğrisi üzerindeki $P_1=(0,0)$ ve $P_2=(-1,1)$ noktalarının toplamını bulalım.

P_1 ve P_2 noktalarından geçen ℓ doğrusunun denklemi $y=-x$ doğrusudur. Bu doğru ile eğrinin kesişiminden $x^3-x^2-2x=0$ elde edilir. Bu eşitliğin iki kökü $x_1=0$, $x_2=-1$ dir. O hâlde $0-1+x=1$ eşitliğinden üçüncü kök $x=2$ ve böylece $y=2$ olarak bulunur. Sonuç olarak $P_3'=(2,-2)$ ve bu noktanın x eksenine göre simetriği alınarak $P_3=P_1+P_2=(2,2)$ noktası bulunur.

Siegel 1929 da E eliptik eğrisi üzerindeki tamsayı bileşenli noktalar için aşağıdaki teoremi ispatlamıştır.

Teorem 2.2.3. $a,b\in\mathbb{Z}$ olmak üzere $\mathbb{Q}$ üzerindeki E eliptik eğrisi $y^2=x^3+ax+b$ olsun. O zaman E sonlu tane tamsayı bileşenli noktaya sahiptir [20].

Eliptik eğriler teorisini bu kadar zengin yapan yönlerinden biri de $E(\mathbb{Q})$ üzerinde bir grup yapısı kurulabilir olmasıdır.

$a,b \in \mathbb{Q}$ olmak üzere P_1 ve P_2 nin bileşenleri $\mathbb{Q}$ cisminden alınırsa P_1+P_2 nin bileşenleri de $\mathbb{Q}$ da olur. Böylece $E(\mathbb{Q})$ yukarıdaki toplama işlemi altında kapalıdır.

Teorem 2.2.4. E, $\mathbb{Q}$ üzerinde tanımlı bir eliptik eğri olsun. Bu durumda E eliptik eğrisi üzerindeki toplama işlemi aşağıdaki özellikleri sağlar [21].

i) Her $P_1,P_2 \in E(\mathbb{Q})$ için $P_1+P_2=P_2+P_1$ dir.

ii) Her $P \in E(\mathbb{Q})$ için $P+\infty=P$ dir.

iii) $P \in E(\mathbb{Q})$ ise $P+P'=\infty$ olacak biçimde $P' \in E(\mathbb{Q})$ vardır. Bu P' noktası $-P$ olarak gösterilecektir ve $-P=(x,-y)$ dir.

iv) $P_1,P_2,P_3 \in E(\mathbb{Q})$ olmak üzere $(P_1+P_2)+P_3=P_1+(P_2+P_3)$ dir.

Diğer bir deyişle E eliptik eğrisi üzerindeki noktalar toplama işlemine göre bir değişmeli grup oluşturur. Burada ∞ grubun birim elemanıdır.

Ayrıca ℓ doğrusu E eliptik eğrisini P_1, P_2, P_3 noktalarında kessin. Bu durumda $(P_1+P_2)+P_3=\infty$ dır.

$E(\mathbb{Q})$ nun grup yapısıyla ilgili daha sonra 1908 de Jules Poincare tarafından tahmin edilen ve 1922 de Luis Mordell tarafından ispat edilen bir çalışma yapılmıştır. Ayrıca bu 1928 de André Weil tarafından genelleştirilmiştir.

Teorem 2.2.5. (Mordell-Weil) $E(\mathbb{Q})$ sonlu üreteçli değişmeli bir gruptur [20].

E deki sonlu mertebeli noktaların, yani torsiyon noktalarının oluşturduğu grup $E(\mathbb{Q})_{tor}=\{P \in E(\mathbb{Q}) : nP=\infty,\ n \in \mathbb{N}\}$ ile gösterilir. Mordell-Weil teoremi ve sonlu üreteçli değişmeli grupların genel yapısından $E(\mathbb{Q}) \cong E(\mathbb{Q})_{tor} \oplus \mathbb{Z}^{R_E}$ yazılır. Yani $E(\mathbb{Q})$ iki değişmeli grubun direkt toplamına izomorftur. Burada ikinci toplam,

$R_E > 0$ için R_E tane $\mathbb{Z}$ den oluşur. Bu ise $E(\mathbb{Q})$ nun sonsuz mertebeli R_E tane üreteci olduğunu belirtir. Bu R_E sayısına E eliptik eğrisinin rankı denir.

2.3. Torsiyon Alt Grubu

Bu bölümde bir eliptik eğrinin torsiyon alt grubu

$$E(\mathbb{Q})_{tor} = \{P \in E(\mathbb{Q}) : nP = \infty,\ n \in \mathbb{N}\}$$

hakkında, literatürden iyi bilinen teoremler verilecektir.

Teorem 2.3.1. (Mazur) $E : y^2 = x^3 + ax + b$ bir eliptik eğri olsun. Bu durumda $E(\mathbb{Q})_{tor}$ aşağıdakilerden birine izomorftur.

$$\mathbb{Z}/n\mathbb{Z} \qquad ; 1 \le n \le 10 \text{ veya } n = 12$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z} \qquad ; 1 \le m \le 4$$

[20].

Yukarıdaki teoremden, $E(\mathbb{Q})$ nun sonlu mertebeli noktalarının mertebelerinin en fazla 12 olacağı söylenebilir. Mazur teoremi, verilen bir eliptik eğrinin torsiyon alt grubunu hesaplarken çok kullanışlı değildir. E. Lutz ve T. Nagell tarafından ispatlanan aşağıdaki teorem $E(\mathbb{Q})_{tor}$ kümesini belirlemek için daha kullanışlıdır.

Teorem 2.3.2. (Nagell-Lutz) $a,b \in \mathbb{Z}$ olmak üzere $E: y^2 = x^3 + ax + b$ biçiminde bir eliptik eğri olsun. O zaman $E(\mathbb{Q})_{tor}$ da alınan her $P = (x(P), y(P)) \neq \infty$ noktası için aşağıdakiler doğrudur.

i) P nin bileşenleri tamsayıdır, yani $x(P), y(P) \in \mathbb{Z}$,

ii) Eğer P nin mertebesi $n \geq 3$ ise $y(P)^2 \mid 4a^3 + 27b^2$,

iii) Eğer P nin mertebesi 2 ise $y(P) = 0$ ve $x(P)^3 + ax(P) + b = 0$

dir [20].

Teorem 2.3.3. $E_n : y^2 = x^3 - n^2 x = x(x-n)(x+n)$ eliptik eğrisi için

$E_n(\mathbb{Q})_{tor} = \{\infty, (0,0), (n,0), (-n,0)\} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

dır ([4], [18]).

Örnek 2.3.4. $E: y^2 = x^3 - 2$ olsun. $y = 0$ için $x^3 - 2 = 0$ polinomunun rasyonel kökü yoktur. Böylece $E(\mathbb{Q})$ nun mertebesi 2 olan noktası yoktur. Ayrıca $4a^3 + 27b^2 = 27 \times 4$ olup $(x(P), y(P))$, $E(\mathbb{Q})$ da torsiyon noktası ise $y(P)$ tamsayıdır ve $y(P)^2 \mid 27 \times 4$ dir. Bu ise $y(P) = \pm 1, \pm 2, \pm 3$ veya ± 6 olmasını gerektirir. Buradan, sırasıyla $x(P)^3 = 3, 6, 11$ veya 38 bulunur. Fakat $x(P)$ tamsayıdır ve 3,6,11 veya 38 sayılarından hiç biri tam küp değildir. Böylece $E(\mathbb{Q})_{tor} = \{\infty\}$ dur [20].

Örnek 2.3.5. $p \geq 2$ asal sayı ve $E_p : y^2 = x^3 + p^2$ bir eliptik eğri olsun. $y = 0$ için $x^3 + p^2 = 0$ polinomunun rasyonel kökü yoktur. Böylece $E_p(\mathbb{Q})$ nun, mertebesi 2 olan elemanı yoktur. P, $E_p(\mathbb{Q})$ da bir torsiyon noktası olsun. $P = (x(P), y(P))$ ise $y(P)^2 \mid 27p^4$ olup buradan mümkün olan y değerleri $y = \pm 1, \pm p, \pm p^2, \pm 3p, \pm 3p^2$ ve ± 3 tür. $(0, \pm p) \in E_p(\mathbb{Q})$ ve ∞ noktasının torsiyon noktası olduğu kolaylıkla gösterilebilir. Böylece $p \geq 2$ asalı için $E_p(\mathbb{Q})$ nun torsiyon alt grubu $\mathbb{Z}/3\mathbb{Z}$ ye izomorftur [20].

Örnek 2.3.6. $E: y^2 = x^3 + 1$ eliptik eğrisinin sonlu mertebeli 6 noktası vardır. $\Delta = -27$ dir. $P = (x, y)$ sonlu mertebeli olsun. Bu takdirde x ve y tamsayıdır ve $y = 0$ veya $y \neq 0$ ise $y^2 \mid \Delta$ dır. Eğer $y = 0$ ise $x^3 = -1$ yani $x = -1$ dir. $(-1, 0)$ mertebesi 2 olan bir noktadır. Eğer $y \neq 0$ ise $y^2 \mid -27$ dir. Buradan $y = \pm 1, \pm 3$ olur. $y = \pm 1$ ise $x^3 = 0$, yani $x = 0$ olur. Buradan mertebesi sonlu olan $(0, \pm 1)$ noktası elde edilir. Benzer biçimde $y = \pm 3$ iken sonlu mertebeli noktaların $(2, \pm 3)$ olduğu kolaylıkla görülür. Diğer yandan,

$2(2,3) = (0,1)$,

$3(2,3) = (0,1) + (2,3) = (-1,0)$,

$4(2,3) = (-1,0) + (2,3) = (0,-1)$,

$5(2,3) = (0,-1) + (2,3) = (2,-3)$,

$6(2,3) = (2,-3) + (2,3) = \infty$

olur. Böylece bu eliptik eğrinin üreteci $P = (2,3)$ noktasıdır ve bu noktanın mertebesi 6 dır. Dolayısıyla $E(\mathbb{Q})_{tor} \simeq \mathbb{Z}/6\mathbb{Z}$ dir [22].

Örnek 2.3.8 ve Örnek 2.3.9 un çözümünde aşağıdaki lemmaya ihtiyaç vardır.

Lemma 2.3.7. $E: y^2 = x^3 + ax + b$ ve $P = (x, y)$ bu eğri üzerinde bir nokta olsun. Bu takdirde $x = \frac{m}{e^2}, y = \frac{n}{e^3}$ ve $(m, e) = (n, e) = 1$ olacak biçimde $m, n \in \mathbb{Z}$ vardır [27].

İspat. $m, n, M, N \in \mathbb{Z}$ ve $(M, m) = (N, n) = 1$ olmak üzere $x = \frac{m}{M}, y = \frac{n}{N}$ olsun. $y^2 = x^3 + ax + b$ eşitliğinde $x = \frac{m}{M}$, $y = \frac{n}{N}$ yazılırsa $\frac{n^2}{N^2} = \frac{m^3}{M^3} + a\frac{m}{M} + b$, yani

$$M^3 n^2 = N^2 m^3 + aN^2 M^2 m + bN^2 M^3 \qquad (2.5)$$

elde edilir. $M^3n^2 = N^2\left(m^3 + aM^2m + bM^3\right)$ olduğundan $N^2 \mid M^3n^2$ dir. $(N,n)=1$ olduğundan

$$N^2 \mid M^3 \tag{2.6}$$

dir.

Diğer yandan $M \mid N^2m^3$ ve $(M,m)=1$ olduğundan $M \mid N^2$ elde edilir. O halde $N^2 = Mk$ olacak şekilde $k \in \mathbb{Z}$ vardır. $N^2 = Mk$ değeri (2.5) te yerine yazılırsa $M^3 \mid N^2m^3$ olduğu kolaylıkla elde edilir. $(M,m)=1$ olduğundan,

$$M^3 \mid N^2 \tag{2.7}$$

olur. Böylece (2.6) ve (2.7) den $N^2 = M^3$ elde edilir. Dolayısıyla $M = e^2$, $N = e^3$ olacak biçimde $e \in \mathbb{N}$ vardır.

Örnek 2.3.8. $E: y^2 = x^3 + x$ eliptik eğrisinin tek tamsayı bileşenli noktası $(0,0)$ dır. $y^2 = x^3 + x$ olan $x, y \in \mathbb{Z}$ mevcut olsun. Lemma 2.3.7 ye göre $(m,e)=(n,e)=1$ olmak üzere $x = \frac{m}{e^2}, y = \frac{n}{e^3}$ olarak yazılabilir. Bu değerler eğri denkleminde yazılırsa,

$$\left(\frac{n}{e^3}\right)^2 = \left(\frac{m}{e^2}\right)^3 + \left(\frac{m}{e^2}\right) \Rightarrow \frac{n^2}{e^6} = \frac{m^3}{e^6} + \frac{m}{e^2} \Rightarrow n^2 = m^3 + me^4 = m\left(m^2 + e^4\right)$$

elde edilir. $\left(m, m^2 + e^4\right)=1$ olduğundan $m = a^2$ ve $m^2 + e^4 = b^2$ olacak biçimde $a, b \in \mathbb{Z}$ vardır. Buradan $a^4 + e^4 = \left(a^2\right)^2 + e^4 = m^2 + e^4 = b^2$ elde edilir. Teorem 1.2.10 a göre, bu denklemin $a>0$, $e>0$, $b>0$ olacak biçimde çözümü olmadığı biliniyor. O halde $y^2 = x^3 + x$ eliptik eğrisinin sıfırdan farklı $x, y \in \mathbb{Z}$ çözümleri yoktur. Sonuç olarak, bu eğrinin tamsayı bileşenli noktası sadece $(0,0)$ noktasıdır. Böylece $E(\mathbb{Q})_{tor} = \{\infty, (0,0)\} \simeq \mathbb{Z}/2\mathbb{Z}$ dir.

Örnek 2.3.9. $E: y^2 = x^3 - x$ eliptik eğrisinin tamsayı bileşenli noktaları $(0,0)$, $(1,0)$, $(-1,0)$ noktalarıdır.

Lemma 2.3.7 ye göre $x = \frac{m}{e^2}, y = \frac{n}{e^3}$, $(m,e) = (n,e) = 1$ olacak biçimde $e \in \mathbb{Z}^+$ ve $m,n \in \mathbb{Z}$ olduğu biliniyor. Bu değerler eğri denkleminde yazılırsa,

$$\left(\frac{n}{e^3}\right)^2 = \left(\frac{m}{e^2}\right)^3 - \left(\frac{m}{e^2}\right) \Rightarrow \frac{n^2}{e^6} = \frac{m^3}{e^6} - \frac{m}{e^2} \Rightarrow n^2 = m^3 - me^4 = m\left(m^2 - e^4\right)$$

elde edilir. $\left(m, m^2 - e^4\right) = 1$ olduğundan $m = a^2$ ve $m^2 - e^4 = b^2$ olacak biçimde $a,b \in \mathbb{Z}^+$ vardır. Buradan $a^4 - e^4 = \left(a^2\right)^2 - e^4 = m^2 - e^4 = b^2$ elde edilir. Teorem 1.2.11 e göre, bu denklemin $a > 0$, $e > 0$, $b > 0$ olacak biçimde tamsayı çözümü olmadığı biliniyor. O halde $e > 0$ olduğundan $a = 0$ veya $b = 0$ olmalıdır. Buradan $y = 0$ veya $x = 0$ elde edilir. Sonuç olarak, bu eğrinin tamsayı çözümleri $(0,0)$, $(1,0)$, $(-1,0)$ noktalarıdır. İkinci bileşeni sıfır olan noktalar torsiyon nokta olduğundan $E(\mathbb{Q})_{tor} = \{\infty, (0,0), (1,0), (-1,0)\} = \mathbb{Z}/4\mathbb{Z}$ dir.

Teorem 2.3.10. $E: y^2 = x^3 + ax$ bir eliptik eğri ve $a \in \mathbb{Z}$ olsun. Bu takdirde,

$$E(\mathbb{Q})_{tor} \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & , -a \text{ tam kare ise} \\ \mathbb{Z}/4\mathbb{Z} & , a = 4 \text{ ise} \\ \mathbb{Z}/2\mathbb{Z} & , \text{diğer durumlarda} \end{cases}$$

dir [18].

Teorem 2.3.11. $b \in \mathbb{Z}$ olmak üzere $E: y^2 = x^3 + b$ olsun. Bu takdirde,

$$E(\mathbb{Q})_{tor} \simeq \begin{cases} \mathbb{Z}/6\mathbb{Z} & , b = 1 \text{ ise} \\ \mathbb{Z}/3\mathbb{Z} & , b = -432 \text{ veya } b \neq 1 \text{ ve } b = x^2, x \in \mathbb{Z} \text{ ise} \\ \mathbb{Z}/2\mathbb{Z} & , b = x^3, x \in \mathbb{Z} \text{ ve } b \neq 1 \text{ ise} \\ 0 & , \text{diğer durumlarda} \end{cases}$$

dir [18].

2.4. Serbest Kısım ve Rank

$E(\mathbb{Q}) \simeq E(\mathbb{Q})_{tor} \oplus \mathbb{Z}^{R_E}$ olduğu daha önce ifade edildi. Bu bölümde direkt toplamın ikinci yani serbest kısmıyla ilgilenilecektir. Bu grup $E(\mathbb{Q})$ nun sonsuz mertebeli R_E tane noktasından üretilir. R_E için herhangi bir üst sınırın olup olmadığı bilinmiyor. Bilinen en büyük rank 28 dir.

Aşağıda eliptik eğriler ve onların grup yapısıyla ilgili bazı örnekler vardır.

Örnek 2.4.1. $E: y^2 = x^3 + 6$ eliptik eğrisinin ∞ dan başka rasyonel noktası yoktur. Dolayısıyla $E(\mathbb{Q}) = \{\infty\}$ ve $R_E = 0$ dır [20].

Örnek 2.4.2. $E: y^2 = x^3 - 2$ eliptik eğrisinin ∞ dan başka torsiyon noktası yoktur. Fakat $P = (3,5)$ bir rasyonel noktadır. Böylece P sonsuz mertebeli nokta olmak zorundadır. $E(\mathbb{Q})$ nun sonsuz çoklukta farklı rasyonel noktaları vardır. Sonuç olarak E eliptik eğrisinin rankı 1 dir ve P, $E(\mathbb{Q})$ nun üretecidir. Yani $E(\mathbb{Q}) = \{nP : n \in \mathbb{Z}\}$ ve $E(\mathbb{Q}) \simeq \mathbb{Z}$ dir [20].

Teorem 2.4.3. p tek asal sayı ve $E: y^2 = x^3 - p^2 x$ bir eliptik eğri olsun. Bu takdirde $E(\mathbb{Q})$ nun rankı için aşağıdakiler doğrudur:

i) $p \equiv 1 \pmod 8$ ise $R_E \leq 2$,

ii) $p \equiv 3 \pmod 8$ ise $R_E = 0$,

iii) $p \equiv 5,7 \pmod 8$ ise $R_E \leq 1$

dir [18].

Teorem 2.4.4. p asal sayı olmak üzere $E: y^2 = x^3 + px$ olsun. Bu durumda $R_E \leq 2$ dir [22].

Önerme 2.4.5. p asal sayı, $p \equiv 7,11 \pmod{16}$ ve $E: y^2 = x^3 + px$ olsun. Bu durumda $R_E = 0$ dır [22].

Önerme 2.4.6. p asal sayı, $p \equiv 3,5,13,15 \pmod{16}$ ve $E: y^2 = x^3 + px$ olsun. Bu durumda, $R_E \leq 1$ dir [22].

Teorem 2.4.7. n pozitif karesiz bir tamsayı olsun. $E_n: y^2 = x^3 - n^2 x$ olsun. Bu takdirde n kongruent sayıdır $\Leftrightarrow$ $R_E \geq 1$ dir.

İspat.

$\Rightarrow$): n kongruent sayı olsun. O halde Lemma 1.2.7 gereği $y^2 = x^3 - n^2 x$ denkleminin aşikar çözümlerinden başka çözümü vardır. Ayrıca Teorem 2.3.3 gereği $E_n(\mathbb{Q})_{tor} = \{\infty, (0,0), (-n,0), (n,0)\}$ dir. Şu halde $y^2 = x^3 - n^2 x$ denkleminin aşikar çözümlerinden başka (x,y) çözümleri sonsuz mertebelidir. Dolayısıyla $E_n: y^2 = x^3 - n^2 x$ eliptik eğrisinin sonsuz mertebeli noktası vardır. Böylece $R_E \geq 1$ dir.

$\Leftarrow$): $R_E \geq 1$ olsun. O halde $E_n: y^2 = x^3 - n^2 x$ nin sonsuz mertebeli noktası vardır. Ayrıca Teorem 2.3.3 gereği E_n nin sonlu mertebeli noktaların kümesi

$\{\infty,(0,0),(-n,0),(n,0)\}$ dır. Böylece $y^2=x^3-n^2x$ denkleminin aşikar çözümlerinden başka rasyonel çözümü vardır. Lemma 1.2.7 gereği n kongruent sayıdır.

2.5. Birch ve Swinnerton-Dyer Konjektürü

p asal sayı olmak üzere $E: y^2=x^3+ax+b$ eliptik eğrisi $\mathbb{Z}_p$ de bir eğri olarak düşünülebilir. Bu durumda bu eğri üzerindeki noktaların sayısı

$$N_p=\left|\{(x,y)\in\mathbb{Z}_p\times\mathbb{Z}_p:\ y^2=x^3+ax+b(\bmod p)\}\right|$$

dir ve Frobenius endomorfizminin izi $a_p=p+1-N_p$ biçiminde tanımlanır.

Örnek 2.5.1. $\mathbb{Z}_3$ te, $y^2=x^3+x$ eliptik eğrisi için $N_p=3$ tür. $y^2=x^3+x(\bmod 3)$ şartını sağlayan elemanlar $(0,1)$, $(2,1)$, $(2,2)$ dir. O halde $N_p=3$ tür ve böylece $a_p=3+1-3=1$ dir [23].

Örnek 2.5.2. Eğer $p\equiv 2(\bmod 3)$ ise $\mathbb{Z}_p$ de $y^2=x^3+17$ eliptik eğrisi için $N_p=p$ dir [23].

Teorem 2.5.3. $y^2=x^3+x$ eliptik eğrisi için,

i) $p\equiv 3\ (\bmod 4)$ ise $N_p=p$ ve dolayısıyla $a_p=p+1-p=1$ dir.

ii) $p\equiv 1(\bmod 4)$ ve $p=a^2+b^2$, a tek, $a>0$, $b>0$ biçiminde ise,

$$N_p=\begin{cases}p+2a\ ; & a\equiv 3(\bmod 4)\\ p-2a\ ; & a\equiv 1(\bmod 4)\end{cases}$$

dir [23].

$E: y^2 = x^3 + ax + b$ eliptik eğrisi verilsin. $s \in \mathbb{C}$ ve $\mathrm{Re}(s) > \frac{3}{2}$ için $\Delta = -\left(4a^3 + 27b^2\right)$ olmak üzere $L(E,s) = \prod_{p \nmid \Delta} \left(1 - a_p p^{-s} + p^{1-2s}\right)^{-1}$ serisi yakınsaktır ve seri tüm kompleks düzleme analitik olarak genişletilebilir ([26], [32]).

Aşağıda vereceğimiz Birch ve Swinnerton-Dyer konjektürü sayılar teorisinin açık problemlerinden biridir. Bu konjektür Clay Mathematik Enstitüsü tarafından ödüllü problemlerden biri olarak gösterilmiştir ve ilk doğru ispat için 1 000 000 dolar ödül teklif edilmiştir.
Birch ve Swinnerton-Dyer Konjektürü konjektürü kısaca BSD konjektürü olarak anılacaktır.

Konjektür 2.5.4. (Birch ve Swinnerton-Dyer Konjektürü) $E: y^2 = x^3 + ax + b$ eliptik eğrisi verilsin.
$E(\mathbb{Q})$ sonsuz bir gruptur $\Leftrightarrow$ $L(E,s) = 0$ dır ([22], [24]).

Teorem 2.5.5. n karesiz pozitif tamsayı olsun. BSD konjektürü $C_n: y^2 = x^3 - n^2 x$ eliptik eğrisi için doğru olsun. Bu durumda, n tek tamsayı ve

$$\left|\left\{(x,y,z) \in \mathbb{Z}^3 : n = 2x^2 + y^2 + 32z^2\right\}\right| = \frac{1}{2}\left|\left\{(x,y,z) \in \mathbb{Z}^3 : n = 2x^2 + y^2 + 8z^2\right\}\right|$$

ise n kongruent sayıdır. n çift tamsayı ve

$$\left|\left\{(x,y,z) \in \mathbb{Z}^3 : \frac{n}{2} = 4x^2 + y^2 + 32z^2\right\}\right| = \frac{1}{2}\left|\left\{(x,y,z) \in \mathbb{Z}^3 : \frac{n}{2} = 4x^2 + y^2 + 8z^2\right\}\right|$$

ise n kongruent sayıdır [21].

$n \equiv 5,6,7 (\text{mod}\, 8)$ ise n nin kongruent sayı olduğu, $n < 1000000$ değerleri için doğrulanmıştır [25].

BSD konjektürü doğru ise aşağıdaki önerme verilebilir.

Önerme 2.5.6. n karesiz pozitif bir tamsayı olmak üzere $n \equiv 5,6,7 \ (\text{mod}\, 8)$ olsun. Ayrıca, BSD konjektürü $C_n : y^2 = x^3 - n^2 x$ eliptik eğrisi için doğru olsun. Bu durumda n bir kongruent sayıdır ([21], [26]).

İspat.

$x^2 \equiv 0,1,4 \ (\text{mod}\, 8)$, $y^2 \equiv 0,1,4 \ (\text{mod}\, 8)$ dir. $\mathbb{Z}/8\mathbb{Z}$ de çalışılırsa,

$$2x^2 + y^2 + 8z^2 = 2x^2 + y^2 + 32z^2 \equiv 0,1,2,3,4,6 \ (\text{mod}\, 8), \qquad \textbf{(2.8)}$$

$$4x^2 + y^2 + 8z^2 = 4x^2 + y^2 + 32z^2 \equiv 0,1,4,5 \ (\text{mod}\, 8) \qquad \textbf{(2.9)}$$

yazılabilir. n tek ise yani $n \equiv 5,7 (\text{mod}\, 8)$ ise (2.8) den istenen elde edilir. Çünkü, $n \equiv 5,7 \ (\text{mod}\, 8)$ iken

$$A = \left\{(x,y,z) \in \mathbb{Z}^3 : n = 2x^2 + y^2 + 32z^2\right\} \text{ ve } B = \left\{(x,y,z) \in \mathbb{Z}^3 : n = 2x^2 + y^2 + 8z^2\right\}$$

kümeleri boştur. Yani,

$$\left|\left\{(x,y,z) \in \mathbb{Z}^3 : n = 2x^2 + y^2 + 32z^2\right\}\right| = \frac{1}{2}\left(\left|\left\{(x,y,z) \in \mathbb{Z}^3 : n = 2x^2 + y^2 + 8z^2\right\}\right|\right)$$

olup n kongruent sayıdır. n çift ise yani $n \equiv 6 \ (\text{mod}\, 8)$ ise $\frac{n}{2} \equiv 3,7 (\text{mod}\, 8)$ olur. (2.9) dan istenen elde edilir. Çünkü,

$$C = \left\{(x,y,z) \in \mathbb{Z}^3 : \frac{n}{2} = 4x^2 + y^2 + 8z^2\right\} \text{ ve } D = \left\{(x,y,z) \in \mathbb{Z}^3 : \frac{n}{2} = 4x^2 + y^2 + 32z^2\right\}$$

kümeleri $\frac{n}{2} \equiv 3,7 \pmod 8$ durumlarında boştur. Yani,

$$\left|\left\{(x,y,z) \in \mathbb{Z}^3 : \frac{n}{2} = 4x^2 + y^2 + 32z^2\right\}\right| = \frac{1}{2}\left(\left|\left\{(x,y,z) \in \mathbb{Z}^3 : \frac{n}{2} = 4x^2 + y^2 + 8z^2\right\}\right|\right)$$

olup n kongruent sayıdır.

2.6. Genelleştirilmiş Kongruent Sayı Problemi

Tanım 2.6.1. $t \in \mathbb{Q} - \{0\}$ olsun. $a^2 = b^2 + c^2 - 2bc\frac{t^2-1}{t^2+1}$ ve $n = bc\frac{t}{t^2+1}$ olacak biçimde a, b, c pozitif rasyonel sayıları varsa n tamsayısına $t-kongruent$ denir.

$t = 1$ alınırsa bilinen kongruent sayı problemi elde edilir.

Önerme 2.6.2. t pozitif rasyonel sayı ve $n \in \mathbb{N}$ olsun. Aşağıdaki ifadeler denktir.

$i)$ n, $t-kongruent$ sayıdır,

$ii)$ $\frac{n}{t}$ ve t^2+1 sıfırdan farklı bir rasyonel sayının karesidir veya $C_{n,t}: y^2 = x(x-n/t)(x+nt)$ eliptik eğrisinin $y \neq 0$ olacak biçimde rasyonel (x,y) çözümü vardır

[26].

İspat.

$i \Rightarrow ii)$: n bir $t-kongruent$ sayı olsun. O halde $a^2 = b^2 + c^2 - 2bc\frac{t^2-1}{t^2+1}$ ve $n = bc\frac{t}{t^2+1}$ olacak biçimde a, b, c pozitif rasyonel sayıları vardır. İkinci eşitlikten $\frac{n}{t} = \frac{bc}{t^2+1}$ yazılabilir. Dolayısıyla $(x,y) = \left(\frac{a^2}{4}, \frac{ab^2 - ac^2}{8}\right)$ noktası $C_{n,t}$ üzerindedir. Eğer $b \neq c$ ise $y \neq 0$ dır.

Diğer durumda, yani $b=c$ ise kolaylıkla $t^2+1=\left(\frac{2b}{a}\right)^2$ ve $\frac{n}{t}=\left(\frac{a}{2}\right)^2$ olduğu gösterilebilir.

$ii \Rightarrow i$): $\frac{n}{t}$ ve t^2+1 sıfırdan farklı bir rasyonel sayının karesi olsun. O halde $a=2\sqrt{n/t}$, $b=c=\sqrt{n\left(t^2+1\right)/t}$ alındığında n sayısının bir $t-kongruent$ sayı olduğu kolaylıkla görülür. $y\neq 0$ olmak üzere $(x,y)\in C_{n,t}$ olsun. O zaman,

$a=\left|\frac{x^2+n^2}{y}\right|$, $b=\left|\frac{(x+nt)(x-n/t)}{y}\right|$, $c=n\left|\frac{x(t+1/t)}{y}\right|$ alınırsa n sayısının bir $t-kongruent$ sayı olduğu görülür.

Teorem 2.6.3. $t\in\mathbb{Q}$ ve $t>0$ olsun. Herhangi karesiz n doğal sayısı $t-kongruent$ sayı olarak alınabilir [21].

Tanım 2.6.4. $\theta\in\mathbb{R}$ öyle ki $0<\theta<\pi$ ve $r,s\in\mathbb{Z}$, $(r,s)=1$, $|s|\leq r$ olmak üzere $\cos\theta=\frac{s}{r}$ olsun. Eğer $n\sqrt{r^2-s^2}$, kenarları rasyonel sayı ve açısı θ olan rasyonel üçgenin alanı ise n doğal sayısına $\theta-kongruent$ denir.

Klasik kongruent sayı problemi, $\theta-kongruent$ sayı probleminin $\theta=\frac{\pi}{2}$ için bir özel halidir.

Önerme 2.6.5. $n>0$ tamsayı olsun. Aşağıdaki ifadeler denktir.

i) n, $\frac{2\pi}{3}-kongruent$ sayıdır,

ii) $C_n: y^2=x^3-2nx^2-3n^2x=x(x+n)(x-3n)$ eliptik eğrisinin $y\neq 0$ olacak biçimde (x,y) rasyonel çözümü vardır,

iii) $C_n(\mathbb{Q})$ grubunun rankı ≥ 1 dir [26].

Önerme 2.6.6. $n>0$ tamsayı olsun. Aşağıdaki ifadeler denktir.

i) n, $\frac{\pi}{3}-$*kongruent* sayıdır,

ii) $C_{-n}: y^2=x^3-2nx^2-3n^2x=x(x-n)(x+3n)$ eliptik eğrisinin $y\neq 0$ olmak üzere (x,y) rasyonel çözümü vardır,

iii) $C_{-n}(\mathbb{Q})$ grubunu rankı ≥ 1 dir [26].

BÖLÜM 3. SONUÇLAR VE ÖNERİLER

İncelemenin ana konusu, hangi tamsayıların kongruent sayı olduğudur. Genelleştirilmiş Fibonacci ve Lucas dizilerinden elde edilen kongruent sayılar verilmiştir.

Ayrıca $y^2 = x^3 - n^2 x$ eliptik eğrisi incelenmiş olup, bu eğri için n sayısının kongruent olması durumunda eliptik eğrinin rankının sıfırdan büyük olacağına değinilmiştir. Fakat rank hesaplama işlemleri basit yöntemlerle yapılamadığından, burada eliptik eğrinin rankını hesaplama işlemleri yapılmamıştır. Bunun için [3] kaynağına bakılabilir.

Tezin sonunda genelleştirilmiş kongruent sayı probleminden kısaca bahsedilmiştir. $t-kongruent$ ve $\theta-kongruent$ sayılarının tanımları ve ilgili birkaç önerme verilmiştir. Bu konu ayrıca araştırılabilir. Detaylar için, konu ile ilgili olarak [21] ve [26], [37] çalışmalarına bakılabilir.

KAYNAKLAR

[1] SERF, P., Congruent numbers and elliptic curves, Computational Number Theory. Walter de Gruyter and Co., Berlin, New York, pp. 227-238, 1991.

[2] KRAMARZ, G., All congruent numbers less than 2000, Mathematische Annalen, Berlin, Göttingen, Heidelberg, 337-340, 1968.

[3] JOHNSTONE, J.A., Congruent numbers and elliptic curves, Master's thesis, The University of British Columbia, 2009.

[4] KOBLITZ, N., Intoduction to elliptic curves and modular forms, 2nd Edition, New York, Springer Verlag, 1993.

[5] SIERPINSKI, W. F., Elementary theory of numbers, Elsevier, 1988.

[6] GENOCCHI, A., Note analitiche sopra tre scritti. Annali di Scienze Matematiche e Fisiche, 6, 273-317, 1855.

[7] HEMENWAY, B., On recognizing congruent primes, Master's thesis, Simon Fraser University, 2006.

[8] REINHOLZ, L.K., Families of congruent and non-congruent numbers, Master's thesis, The University of British Columbia, 2011.

[9] HEEGNER, K., Diophantische analysis und modulfunktionen. Math. Z., 56(3), 227-253, 1952.

[10] BIRCH, B. J., Diophantine analysis and modular functions, Internat. Colloq. on Algebraic Geometry, Tata Inst. Studies in Math., 4:35-42, 1968.

[11] STEPHENS, N. M.,. Congruence properties of congruent numbers, Bull. London Math. Soc., 7:182-184, 1975.

[12] MONSKY, P., Heegner points and congruent numbers. Math.Z., 204(1):45-68, 1990.

[13] TUNNELL, J.B., A classical Diophantine problem and modular forms of weight 3/2, Invent. Math. 80, 223-257, 1948.

[14] IZADI, F., Congruent numbers via the Pell equation and its analogous counterpart, arxiv: 1004.0261v4 [math,HO] 30 Dec. 2010.

[15] KESKİN, R., GÜNEY DUMAN, M., Positive integer solutions of some Pell equations (submitted).

[16] SILVERMAN, J.S., The arithmetic of elliptic curves, Springer, New York, Berlin, Heidelberg, 1985.

[17] SILVERMAN, J.H., TATE, J., Rational points on elliptic curves, Springer Verlag, 1992.

[18] KNAPP, A. W., Elliptic curves, Math Notes 40, Princeton University Press, Princeton, N.J. 1992.

[19] HUSEMÖLLER, D., Elliptic curves, 111 in Graduate Texts in Mathematics, Springer-Verlag, 1987.

[20] LOZANO-ROBLEDO, A., Elliptic curves, modular forms and L functions, Students Mathematical Library, 2010.

[21] RAZAFINDRAMAHATSIARO, C.T., Elliptic curves and congruent numbers, African Institute for Mathematical Sciences, Master's Thesis, 20 May 2010.

[22] GICA, A., Rational points on elliptic curve, April 8, 2012 (Lecture notes).

[23] SILVERMAN, J.S., A friendly introduction to number theory, Pearson Prencite Hall, 2006.

[24] STEIN, W. A., The Birch and Swinnerton-Dyer conjecture, a computational approach, Department of Mathematics, University of Washington, wstein.org/books/bsd/bsd.pdf.

[25] RUBIN, K., Right triangles and elliptic curves, University of California Irvine, March 2007.

[26] TOP, J., YUI N., Congruent number problems and their variants, Algorithmic Number Theory, MSRI Publications, V:44, 2008.

[27] LEMMERMEYER, F., Introduction to elliptic curves, Lecture notes, September 13, 2003.

[28] CHAHAL, J.S., Congruent numbers and elliptic curves, Amer. Math. Monthly, 113(4):308-317, 2006.

[29] COATES, J., WILES, A., On the conjecture of Birch and Swinnerton Dyer. Invent. Math. 39, 223-251, 1977.

[30] DICKSON, L.E., History of the theory of numbers volume II, American Mathematical Association, 1920.

[31] HARMAN, A., The group of rational points on an elliptic curve, Final year project, May 8 2012.

[32] DALAWAT, C. H., Congruent numbers, elliptic curves and passage from the local to the global, arXiv:0704.3783v1 [math.HO] 28 April 2007.

[33] ALTER, R., CURTZ, T.B., A note on congruent numbers, Math. Comp., 28(125):303-305, 1974.

[34] MOLLIN, R.A., Advanced number theory with applications, Chapman and Hall/CRC Press, Boca Raton, London, New York, 2010.

[35] COATES, J., Congruent number problem, Pure and Appl. Math. Quaterly, 1(1): 14-27, 2005.

[36] HENNIART, G., Congruent numbers, elliptic curves and modular forms, Çeviri: Franz Lemmermeyer, www.fen.bilkent.edu.tr/franz/publ/guy.pdf

[37] KAN, M., θ-congruent numbers and elliptic curves, Acta Aritmetica 94, no .2, 153-160, 2000.

EKLER

1000'den küçük kongruent sayılar aşağıdaki gibidir [21].

5 6 7 13 14 15 20 21 22 23 24 28 29 30 31 34 37 38 39 41 45 46 47 52 53 54 55 56
60 61 62 63 65 69 70 71 77 78 79 80 84 85 86 87 88 92 93 94 95 96 101 102 103 109
110 111 112 116 117 118 119 120124 125 126 127 133 134 135 136 137 138 141
142 143 145 148 149 150 151 152 154 156 157 158 159 161 164 165 166 167 173
174 175 180 181 182 183 184 188 189 190 191 194 197 198 199 205 206 207 208
210 212 213 214 215 216 219 220 221 222 223 224 226 229 230 231 237 238 239
240 244 245 246 247 248 252 253 254 255 257 260 261 262 263 265 269 270 271
276 277 278 279 280 284 285 286 287 291 293 294 295 299 301 302 303 306 308
309 310 311 312 313 316 317 318 319 320 323 325 326 327 330 333 334 335 336
340 341 342 343 344 348 349 350 351 352 353 357 358 359 365 366 367 368 369
371 372 373 374 375 376 380 381 382 383 384 386 389 390 391 395 397 398 399
404 405 406 407 408 410 412 413 414 415 421 422 423 426 429 430 431 434 436
437 438 439 440 442 444 445 446 447 448 453 454 455 457 461 462 463 464 465
468 469 470 471 472 476 477 478 479 480 485 486 487 493 494 495 496 500 501
502 503 504 505 508 509 510 511 514 517 518 519 525 526 527 532 533 534 535
536 540 541 542 543 544 546 548 549 550 551 552 557 558 559 561 564 565 566
567 568 572 573 574 575 580 581 582 583 585 589 590 591 592 596 597 598 599
600 602 604 605 606 607 608 609 613 614 615 616 621 622 623 624 628 629 630
631 632 636 637 638 639 644 645 646 647 651 653 654 655 656 658 660 661 662
663 664 668 669 670 671 674 677 678 679 685 686 687 689 692 693 694 695 696
700 701 702 703 709 710 711 717 718 719 720 721 723 724 725 726 727 728 731
732 733 734 735 736 741 742 743 749 750 751 752 756 757 758 759 760 761 764
765 766 767 773 774 775 776 777 781 782 783 788 789 790 791 792 793 796 797
798 799 805 806 807 813 814 815 820 821 822 823 824 828 829 830 831 832 837
838 839 840 845 846 847 848 850 852 853 854 855 856 860 861 862 863 864 866
869 870 871 876 877 878 879 880 884 885 886 887 888 889 890 892 893 894 895
896 901 902 903 904 905 909 910 911 915 916 917 918 919 920 924 925 926 927
933 934 935 941 942 943 948 949 950 951 952 956 957 958 959 960 965 966 967
973 974 975 976 980 981 982 983 984 985 987 988 989 990 991 992 995 997 998
999

ÖZGEÇMİŞ

Ümmügülsüm ÖĞÜT, 01.04.1988 de Darende'de doğdu. İlk, orta ve lise eğitimini Gebze'de tamamladı. 2006 yılında Gebze Anadolu Lisesi'nden mezun oldu. 2007 yılında başladığı Uludağ Üniversitesi, Fen Edebiyat Fakültesi Matematik bölümünü 2011 yılında bitirdi. Şu anda Sakarya Üniversitesi, Fen-Edebiyat Fakültesi Matematik Bölümünde Araştırma Görevlisi olarak çalışmaktadır.