ESKİŞEHİR
ANADOLU ÜNİVERSİTESİ

BİLECİK
ŞEYH EDEBALİ ÜNİVERSİTESİ

Fen Bilimleri Enstitüsü
Matematik Anabilim Dalı

ELİPTİK EĞRİLERİN RANKLARI ÜZERİNE

Ayşe GÖR
Yüksek Lisans

Tez Danışmanı
Doç. Dr. İlker İNAM

BİLECİK, 2019
Ref.No: 10236507

ESKİŞEHİR
ANADOLU ÜNİVERSİTESİ

BİLECİK
ŞEYH EDEBALİ ÜNİVERSİTESİ

Fen Bilimleri Enstitüsü
Matematik Anabilim Dalı

ELİPTİK EĞRİLERİN RANKLARI ÜZERİNE

Ayşe GÖR
Yüksek Lisans

Tez Danışmanı
Doç. Dr. İlker İNAM

BİLECİK, 2019

ESKISEHIR
ANADOLU UNİVERSİTY

BILECIK
SEYH EDEBALI UNİVERSİTY

Graduate School of Sciences
Department of Mathematics

ON THE RANK OF ELLIPTIC CURVES

Ayşe GÖR
Master's Thesis

Thesis Advisor
Assoc. Prof. Dr. Ilker INAM

BILECIK, 2019

BİLECİK ŞEYH EDEBALİ ÜNİVERSİTESİ

BİLECİK ŞEYH EDEBALİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS
JÜRİ ONAY FORMU

Bilecik Şeyh Edebali Üniversitesi Fen Bilimleri Enstitüsü Yönetim Kurulunun 31.01.2019 tarih ve ....17..... sayılı kararıyla oluşturulan jüri tarafından 15.02.2019 tarihinde tez savunma sınavı yapılan Ayşe Gör'ün "Eliptik Eğrilerin Rankları Üzerine" başlıklı tez çalışması Matematik Anabilim Dalında YÜKSEK LİSANS tezi olarak oy birliği/ oy çokluğu ile kabul edilmiştir.

JÜRİ

ÜYE
(TEZ DANIŞMANI) : Doç. Dr. İlker İNAM

ÜYE : Prof. Dr. Nülifer Özdemir

ÜYE : Dr. Öğr. Üyesi Bilal DEMİR

ONAY

Bilecik Şeyh Edebali Üniversitesi Fen Bilimleri Enstitüsü Yönetim Kurulunun ..../..../..... tarih ve ...../..... sayılı kararı.

İMZA/ MÜHÜR

TEŞEKKÜR

Bu çalışmanın yürütülmesi sırasında desteğini esirgemeyen danışmanım Doç. Dr. İlker İnam' a, yoğun çalışmalarım sırasında sabır gösterdiği ve bana katlandığı için biricik eşim Orhan'a, motivasyon desteği ve ümit verici konuşmaları ile beni rahatlatan anne ve babama, yazım sırasında ve oluşan aksaklıklarda destek veren ve işleri yoluna koymaya gayret gösteren Bilecik Şeyh Edebali Üniversitesi Fen Bilimleri Enstitüsü personeline ve çalışmam sırasında küçük veya büyük yardımını esirgemeyen herkese teşekkür ederim.

Ayşe GÖR

ÖZET

Altı bölümden oluşan bu çalışmada eliptik eğriler teorisinin bazı temel konuları ele alınmıştır. İlk bölümde eliptik eğriler tanıtılmış, ikinci bölümde ise eliptik eğrilerin grup yapısı verilmiştir. Eliptik eğrilerin noktaları üzerinde özel bir toplama işlemini tanımlanıp, değişmeli grup elde edilebilmesi için projektif koordinatların kullanılıp "sonsuz noktasının" elde edilmesi gereklidir. Bu ise üçüncü bölümün içeriğini oluşturmaktadır. Dördüncü bölümde gösterilmesi zahmetli olan birleşme özelliği başta olmak üzere diğer grup aksiyomları gösterilerek eliptik eğrilerin değişmeli grup olduğu görülmüştür. Beşinci bölümde ise eliptik eğrilerin cebirsel yapısının belirlenmesi adına önemli sonuçlar olan Mordell, Lutz-Nagell ve Mazur'un verdiği sonuçlar incelenmiştir. Son bölümde ise eliptik eğrilerin rankları kavramı ele alınmış ve kuadratik twist ailelerinin rankları üzerine bazı sonuçlar verilmiştir. Bu çalışma derleme niteliğindedir.

Anahtar Kelimeler: Eliptik eğriler; rank; eliptik eğrilerin grup yapısı

ABSTRACT

In this six-part study, some basic topics of elliptic curves theory are discussed. In the first part, elliptic curves are introduced and in the second part, the group structure of the elliptic curves is given. A special point addition rule on the points of elliptic curves is defined and the projective coordinates should be used to obtain "point at infinity" in order to have a commutative group. This constitutes the content of the third chapter. In the fourth chapter, it is seen that elliptic curves form a commutative group by showing the other group axioms, especially associativity which needs hard working. In the fifth chapter, the results of Mordell, Lutz-Nagell and Mazur which are important results for the determination of the algebraic structure of elliptic curves are investigated. In the last chapter, the concept of rank of elliptic curves is considered and some results are given on the rank of quadratic twist families. This study is compiled.

Keywords: Elliptic curves; rank; elliptic curves group structure

İÇİNDEKİLER

Sayfa No

ÇİZELGELER DİZİNİ

ŞEKİLLER DİZİNİ

SİMGELER VE KISALTMALAR

Simgeler

$\mathbb{R}$	: Reel Sayılar
$\mathbb{Z}$	: Tam Sayılar
$\mathbb{C}$	: Kompleks Sayılar
$char(K)$	: K cisminin karakteristiği
$rank(E)$	: E eliptik eğrisinin rankı

1. ELİPTİK EĞRİLERE GİRİŞ

Eliptik eğriler matematikte son yılların en önemli konularından birisidir ve yaygın şekilde çalışılmaktadır, bundan başka geniş bir kullanım alanına sahiptir. 359 yıllık Fermat'ın Son Teoremi probleminin Gerhard Frey, Ken Ribet, Jean Pierre Serre, Barry Mazur, Richard Taylor, Nick Katz, Peter Sarnak ve bazı diğer matematikçilerin önemli katkılarıyla 1994'te İngiliz matematikçi Andrew Wiles tarafından Taniyama-Shimura Konjektürü'nün ispatlanarak çözülmesi, konuyu daha da popüler hale getirmiştir.

Bu bölümde eliptik eğriler tanıtılacaktır. Konuyla ilgili temel kaynaklar (Silverman 1992), (Silverman 2016), (Koblitz 1993) ve (Washington 2003) şeklindedir.

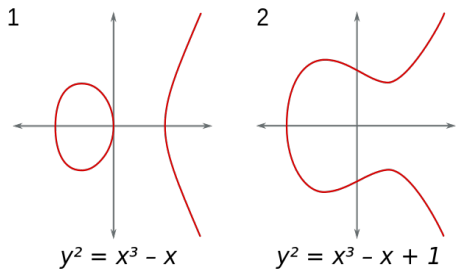
Tanım 1.1. $A, B \in \mathbb{Z}$ ve $\Delta = -16(4A^3 + 27B^2) \neq 0$ olmak üzere

$$y^2 = x^3 + Ax + B$$

biçiminde gösterilen denklemin belirttiği grafiğe eliptik eğri denir ve bu eğri E ile gösterilir (Washington 2003).

Yukarıdaki denkleme eliptik eğrinin "*kısa Weierstrass denklemi*" adı verilir. Eliptik eğriler üzerinde çalışıldıkları cisimlere göre farklı ve zengin özellikleri içinde barındırmaktadır. Öte yandan tanımı yapılırken hangi cisim üzerinde tanımlandığını da belirtilmelidir. Genel olarak kullanılan cisimler, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, p asal sayı olmak üzere $\mathcal{F}_p$ ve $k \geq 1$ ve $q = p^k$ olmak üzere $\mathcal{F}_q$ cisimleridir. Eğer K herhangi bir cisim ve $x, y \in K$ ise bu durumda "E eliptik eğrisi K cismi üzerinde tanımlansın" denir.

Eliptik eğrileri anlamlı olarak canlandırabilmek ve grafiklerini çizebilmek için E eliptik eğrisini $\mathbb{R}$ üzerinde tanımlamak gerekir. Şekil 1'de $\mathbb{R}$ üzerinde tanımlanmış iki eliptik eğrinin grafikleri yer almaktadır.



Şekil 1.1. Eliptik eğri örnekleri.

Tanım 1.2. K bir cisim ve E eliptik eğrisi K üzerinde tanımlansın. Bu durumda

$$E(K) = \{ (x, y) \in K \times K \mid y^2 = x^3 + Ax + B \} \cup \{\infty\}$$

olarak tanımlanan kümeye E eliptik eğrisinin üzerindeki rasyonel noktaların kümesi bu kümenin elemanlarına ise E eliptik eğrisinin rasyonel noktaları adı verilir (Silverman 1992).

Uyarı 1.3. Yukarıdaki tanımda verilen ve E eliptik eğrisinin rasyonel noktalarının kümesine eklenen ∞ noktası bu eğrinin grup yapısı oluşturulurken ihtiyaç duyulan bir "eleman" olup, ilerleyen bölümlerde gerekçesi açıklanacaktır.

Tanım 1.1'de konulan $\Delta \neq 0$ olması koşulu oldukça kritik bir koşul olup eliptik eğrilerin "rasyonel noktaları" kümesi üzerinde tanımlanacak olan "nokta toplamı" işleminde belirleyici olacaktır. Bu özelliği sağlayan eliptik eğrilere singüler olmayan eliptik eğri adı verilir.

E eliptik eğrisi $\mathbb{R}$ üzerinde $y^2 = x^3 - x$ eşitliği ile tanımlansın. Bu eliptik eğri üç tane ayrık reel köke sahiptir, tam olarak bu kökler $x = 0$, $x = 1$ ve $x = -1$ şeklindedir. İkinci kübik denklem olan $y^2 = x^3 + x$ eliptik eğrisi ele alındığında ise bu denklem sadece bir reel köke sahiptir, yani kökleri $x = 0$, $x = i$ ve $x = -i$ dir. Ancak bir eliptik eğri denkleminde katlı köke izin verilmez, bu durum grup yapısının oluşturulmasına engel olacaktır. Kübik denklemin kökleri r_1, r_2, r_3 olsun. O halde diskriminant kökler cinsinden

$$\big((r_1 - r_2)(r_1 - r_3)(r_2 - r_3)\big)^2 = -(4A^3 + 27B^2)$$

olur. Dikkat edilirse burada $\Delta \neq 0$ olması koşulu köklerin birbirinden farklı olmasına denktir.

Tanım 1.4. K karakteristiği 2 veya 3'ten farklı bir cisim ve a_1 , … , $a_6 \in K$ olsun. K cismi üzerindeki E eliptik eğrisi

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

denklemiyle tanımlansın. Bu durumda bu eşitliğe E eliptik eğrisinin genel Weierstrass denklemi denir (Silverman 2016).

Uyarı 1.5. E eliptik eğrisi eğer karakteristiği 2 ve 3 olan cisim üzerinde tanımlanmış ise genel Weierstrass denklemi kullanılır. Aslında cismin karakteristik 2

veya 3 değilse genel Weierstrass denkleminden kısa Weierstrass denklemi kolayca elde edilebilir. Gerçekten de, eğer cismin karakteristiği 2 değil ise, bu denklemin her iki yanı 2'ye bölüp tamkareye tamamlandığında

$$\left(y+\frac{a_1x}{2}+\frac{a_3}{2}\right)^2 = x^3+\left(a_2+\frac{{a_1}^2}{4}\right)x^2+\left(a_4+\frac{a_1a_3}{2}\right)x+\left(\frac{{a_3}^2}{4}+a_6\right)$$

elde edilir ve burada

$y_1 = y+\frac{a_1x}{2}+\frac{a_3}{2}$ ve $a_2{}'$, $a_4{}'$, $a_6{}'$ sabitler olmak üzere

$$y_1{}^2 = x^3+a_2{}'x^2+a_4{}'x+a_6{}'$$

şeklinde yazılabilir. Eğer karakteristik 3 de değilse, sonra $x_1 = x+\frac{a_2{}'}{3}$ alınır ve $x = x_1-\frac{a_2{}'}{3}$ olarak yerine yazılırsa

$$y_1{}^2 = \left(x_1-\frac{a_2{}'}{3}\right)^3+a_2{}'\left(x_1-\frac{a_2{}'}{3}\right)^2+a_4{}'\left(x_1-\frac{a_2{}'}{3}\right)+a_6{}'$$

$$y_1{}^2 = {x_1}^3+x_1\left(\frac{(a_2{}')^2}{3}-\frac{2}{3}(a_2{}')^2+a_4{}'\right)$$
$$+\left(-\frac{(a_2{}')^3}{27}+\frac{(a_2{}')^3}{9}-\frac{a_4{}'a_2{}'}{3}+a_6{}'\right)$$

olur ve bu denklemde $A = \frac{(a_2{}')^2}{3}-\frac{2}{3}(a_2{}')^2+a_4{}'$ ve $B = -\frac{(a_2{}')^3}{27}+\frac{(a_2{}')^3}{9}-\frac{a_4{}'a_2{}'}{3}+a_6{}'$ alınırsa

$$y_1{}^2 = {x_1}^3+Ax_1+B$$

denklemi elde edilmiş olur. Böylelikle genelleştirilmiş denklem verildiğinde Weierstrass denklemi oluşturulur. Denklemin verilen katsayıları tamsayı olmak zorunda değildir çünkü bu verilen katsayılar düzenlenerek Weierstrass denklemi oluşturulabilir. Kabul edelim ki $cy^2 = dx^3+ax+b$ ve $c\,,d\neq 0$ denklemi ile başlansın ve her iki tarafı da c^3d^2 ile çarpıldığında $(c^2dy)^2 = (cdx)^3+(ac^2d)(cdx)+(bc^3d^2)$ elde edilir sonra değişkenleri $y_1 = c^2dy$ ve $x_1 = cdx$ ile değiştirildiğinde

$$y_1{}^2 = {x_1}^3+Ax_1+B$$

olarak Weierstrass formu elde edilmiş olur (Silverman 2016).

2. ELİPTİK EĞRİLERİN GRUP YAPISI

Bu kısımda eliptik eğrilerin rasyonel noktaları kümesi üzerinde özel bir toplama işlemi tanımlanacak ve bu toplama işlemi yardımıyla bu kümenin bir abelyan grup olduğu görülecektir.

Tanım 2.1. E singüler olmayan bir eliptik eğri ve $P_1 = (x_1, y_1)$ ve $P_2 = (x_2, y_2)$ noktaları bu eğri üzerinde iki rasyonel nokta olsun. Bu iki noktadan geçen L doğrusu $y^2 = x^3 + Ax + B$ denklemini üçüncü bir nokta olan $P_3{}'$ noktasında kessin. Dikkat edilirse eliptik eğriyi tanımlayan eşitliğin ikinci tarafı üçüncü dereceden bir polinom olduğu için singüler olmayan bir eliptik eğri üzerindeki iki noktadan geçen doğru eğriyi mutlaka üçüncü bir noktada kesmek zorundadır. $P_1 = P_2$ olarak alınırsa bu durumda L doğrusu E eliptik eğrisine P_1 noktasında çizilen teğet doğrusu olarak alınır. $P_3{}'$ noktasının x-eksenine göre simetriği alındığında P_3 noktası elde edilir. Bu nokta verilen iki noktanın toplamı olarak, yani $P_3 = P_1 + P_2$ olarak tanımlanır (Silverman 2016).

Yukarıda verilen nokta toplamını detaylı olarak analiz edelim, böylece iki veya daha çok nokta verildiğinde bunların toplamlarını nokta koordinatları cinsinden ifade edebiliriz.

Kabul edelim ki, $P_1 \neq P_2$ ve bu iki nokta da ∞ noktası olmasın o zaman eğim aşikar olarak $m = \frac{y_2 - y_1}{x_2 - x_1}$ olur.

Eğer $x_1 = x_2$ ise, L dikey bir doğru olur.

Eğer $x_1 \neq x_2$ ise, L'nin denklemi $y = m(x - x_1) + y_1$ olur ve bu eşitlik Weierstrass denkleminde yerine yazılırsa

$$(m(x - x_1) + y_1)^2 = x^3 + Ax + B$$

olur. Bu ifade bir tarafa toplandığında ise

$$0 = x^3 - m^2x^2 + \cdots$$

elde edilir ve x_1, x_2, x kökler olmak üzere kökler toplamından

$$x = m^2 - x_1 - x_2$$

olacağından $P_3 = (x_3, y_3)$ noktasının x-eksenine göre simetrisi olan $P_3{}' = (x_3, -y_3)$ noktasının koordinatları $x_3 = m^2 - x_1 - x_2$ ve $y_3 = m(x_1 - x_3) - y_1$ olarak elde edilir.

Eğer $x_1 = x_2$ fakat $y_1 \neq y_2$ ise, oluşan L doğrusu dikey bir doğrudur ve eğriyi ∞ noktasında keser. ∞ noktasının x-eksenine göre simetriği alındığında yine aynı nokta olacağından $P_1 + P_2 = \infty$ olur.

$P_1 = P_2$ olarak alınırsa bu sefer L doğrusu E eliptik eğrisine P_1 noktasında çizilen teğet doğru olacağından türev yardımıyla L doğrusunun eğimi bulunur, yani

$$2y\frac{dy}{dx} = 3x^2 + A$$

bu yüzden

$$m = \frac{dy}{dx} = \frac{3{x_1}^2 + A}{2y_1}$$

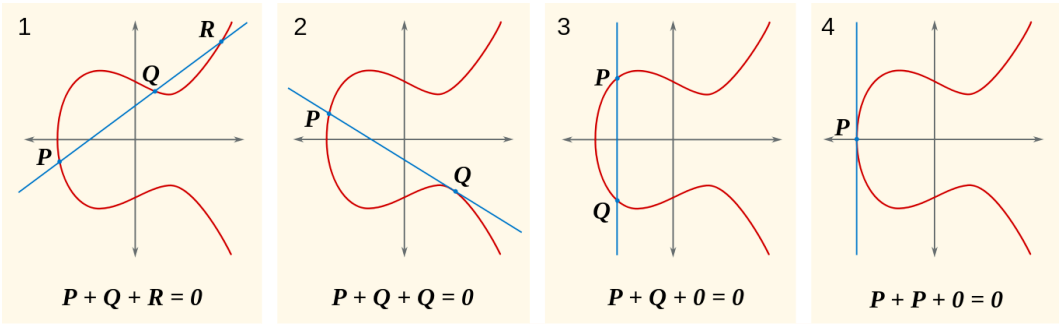
olur.

Eğer $y_1 = 0$ ise doğru dikey doğru olur ve bu yüzden toplam ∞ olur. Sonuç olarak $y_1 \neq 0$ iken teğet doğru denklemi ile eliptik eğrinin denkleminin ortak çözümü yapılıp kökler toplamı yazıldığında diğer noktanın koordinatları

$$x_3 = m^2 - 2x_1 \text{ ve } y_3 = m(x_1 - x_3) - y_1$$

olarak elde edilir.

Son durum olarak da, $P_2 = \infty$ iken P_1 ve ∞ dan geçen doğru eğriyi P_3 noktasında kesmiş olsun. Sonra da bu noktanın simetriği alındığında yine aynı noktaya dönüldüğünden dolayı $P_1 + \infty = P_1$ dir. Şekil 2'de çeşitli durumlarda nokta toplamı gösterilmiştir.



Şekil 2.1. Nokta toplamı.

Yukarıdaki tartışmaların ardından elde edilen sonuçlar aşağıdaki teoremde özetlenmiştir.

Teorem 2.2. (Washington 2003) $P_1 = (x_1 , y_1)$ ve $P_2 = (x_2 , y_2)$ olsun. $P_3 = (x_3, y_3)$ olmak üzere

(i) Eğer $x_1 \neq x_2$ ise, $m = \frac{y_2 - y_1}{x_2 - x_1}$, $x_3 = m^2 - x_1 - x_2$, $y_3 = m(x_1 - x_3) - y_1$ olur, yani

$$P_1 + P_2 = \left(\left(\frac{y_2 - y_1}{x_2 - x_1} \right)^2 - x_1 - x_2 , \left(\frac{y_2 - y_1}{x_2 - x_1} \right) x_3 - \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1} \right).$$

(ii) Eğer $x_1 = x_2$ fakat $y_1 \neq y_2$ ise, $P_1 + P_2 = \infty$ olur.

(iii) Eğer $P_1 = P_2$ ve $y_1 \neq 0$ ise, $m = \frac{3{x_1}^2 + A}{2y_1}$, $x_3 = m^2 - 2x_1$, $y_3 = m(x_1 - x_3) - y_1$ olur.

(iv) Eğer $P_1 = P_2$ ve $y_1 = 0$ ise, $P_1 + P_2 = \infty$ olur.

(v) E eliptik eğrisi üzerindeki bütün noktalar için $P + \infty = P$ olur.

3.PROJEKTİF UZAY VE ELİPTİK EĞRİ ÜZERİNDEKİ SONSUZ NOKTASI

Eliptik eğrilerin üzerindeki grup yapısının "sağlıklı şekilde" belirlenebilmesi adına projektif uzaya ihtiyaç duyulmaktadır. Bu bölümde öncelikle projektif uzay tanıtılacak olup eliptik eğrinin grup yapılması adına tanıma eklenen sonsuz noktasının nasıl elde edildiği anlatılacaktır. Buradaki temel nokta ise şudur: soyut cebirde bir grupta etkisiz elemanın bir tek olması gerekir (Asar vd. 2012). Buradan hareketle eliptik eğrinin üzerinde tanımlanan toplama işleminde etkisiz eleman rolü üstlenecek olan "sonsuz noktası"nın bu eğri üzerinde yer alabilmesi için projektif uzayda çalışılması gereklidir. Eliptik eğrinin projektif uzaya nasıl taşındığı ve böylece sonsuz noktasının nasıl eliptik eğrinin üzerine düşürüldüğü görülecektir. İlk olarak projektif uzayla ilgili olarak temel tanım ve kavramlar tanıtılacaktır. Bu konuyla ilgili olarak (Kaya 2005) kaynağından faydalanılmıştır.

Tanım 3.1. Noktalardan oluşan küme N ve doğrulardan oluşan küme D olsun. N ve D ayrıktır, yani ortak elemanları yoktur. $N = \{N_1, N_2, N_3, \dots\}$ ve $D = \{d_1, d_2, d_3, \dots\}$ olsun. Eğer (N, d) yazılırsa, bu N noktası d doğrusu üzerindedir ya da d doğrusu N noktasından geçer denilmektedir (Kaya 2005).

Biri noktalardan diğeri doğrulardan oluşan ayrık N ve D kümeleri ile $N \times D$ üzerinde bir $\circ$ bağıntısından meydana gelen $(N, D, \circ)$ üçlü sistemleri söz konusudur.

Tanım 3.2. $N_1, N_2, N_3, \dots \in N$ noktaları için $N_i \circ d$, $i = 1,2,3, \dots$ olacak şekilde bir $d \in D$ doğrusu var ise yani N_i noktası d doğrusu üzerinde ise bunlara doğrudaş noktalar denir (Kaya 2005).

Tanım 3.3. $d_1, d_2, d_3, \dots \in D$ doğruları için $M \circ d_i$, $i = 1,2,3, \dots$ olacak şekilde bir $M \in N$ noktası var ise bunlara noktadaş doğrular denir (Kaya 2005).

Tanım 3.4. $d_1, d_2 \in D$ ve $d_1 \neq d_2$ olsun. Eğer $M \circ d_1$ ve $M \circ d_2$ olacak şekilde hiçbir $M \in N$ noktası yoksa bu iki doğru birbirine paraleldir ve $d_1 \parallel d_2$ olarak gösterilir (Kaya 2005).

Tanım 3.5. N noktalar ve D doğrular kümesi ve $N \cap D = \emptyset$ olsun. $\circ$ da $N \times D$ kümesi üzerinde tanımlanan üzerinde bulunma bağıntısı olmak üzere;

(i) Her $M, L \in N$, $M \neq L$ noktaları için $M \circ d$ ve $L \circ d$ olacak şekilde bir tek $d \in D$ doğrusu vardır.

(ii) N noktası d doğrusu üzerinde olmamak üzere her $L \in N$ ve her $d \in B$ için $L \circ c$ ve $d \,||\, c$ olacak şekilde bir tek $c \in D$ doğrusu vardır.

(iii) Doğrudaş olmayan üç nokta vardır.

şartlarını gerçekleyen $(N, D, \circ)$ sistemine afin düzlem denir (Kaya 2005).

Birinci aksiyom farklı M, L noktaları bir doğru belirtir, ikinci aksiyom bir doğrunun dışındaki bir noktadan geçen ve bu doğruya paralel olan yalnız bir doğru vardır ve üçüncü aksiyom da aynı doğru üzerinde bulunmayan üç noktanın varlığını garantiler. Afin düzlem $\mathbb{A}$ ile gösterilir.

Teorem 3.6. (Kaya 2005) Bir $\mathbb{A}$ afin düzleminde farklı iki doğru üzerinde bulunan en çok bir nokta vardır.

Sonuç 3.7. (Kaya 2005) Bir afin düzlemde paralel olmayan farklı iki doğru üzerinde bulunan bir tek tane nokta vardır, yani tek noktada kesişirler.

Tanım 3.8. Paralel olmayan c ve d doğrularının üzerinde bulunan bu tek noktaya bu doğruların ara kesiti ya da kesişme noktası denir (Kaya 2005).

Teorem 3.9. (Kaya 2005) Bir $\mathbb{A}$ afin düzleminde paralel iki doğrudan biriyle kesişen bir doğru diğer doğru ile de kesişir.

Teorem 3.10. (Kaya 2005) Bir $\mathbb{A}$ afin düzleminde $b, c, d \in D$ için $b \,||\, c$ ve $c \,||\, d$ ise $b \,||\, d$ dir.

Teorem 3.11. (Kaya 2005) Verilen her K cismi için nokta ve doğruları bu cismin elemanlarıyla cebirsel olarak belirtilebilen bir afin düzlem vardır ve $\mathbb{A}^2K$ ile gösterilir.

Öklid düzlemi bir afin düzlemdir ve $\mathbb{A}^2\mathbb{R}$ ile gösterilir.

Teorem 3.12. (Kaya 2005) Her sonlu $\mathbb{A}$ düzlemi için aşağıdaki koşullara uyan bir $n \geq 2$ tamsayısı vardır ve bu tamsayı afin düzlemin mertebesidir:

(i) $\mathbb{A}$ nın her doğrusu üzerinde n tane nokta bulunur.

(ii) $\mathbb{A}$ nın her noktası $n + 1$ tane doğru üzerindedir.

(iii) $\mathbb{A}$ daki noktaların toplam sayısı n^2 dir.

(iv) $\mathbb{A}$ daki doğruların toplam sayısı $n^2 + n$ dir.

Tanım 3.13. (Kaya 2005) N ve D elemanları sırasıyla noktalar ve doğrular olan ayrık iki küme ve $\circ$ da $N \times D$ kümesi üzerinde bulunma bağıntısı olmak üzere;

(i) Her $M, L \in N$, $M \neq L$ için $M \circ d$ ve $L \circ d$ olacak şekilde bir tek $d \in D$ doğrusu vardır.

(ii) Her $c, d \in D$ için $L \circ c$ ve $L \circ d$ olacak şekilde en az bir $L \in N$ noktası vardır.

(iii) Herhangi üçü doğrudaş olmayan dört nokta vardır.

şartlarını sağlayan $(N, D, \circ)$ sistemine projektif düzlem denir ve $\mathbb{P}$ ile gösterilir.

Teorem 3.14. (Kaya 2005) $\mathbb{P}$ projektif düzleminde farklı iki doğru tek bir noktada kesişirler.

Teorem 3.15. (Kaya 2005) $\mathbb{P}$ Projektif düzleminde herhangi farklı iki doğrunun dışında bir nokta daima vardır.

Teorem 3.16. (Kaya 2005) Her sonlu $\mathbb{P}$ projektif düzlemi için aşağıdaki koşullara uyan bir n pozitif tamsayısı vardır ve bu tamsayıya projektif düzlemin mertebesi denilir.

(i) $\mathbb{P}$ nin her doğrusu üzerinde $n + 1$ nokta vardır.

(ii) $\mathbb{P}$ nin her noktasından $n + 1$ doğru geçer.

(iii) $\mathbb{P}$ deki tüm noktaların sayısı $n^2 + n + 1$ dir.

(iv) $\mathbb{P}$ deki tüm doğruların sayısı $n^2 + n + 1$ dir.

Bir projektif düzlemde her noktadan geçen en az üç doğru ve her doğru üzerinde en az üç nokta vardır, yani bir projektif düzlemin mertebesi en az 2 olmalıdır.

Tanım 3.17. Verilen her K cismi için nokta ve doğruları bu cismin elemanlarıyla cebirsel olarak belirtebilen bir projektif düzlem vardır (Kaya 2005).

K cismi yardımıyla tanımlanan bu projektif düzlemlere cisim düzlemleri denir ve genellikle $\mathbb{P}^2 K$ olarak gösterilir.

Tanım 3.18. Nokta, doğru ve düzlem boş olmayan ve aynı zamanda tanımsız geometrik nesnelerden oluşan üç ayrık küme olsun. Eğer bu üç küme elamanları arasında tanımlı üzerinde bulunma bağıntıları ile birlikte aşağıda bulunan aksiyomları gerçekleştiriyor ise bunların hepsine birden bir projektif 3-uzay denir.

U1: Farklı iki nokta bir tek doğru üzerindedir.

U2: Her doğru üzerinde en az üç nokta vardır.

U3: Doğrudaş olmayan üç nokta bir tek düzlem üzerindedir.

U4: Herhangi üçü doğrudaş olmayan ve hepsi aynı düzlemde bulunmayan dört nokta vardır.

U5: bir doğru ve bir düzlemin en az bir ortak noktası vardır.

U6: İki düzlemin en az bir ortak doğrusu vardır (Kaya 2005).

Örnek 3.19. Gerçel projektif 3-uzay. Bir afin düzlemin bir projektif düzleme genişletilmesine benzer şekilde 3-boyutlu Öklid uzayı gerçel projektif 3-uzaya genişletilebilir. Uzaydaki her Öklid düzlemi projektif düzleme genişletilir. Bu genişletme ile bulunan ideal nokta ve doğruları üzerinde bulunduran bir ideal düzlem uzaya katılır. Elde edilen bu yapı gerçel projektif 3-uzaydır. Bu uzay homojen koordinatlarla analitik olarak da kurulabilir: Burada bir nokta x_i lerin hepsi birden sıfır olmamak koşulu ile ve $x_i \in \mathbb{R}$, $\ell \in \mathbb{R}$ ve $\ell \neq 0$ olmak üzere $\ell\,(x_1, x_2, x_3, x_4)$ orantılı dörtlülerinin denklik sınıfıdır. Bu uzayda düzlem

$\sum_{i=1}^{4} a_i x_i = 0$, $a_i \in \mathbb{R}$, (a_i lerin hepsi birlikte sıfır değil)

Denklemini sağlayan noktalar cümlesidir. Doğru ise iki düzlemin ortak noktalarının kümesidir. Bu uzay $\mathbb{P}_3\mathbb{R}$ ile gösterilir.

Teorem 3.20. (Kaya 2005) Bir projektif 3-uzayda aşağıdakiler geçerlidir:

i) Farklı iki düzlem bir tek doğru boyunca kesişir.

ii) Bir düzlemde bulunan farklı iki noktayı birleştiren doğrunun her noktası bu düzlemde bulunur.

iii) Bir doğru ve bu doğru dışında bulunan bir nokta bir tek düzlem belirtir.

iv) Bir düzlem ve bu düzlemde bulunmayan bir doğru bir tek noktada kesişirler.

Teorem 3.21. (Kaya 2005) Bir projektif 3 –uzayın her düzlemi projektif düzlemdir.

3.1. Eliptik Eğri Üzerinde Sonsuz Noktasının Oluşturulması

Tanım 3.1.1. K bir cisim olsun. $x, y, z \in K$ ve hepsi aynı anda sıfır olmamak koşuluyla (x, y, z) sıralı üçlüsü projektif uzay üzerinde bir nokta olsun. Bu sıralı üçlü ile orantılı bütün üçlüler yine bu noktayı gösterirler, yani her $\lambda \in K$, $\lambda \neq 0$ için

$(x_1, y_1, z_1) = (\lambda x_2, \lambda y_2, \lambda z_2)$ şartını sağlıyorsa (x_1, y_1, z_1) ile (x_2, y_2, z_2) eşittirler denir ve $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$ yazılır (Kaya 2005).

Sıralı üçlüler x, y, z nin oranlarından oluşur ve sonuç olarak (x, y, z) nin sıralı üçlüleri $(x: y: z)$ olarak tanımlanır. Eğer $(x: y: z)$ için $z \neq 0$ ise $(x: y: z) = (\frac{x}{z} : \frac{y}{z} : 1)$ yazılabilir. Bunlar $\mathbb{P}^2K$ içinde sonlu noktalarıdır. Buna rağmen eğer $z = 0$ ise, z 'ye bölümde oluşan nokta ∞ noktası olarak bilinir ve sonuç olarak $(x: y: 0)$ noktası $\mathbb{P}^2K$ de sonsuz noktası olarak adlandırılır.

Şimdi afin düzleme bir takım yeni noktalar ve bütün bu yeni noktaları üzerinde bulunduran bir tek doğru katarak bir projektif düzlem elde edilebilir. Afin düzleme katılacak bu doğruya ideal doğru denir.

Tanım 3.1.2. $\mathbb{A} = (N, D, \circ)$ bir afin düzlem olsun. Bu düzlemde birbirine paralel olan bütün doğrular kümesine paralel doğru demeti denir (Kaya 2005).

Tanım 3.1.3. Düzlemde her bir demet için bu demetin tüm doğrularının üzerinde bulunan ama A da bulunmayan yeni bir nokta göz önüne alınsın. Böylece düzleme her doğrultuda bir ideal nokta katılmış olur ve genişletilmiş nokta kümesi

$$A' = A \cup \{ideal\ noktalar\}$$

olarak bulunur. Afin düzleme ideal noktalar katılırken her bir d doğrusu genişletilmiş olur. d doğrusu ve d'ye paralel olan tüm doğrular üzerine konulan bu ideal nokta D_∞ ile gösterilsin. Tüm ideal noktaların üzerinde bulunduğu ideal doğruya da d_∞ denilerek $\mathbb{A}$ afin düzlemine katılsın. Böylelikle afin düzlem genişletilerek $(N', D', \circ)$ sistemi elde edilir. Bu sisteme $\mathbb{A}$ afin düzleminin kapanışı denir (Kaya 2005).

Teorem 3.1.4. (Kaya 2005) Her afin düzlemin kapanışı bir projektif uzaydır.

Teorem 3.1.5. (Kaya 2005) $\mathbb{A}^2K$ afin düzleminin tamamlanışı $\mathbb{P}^2K$ projektif düzlemine izomorftur. Bu izomorfizm net olarak

$$\mathbb{A}^2K \cong \mathbb{P}^2K$$

$$(x, y) \to (x: y: 1)$$

şeklindedir.

Tanım 3.1.6. K bir cisim ve $a \in K$ olsun. n.dereceden homojen bir polinomun bütün terimleri $i + j + k = n$ olmak üzere $ax^i y^j z^k$ şeklinde olur (Kaya 2005).

Örneğin $F(x,y,z) = 5x^2y - 3xyz + 2y^3$ denklemi 3. dereceden homojen denklemdir.

Tanım 3.1.7. K bir cisim olsun. Eğer F n. dereceden homojen bir polinom ise, her $\lambda \in K$ için $F(\lambda x, \lambda y, \lambda z) = \lambda^n F(x,y,z)$ olur (Kaya 2005).

F homojen bir denklem ve $(x_1,y_1,z_1) \sim (x_2,y_2,z_2)$ ise, $F(x_1,y_1,z_1) = 0$ ancak ve ancak $F(x_2,y_2,z_2) = 0$. Sonuç olarak $\mathbb{P}^2K$ daki F in sıfırıncı mertebesi sıralı üçlülerinin seçimine bağlı değildir bu yüzden F nin sıfırlarının kümesi $\mathbb{P}^2K$ da iyi tanımlıdır.

Eğer $F(x,y,z)$ keyfi bir fonksiyon ise, $\mathbb{P}^2K$ projektif düzleminde $F(x,y,z) = 0$ olan noktalar hakkında konuşmak güçleşir çünkü bu sıralı üçlülerin (x,y,z) li gösterimlerine bağımlıdır.

$F(x,y,z) = x^2 + 2y - 3z$ olsun. $F(1,1,1) = 0$ olur, burdan F fonksiyonun $(1:1:1)$'de sıfır değerini aldığını söyleyebiliriz. Fakat $F(2,2,2) = 2$ olur ve bu da $(1:1:1) = (2:2:2)$ demektir. Bu problemden kurtulabilmek için homojen polinomlar seçilmesi gerekir.

$f(x,y)$ fonksiyonu x ve y değişkenlerine bağlı bir polinom olsun. z'nin kuvvetleri ara terim olarak eklendiğinde Weierstrass denklemi homojen denklem formuna dönüştürülebilir. Örneğin; $f(x,y) = y^2 - x^3 - Ax - B$ olur ve $F(x,y,z) = y^2z - x^3 - Axz^2 - Bz^3$ olarak yazılabilir. Burdan F fonksiyonu n.dereceden homojen bir polinom ise, $F(x,y,z) = z^n f\left(\frac{x}{z}, \frac{y}{z}\right)$ ve $f(x,y) = F(x,y,1)$ olur.

$y = mx + b_1$ ve $y = mx + b_2$ paralel doğrular olsun. Bunların sonsuz noktasında kesiştiklerini göstermek için öncelikle $b_1 \neq b_2$ ve dikey olmayan iki doğru olsunlar. Bu doğruların homojen formları $y = mx + b_1z$ ve $y = mx + b_2z$ olur. Bu denklemlerin kesişimlerinden $z = 0$ ve $y = mx$ elde edilir. Bütün bilinmeyenlerin hepsi sıfır olamayacağından dolayı $x \neq 0$ olmalıdır. Sonuç olarak x ile bölersek iki doğrunun kesişimi $(x:mx:0) = (1:m:0)$ olarak bulunur.

Benzer şekilde eğer $x = c_1$ ve $x = c_2$ iki dikey doğru ise, bunlar $(0:1:0)$ noktasında kesişmeliler. Bu nokta $\mathbb{P}^2K$ için sonsuz noktasıdır.

E eliptik eğrisi olan $y^2 = x^3 + Ax + B$ denkleminin homojen formu $y^2z = x^3 + Axz^2 + Bz^3$ olur. (x,y) noktasının projektif versiyonu $(x:y:1)$ noktasıdır.

Sonsuz noktasının elde edilebilmesi için $z = 0$ yerine yazıldığında $0 = x^3$ elde edilmiş olur. Sonuç olarak $x = 0$ olacağından $y \neq 0$ olmak zorunda kalır. Nokta $(0: y: 0)$ olur ve y yeniden ölçeklendirildiğinde $(0: y: 0) = (0: 1: 0)$ noktası E üzerinde tek sonsuz noktası olur. Yukarıda görüldüğü üzere $(0: 1: 0)$ her dik doğrunun üzerindedir, bu yüzden her dik doğru E yi bu noktada keser. $(0: 1: 0) = (0: -1: 0)$ "en üst" ve "en dip" olduğundan bunlar aynı noktalardır. Böylece eliptik eğri üzerindeki sonsuz noktası $(0: 1: 0)$ olarak bulunur (Washington 2003).

4. $E(K)$ KÜMESİNDEN DEĞİŞMELİ GRUBA

Bu bölümde daha önce tanımladığımız nokta toplamı işlemi yardımıyla eliptik eğrilerin birer değişmeli grup olmasının tam bir ispatı verilecektir.

Teorem 4.1. (Washington 2003) E eliptik eğrisi $char(K) \neq 2,3$ özelliğindeki K cismi üzerinde tanımlanmış bir eliptik eğri olsun. Bu durumda Tanım 2.1'de verilen nokta toplamı aşağıdaki özellikleri sağlar;

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

(ii) Her $P_1 \in E$ için, $P_1 + \infty = P_1$ dir.

(iii) Her $P \in E$ için, $P + P' = \infty$ şartını gerçekleyen bir tek $P' \in E$ vardır. Bu ters nokta $P' = -P$ olarak ifade edilir.

(iv) Her $P_1, P_2, P_3 \in E$ için, $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$ dür.

Başka bir deyişle $E(K)$ bir değişmeli grup olur.

İspat. P_1 ve P_2 noktalarından geçen doğru ve P_2 ve P_1 noktalarından geçen doğru aynı doğrular olduklarından dolayı değişme özelliğinin sağlandığı aşikardır. Birim eleman ise ∞ elemanının tanımından gelir. Ters elemanların tanımı için ise herhangi bir P noktasının x-eksenine göre simetriği P' alındığında $P + P' = \infty$ olur. Sonuç olarak gösterilmesi gereken tek özellik birleşme özelliğidir. E eliptik eğrisi üzerinde toplama işleminin birleşme özelliğini sağladığını görmek için uzun adımları takip etmemiz gerekiyor. P_1 ve P_2 olarak iki nokta alındığında bu iki noktanın toplamından P_1+P_2 noktası tanımlanır. Daha sonra toplama işlemini P_1+P_2 ve P_3 noktasına uygulandığında $(P_1+P_2) + P_3$ elde edilmiş olur. Eğer ilk aşamayı P_2 ve P_3 noktaları ile başlanılmış olsaydı, bu noktaların toplamından $P_2 + P_3$ noktası bulunur. En sonunda toplama işlemi P_1 ve $P_2 + P_3$ noktaları için uygulanırsa $P_1 + (P_2 + P_3)$ elde edilmiş olunacaktı. Burada zor olan kısım bu noktaların aynı nokta olduklarını gösterebilmektir. Bu noktaların aynı noktayı verdiği çok açık değil çünkü $P_1 = P_2$ ya da $P_3 = P_1 + P_2$ gibi durumlar olduğunda yukarıdaki gösterim çok doğru olmayacağından ispat üzerinde çalışan durumlara göre dallanma gösterecek.

P, Q, R noktaları E eliptik eğrisi üzerinde olsun. $-((P + Q) + R)$ noktasını hesaplayabilmek için $l_1 = \overline{PQ}$, $m_2 = \overline{\infty, P + Q}$ ve $l_3 = \overline{R, P + Q}$ doğrularına ihtiyacımız var ve bunlar E eliptik eğrisini keserler. $-(P + (Q + R))$ noktasını

hesaplayabilmek için $m_1 = \overline{QR}$, $l_2 = \overline{\infty, Q+R}$ ve $m_3 = \overline{P, Q+R}$ doğrularına da ihtiyacımız var ve bunlar da E eliptik eğrisini keserler. Burada $P_{ij} \neq P_{33}$ olmak üzere $P_{ij} = l_i \cap m_j$ noktaları E üzerindedir ve bu sistemin sekiz noktası vardır. P_{33} noktasının ise E eğrisi üzerinde olmak zorundadır gerçekten de l_3 doğrusu E eğrisini R , $P+Q$ ve $-((P+Q)+R)$ noktalarında keser, $-\big((P+Q)+R\big) = P_{33}$ elde edilir. Benzer şekilde m_3 doğrusu ele alındığında $-\big(P+(Q+R)\big) = P_{33}$ olur, bu yüzden $-\big((P+Q)+R\big) = -\big(P+(Q+R)\big)$ elde edilir. Bu tartışmanın ardından sezgisel olarak birleşme özelliği gösterilmiş olur ancak burada dikkat edilmesi gereken üç durum söz konusudur:

1) P_{ij} noktalarından bazıları sonsuz olabileceğinden dolayı projektif koordinatlar kullanılmalı,

2) Bir doğru E nin teğet doğrusu olabilir yani iki P_{ij} noktası eşit olabilir o yüzden eğriyi kesen doğrunun mertebesinin tanımında dikkatli olunmalı,

3) Doğruların ikisi eşit olabilir.

Bu yüzden ispatı bu üç durumu göz önüne alarak yapmalıyız.

Öncelikle K, $char(K) \neq 2{,}3$ özelliğindeki bir cisim ve $\mathbb{P}^2K$ projektif uzay olsun. Bu projektif uzaydaki doğrular en basit anlamda lineer denklemler yoluyla gösterilebilir, yani $ax+by+cz=0$ olur. Bazen ise parametrik hali kullanılabilir, yani

$$\left.\begin{aligned} x &= a_1u + b_1v \\ y &= a_2u + b_2v \\ z &= a_3u + b_3v \end{aligned}\right\} \tag{4.1}$$

biçiminde gösterilişe $ax+by+cz=0$ lineer denkleminin parametrik biçimi denilir.

Eğer $a \neq 0$ ise, $ax+by+cz=0$ lineer denklemi $x = -\left(\frac{b}{a}\right)u - \left(\frac{c}{a}\right)v$, $y = u$ ve $z = v$ biçiminde ifade edilebilir.

Bütün (a_i, b_i) vektörleri her birinin çarpımları olarak yazılabileceği düşünülürse $(a_i, b_i) = \lambda_i(a_1, b_1)$ olur. Sonra her u , v için $x \neq 0$ olmak üzere $(x, y, z) = x(1, \lambda_1, \lambda_3)$ olur. Böylelikle projektif uzayda bir nokta elde edilir ama $a_1, \dots, b_3$katsayılarının bu doğru üzerinde olduğunu garantileyebilmek için rankı 2 olan $\begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \\ a_3 & b_3 \end{pmatrix}$ matrisine ihtiyaç vardır.

Tanım 4.2. Eğer bazı $\lambda \in K^x$ ler için $(u_1, v_1) = \lambda(u_2, v_2)$ ise, bu takdirde (u_1, v_1) ve (u_2, v_2) nin sıralı üçlülerinin $(x: y: z)$ biçimindedir (Washington 2003).

Sonuç olarak $\mathbb{P}^1K$ bir boyutlu projektif uzayında $(u: v)$ noktalarından geçen (u, v)'ler dikkate alınırsa ve bu doğru projektif uzayın içinde gömülü $\mathbb{P}^1K$ projektif doğrusunun bir kopyasına karşılık gelir. Şimdi ise eğriyi kesen doğrunun mertebesinin belirlenmesi gerekiyor.

Lemma 4.3. (Washington 2003) $G(u, v)$ özdeşliğin sıfırından farklı homojen bir polinom ve $(u_0: v_0) \in \mathbb{P}^1K$ olsun. Bu durumda $H(u_0, v_0) \neq 0$ olmak üzere $H(u, v)$ polinomu ve $k \geq 0$ olan bir tamsayı vardır öyle ki

$$G(u, v) = (v_0 u - u_0 v)^k H(u, v).$$

İspat. Kabul edelim ki $v_0 \neq 0$ ve G fonksiyonun derecesi m olsun. $g(u) = G(u, v_0)$ olsun. $g(u)$ fonksiyonunu $u - u_0$ ın kuvvetlerinin çarpanlarına ayırılırsa, $h(u_0) \neq 0$ ve derecesi $m - k$ olan belli bir h polinomu vardır ve belli k lar için $g(u, v) = (u - u_0)^k h(u)$ olur.

$H(u, v) = \left(\frac{v^{m-k}}{{v_0}^m}\right) h\left(\frac{uv_0}{v}\right)$ olsun, böylelikle $H(u, v)$ fonksiyonu $m - k$ dereceden homojen bir polinom olur ve sonra

$$G(u, v) = \left(\frac{v}{v_0}\right)^m g\left(\frac{uv_0}{v}\right) = \frac{v^{m-k}}{{v_0}^m} (v_0 u - u_0 v)^k h\left(\frac{uv_0}{v}\right) = (v_0 u - u_0 v)^k H(u, v)$$

olur ve istenilen elde edilmiş olur. Eğer $v_0 = 0$ ise, sonra $u_0 \neq 0$ olur ve yukarıdaki işlemlerde u, v nin rolleri değiştirildiğinde bu durumda ispat edilmiş olur. Bu da ispatı bitirir.

Tanım 4.4. f bir polinom olsun ve $f(x, y) = 0$ afin uzayda bir eğri belirtsin. Ayrıca L doğrusunun terimleri parametrik olarak $x = a_1 t + b_1$ ve $y = a_2 t + b_2$ şeklinde gösterilsin. O zaman $\tilde{f}(t) = f(a_1 t + b_1, a_2 t + b_2)$ olur. Eğer $\tilde{f}(t_0) = 0$ ise, $t = t_0$ olduğu zaman L doğrusu C eğrisini keser. Eğer $(t - t_0)^2$ $\tilde{f}(t)$ yi bölerse, L doğrusu C eğrisine teğettir. Eğer $\tilde{f}(t)$ fonksiyonunu bölen $t - t_0$ ın en yüksek kuvveti $(t - t_0)^n$ ise, L doğrusu (x, y) noktasının karşılığı olan $t = t_0$ noktasında n.mertebede C eğrisini keser denir (Washington 2003).

$F(x,y,z)$ homojen bir polinom olsun, bu yüzden $\mathbb{P}^1K$ projektif uzayında $F(x,y,z)=0$ denklemi bir C eğrisi tanımlar. L eğrisi (6.1) formatında parametrik bir eğri olarak ele alınırsa

$$\tilde{F}(u,v)=F(a_1u+b_1v\,,a_2u+b_2v\,,a_3u+b_3v)$$

olur. Eğer $\tilde{F}(u,v)$ fonksiyonunu bölen $(v_0u-u_0v)^n$ ise, L doğrusu $P(x_0:y_0:z_0)$ noktasında $(u:v)=(u_0:v_0)$ karşılık gelen noktada C eğrisini n.mertebede keser ve bu durum $ord_{L,P}(F)=n$ olarak gösterilir. Eğer $\tilde{F}$ özdeşliğin sıfırı ise, $ord_{L,P}(F)=\infty$ olur. $ord_{L,P}(F)$ değeri L doğrusunun parametrik gösterimine bağlı değildir. Ek olarak, üstteki homojen olmayan durum $v=v_0=1$ e karşılık gelir ve $z\neq 0$ olduğunda elde edilen tanımlarla çakışıyor.

Lemma 4.5. (Washington 2003) L_1 ve L_2 doğruları P noktasında kesişen iki doğru olsun ve $i=1,2$ için $L_i(x,y,z)$ bir lineer polinom olsun ve kısaca L_i olarak tanımlansın. Eğer belli α katsayıları için $L_1(x,y,z)=\alpha L_2(x,y,z)$ (ki bu eşitlik $ord_{L_1,P}(L_2)=\infty$ olması demektir) olmazsa, $ord_{L_1,P}(L_2)=1$ dir.

İspat. L_1 in parametrik halini L_2 ye yazarsak $\widetilde{L_2}$ nin u,v ye bağımlı lineer formunu elde etmiş oluruz. P noktası $(u_0:v_0)$ a karşılık geliyor olsun. $\widetilde{L_2}(u_0,v_0)=0$ olduğundan belli β sabitleri için $\widetilde{L_2}(u,v)=\beta(v_0u-u_0v)$ elde edilir. Eğer $\beta\neq 0$ ise, $ord_{L_1,P}(L_2)=1$ dir. Eğer $\beta=0$ ise, L_1 üzerindeki bütün noktalar L_2 doğrusu üzerinde olur. $\mathbb{P}^2K$ projektif uzayında iki nokta bir doğru tanımladığından dolayı L_1 doğrusu en azından üç noktaya sahiptir. ($\mathbb{P}^1K$ projektif uzayı $(1:0),(0:1),(1:1)$ noktalarını her zaman içerir.) Burdan yola çıkarak da L_1 ve L_2 doğrularının aynı doğrular olduğu söylenir ve sonuç olarak $L_1(x,y,z)$ ve $L_2(x,y,z)$ orantılı olur. Bu yüzden $ord_{L_1,P}(L_2)=\infty$ olur, bu da ispatı bitirir.

2.mertebeden bir eğriyi kesen doğru genellikle eğrinin teğet doğrusudur. Buna rağmen C eğrisi $F(x,y,z)=y^2z-x^3=0$ olarak tanımlanır. $x=au$, $y=bu$, $z=v$ olsun ve $P=(0:0:1)$ noktasından geçen bir doğru olsun. P noktası $(u,v)=(0,1)$'e karşılık gelir. Bu yüzden $\tilde{F}(u,v)=u^2(b^2v-a^3u)$ olur, böylelikle P noktasından geçen her doğru en az 2.mertebeden C eğrisini keserler. $b=0$ için P deki tanjant doğrusu için seçiminde en uygun durumdur ve 3. mertebeden C yi keser. C eğrisinin afin parçası $y^2=x^3$ tür. Bu eğride $(0,0)$ noktası eğrinin singülaritesi olduğundan, P

noktasındaki kesişimlerin daha yüksek mertebeye sahip olurlar, bu da istenilmeyen bir durumdur. O halde bir eğrinin singülaritesinin de incelenmesi gerekir.

Tanım 4.6. C eğrisi $\mathbb{P}^2K$ da bir eğri olsun ve $F(x,y,z)=0$ olarak tanımlansın. Eğer kısmi türevlerin F_x , F_y , F_z nin en azından biri P noktasında sıfırdan farklı ise bu eğri singüler değildir denir (Washington 2003).

$F(x,y,z)=y^2z-x^3-Axz^2-Bz^3=0$ olacak şekilde bir eğri ele alınsın ve üzerinde çalışılan K cisminin karakteristiğinin 2 ya da 3 olmadığı kabul edilsin, bu durumda kısmi türevler

$$F_x=-3x^2-Az^2$$

$$F_y=2yz$$

$$F_z=y^2-2Axz-3Bz^2$$

olur. $P=(x:y:z)$ noktası bu fonksiyon için bir singüler nokta olsun. Eğer $z=0$ ise, $F_x=0$ olması $x=0$ olmasını gerektirir ve $F_z=0$ şartı da $y=0$ olduğunu belirtir, böylelikle $P=(0:0:0)$ olur ki bu bir çelişkidir. Bu yüzden $z\neq 0$ olmalıdır, genelliği bozmadan $z=1$ olsun. Eğer $F_y=0$ ise, $y=0$ olur. $(x:y:1)$ eğri üzerinde olacağından bu nokta $x^3+Ax+B=0$ denklemini sağlamalıdır. Eğer $F_x=-(3x^2+A)=0$ ise, x bir polinomun köküdür ve türevinin bir köküdür, sonuç olarak bir çift kat köktür. Kübik polinomun çarpımsal kökünün olmadığı kabul edildiğinden dolayı, bu bir çelişkidir. Sonuç olarak, bu da bir eliptik eğrinin singüler noktası olamayacağını söyler. Böyle bir noktanın olduğu kabul edilse bile bu durumda $\overline{K}$ cisminin elemanları da hesaba katılır. Genellikle, $\overline{K}$'da singüler noktaları yoksa bu eğrinin singüler olmayan eğri olduğu anlamına gelir. Eğer, kübik polinomun x köklerinin çarpımının olmasına izin verilirse bu durumda $(x:0:1)$ de bu eğrinin aykırılığının olduğunu gösterir.

Eğer P noktası $F(x,y,z)=0$ eğrisinin bir singüler noktası ise, P noktasındaki teğet doğrusu $F_x(P)x+F_y(P)y+F_Z(P)z=0$ şeklindedir. $F(x,y,z)=y^2z-x^3-Axz^2-Bz^3=0$ ise, $(x_0:y_0:z_0)$ noktasındaki teğet doğrusu

$$(-3{x_0}^2-A{z_0}^2)x+2y_0z_0y+({y_0}^2-2Ax_0z_0-3B{z_0}^2)z=0.$$

$z=z_0=1$ yerine yazılırsa

$$(-3{x_0}^2-A)x+2y_0y+({y_0}^2-2Ax_0-3B)=0$$

elde edilir ve ${y_0}^2={x_0}^3+Ax_0+B$ olduğu kullanılıp yerine yazıldığında

$$(-3{x_0}^2 - A)(x - x_0) + 2y_0(y - y_0) = 0$$

olur. Bu ise afin koordinattaki teğet doğrusudur. Eliptik eğri üzerine nokta eklenirse bu denklem elde edilir.

Gerçekten de eğri üzerindeki $(x_0 : y_0 : z_0) = (0 : 1 : 0)$ noktası sonsuz noktasıdır. Teğet doğrusundan $\mathbb{P}^2K$'da $0x + 0y + z = 0$ denklemi elde edilir. Bu doğru "sonsuz doğrusu" dur. Bu doğru eliptik eğriyi sadece (0:1:0) noktasında keser ve bu da eliptik eğri üzerinde $\infty + \infty = \infty$ ifadesinin doğru olduğu anlamına gelir.

Lemma 4.7. (Washington 2003) C bir eğri ve $F(x, y, z) = 0$ olsun. Eğer P noktası C eğrisinin bir singüler olmayan noktası ise, $\mathbb{P}^2K$'da en az ikinci mertebeden C eğrisini kesen kesinlikle bir doğru vardır ve bu doğru P noktasında C eğrisine teğettir.

İspat. L mertebesi $k \geq 1$ olan C eğrisini kesen bir doğru olsun. L doğrusu parametrize edip F'de yerine konulursa $\tilde{F}(u, v)$ fonksiyonu elde edilir. P noktasına karşılık gelen nokta $(u_0 : v_0)$ olsun. Sonra $H(u_0, v_0) \neq 0$ olmak üzere belli $H(u, v)$ fonksiyonu için $\tilde{F} = (v_0u - u_0v)^k H(u, v)$ dir. Sonuç olarak,

$$\widetilde{F_u}(u, v) = kv_0(v_0u - u_0v)^{k-1}H(u, v) + (v_0u - u_0v)^k H_u(u, v)$$

ve

$$\widetilde{F_v}(u, v) = -ku_0(v_0u - u_0v)^{k-1}H(u, v) + (v_0u - u_0v)^k H_v(u, v)$$

olur. $\widetilde{F_u}(u_0, v_0) = \widetilde{F_v}(u_0, v_0) = 0$ ancak ve ancak $k \geq 2$ dir. O halde kabul edelim ki $k \geq 2$ olsun. P noktasında zincir kuralı kullanılırsa

$$\left.\begin{aligned} \widetilde{F_u} &= a_1F_x + a_2F_y + a_3F_z = 0 \\ \widetilde{F_v} &= b_1F_x + b_2F_y + b_3F_z = 0 \end{aligned}\right\} \tag{4.2}$$

oluşur. (4.2)'nin parametrize edilmiş hali bir doğruya karşılık geldiğinden dolayı (a_1, a_2, a_3) ve (b_1, b_2, b_3) vektörleri lineer bağımsız olur.

L' en az ikinci mertebeden olan C eğrisini kesen diğer bir doğru olsun. P noktasında (4.2)'de olduğu gibi yine bir denklem sistemi oluşur, yani

$${a_1}'F_x + {a_2}'F_y + {a_3}'F_z = 0$$

$${b_1}'F_x + {b_2}'F_y + {b_3}'F_z = 0.$$

elde edilir. Eğer $a' = ({a_1}', {a_2}', {a_3}')$ ve $b' = ({b_1}', {b_2}', {b_3}')$ vektörleri $a = (a_1, a_2, a_3)$ ve $b = (b_1, b_2, b_3)$ vektörleri gibi K^3'de aynı düzlemi geriyorsa bu durumda belli

terslenebilir matrisler olan $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ için $a' = \alpha a + \beta b$ ve $b' = \gamma a + \delta b$ olur. Sonuç olarak, u_1, v_1 yeni parametrelerin seçimi ile

$$ua' + vb' = (u\alpha + v\gamma)a + (u\beta + v\delta)b = u_1 a + v_1 b$$

elde edilir. Buradan da L ve L' aynı doğrular olduğu sonucuna ulaşılır. Eğer bu doğrular farklı ise, a, b ve a', b' farklı düzlemleri gererler ve bu yüzden a, b, a', b' vektörleri K^3 ün tamamını germelidir. O halde (F_x, F_y, F_z)'nin bu vektörlerle noktasal çarpımı sıfır olmalıdır sonuç olarak bu P'nin singüler nokta olduğunu belirtir ve bu da varsayım ile çelişir.

Sonuç olarak teğet doğrusunun en az ikinci mertebeden C eğrisini kestiği gösterilmelidir. Kabul edelim ki P'de $F_x \neq 0$ olsun ($F_y \neq 0$ ve $F_z \neq 0$ olduğu durumlar da benzerdir). Teğet doğrusunun parametrik gösterimi (4.2)'den

$$x = -\left(\frac{F_y}{F_x}\right)u - \left(\frac{F_z}{F_x}\right)v \text{ , } y = u \text{ , } z = v$$

verilsin, böylelikle $a_1 = -\frac{F_y}{F_x}$, $b_1 = -\frac{F_z}{F_x}$, $a_2 = 1$, $b_2 = 0$, $a_3 = 0$, $b_3 = 1$ olur. Bu değerler (6.2)'de yerine yazılırsa

$$\widetilde{F_u} = -\left(\frac{F_y}{F_x}\right)F_x + F_y = 0 \text{ ve } \widetilde{F_v} = -\left(\frac{F_z}{F_x}\right)F_x + F_z = 0$$

elde edilir. Böylece istenilen sonuç elde edilmiş olur.

Aşağıda gösterilen teoremin ispatından sonra eliptik eğrilerin birleşme özelliği kolaylıkla gösterilebilir. Eğer P_{ij} noktalarının farklı olduğu düşünülürse, ispat sadeleştirilebilir. Noktaların eşit olduğu durumlar nokta toplamı kuralına uyuyor.

Teorem 4.8. (Washington 2003) $C(x, y, z)$ $\mathbb{P}^2K$'da tanımlı homojen kübik bir polinom olsun ve kısaca C olarak gösterilsin. $\mathbb{P}^2K$ da tanımlı l_1 , l_2 , l_3 ve m_1 , m_2 , m_3 doğruları her i, j için $l_i \neq m_j$. l_i ve m_j doğrularının kesişimlerinin noktası P_{ij} olacak şekilde verilsin. Üstelik her $(i, j) \neq (3,3)$ için P_{ij} noktaları C eğrisi üzerinde singüler olmayan bir nokta olduğu varsayılsın. Bu takdirde eğer belli i ler için P_{i1} , P_{i2} , P_{i3} noktalarının $k \geq 2$ için aynı noktaya eşitse, l_i bu noktada en azından k.mertebeden C yi keser. Ayrıca, eğer belli j ler için P_{1j} , P_{2j} , P_{3j} noktaları $k \geq 2$ için aynı noktaya eşitse, m_j bu noktada en azından k.mertebeden C yi keser. Üstelik P_{33} bu eğri üzerinde bulunur.

İspat. l_1 doğrusu (4.1) formu ile ifade edilsin. $C(x,y,z)$ eğrisi bu durumda $\tilde{C}(u,v)$'ye dönüşür. l_1 doğrusu P_{11} , P_{12} , P_{13} noktalarından geçtiği açıktır. Bu noktaların l_1 doğrusu üzerindeki parametreleri $(u_1 : v_1)$, $(u_2 : v_2)$, $(u_3 : v_3)$ olsun. Bu noktalar C üzerinde olduğundan, $i = 1,2,3$ için $\tilde{C}(u_i, v_i) = 0$ olur. m_j'nin denklemi $m_j(x,y,z) = a_j x + b_j y + c_j z = 0$ olsun. Parametreleri yerine yazıldığında l_1 doğrusu $m_j(u,v)$ olarak genişletilir. P_{ij} noktaları m_j üzerinde olduğundan, $j = 1,2,3$ için $m_j(u_j, v_j) = 0$ olur. $l_1 \neq m_j$ olduğundan ve $\widetilde{m_j}$ nin sıfırları l_1 ve m_j nin kesişimlerini verir, $\widetilde{m_j}(u,v)$ fonksiyonu sadece P_{1j}'de sıfır olur, bu yüzden $\widetilde{m_j}$ in lineer formu sıfırdan farklıdır. Sonuç olarak, $\widetilde{m_1}(u,v)\widetilde{m_2}(u,v)\widetilde{m_3}(u,v)$ çarpımı sıfır olmayan kübik homojen polinomdur. Bu çarpım $\tilde{C}$ ile ilgilidir.

İspata aşağıdaki lemma ile devam edelim.

Lemma 4.9. (Washington 2003) $S(u,v)$ özdeşliğin sıfırı olmamak üzere, $R(u,v)$ ve $S(u,v)$ üçüncü dereceden homojen polinomlar olsun ve R ve S nin kaybolduğu üç noktanın $i = 1,2,3$ üzere $(u_i : v_i)$ olduğu farzedilsin. Ayrıca, eğer $(v_i u - u_i v)^k$ R ve S yi bölerse, sonra $\alpha \in K$ gibi bir sabit vardır öyle ki $R = \alpha S$ dir (Washington 2003).

Teorem 4.8.'in ispatına dönülecek olursa, $\tilde{C}$ ve $\widetilde{m_1}\widetilde{m_2}\widetilde{m_3}$ $i = 1,2,3$ için $(u_i : v_i)$ noktalarında sıfır olur. Sonuç olarak, eğer P_{1j} noktalarının mertebesi olan k aynı ise, lineer fonksiyonun mertebesi olan k bu noktada sıfır olur bu yüzden, $\widetilde{m_1}(u,v)\widetilde{m_2}(u,v)\widetilde{m_3}(u,v)$ çarpımı en az k.mertebede sıfır olur ayrıca $\tilde{C}$ nin en az k.mertebede sıfır olduğu kabul edildiğinden dolayı, Lemma 4.9 gereği öyle bir α katsayısı vardır ki

$$\tilde{C} = \widetilde{m_1}\widetilde{m_2}\widetilde{m_3}$$

olur. $C_1(x,y,z) = C(x,y,z) - \alpha m_1(x,y,z)m_2(x,y,z)m_3(x,y,z)$ olsun. l_1 doğrusu $l_1(x,y,z) = ax + by + cz = 0$ lineer denklemi ile tanımlansın. En azından bir katsayı sıfırdan farklı olduğundan dolayı, genellik bozulmadan $a \neq 0$ olsun (diğer durumlar da benzer şekilde yapılır) ve doğru aşağıdaki şekilde parametrize edildiğinde;

$$x = -\left(\frac{b}{a}\right)u - \left(\frac{c}{a}\right)v \quad , \quad y = u \quad , \quad z = v \tag{4.3}$$

elde edilir. O halde $\widetilde{C_1}(u,v) = C_1\left(-\left(\frac{b}{a}\right)u - \left(\frac{c}{a}\right)v, u, v\right)$ olur. $C_1(x,y,z)$'yi y,z nin katsayı olduğu ve x'e bağlı bir polinom olarak yazılabilir, öyle ki

$$x^n = \left(\frac{1}{a^n}\right)\big((ax+by+cz)-(by-cz)\big)^n = \left(\frac{1}{a^n}\right)((ax+by+cz)^n + \cdots),$$

ve $C_1(x,y,z)$ yeniden düzenlendiğinde $ax+by+cz$ lineer denklem formatına benzer olur. Gerçekten de

$$C_1(x,y,z) = a_3(y,z)(ax+by+cz)^3 + \cdots + a_0(y,z) \tag{4.4}$$

(6.3) parametrik formları (6.4)'de yerine yazılırsa $0 = \widetilde{C_1}(u,v) = a_0(u,v)$ olur, çünkü $ax+by+cz$ denkleminde x,y,z değişkenleri u,v nin terimleri olarak yazıldığında tamamen sıfır oluyor. Sonuçta $a_0(y,z) = a_0(u,v)$ sıfır polinomudur. (4.4)'ten $C_1(x,y,z)$ kübik polinomu $l_1(x,y,z) = ax+by+cz$ nin çarpımı olduğu görülür. Benzer şekilde bir öyle bir β sabit sayısı vardır ki $C(x,y,z) - \beta l_1 l_2 l_3$ ifadesi m_1 in çarpımıdır. $D(x,y,z) = C(x,y,z) - \alpha m_1 m_2 m_3 - \beta l_1 l_2 l_3$ olsun. O halde $D(x,y,z)$ ifadesi l_1 ve m_1 in çarpımıdır.

Lemma 4.10. $D(x,y,z)$ ifadesi $l_1(x,y,z)m_1(x,y,z)$ nin çarpımıdır. (Washington 2003)

Lemma 4.11. $l(P_{22}) = l(P_{23}) = l(P_{32}) = 0$ (Washington 2003).

İspat. İlk durum olarak $P_{13} \neq P_{23}$ olsun. Eğer $l_1(P_{23}) = 0$ ise, P_{23} noktası l_1 doğrusu üzerinde olur ve tanımdan dolayı l_2 ve m_3 üzerindedir. Böylelikle, P_{23} noktası l_1 ve m_3 den olan P_{13} ün kesişimine eşittir. $P_{13} \neq P_{23}$ olarak kabul edildiğinden dolayı bu bir çelişki oluşturur ve sonuç olarak $l_1(P_{23}) \neq 0$ yazılabilir. $D(P_{23}) = 0$ olduğundan dolayı $m_1(P_{23})l(P_{23}) = 0$ olur.

Şimdi bu durumun tam tersi yani $P_{13} = P_{23}$ durumu göz önüne alınsın. Daha sonra teoremin varsayımından dolayı m_3 doğrusu P_{23} noktasında C eğrisine teğettir, bu yüzden de $ord_{m_3,P_{23}}(C) \geq 2$ olur. $P_{13} = P_{23}$ olduğundan ve P_{23} noktasını m_3 üzerinde olduğundan dolayı $ord_{m_3,P_{23}}(l_1) = ord_{m_3,P_{23}}(l_2) = 1$ elde edilir. Sonuç olarak $ord_{m_3,P_{23}}(\alpha l_1 l_2 l_3) \geq 2$ ve ayrıca $ord_{m_3,P_{23}}(\beta m_1 m_2 m_3) = \infty$.

O halde $ord_{m_3,P_{23}}(D) \geq 2$, bu yüzden D terimlerin toplamı olur ve en azından 2. mertebede sıfır olur. Fakat $ord_{m_3,P_{23}}(l_1) = 1$ olduğundan dolayı

$$ord_{m_3,P_{23}}(m_1 l) = ord_{m_3,P_{23}}(D) - ord_{m_3,P_{23}}(l_1) \geq 1$$

elde edilir ve sonuçta $m_1(P_{23})l(P_{23}) = 0$ sonucu elde edilir.

Eğer $m_1(P_{23}) \neq 0$ ise, $l(P_{23}) = 0$ olur ve istenilen elde edilmiş olur.

Eğer $m_1(P_{23}) = 0$ ise, P_{23} noktası l_1 doğrusu üzerindedir ve bu nokta tanımından dolayı m_3 ve m_2 doğruları üzerinde olur ve böylelikle $P_{23} = P_{21}$'dir çünkü l_2 ve m_1 doğruları tek noktada kesişiyor. Varsayımdan dolayı l_2 doğrusu C eğrisine P_{23} noktasında tanjanttır. Sonuç olarak $ord_{l_2,P_{23}}(C) \geq 2$ olur ve yukarıdaki gösterimden dolayı $ord_{l_2,P_{23}}(D) \geq 2$ olduğundan dolayı $ord_{l_2,P_{23}}(l_1 l) \geq 1$ elde edilir.

Eğer bu durumda $l_1(P_{23}) = 0$ ise, P_{23} noktası l_1, l_2, m_3 üzerindedir ve dolayısıyla $P_{13} = P_{23}$ olur. Varsayımdan dolayı m_3 doğrusu C eğrisine P_{23} noktasında teğettir. P_{23} noktası C eğrisinin bir singüler olmayan noktası olduğundan dolayı, Lemma 6.7 kullanıldığında $l_2 = m_3$ olduğu söylenir ve bu durumda hipoteze ters düşer.

Sonuç olarak $l_1(P_{23}) \neq 0$ olur ve böylelikle $l(P_{23}) = 0$ dır. Benzer şekilde $l(P_{22}) = l(P_{23}) = 0$ olur. Bu ise ispatı bitirir.

Eğer $l(x, y, z)$ özdeşliğin sıfırı ise, D tamamen sıfırdır. Sonuç olarak $l(x, y, z)$ nin özdeşliğin sıfırı olmadığı düşünülüp böyle bir doğru tanımlansın.

İlk olarak P_{23}, P_{22}, P_{32} noktalarının farklı noktalar olduğu varsayılsın. l ve l_2 doğruları P_{23} ve P_{22} noktalarından geçer böylelikle $l = l_2$ olur. Benzer şekilde $l = m_2$ olduğu da söylenebilir ve bunların ikisi birleştirildiğinde $l_2 = m_2$ olur bu ise bir çelişkidir.

O halde $P_{32} = P_{22}$ olduğu düşünülsün. Sonra m_2 doğrusu C eğrisine P_{22} noktasında teğettir. Önceden gösterildiğinden dolayı $ord_{m_2,P_{22}}(l_1 m_1 l) \geq 2$ olur. İstenilen l doğrusunun m_2 doğrusu ile aynı doğru olduğunu göstermektir.

Eğer $m_1(P_{22}) = 0$ ise, P_{22} noktası m_1, m_2, l_2 doğruları üzerindedir ve sonuç olarak $P_{21} = P_{22}$ dir. Bunun anlamı ise l_2 doğrusu C eğrisine P_{22} noktasında teğettir. Lemma 4.7'den dolayı $l_1 = l_2$ olur ve bu da çelişkidir. Böylelikle $m_1(P_{22}) \neq 0$ olduğu elde edilir.

Eğer $l_1(P_{22}) \neq 0$ ise, $ord_{m_2,P_{22}}(l) \geq 2$ dir ve bunun anlamı ise l doğrusu m_2 doğrusu ile aynı doğrudur.

Eğer $l_1(P_{22}) = 0$ ise, $P_{22} = P_{32}$ l_1, l_2, l_3, m_3 doğğruları üzerindedir ve bu yüzden $P_{12} = P_{22} = P_{32}$. Sonuç olarak $ord_{m_2,P_{22}}(C) \geq 3$. yukarıdaki sebepten dolayı

$ord_{m_2,P_{22}}(l_1 m_1 l) \geq 3$ olur. Şimdi $m_1(P_{22}) \neq 0$ olduğu ispatlandığından dolayı, $ord_{m_2,P_{22}}(l) \geq 2$ olur ve bunun anlamı l doğrusu m_2 doğrusu ile aynı doğrudur.

Varsayımlar ışığında $P_{32} = P_{22}$ olduğu ispatlandı, l doğrusu m_2 doğrusu ile aynı doğrudur. Lemma 4.11'den dolayı P_{23} noktası l doğrusu üzerindedir ve sonuç olarak m_2 üzerindedir ve ayrıca tanımından dolayı l_2 ve m_3 üzerindedir. Sonuç olarak $P_{22} = P_{23}$. Bu eşitliğin anlamı ise, l doğrusu C eğrisine P_{22} noktasında teğet demektir. $P_{32} = P_{22}$ eşitliğinin anlamı m_2 doğrusu C eğrisine P_{22} noktasında teğet demek olduğundan dolayı, $l_2 = m_2$ elde edilir ve buda çelişkidir. Sonuç olarak $l \neq 0$ varsayımı altında $P_{32} \neq P_{22}$ olur. Benzer şekilde $P_{23} = P_{22}$ de gösterilebilir.

Sonunda $P_{23} = P_{32}$ olduğu düşünülsün. Sonra P_{23} noktası l_2, l_3, m_2, m_3 üzerinde olsun. Böylelikle bu durumda $P_{22} = P_{32}$ olmasını zorunlu kılar bunun imkansız olduğu ise yukarıda söylenmişti.

Sonuç olarak bütün olasılıklar çelişkiye yol açıyor ve buradan yola çıkılarak $l(x, y, z)$ doğrusunun özdeşliğin sıfırı olmasını gerektirir. Sonuç olarak $D = 0$ olur ve bu yüzden de

$$C = \alpha l_1 l_2 l_3 + \beta m_1 m_2 m_3$$

olur. l_3 ve m_3 doğruları P_{33} noktasında yok olduklarından dolayı, $C(P_{33}) = 0$ olur ve istenilen de bu idi. Buda Teorem 4.8'in ispatını tamamlar.

Uyarı 4.12. Belli α, β lar için $C = \alpha l_1 l_2 l_3 + \beta m_1 m_2 m_3$ şeklindedir.

C eğrisinin P_{ij} noktaları ayrık olarak tanımlandığı zaman sekiz nokta ve homojen kübik polinomunun 3 değişkeni ve 10 katsayısı vardır. Olası polinomların kümesi iki parametreli ailelerdir. P_{ij} noktaları ayrık olmadığında ise yeterli kısıtlamalar getirilerek teğet durumları iki parametreli aileler elde edilebilir.

Şimdi eliptik eğrilerin üzerinde tanımlanan nokta toplamı işleminin birleşme özelliğini sağladığı ispat edilebilir. P, Q, R noktaları E eliptik eğrisi üzerinde bulunan noktalar olsun ve doğrular $l_1 = \overline{PQ}$, $l_2 = \overline{\infty, Q + R}$, $l_3 = \overline{R, P + Q}$, $m_1 = \overline{QR}$, $m_2 = \overline{\infty, P + Q}$ ve $m_3 = \overline{P, Q + R}$ olarak tanımlansın.

Kesişimler tablo şeklinde gösterilirse:

	l_1	l_2	l_3
m_1	Q	$-(Q+R)$	R
m_2	$-(P+Q)$	∞	$P+Q$
m_3	P	$Q+R$	X

Çizelge 4.1. Kesişimler.

Şimdi teoremin bütün hipotezlerinin sağlandığı kabul edilsin, bu takdirde bütün noktalar X'i içeriyor ve E eliptik eğrisinin üzerindedir. l_3 doğrusu E eliptik eğrisi üzerinde üç tane kesişim noktasına sahiptir ve bunlar $R, P+Q, X$'dir. Toplama kuralından dolayı $X = -\big((P+Q)+R\big)$ olur. Benzer şekilde, m_3 doğrusu C eğrisini üç noktada keser ve bunun anlamı da $X = -(P+(Q+R))$ olduğudur. Sonuç olarak bunların x-eksenine göre simetrikleri alındığında $(P+Q)+R = P+(Q+R)$ elde edilir ve istenilen de bu idi. Bu eşitlik de teoremin hipotezini doğrulamaktadır. Kesişimlerin mertebeleri ve l_i ve m_j doğruları ayrıktır.

İlk olarak, sonsuzun olduğu yerlerde durumlar ayrı olarak ele alınmalıdır. Problem olan nokta ise, ∞ noktasında grup kuralından dolayı özel bir durum gibi davranılmasıdır. Buna rağmen, ∞ noktasında ki teğet doğrusu eğriyi sadece ∞'da keser.

Yukarıdaki tablodan bir satır ve bir sütunun iki tanesinin kesişimi ∞'a eşittir, o halde eğriyi üçüncü bir nokta keser ve sonuç olarak bu da hipotezi tanımlar.

Bazı kesişim noktaları olan $P, Q, R, \pm(P+Q), \pm(Q+R), \infty$ da direk durumlara göre hareket etmek de mümkündür. En azından bu noktaların P, Q, R noktalarından birinin olduğu durumda ∞ olduğu ve birleşme özelliğini sağladığı açıktır.

Eğer $P+Q=\infty$ ise, sonra $(P+Q)+R = \infty + R = R$.

Diğer taraftan, $Q+R$ nin toplamı hesaplanırken ilk olarak L doğrusu Q ve R noktalarından geçen doğru olarak çizilir ve bu doğru da eğriyi $-(Q+R)$ noktasında da keser. Bu yüzden $P+Q=\infty$ ve böylece Q noktasının x eksenine göre simetriği P noktasıdır. Sonuç olarak L doğrusunun yansıması olan $P, -R$ ve $Q+R$ den geçen doğru L' olsun. $P+(Q+R)$ toplamı P ve $Q+R$ den geçen doğrular çizilerek bulunabilir ve bu doğru L' doğrusudur. E eğrisinde L' doğrusunun üçüncü kesişim noktasının $-R$ olduğu gösterildi ve bu yansıtılırsa $P+(Q+R)=R$ olur ve birleşme özelliği bu

durum için sağlanmış olur. Benzer şekilde birleşme $Q + R = \infty$ olduğu zamanda sağlanır. Sonunda, eğer belli l_i doğruları ile belli m_j doğruları eşit olduklarında Teorem 6.8'e başvurulamayacağından bu durum ayrıca ele alınmalı.

İlk olarak, eğer P, Q, R noktaları kolineer ise, birleşme özelliği direk olarak sağlanır. İkinci olarak, $P, Q, Q + R$ noktalarının kolineer olduğu kabul edilirse bu durumda $P + (Q + R) = -Q$ olur. Ayrıca $P + Q = -(Q + R)$, bu yüzden $(P + Q) + R = -(Q + R) + R$ yazılır ve bu da birleşme özelliğinin bu durumda da sağlandığını gösterir.

Lemma 4.13. (Washington 2003) P_1 ve P_2 noktaları eliptik eğri üzerinde iki nokta olsun. Bu takdirde $(P_1 + P_2) - P_2 = P_1$ ve $-(P_1 + P_2) + P_2 = -P_1$ olur.

İspat. Bu iki eşitlik birbirinin simetrisi olduğundan dolayı birini ispatlamak yeterlidir. P_1 ve P_2 noktalarından geçen doğru L doğrusu olsun ve bu doğru eliptik eğriyi $-(P_1 + P_2)$ de keser. $-(P_1 + P_2)$ ve P_2 noktalarından geçen doğrunun simetriği alınırsa $-(P_1 + P_2) + P_2 = -P_1$ elde edilir. Bu da ispatı bitirir.

Belli i, j ler için $l_i = m_j$ olduğu farzedilsin. Çeşitli durumlar oluşur. Üstteki tabloda ∞ ve X dışındaki bütün noktaların sonlu olduğu düşünülmüştü. l_i ve m_j doğrularının E eliptik eğrisinde üç noktada kesiştikleri varsayılmıştı ve bunlar P_{ij} noktalarıydı. Eğer iki doğru çakışık ise, diğer iki nokta da aynı noktalarda çakışıktır. Böylece:

1. $l_1 = m_1$: Sonra P, Q, R kolineerdir ve birleşme yukarıda ki gibidir.

2. $l_1 = m_2$: Bu durumda P, Q, ∞ kolineerdir. Bu yüzden $P + Q = \infty$ olur ve birleşme özelliği yukarıdaki gibi direk hesaplanabilir.

3. $l_2 = m_1$: Birinci durumdaki gibidir.

4. $l_1 = m_3$: Sonra $P, Q, Q + R$ kolineerdir ve birleşme yukarıda ki gibidir.

5. $l_3 = m_1$: Birinci durumdaki gibidir.

6. $l_2 = m_2$: $P + Q = \pm(Q + R)$ olmalıdır. Eğer $P + Q = Q + R$ ise, o halde Lemma 6.13 gereği $P = (P + Q) - Q = (Q + R) - Q = R$. Sonuç olarak $(P + Q) + R = R + (P + Q) = P + (P + Q) = P + (R + Q) = P + (Q + R)$. Eğer $P + Q = -(Q + R)$ ise, sonra $(P + Q) + R = -(Q + R) + R = -Q$ ve $P + (Q + R) = P - (P + Q) = -Q$ olur ve birleşme özelliği sağlanır.

7. $l_2 = m_3$: Bu durumda, P ve $Q + R$ noktalarından geçen m_3 doğrusu E eğrisini ∞ noktasında keser, bu yüzden $P = -(Q + R)$ olur. Bu yüzden $-(Q + R), Q, R$ noktaları kolineerdir ve böylece P, Q, R kolineer olur ve birleşme sağlanır.

8. $l_3 = m_2$: Birinci durumdaki gibidir.

9. $l_3 = m_3$: l_3 doğrusu E eğrisini dört noktada kesmediğinden dolayı, $P = R$ ya da $P = P + Q$ ya da $Q + R = P + Q$ ya da $Q + R = R$ olduğu kolayca görülür. $P = R$ eşit olma durumunu $l_2 = m_2$ durumunda gösterildi. Farzedelim $P = P + Q$ olsun. Bu eşitliğe $-P$ noktasını ekleyip Lemma 6.13'ü kullanırsak $\infty = Q$ olur ve birleşme özelliği sağlanır. Eğer $Q + R = R$ alınırsa bu durumda benzerdir. Eğer $Q + R = P + Q$ ise, $-Q$ noktası eklenir ve Lemma 6.13'ten $P = R$ elde edilir ve birleşme özelliği sağlanır.

Eğer her i, j için $l_i \neq m_j$ ise, teoremin şartları sağlanır ve bu yüzden toplama işlemi için birleşme özelliği sağlanmış olur. Bu da eliptik eğriler üzerinde tanımlanan nokta toplamı işleminin birleşme özelliğini sağladığının ispatını tamamlamış olur (Washington 2003).

5. MORDELL, NAGELL-LUTZ VE MAZUR TEOREMLERİ

Bu bölümde eliptik eğriler teorisinin önemli sonuçlarından birisi olan Mordell Teoremi verilecektir. Bu teoremin ispatını Mordell, Fermat'ın alçalma metodunu kullanarak ispatlamıştır. Bu yüzden ispatın yapılabilmesi için öncelikle yükseklik (height) ve alçalma açıklanıp sonrasında dört lemma yardımıyla bu teoremin ispatı verilecektir. Sonrasında Nagell-Lutz Teoremi ve Mazur Teoremi verilerek örneklerle desteklenmiştir.

5.1. Yükseklik ve Alçalma

Tanım 5.1.1. $x = \frac{m}{n}$ rasyonel sayısı en sade şekilde yazılmış olsun. Yükseklik pay ve paydanın maksimumu olarak tanımlanır ve $H(x)$ olarak yazılır; yani,

$$H(x) = H\left(\frac{m}{n}\right) = \max\{|m|, |n|\}$$

olarak ifade edilir.

Rasyonel sayıların yüksekliği pozitif bir tamsayıdır (Silverman 1992).

Teorem 5.1.2. (Silverman 1992) Belli bir sabit sayıdan daha küçük olan bütün rasyonel sayıların kümesinin yüksekliği sonlu bir kümedir.

Tanım 5.1.3. $y^2 = f(x) = x^3 + ax^2 + bx + c$ eğrisi a, b, c katsayıları ile singüler olmayan bir eliptik eğri olsun. $P = (x, y)$ bu eğri üzerinde bir nokta olsun. P noktasının yüksekliği x koordinatına yüksekliğinin sadeleştirilmesi olarak tanımlanır ve $H(P) = H(x)$ olur (Silverman 1992).

Notasyon kaygısından dolayı yüksekliğin logaritması alınarak başka bir yükseklik tanımlansın ve bu yükseklikte $h(P) = \log H(P)$ eşitliği şeklinde gösterilsin. Logaritma fonksiyonu kullanıldığından dolayı $h(P)$ asla negatif bir reel sayı olamaz.

E bir eliptik eğri olsun. Bu eğri üzerindeki rasyonel noktalar da ayrıca sonluluk özelliğine sahiplerdir.

Tanım 5.1.4. M herhangi bir pozitif tamsayı olsun. $\{P \in E(\mathbb{Q}): H(P) \leq M\}$ kümesi sonlu bir kümedir. Bu ifade aynı zamanda $H(P)$ yerine $h(P)$ alındığında da doğrudur (Silverman 1992).

Kümedeki noktalar onların x koordinatları için sadece sonlu olasılıklara sahipler ve her bir x koordinatı için y koordinatında sadece iki olasılık vardır. Bu sonsuzda

olmayan noktaları karşılar. Sonsuzda bir nokta var ve bu nokta ∞ alındığında yüksekligi $H(\infty) = 1$ ya da eşdeğer ifade ile $h(\infty) = 0$ olarak tanımlanabilir.

Mordell teoreminin ispatı için gerekli olan dört temel lemma verilip en sonunda $E(\mathbb{Q})$ rasyonel noktaların grubunun sonlu üreteçli olduğu ispat edilecektir.

Lemma 5.1.5. (Silverman 1992) C bir eğri olsun. Her bir M reel sayısı için $\{P \in C(\mathbb{Q}): h(P) \leq M\}$ kümesi sonludur.

Lemma 5.1.6. (Silverman 1992) P_0 noktası C eğrisi üzerinde sabit rasyonel bir nokta olsun. P_0 ve a, b, c ye bağlı bir κ_0 sabiti vardır öyle ki, her $P \in C(\mathbb{Q})$ için

$$h(P + P_0) \leq 2h(P) + \kappa_0$$

olur.

Lemma 5.1.7. (Silverman 1992) κ sabiti a, b, c ye bağlı olan bir sabit olsun öyle ki, her $P \in C(\mathbb{Q})$ için

$$h(2P) \geq 4h(P) - \kappa$$

olur.

$2C(\mathbb{Q})$ notasyonu $C(\mathbb{Q})$ nun altgrubudur ve $C(\mathbb{Q})$nun noktalarının iki katından meydana gelen noktaları temsil eder.

Lemma 5.1.8. (Silverman 1992) $(C(\mathbb{Q}): 2C(\mathbb{Q}))$ indeksi sonludur.

Tanım 5.1.9. (Silverman 1992) Γ herhangi bir değişmeli grup olsun. Bu grubun m ile çarpım dönüşümü

$$\Gamma \to \Gamma$$

$$P \to \underbrace{P + P + \cdots + P}_{m-terim} = m \cdot P$$

şeklinde tanımlanır ve bu çarpım dönüşümü bir homomorfizmdir. Bu homomorfizmin görüntüsü Γ nin bir $m\Gamma$ alt grubudur.

Lemma 5.1.8. bu değişmeli grubun $\Gamma = E(\mathbb{Q})$ olduğunu söyler ve Γ içinde 2Γ alt grubu sonlu bir indekse sahiptir.

Şimdi yukarıda verilen lemmaların $E(\mathbb{Q})$ yu nasıl sonlu üreteçli olduğunu göstermesi için öncelikle Γ değişmeli bir grup olsun. Bu grup üzerinde toplam tanımlı olsun ve yükseklik fonksiyonu $h: \Gamma \to [0, \infty]$ olarak tanımlı olsun. Bu fonksiyonun yukarıda verilen dört lemmayı sağladığı kabul edilsin. Şimdi bazı hipotezler söylenip Γ'nın sonlu üreteçli olduğu ispat edilecek.

Teorem 5.1.10. (Silverman 1992) (Alçalma Teoremi) Γ değişmeli bir grup olsun. $h: \Gamma \to [0, \infty]$ a tanımlı ve aşağıdaki üç özelliği sağlayan bir fonksiyon olsun:

(i) Her bir M reel sayısı için $\{P \in \Gamma: h(P) \leq M\}$ kümesi sonludur.

(ii) Her bir $P_0 \in \Gamma$ için κ_0 sabit sayısı vardır öyle ki

$h(P + P_0) \leq 2h(P) + \kappa_0$.

(iii) Her $P \in \Gamma$ için κ sabiti vardır öyle ki

$h(2P) \geq 4h(P) - \kappa$.

Ek olarak altta verilen dördüncü şartın varlığı da kabul edilsin.

(iv) 2Γ altgrubu Γ de sonlu bir indekse sahiptir.

Bu takdirde Γ sonlu üreteçlidir.

İspat. Öncelikle Γ içinde 2Γ nin her bir kosetinin karşılıkları alınsın. Sadece sonlu sayıda kosetlerin olduğunu bildiğimizden dolayı bu kosetlerin sayısına n diyelim ve bu kosetlerin temsilcileri $Q_1, Q_2, \dots, Q_n$ olsun. Bu ifadenin anlamı aynı zamanda herhangi bir $P \in \Gamma$ için P ye bağlı bir i_0 indeksi vardır öyle ki

$$P - Q_{i_1} \in 2\Gamma$$

olur. Daha sonra P bu kosetlerin biri cinsinden yazılabilir bunun anlamı ise belli bir $P_1 \in \Gamma$ için

$$P - Q_{i_1} = 2P_1$$

yazılabileceğidir. Aynı şeyi bu kez P_1 için yapar ve buna devam edilirse

$$P_1 - Q_{i_2} = 2P_2$$

$$P_2 - Q_{i_3} = 2P_3$$

$$\vdots$$

$$P_{m-1} - Q_{i_m} = 2P_m$$

olur ve yukarıda yazılan $Q_{i_1}, Q_{i_2}, \dots, Q_{i_m}$ ifadeleri $Q_1, Q_2, \dots, Q_m$ in koset temsilcilerinden seçilsinler, ayrıca $P_1, \dots, P_m$ noktaları Γ nın elemanları olsun. P_i noktası "aşağı yukarı" $2P_{i+1}$ e eşittir. P_{i+1} in yüksekliği de P_i nin dördüncü yüksekliğine "aşağı yukarı" eşittir. Bu yüzden $P, P_1, P_2, \dots$ noktalar dizisinin yüksekliği azaltılmalı ve sınırlı yükseklikliere sahip noktaların kümelerinde son bulacak ve (i) özelliğinden dolayı küme sonlu olacak bu da ispatı tamamlayacaktır. İlk denklemden $P = Q_{i_1} + 2P_1$ ifadesini ikinci denklem olan $P_1 = Q_{i_2} + 2P_2$ de yerine yazıldığında

$$P = Q_{i_1} + 2Q_{i_2} + 4P_2$$

elde edilir ve bu şekilde devam edilirse sonucunda

$$P = Q_{i_1} + 2Q_{i_2} + 4Q_{i_3} + \cdots + 2^{m-1}Q_{i_m} + 2^m P_m$$

eşitliği elde edilmiş olur.

Sonuç olarak, P noktası Γ nın altgrubu içinde olan ve Q_i ve P_m ler tarafından üretilir. m sayısı yeterince büyük seçildiğinde P_m belli sabit bir sınırdan daha az bir yüksekliğe sahip olmaya zorlanır. Sonra yüksekliği bu sınırdan daha az olan sonlu noktaların kümesi Q_i ler ile birlikte Γ yi üretecektir.

$P, P_1, P_2, \ldots$ noktalarının dizisinin içinden bir nokta alınsın ve bu nokta P_j olsun. Burada amaç P_j nin yüksekliğinin oldukça küçük olduğunu göstermektir. Bunu yapmak için bazı değişkenleri özel isimlendirmeye ihtiyaç olacaktır. Eğer (ii) deki verilmiş olan ifadede P_0 yerine $-Q_i$ ile değiştirilirse, her $P \in \Gamma$ için bir κ_i sabiti vardır öyle ki

$$h(P - Q_i) \leq 2h(P) + \kappa_i$$

ayrıca bu her bir Q_i ve $1 \leq i \leq n_0$ için yapılabilir. Buradan yola çıkılırsa κ_i lerin en genişine κ' denilirse, her bir $P \in \Gamma$ ve bütün $1 \leq i \leq n$ için

$$h(P - Q_i) \leq 2h(P) + \kappa'$$

yazılır çünkü sadece sonlu sayıda Q_i ler vardır. Bu tek olduğundan (iv) özelliği kullanılırsa 2Γ grubu Γ içinde sonlu bir indekse sahiptir.

(iii)'den dolayı κ sabit olsun. O halde

$$4h(P_j) \leq h(2P_j) + \kappa = h(P_{j-1} - Q_{ij}) + \kappa \leq 2h(P_{j-1}) + \kappa' + \kappa$$

olarak hesaplanır ve ayrıca bu eşitlik

$$h(P_j) \leq \frac{1}{2}h(P_{j-1}) + \frac{\kappa'+\kappa}{4} = \frac{3}{4}h(P_{j-1}) - \frac{1}{4}(h(P_{j-1}) - (\kappa' + \kappa))$$

olarak yeniden düzenlenebilir. Böylelikle eğer $h(P_{j-1}) \geq \kappa' + \kappa$ ise, sonra $h(P_j) \leq \frac{3}{4}h(P_{j-1})$ olur. Bu yüzden $P, P_1, P_2, \ldots$ noktalarının dizisinin içinde P_j noktası $h(P_j) \geq \kappa' + \kappa$ eşitsizliğini sağladığı sürece, bir sonraki nokta dizi içinde küçük yüksekliğe sahiptir öyle ki

$$h(P_{j+1}) \leq \frac{3}{4}h(P_j)\,.$$

Fakat eğer bir sayı ile başlayıp $3/4$ ile çarpılırsa bu durumda sıfıra yaklaşır. Bu yüzden m indeksi bulunabilir böylelikle $h(P_m) \leq \kappa' + \kappa$ olur.

Şimdi her bir $P \in \Gamma$ elemanları için

$$P = a_1 Q_1 + a_2 Q_2 + \cdots + a_n Q_n + 2^m R$$

formu şeklinde yazılabileceği gösterilecek ve burada $a_1, \dots, a_n$ kesinlikle tamsayılar ve $R \in \Gamma$ noktası $h(R) \leq \kappa' + \kappa$ eşitliğini sağlayan belli bir noktadır. Sonuç olarak

$$\{a_1, a_2, \dots, a_n\} \cup \{R \in \Gamma : h(R) \leq \kappa' + \kappa\}$$

kümesi Γ yi üretir. (i) ve (iv) den dolayı bu küme sonludur ve buda ispatı tamamlar ve Γ sonlu üreteçlidir.

Üstte Lemma 5.1.5. in ispatı verilmişti. Şimdi Mordell teoreminin ispatında kullanılacak olan bu diğer üç teoremin ispatı verilecektir.

5.2. $P + P_0$ Yüksekliği

Bu bölümde Lemma 5.1.6'nın ispatı yapılacak bunun için öncelikle birkaç uyarı verilecektir.

Uyarı 5.2.1. Eğer $P = (x, y)$ eğri üzerinde rasyonel bir nokta ise, $e > 0$ ve $\text{obeb}(m, e) = \text{obeb}(n, e) = 1$ olmak üzere m, n, e tamsayıları için $x = \frac{m}{e^2}$ ve $y = \frac{n}{e^3}$ formundadır.

Uyarı 5.2.2. x koordinatının yüksekliği göz önünde alınsın. Eğer P noktası $P = (\frac{m}{e^2}, \frac{n}{e^3})$ gibi en küçük terimlerden verilmiş olan bir nokta ise, sonra P nin yüksekliği $|m|$ ve e^2 nin maksimumudur. Özellikle $|m| \leq H(P)$ ve $e^2 \leq H(P)$ olur. Ayrıca $H(P)$'nin terimlerinin y koordinatlarının payları da sınırlandırılabilir. a, b, c ye bağlı bir $K > 0$ tamsayısı vardır öyle ki

$$|n| \leq KH(P)^{3/2} \ .$$

Bunu ispatlamak için noktaları eliptik eğrimiz olan $y^2 = x^3 + ax^2 + bx + c$ denkleminde P noktası yerine yazılıp oluşan denklem e^6 ile çarpılırsa

$$n^2 = m^3 + ae^2m^2 + be^4m + ce^6$$

denklemi elde edilir. Bu denklemin mutlak değerleri alınıp üçgen eşitsizliği uygulanırsa

$$|n^2| \leq |m^3| + |ae^2m^2| + |be^4m| + |ce^6|$$
$$\leq H(P)^3 + |a|H(P)^3 + |b|H(P)^3 + |c|H(P)^3$$

elde edilir ve burada da $K = \sqrt{1 + |a| + |b| + |c|}$ alınabilir.

Şimdi Lemma 5.1.6. nın ispatına geçilebilir.

Lemma 5.1.6'ın İspatı. Bu lemmanın ispatında iki noktanın toplamı yazılıp üçgen eşitsizliği uygulanmıştır. Eğer $P_0 = \infty$ ise sonuç Uyarı 5.2.1'den dolayı aşikardır, bu yüzden $P_0 \neq \infty$ olsun ve $P_o = (x_0, y_0)$ olsun. κ_o'ın varlığının ispatı için belli bir sonlu küme içindekiler dışında kalan bütün P'ler için eşitsizliğin sağlandığını

ispatlamak yeterlidir, çünkü herhangi bir sonlu sayı olan P için farka bakılabilir ve bu fark $h(P+P_0)-2h(P)$ olsun ve κ_0 sayısını meydana gelen sonlu sayı değerlerinden daha büyük alınabilir. Buna sahipse de $P \notin \{P_0, -P_0, \infty\}$ ile bütün P noktaları için Lemma 5.1.6'yı ispatlamak yeterlidir.

$P=(x,y)$ olsun. P_0 ve $-P_0$ olasılıklarından kaçmak adına $x \neq x_0$ olsun, aksi takdirde bir noktanın iki katına götüren nokta toplamında sıkıntı çıkabilir ve böylelikle $P+P_0=(\xi,\eta)$ yazılabilir. $P+P_0$ nın yüksekliğini elde edebilmek için ξ'nin yüksekliği hesaplanmalı ve (x,y) ve (x_0,y_0) ın kullanıldığı ξ formülü

$$\xi + x + x_0 = \lambda^2 - a \quad , \quad \lambda = \frac{y-y_0}{x-x_0}$$

olarak bulunur. Bu ifadeler yerine yazıp düzenlenirse

$$\xi = \frac{(y-y_0)^2}{(x-x_0)^2} - a - x - x_0 = \frac{(y-y_0)^2-(x-x_0)^2(x+x_0+a)}{(x-x_0)^2}$$

elde edilir.

Eğer bunun dışındakilerin hepsini çarparsak, sonra paydaların içinde y^2-x^3 görünen yerlere P eğri üzerinde bir nokta olduğundan dolayı ax^2+bx+c ile yer değiştirilebilir. Bu verilen ifade ile düzenlendiğinde A,B,C,D,E,F,G belirli rasyonel sayıları a,b,c ve (x_0,y_0) terimleri ile ifade edildiğinde

$$\xi = \frac{Ay+Bx^2+Cx+D}{Ex^2+Fx+G}$$

şeklinde ifade edilen $P=(x,y) \notin \{P_0,-P_0,\infty\}$ noktası için $P+P_0$ ın x koordinatı elde edilir. A,B,C,D,E,F,G en küçük ortak paydaları tarafından pay ve paydanın çarpımı ile bu sayıların hepsinin tamsayılar olduğu düşünülür. Bu eşitlik her P noktası için doğru olduğundan dolayı $x=\frac{m}{e^2}$ ve $y=\frac{n}{e^3}$ yerine yazılır ve e^4 ile çarpılırsa

$$\xi = \frac{Ane+Bm^2+Cme^2+De^4}{Em^2+Fme^2+Ge^4}$$

eşitliği elde edilir. Bunun en küçük terim olduğunu bilmiyoruz ama çıkartma sadece yüksekliği küçültebilir, bu yüzden

$$H(\xi) \leq \max\{|Ane+Bm^2+Cme^2+De^4|, |Em^2+Fme^2+Ge^4|\}$$

eşitsizliği yazılabilir. Böylelikle yukarıda verilen eşitsizlikten K sadece a,b,c ye bağlı olmak üzere

$$e \leq H(P)^{1/2} \quad , \quad n \leq KH(P)^{3/2} \quad , \quad m \leq H(P)$$

ifadeleri yazılabilir. Bunlar yardımıyla üçgen eşitsizliği kullanıldığında

$$|Ane+Bm^2+Cme^2+De^4| \leq |Ane|+|Bm^2|+|Cme^2|+|De^4|$$

$$\leq (|AK| + |B| + |C| + |D|)H(P)^2$$

ve

$$|Em^2 + Fme^2 + Ge^4| \leq |Em^2| + |Fme^2| + |Ge^4| \leq (|E| + |F| + |G|)H(P)^2$$

elde edilir. Sonuç olarak

$$H(P + P_0) = H(\xi) \leq \max\{|AK| + |B| + |C| + |D|, |E| + |F| + |G|\}\, H(P)^2.$$

Her iki tarafın logaritması alındığında $\kappa_0 = \log \max\{|AK| + |B| + |C| + |D|, |E| + |F| + |G|\}$ sabiti a, b, c ve (x_0, y_0) a bağlı ayrıca $P = (x, y)$ noktasna bağlı olmamak üzere

$$h(P + P_0) \leq 2h(P) + \kappa_0$$

eşitsizliğini verir. Bu eşitsizlik de Lemma 5.1.6'nın ispatını tamamlar.

Bu lemma ile $P + P_0$ toplamının yüksekliğinin P nin yüksekliğinin iki katından daha küçük olduğunu ispatlar.

5.3. Kullanışlı Bir Homomorfizma

Lemma 5.3.1. (Silverman 1992) $2E(\mathbb{Q})$ alt grubunun $E(\mathbb{Q})$ içinde sonlu indekse sahiptir.

Bu kısım Mordell teoreminin hemen göze çarpmayan kısmını oluşturur. Notasyon açısından gösterimin rahat olması için $C(\mathbb{Q}) = \Gamma$ olarak alınsın.

$f(x)$ fonksiyonun x_0 adlı reel bir kökü olsun yani $f(x_0) = 0$ ve f tamsayı katsayılı bir polinom olsun. Koordinatları değiştirerek $(x_0, 0)$ noktasını orijine hareket ettirilebilir. Bu Γ grubunu etkilemez. Yeni koordinatlar ile eğri a, b tamsayılar olmak üzere

$$C: y^2 = f(x) = x^3 + ax^2 + bx$$

olur. $T = (0,0)$ noktası bu eğri üzerinde rasyonel bir noktadır ve $2T = \infty$ şartını da sağlar. f nin daha önce verilen formülüne göre diskriminantı $D = b^2(a^2 - 4b)$ olur. Burada eğrinin singüler olmadığı varsayılıyor. $(\Gamma: 2\Gamma)$ indeksi ya da denk olarak $\Gamma/2\Gamma$ bölümünün mertebesi ile ilgilenileceğinden dolayı, $P \to 2P$ dönüşümünü bilmek faydalı olacaktır. Bir noktayı iki katına götüren dönüşüm dördüncü dereceden değerleri içine alır çünkü $2P$ nin x kordinatını veren rasyonel fonksiyon P deki x kordinatının içinde derecesi dörttür. $P \to 2P$ ye dönüşümü kolayca ele alınabilen derecesi iki olan iki dönüşümün bileşkesi olarak yazılabilir ama bu iki dönüşüm C den kendisine olmayacak, $\bar{a} = -2a$ ve $\bar{b} = a^2 - 4b$ olmak üzere C den $\bar{C}$ eğrisine tanımlı dönüşüm olsun ve eğri $\bar{C}: y^2 = x^3 + \bar{a}x^2 + \bar{b}x$ olsun. Anı şeyler tekrar edilirse $\bar{\bar{a}} = -2\bar{a} = 4a$ ve $\bar{\bar{b}} = \bar{a}^2 -$

$4\bar{b} = 4a^2 - 4(a^2 - 4b) = 16b$ olmak üzere yeni eğri $\bar{\bar{C}}: y^2 = x^3 + \bar{\bar{a}}x^2 + \bar{\bar{b}}x$ olur. İfadeler yerine yazıldığında eğri $\bar{\bar{C}}: y^2 = x^3 + \bar{\bar{a}}x^2 + \bar{\bar{b}}x = x^3 + 4ax^2 + 16bx$ olur ve bu eğri C eğrisi ile tamamen aynıdır sadece $x \to 4x$ ve $y \to 8y$ ile değiştirilip denklem 64'e bölünmüştür. Sonuç itibariyle $\bar{\bar{C}}$ üzerindeki rasyonel noktaların $\bar{\bar{\Gamma}}$ grubu C üzerindeki rasyonel noktaların Γ grubuna izomorftur. Öncelikle $\phi: C \to \bar{C}$ ye dönüşümü tanımlansın ve grup homomorfizması olsun ayrıca $\bar{\Gamma}$ rasyonel noktaları içindeki Γ nın rasyonel noktalarını taşısın. Sonra, aynı şekilde bir $\psi: \bar{C} \to \bar{\bar{C}}$ ye bir dönüşüm olsun. Burada $\psi \circ \phi: C \to C$ birleşimi bir homomorfizma olsun ve bu homomorfizma iki tarafından çarpılanları dışarı atsın.

$\phi: C \to \bar{C}$ üstteki benzer şekilde tanımlansın. Eğer $P = (x, y) \in C$ noktası $x \neq 0$ şartını sağlayan bir nokta ise, sonra $\phi(x, y) = (\bar{x}, \bar{y})$ noktasını veren formül $\bar{x} = x + a + \frac{b}{x} = \frac{y^2}{x^2}$ ve $\bar{y} = y\left(\frac{x^2 - b}{x^2}\right)$ olur.

ϕ iyi tanımlıdır. Bunun görülebilmesi için $\bar{x}$ ve $\bar{y}$ nin $\bar{C}$ denklemini sağladığı görülmelidir, yani

$$\bar{x}^3 + \bar{a}\bar{x}^2 + \bar{b}\bar{x} = \bar{x}\left(\bar{x}^2 - 2a\bar{x} + (a^2 - 4b)\right)$$

$$= \frac{y^2}{x^2}\left(\frac{y^4}{x^4} - 2a\frac{y^2}{x^2} + (a^2 - 4b)\right) = \frac{y^2}{x^2}\left(\frac{(y^2 - ax^2)^2 - 4bx^4}{x^4}\right)$$

$$= \frac{y^2}{x^6}((x^3 + bx)^2 - 4bx^4) = \left(\frac{y(x^2 - b)}{x^2}\right)^2 = \bar{y}^2 .$$

Sonuç olarak bu ϕ dönüşümünü tanımlar ve $T = (0,0)$ ve ∞ noktası haricindeki bütün noktaları tanımlar. Burada $\phi(T) = \bar{\infty}$ ve $\phi(\infty) = \bar{\infty}$ şartları ekleyerek tanım tamamlansın.

Teorem 5.3.2. (Silverman 1992) C ve $\bar{C}$ eliptik eğriler olsun. $\bar{a} = -2a$ ve $\bar{b} = a^2 - 4b$ olmak üzere $C: y^2 = x^3 + ax^2 + bx$ ve $\bar{C}: y^2 = x^3 + \bar{a}x^2 + \bar{b}x$ olarak eğriler tanımlansın. $T = (0,0) \in C$ olsun.

(i) $\phi: C \to \bar{C}$ bir homomorfizma vardır ve

$$\phi(P) = \begin{cases} \left(\frac{y^2}{x^2}, \frac{y(x^2 - b)}{x^2}\right) & , eğer\ P = (x, y) \neq \infty, T \\ \bar{\infty} & , eğer\ P = \infty\ ya\ da\ P = T \end{cases}$$

olarak tanımlansın ve ϕ nin çekirdeği $\{\infty, T\}$dir.

(ii) $\bar{C}$ yi bazı işlemlerden geçirildiğinde $\bar{\phi}: \bar{C} \to \bar{\bar{C}}$ dönüşümü elde edilir. $\bar{\bar{C}}$ eğrisi C ye $(x, y) \to \left(\frac{x}{4}, \frac{y}{8}\right)$ dönüşümü üzerinden izomorfiktir. $\psi: \bar{C} \to C$ ayrıca bir homomorfizma vardır ve

$$\psi(\bar{P}) = \begin{cases} \left(\frac{\bar{y}^2}{\bar{x}^2}, \frac{\bar{y}(\bar{x}^2 - \bar{b})}{8\bar{x}^2}\right) & , eğer\ \bar{P} = (\bar{x}, \bar{y}) \neq \bar{\infty}, \bar{T} \\ \bar{\infty} & , eğer\ \bar{P} = \bar{\infty}\ ya\ da\ \bar{P} = \bar{T} \end{cases}$$

olarak tanımlansın. $\psi \circ \phi: C \to C$ birleşimi $\psi \circ \phi(P) = 2P$ olan bir çarpımdır.

Lemma 5.3.1'in ispatına dönülecek olunursa eğer $(\bar{\Gamma}: \phi(\Gamma))$ indeksinin sonlu olduğu ispatlanabilirse, böylelikle ayrıca $(\Gamma: \psi(\bar{\Gamma}))$ indeksi de sonludur. $\bar{b} = a^2 - 4b$ nin farklı asal çarpanlarının sayısı s olduğunda $(\bar{\Gamma}: \phi(\Gamma) \leq 2^{s+1}$ ve ayrıca b nin farklı asal çarpanlarının sayısı r olduğunda $(\Gamma: \psi(\bar{\Gamma})) \leq 2^{r+1}$ olduğu gösterilecek. Bunların birini göstermek yeterlidir, bu yüzden sadece ikincisi ispatlanacak. Kolayca görülebilir ki $\psi(\bar{\Gamma})$ kümesi $(x, y) \in \Gamma$ noktalarının kümesidir öyle ki $x \neq 0$ rasyonel bir tamkaredir. Bu küme ∞ ve eğer b bir tam kare ise ayrıca T ile birlikte bir kümedir. İspatı yapabilmek için $\Gamma/\psi(\bar{\Gamma})$ bölüm grubundan sonlu bir gruba monomorfizm bulunmalı.

$\mathbb{Q}^*$ sıfırdan farklı rasyonel sayıların çarpımsal grubunu temsil etsin. Ek olarak, $\mathbb{Q}^{*2}$ grubu $\mathbb{Q}^*$ elemanlarının tamkaresinin altgrubu olarak gösterilsin ve $\mathbb{Q}^{*2} = \{u^2: u \in \mathbb{Q}^*\}$ olsun.

Böylece bir $\alpha: \Gamma \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ ye bir dönüşüm tanımlansın ve

$\alpha(\infty) \equiv 1\ (mod\ \mathbb{Q}^{*2})$,

$\alpha(T) \equiv b\ (mod\ \mathbb{Q}^{*2})$,

ve eğer $x \neq 0$ ise

$\alpha(x, y) \equiv x\ (mod\ \mathbb{Q}^{*2})$

olarak belirleniyor olsun. Bu dönüşümün bir homomorfizma belirttiği ve α nın çekirdeğinin kesinlikle ψ nin görüntüsü olduğu iddia ediliyor.

Teorem 5.3.3. (Silverman 1992)

(i) $\alpha: \Gamma \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ yukarıda tanımlanan dönüşümü homomorfizmdir.

(ii) α nın çekirdeği $\psi(\bar{\Gamma})$ nin görüntüsüdür ve sonuç olarak α dönüşümü $\frac{\Gamma}{\psi(\bar{\Gamma})} \hookrightarrow \frac{\mathbb{Q}^*}{\mathbb{Q}^{*2}}$ ye 1-1 bir homomorfizm tanımlar.

(iii) $p_1, p_2, \dots, p_n$ asalları birbirinden farklı olsun ve b sayısını bölsünler. Sonra α nın görüntüsü $\mathbb{Q}^*/\mathbb{Q}^{*2}$ nin $\{\pm {p_1}^{\varepsilon_1}{p_2}^{\varepsilon_2} \dots {p_n}^{\varepsilon_n} : her\ bir\ \varepsilon_i\ 0\ ya\ da\ 1\}$ elemanlarını içeren alt grubunu kapsar.

(iv) $(\Gamma : \psi(\bar{\Gamma}))$ indeksi en çok 2^{t+1} dir.

Lemma 5.3.1'in ispatını tamamlanabilmesi için son olarak bir lemma daha verilmelidir. Böylece Γ içinde 2Γ nin sonlu bir indekse sahip olduğu gösterilecektir.

Lemma 5.3.4. (Silverman 1992) A, B abelyan gruplar olsun ve $\phi: A \to B$ ve $\psi: B \to A$ ya iki tane homomorfizma ele alınsın. Her $a \in A$ için $\psi \circ \phi(a) = 2a$ ve her $b \in B$ için $\phi \circ \psi(b) = 2b$ olduğu kabul edilsin.

Buna ek olarak $\phi(A)$, B kümesi içinde ve $\psi(B)$, A kümesi içinde sonlu bir indekse sahip olsun. Sonra $2A$, A içinde sonlu bir indekse sahiptir ve indeks

$$(A: 2A) \leq (A: \psi(B))(B: \phi(A))$$

eşitsizliğini sağlar.

Teorem 5.3.5. (Mordell 1922) E eliptik eğrisi singüler olmayan a, b tamsayılı katsayıları olan bir eğri olsun ve $y^2 = x^3 + ax^2 + bx$ olarak tanımlansın. $E(\mathbb{Q})$ rasyonel sayıların grubu sonlu üreteçli abelyan bir gruptur.

İspat. Yukarıda verilen dört lemmanın sonucu olarak açıktır.

Böylece $E: y^2 = x^3 + ax^2 + x$ eğrisi üzerindeki rasyonel noktaların grubu Γ sonlu üreteçlidir. Bu yüzden cebirin temel teoremi gereği uygulanabilir. Aşağıdaki tanımı verelim.

Tanım 5.3.6. Mordell teoreminden dolayı r negatif olmayan bir tamsayı ve $E(\mathbb{Q})_{tors}$, $E(\mathbb{Q})$ içinde sonlu mertebeli elemanların altgrubu olsun. O halde

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{tors}$$

yazılabilir. Bu alt grup $E(\mathbb{Q})$ nin torsiyon altgrubu olarak tanımlanır. r sayısı E eğrisinin rankı olarak adlandırılır ve $rank(E)$ olarak yazılır (Washington 2003).

Daha açık bir şekilde yazılmak istenirse, $\mathbb{Z}$ tamsayıların toplamsal gruplarını temsil etsin ve $\mathbb{Z}_m$ ifadesi $mod\ m$ tamsayılarının $\mathbb{Z}/m\mathbb{Z}$ devirli gruplarını ifade etsin. Böylece Mordell teoreminden

$$E(\mathbb{Q}) \cong \underbrace{\mathbb{Z} \oplus \mathbb{Z} \oplus \dots \oplus \mathbb{Z}}_{r-tane} \oplus \mathbb{Z}_{{p_1}^{v_1}} \oplus \mathbb{Z}_{{p_2}^{v_2}} \oplus \dots \oplus \mathbb{Z}_{{p_s}^{v_s}}$$

yazılabilir.

Şimdi Lutz ve Nagell tarafından birbirinden bağımsız olarak verdiği aşağıdaki teoremi verelim.

Teorem 5.3.7. (Nagell 1935, Lutz 1937) E eliptik eğrisi $y^2 = x^3 + ax + b$ olsun. Eğer $(x, y) \in E(\mathbb{Q})_{tors}$ ve $(x, y) \neq \infty$ ise, bu takdirde

▪ $x, y \in \mathbb{Z}$

▪ ya $y = 0$ ya da y^2 sayısı Δ yı böler.

Örnek 5.3.8. $E: y^2 = x^3 - x$ olsun. O halde $\bar{E}: y^2 = x^3 + 4x$ olur. Burada $a = 0$ ve $b = -1$ şeklindedir. İlk olarak b yi olabilecek bütün çarpım durumları göz önüne alınırsa iki durum oluşur ve bunlar

$$-1 = (-1)\times 1 \quad , \quad -1 = 1\times(-1)\,.$$

Sonuç olarak, b_1 sadece ± 1 olabilir. $\alpha(\infty) = 1$ ve $\alpha(T) = b = -1$ olduğundan dolayı

$$\alpha(\Gamma) = \{\pm 1 \ (mod\ \mathbb{Q}^{*2})\}$$

iki elemanlı bir grup olduğu görülür. Bir sonraki aşamada $\bar{\alpha}(\bar{\Gamma})$ hesaplanmalı, bu yüzden $\bar{E}: y^2 = x^3 + 4x$ eğrisi kullanılmalıdır.. Şimdi $\bar{b} = 4$ bir çok çarpımsal değere sahiptir bu yüzden

$$b_1 = 1, -1, 2, -2, 4, -4$$

sayıları seçilebilir. Fakat $4 \equiv 1\ (mod\ \mathbb{Q}^{*2})$ ve $-4 \equiv -1\ (mod\ \mathbb{Q}^{*2})$, bu yüzden $\bar{\alpha}(\bar{\Gamma})$ en çok dört elemana $\{\pm 1, \pm 2\}$ ye sahip olabilir. Tabiki her zaman $\bar{b} \in \bar{\alpha}(\bar{\Gamma})$'dir, fakat bu durumda $\bar{b} = 4$ bir tamkaredir bu yüzden bir faydası olmaz böylelikle dört denklem elde edilir öyle ki;

(i) $N^2 = M^4 + 4e^4$

(ii) $N^2 = -M^4 - 4e^4$

(iii) $N^2 = 2M^4 + 2e^4$

(iv) $N^2 = -2M^4 - 2e^4$

$N^2 \geq 0$ olduğundan dolayı ve $M = 0$ ile çözüme mümkün olmayacağı için (ii) ve (iv) denklemlerinin tamsayılar içinde çözümleri yoktur, çünkü sol tarafları negatiftir ve $M \neq 0$ iken çözüm bulunamaz. (i) denklemi $(M, e, N) = (1,0,1)$ aşikar çözümüne sahiptir ve bu da $1 \in \bar{\alpha}(\bar{\Gamma})$ ye karşılık gelir, bu yüzden yeni bir çözüm değil. Sonuç olarak, Mordell Teoremi gereği $\#\alpha(\Gamma) \cdot \#\bar{\alpha}(\bar{\Gamma})$ en azından 4 olduğunu söyler, bu yüzden bu örnek için $\in \bar{\alpha}(\bar{\Gamma})$ en azından ikinci dereceden olmalı. Böylece, (iii) denklemi bir çözüme sahiptir ve bu aşikar çözüm $2^2 = 2 \cdot 1^4 + 2 \cdot 1^4$ olur. Bu yüzden $\bar{\alpha}(\bar{\Gamma})$ ikinci mertebeye sahiptir. Sonuç olarak, Γ nin rankı sıfırdır ve $\bar{\Gamma}$ nin rankı içinde

aynıdır. Bu da C ve $\bar{C}$ üzerindeki rasyonel noktaların grubunun her ikisinin de sonlu olduğunu söyler ve bütün rasyonel noktalar sonlu mertebeye sahiptirler.

Sonlu mertebeli noktaları bulunabilmesi için Nagell-Lutz teoremi kullanılır, yani; eğer $P=(x,y)$ noktası $E(\mathbb{Q})$ içinde sonlu bir nokta ise, sonra $y=0$ ya da y sayısı $b^2(a^2-4b)=4$ ü böler. $y=0$ olan noktalar $(0,0),(-1,0)$ ve $(1,0)$ noktalarıdır ve $y=\pm 1\,, y=\pm 2$ veya $y=\pm 4$ durumları ile noktanın olmadığı aşikardır. $E: y^2=x^3-x$ eğrisi üzerindeki rasyonel noktaların grubu

$$E(\mathbb{Q})=\{\infty,(0,0),(1,0),(-1,0)\}\cong \frac{\mathbb{Z}}{2\mathbb{Z}}\oplus\frac{\mathbb{Z}}{2\mathbb{Z}}$$

olduğu ispatlanmış olur. Bu yüzden, bu kübik denklemin bütün rasyonel çözümleridir.

Benzer şekilde yine Nagell-Lutz teoreminden $\overline{E(\mathbb{Q})}$ içinde sonlu mertebeli noktalar $y=0$ ya da y sayısı $\bar{b}^2\left(\bar{a}^2-4\bar{b}\right)=-256$ ü böler. İşlemler yapıldığında sonlu mertebeli dört nokta bulunur ve

$$\overline{E_{tors}}(\mathbb{Q})=\{\infty,(0,0),(2,4),(2,-4)\}\cong\frac{\mathbb{Z}}{4\mathbb{Z}}$$

olur. Bu durumda rasyonel noktalar grubu, dördüncü dereceden devirli gruptur, çünkü $(2,4)+(2,4)=(0,0)$ dır.

Örnek 5.3.9. $E: y^2=x^3+x$ olsun. O zaman $\bar{E}: y^2=x^3-4x$ olur. Bu eğri için yukarıdaki gibi rank hesaplandığında sıfır bulunur ve rasyonel noktaların sonlu grupları

$$E(\mathbb{Q})=\{\infty,T\}\cong\frac{\mathbb{Z}}{2\mathbb{Z}}\,,$$

$$\bar{E}(\mathbb{Q})=\{\infty,(0,0),(2,0),(-2,0)\}\cong\frac{\mathbb{Z}}{2\mathbb{Z}}\oplus\frac{\mathbb{Z}}{2\mathbb{Z}}$$

şeklindedir. $e\neq 0$ için $N^2=M^4+e^4$ denkleminin herhangi bir tamsayı çözümü E eğrisi üzerinde bir rasyonel nokta verir ve bu nokta $\left(\frac{M^2}{e^2},\frac{MN}{e^3}\right)$ olur. Öncelikle Γ'nın sadece ∞ ve $(0,0)$ elemanlarına sahip olduğu biliniyor. Böylece M,N,e sayılarının hepsi sıfırdan farklı olduğunda $N^2=M^4+e^4$ denkleminin çözümü yoktur, yani; $Z^4=X^4+Y^4$ şeklinde tanımlanan Fermat denkleminin sıfırdan farklı tamsayıları için çözüme sahip değildir.

Örnek 5.3.10. $E: y^2=x^3-5x$ olsun. O zaman $\bar{E}: y^2=x^3+20x$ olur. E eğrisi için $a=0$ ve $b=-5$ olur böylece $b_1=1,-1,5,-5$ olabilir. Bunlara karşılık gelen denklemler

(v) $N^2=M^4-5e^4$

(vi) $N^2=-M^4+5e^4$

(vii) $N^2 = 5M^4 - e^4$

(viii) $N^2 = -5M^4 + e^4$

Bu denklemler toplu olarak incelendiğinde (i) ve (ii) denklemleri (iii) ve (iv) denklemleri M ile e'nin yerleri değiştirildiğinde aynı denkleme tekabül eder bu yüzden bulunan sonuçlar için şart olarak $Me \neq 0$ olmalı. Bu denklemler aynı olduklarından dolayı ilk iki denklem kullanıldığında (i) ve (ii)'nin çözümleri

$1^2 = 3^4 - 5 \cdot 2^4$

$2^2 = -(1^4) + 5 \cdot 1^4$

olur. Sonuç olarak bütün b_1 sayıları meydana gelir ayrıca çarpım metodundan $x = \frac{b_1 M^2}{e^2}$ ve $y = \frac{b_1 MN}{e^3}$ kordinatları kullanılabilir ve E eğrisi üzerindeki rasyonel noktalar $\left(\frac{9}{4}, \frac{3}{8}\right)$ ve $(-1, -2)$ elde edilir. Buradan

$\alpha(\Gamma) = \{\pm 1, \pm 5\}\ (mod\ \mathbb{Q}^{*2})$

elde edilir. $\bar{\alpha}(\bar{\Gamma})$ kümesi için $\bar{b}^2(a^2 - 4b) = 20$ olduğundan dolayı $\overline{b_1}$ için olası durumlar $\pm 1, \pm 2, \pm 4, \pm 5, \pm 10, \pm 20$ olur. Fakat, $\pm 4 = \pm(2^2)$ ve $\pm 20 = \pm(5 \cdot 2^2)$ olduğundan dolayı $\overline{b_1}$ için mutlak tamkareler $\pm 1, \pm 2, \pm 5, \pm 10$ dur.

$\overline{b_1} \cdot \overline{b_2} = \bar{b} = 20$ olduğundan dolayı $\overline{b_1}$ ve $\overline{b_2}$ aynı işaretli olmalı. Eğer bu sayıların her ikisi de negatif ise denklem $N^2 = \overline{b_1} M^4 + \overline{b_2} e^4$ sıfırdan farklı rasyonel çözüme sahip değildir çünkü sıfırdan farklı reel çözümleri çiftlerine sahip değildir. Bu yüzden

$\bar{\alpha}(\bar{\Gamma}) \subseteq \{1,2,5,10\ (mod\ \mathbb{Q}^{*2})\}$

olur. O halde $\bar{\alpha}(\infty) = 1$ ve $\bar{\alpha}(\bar{T}) = \bar{b} = 20 \equiv 5\ (mod\ \mathbb{Q}^{*2})$ elemanlarının ikiside $\bar{\alpha}(\bar{\Gamma})$ içindedir. Diğer olan iki sayı ele alındığında $\bar{\alpha}(\bar{\Gamma})$ grubu $\mathbb{Q}^*/\mathbb{Q}^{*2}$ nin bir alt grubu olduğundan dolayı 5 bu grup içinde ve 2,10 bu grupta değildir. Böylelikle,

$\bar{\alpha}(\bar{\Gamma}) = \{1,5\}\ (mod\ \mathbb{Q}^{*2})$

olur. Bunların hepsi yerine yazılırsa

$2^r = \frac{\#\alpha(\Gamma) \cdot \#\bar{\alpha}(\bar{\Gamma})}{4} = \frac{4 \cdot 2}{4} = 2$

ve bu yüzden $E(\mathbb{Q})$ nun rankı 1'dir.

Teorem 5.3.11. (Mazur 1977) E bir eliptik eğri olsun. Bu takdirde $E(\mathbb{Q})_{tors}$ aşağıdaki 15 gruptan biridir.

(i) $1 \leq n \leq 10$ ya da $n = 12$ için $\mathbb{Z}/n\mathbb{Z}$

(ii) $1 \leq m \leq 4$ için $\mathbb{Z}/2m\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Örnek 5.3.12. Örnek 5.3.8'de gösterildiği üzere, eğer eğri $y^2 = x^3 - x$ olduğunda Nagell-Lutz teoreminden aşikar olmayan rasyonel büküm noktaları için $y \in \{0, \pm 1, \pm 2\}$ özelliğine sahiptir.

Örnek 5.3.13. $t \in \mathbb{Q}$ ve $t \neq 0, -1$ ve ayrıca E eliptik eğrisi

$y^2 + (1 - t - t^2)xy + (t^2 + t^3)y = x^3 + (t^2 + t^3)x^2$

olsun. Bu eliptik eğri için; $(0,0) \in E(\mathbb{Q})$ elemanı için $7 \cdot (0,0) = \infty$ olur ve böylelikle bütün $E(\mathbb{Q})_{tors}$ altgrupları tarafından üretilir ve Mazur teoreminden böylelikle

$E(\mathbb{Q})_{tors} \cong \mathbb{Z}/7\mathbb{Z}$

yazılabilir.

6. ELİPTİK EĞRİLERİN RANKLARI ÜZERİNE ÇEŞİTLİ SONUÇLAR

E eliptik eğrisi verildiğinde $rank\,(E)$'nin nasıl hesaplanacağı önemli problemlerden biridir. Bu soru da otomatik olarak şu soruları akla getirmektedir:

▪ Hangi negatif olmayan tamsayılar bir eliptik eğrinin rankı olabilir?

▪ Bir eliptik eğrinin rankı keyfi büyüklükte olabilir mi?

▪ Rankların dağılımı nasıl?

O halde bir eliptik eğrinin rankını hesaplamayı garantileyen bir algoritma yoktur. Şans ve yeterli çalışma ile en üst sınır ve en alt sınır hesaplamak için bazı işlemler vardır. Aşağıda eliptik eğrilerin ranklarıyla ilgili rekorlar, ilgili yılları ve bulan bilim insanlarının isimleri listelenmiştir.

Rank≥	***Yıl***	***Bulanlar***
3	1945	Billing
4	1945	Wiman
6	1974	Penney &Pomerance
7	1975	Penney &Pomerance
8	1977	Gurunewald & Zimmert
9	1977	Brumer & Kramer
12	1982	Mestre
14	1986	Mestre
15	1992	Mestre
17	1992	Nagao
19	1992	Fermigier
20	1993	Nagao
21	1994	Nagao & Kouya
22	1997	Fermigier
23	1998	Martin & McMillen
24	2000	Martin & McMillen

Çizelge 6.1. Rank rekorları.

Yukarıda Tablo 2'de verilen rank rekorları tablosunda rankı en az 24 olan

$$y^2 + xy + y =$$

$$x^3 - 120039822036992245303534619191166796374x$$

$$+5042249924849106700108017991680827267594437562229114151 16$$

eliptik eğrisidir. Bu eliptik eğri üzerinde sonsuz mertebeli en az 24 nokta bulunduğu için rankının en az 24 olduğu söylenebilir. Eliptik eğrinin bir kaç bağımsız noktalarına örnek yazılırsa:

$$(2005024558054813068, -164803715834308510823488 8252)$$

$$(-4690836759490453344, -310498835257858015147445248 04)$$

$$(4700156326649806635, -662211625015842494578185974 3)$$

olur.

6.1. Birch ve Swinnerton-Dyer Konjektürü

$E: y^2 = x^3 + ax + b$ eliptik eğrisi $\mathbb{Q}$ üzerinde tanımlansın. Bu eliptik eğrinin diskriminantı $\Delta = 16(4a^3 + 27b^2)$'yı bölmeyen her p asal sayısı için eliptik eğrinin denklemi mod p'ye göre indirgenebilir ve bu eliptik eğri $\mathbb{F}_p$ sonlu cismi üzerinde yine bir eliptik eğri olur. Bu indirgeme bir $E(\mathbb{Q}) \to E(\mathbb{Z}/p\mathbb{Z})$ grup homomorfizmine neden olur.

Birch ve Swinnerton-Dyer X büyürken

$$\prod_{p<X} \frac{\#(E(\mathbb{Z}/p\mathbb{Z}))}{p} \tag{6.1}$$

değerini hesapladılar (Birch ve Swinnerton-Dyer 1965). Burada sorun çıkartan kısım ise $E(\mathbb{Q})$ nun boyutu $rank(E)$ tarafından ölçülebilir fakat $E(\mathbb{Z}/p\mathbb{Z})$ nin ortalama boyutunun ölçümü nasıl yapılabilir? Bunun için bazı hazırlıklar yapalım.

Tanım 6.1.1. Δ'yı bölmeyen her p asal asal sayısı için N_p sayısı

$$N_p = \#E(\mathbb{F}_p) = \#E(\mathbb{Z}/p\mathbb{Z})$$

$$= 1 + \#\{0 \le x, y \le p-1 : \ y^2 \equiv x^3 + ax + b \ (mod\ p)\}$$

olarak tanımlanır (Silverman 2016).

Teorem 6.1.2. (Silverman 2016) Δ'yı bölmeyen her p asal asal sayısı için

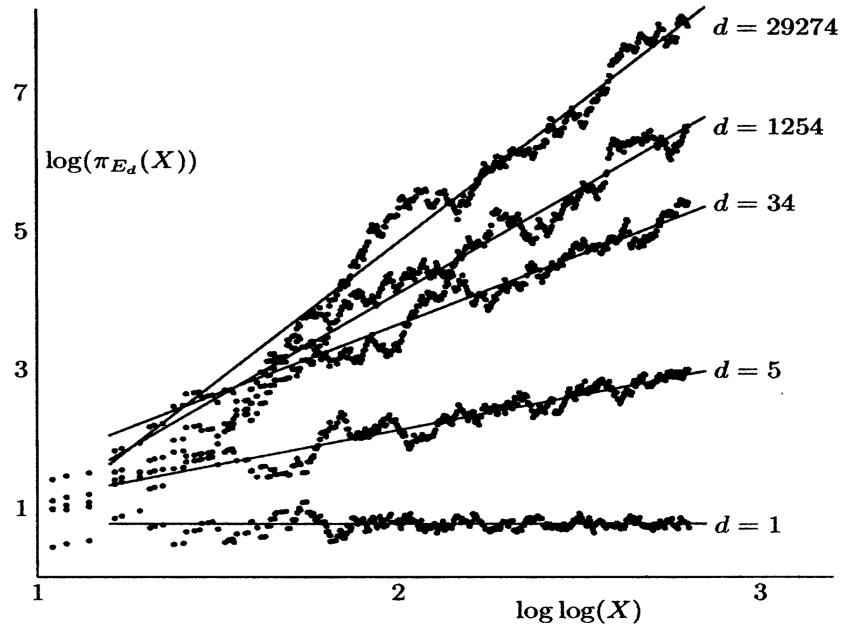
$$p + 1 - 2\sqrt{p} < N_p < p + 1 + 2\sqrt{p}$$

olur.

İddialarını test için belli bir eliptik eğri için X büyürken 1950'de Birch ve Swinnerton-Dyer (6.1) değerini hesapladılar (Birch ve Swinnerton-Dyer 1965). Bu değer kısaca

$$\pi_E(X) = \prod_{p \le X, p \nmid \Delta} \frac{N_p}{p} \tag{6.2}$$

olarak tanımlansın.



Şekil 6.1. Belli d değerleri için $y^2 = x^3 - d^2x$ için Birch ve Swinnerton-Dyer datası.

Yukarıdaki verilen Şekil 3'de Birch ve Swinnerton-Dyer'in $E_d: y^2 = x^3 - d^2x$ eğrisi için $\pi_{E_d}(X)$ değerinin X değişkeninin $1{,}5\times10^7$'ye çıkarken beş farklı eğrinin davranışını göstermektedir. Burada yatay eksen $\log(\log(X))$ ve dikey eksen $\log(\pi_{E_d}(X))$ dir.

Sadece eliptik eğriye bağlı olan belli bir C sabiti için X sonsuza giderken, bu verilerden yola çıkıldığında Birch ve Swinnerton-Dyer

$$\pi_E(X) \sim C(\log(X))^{rank(E)} \tag{6.3}$$

konjektürüne yol açtılar. $\pi_E(X)$ fonksiyonu düzgün davranmadığından üzerinde çalışmak zor olduğundan dolayı bu fonksiyonun yerine eliptik eğrinin $L-$fonksiyonu kullanılarak ilgili konjektürü elde etmişlerdir.

Tanım 6.1.3 E eğrisi verilmiş olsun. $a_p = 0$ ya da ± 1 açık bir formül olarak verilen s kompleks değişkenli bir fonksiyon olan Dirichlet serisi

$$L(E,s) = \prod_{p \nmid \Delta} \left(1 - \frac{1+p-N_p}{p^s} + \frac{p}{p^{2s}}\right)^{-1} \prod_{p \mid \Delta} \left(1 + \frac{a_p}{p^s}\right)^{-1}$$

şeklinde tanımlanır (Washington 2003).

Teorem 6.1.2'den dolayı $L(E,s)$ kompleks yarı düzleminde $\{s \in \mathbb{C}: Re(s) > {}^{3}/_{2}\}$ kümesi üzerinde mutlak ve düzgün yakınsaktır.

Teorem 6.1.4. (Washington 2003) $L(E,s)$ fonksiyonu $\mathbb{C}$'nin hepsine bir analitik sürekliliğe sahip ve $w_E = \pm 1$ ve belli bir pozitif N tamsayısı için

$$\wedge(s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(E,s)$$

olduğunda E ye bağlı bir fonksiyonel denklem

$$\wedge(s) = w_E \wedge(2-s)$$

olarak elde edilir.

Yukarıda Euler çarpımı yapılırken $L(E,s)$ için $s = 1$'de yakınsamasına ihtiyaç yoktur ama sade bir şekilde ifade edilmiş hali $s = 1$ de

$$L(E,1) \text{ "=" } \left(\prod_{p \nmid \Delta} \frac{N_p}{p} \times \prod_{p \mid \Delta} l_p(E,1)\right)^{-1}$$

şeklinde verilir. İkinci çarpımda sadece sonlu sayıda terim var olduğundan dolayı $s = 1$'in yakınında $L(E,s)$ fonksiyonunun davranışı tahmin edilebilir. Bu yüzden buluşsal olarak $E(\mathbb{Q})$ değeri büyüdükçe N_p'den daha hızlı büyüyecek ve $L(E,s)$ fonksiyonu daha hızlı bir şekilde $s \to 1$ iken sıfıra yaklaşmalıdır.

Aşağıda Clay Matematik Enstitüsü'nün milenyum problemleri arasında yer alan ve ilk doğru ispata 1 milyon dolar ödül vaat edilen Birch-Swinnerton Dyer Konjektürü'nün rank konjektürünün ifadesi verilmektedir.

Konjektür 6.1.5 (Birch ve Swinnerton-Dyer, 1965) Her E eliptik eğrisi için

$rank\ (E) = \mathrm{ord}_{s=1}\, L(E,s)$.

Bunun sonrasında Goldfeld yukarıdaki ifadede $\pi_E(X)$ ve $L(E,s)$ arasında bağlantının bir $\sqrt{2}$ çarpanı tarafından sağlandığını ispatladı.

Teorem 6.1.6. (Goldfeld 1979) $C \in \mathbb{R}^+$ ve $r \in \mathbb{R}$ sabitleri ile $\pi_E(X) \sim C(\log(X))^r$ olduğu varsayılsın. Sonra $r = \mathrm{ord}_{s=1}\, L(E,s)$ olur ve γ Euler sabiti olduğunda

$$\lim_{s \to 1} \frac{L(E,s)}{(s-1)^r} = \sqrt{2}\, e^{r\gamma} C^{-1} \prod_{p \mid \Delta} l_p(E,1)^{-1} \ .$$

Özellikle, eğer $r = 0$ ise, bu takdirde

$$L(E,1) = \sqrt{2}\left(\prod_{p\nmid\Delta}\frac{N_p}{p} \times \prod_{p\,|\Delta} l_p(E,1)\right)^{-1}$$

olur.

Tanım 6.1.7. Birch ve Swinnerton-Dyer konjektörü ile $s = 1$ noktasında $L(E,s)$ fonksiyonunun sıfırının mertebesi E eliptik eğrisinin analitik rankı olarak tanımlanır ve

$$rank_{an}(E) = \mathrm{ord}_{s=1}\, L(E,s)$$

şeklinde gösterilir (Birch ve Swinnerton-Dyer 1965).

Böylece alttaki teorem Kolyvagin, Gross ve Zagier ve diğerlerinin çeşitli çalışmaları ile Birch ve Swinnerton-Dyer konjektörünün doğrultusunda şu an için literatürde elde edilen en iyi sonuçlar verilmiştir.

Teorem 6.1.8. (Kolyvagin 1988), (Gross ve Zagier 1986)

(i) $\mathrm{ord}_{s=1}\, L(E,s) = 0 \quad \Rightarrow \quad rank\,(E) = 0$

(ii) $\mathrm{ord}_{s=1}\, L(E,s) = 1 \quad \Rightarrow \quad rank\,(E) = 1$

(iii) $\mathrm{ord}_{s=1}\, L(E,s) \geq 2 \quad \Rightarrow \quad rank\,(E) =$ bilinmiyor.

Analitik rankı 0, 1, 2 ve 3 olan eliptik eğriler için varlığı ispat edilmiş yalnız analitik rankı 3'ten büyük hesaplanmış bir eliptik eğri yoktur.

Örnek 6.1.9. Eliptik eğri olarak $y^2 = x^3 - x$ denklemi ele alındığında $\Delta = 64$'tür. Burada $l_p(E,s) = 1 + \frac{a_p}{p^s}$ iken

$$a_p = \begin{cases} 0 & , eğer\ p \equiv 3\ (mod\ 4) \\ 2n & , eğer\ p = n^2 + m^2\ için\ n\ tek\ p \equiv 1\ (mod\ 4) ile\ birlikte\ n \equiv m+1\ (mod\ 4) \end{cases}$$

olmak üzere

$$L(E,s) = \prod_{p\neq 2}\left(1 - \frac{a_p}{p^s} + \frac{p}{p^{2s}}\right)^{-1}$$

olur. Burada $L(E,1) = 0{,}65551538857302995 \ldots \neq 0$. Sonuç olarak Fermat'ın ispatladığı gibi $E(\mathbb{Q})$ sonludur ve bu eğrinin rankı sıfırdır.

Tanım 6.1.10. $w_E = \pm 1$ ile $\wedge(s) = w_E \wedge (2-s)$ fonksiyon denklemi ele alındığında

$$rank_{an}(E) = \mathrm{ord}_{s=1}\, L(E,s) =$$

$$\mathrm{ord}_{s=1} \wedge (E,s) \ \ e\text{ş}itli\breve{g}i \ \begin{cases} çift & , eğer\ w_E = +1 \\ tek & , eğer\ w_E = -1 \end{cases}$$

olarak tanımlanır.

Birch ve Swinnerton-Dyer konjektörü özellikle $rank(E)$ ve $rank_{an}(E)$ birbirine eşit olduklarını düşündükleri için BSD'nin zayıf sonucu olarak bilinen aşağıdaki konjektürü ortaya atmışlardır.

Konjektür 6.1.11. (Rubin ve Silverberg 2002) (Parite Konjektürü)

$$rank\ (E) = \begin{cases} çift & , eğer\ w_E = +1 \\ tek & , eğer\ w_E = -1 \end{cases}$$

Örnek 6.1.12. d nin içinde tam kare bulunmayan tamsayı olduğu $E_d: y^2 = x^3 - d^2x$ eliptik eğrisi ele alınmış olsun.

$$w_E = \begin{cases} +1 & , eğer\ |d| \equiv 1{,}2\ ya\ da\ 3\ (mod\ 8) \\ -1 & , eğer\ |d| \equiv 5{,}6\ ya\ da\ 7\ (mod\ 8) \end{cases}$$

Parite konjektürü $rank\ (E_d)$, d squarefree tamsayılarının yarısı için tektir (ve aynı zamanda sıfırdan farklıdır!).

Teorem 6.1.13. (Rubin ve Silverberg 2002) Eğer $p \equiv 5\ ya\ da\ 7\ (mod\ 8)$ asal ise, sonra $rank\ (E_d) = 1$ dir.

Örnek 6.1.14. $p = 157$ için $y^2 = x^3 - (157)^2x$ üzerindeki sonsuz mertebeli en sade rasyonel nokta

$$\left(-\frac{435655826106914072505519 97}{609760250665615167250729}, \frac{562653616877732252460938736830 7126580}{476144382506163554005382044222449067}\right)$$

olur.

6.2. Eliptik Eğrilerin Kuadratik Twistlerinin Rankları Üzerine

Yukarıdaki bölümde $\mathbb{Q}$ üzerinde keyfi eliptik eğrilerin rankı üzerinde düşünülmüştü. Bu haliyle problem fazlasıyla zordur. Ancak rankın yapısını anlayabilmek için eliptik eğrilerin kuadratik twist ailesinin üzerinde düşünmek faydalı olacaktır. Eliptik eğrilerin aritmetik değişkenleri olmasına rağmen belki de en sade eliptik ailesi olduğundan dolayı bu bölümde kuadratik twistler üzerinde duruldu.

d	r_d	*Bulan*	$x-$*koordinatında bağımsız noktalar*
1	0	Fermat(~1640)	
5	1	Billing (1937)	9
34	2	Wiman (1945)	$17, \frac{17}{8}$
1254	3	Wiman (1945)	$\frac{11}{8}, \frac{22}{3}, \frac{19}{8}$
29274	4	Wiman (1945)	$\frac{41}{34}, \frac{24}{17}, \frac{34}{7}, \frac{121}{2}$
205015206	5	Rogers (2000)	$\frac{649}{323}, \frac{1650}{1121}, \frac{326}{323}, \frac{19234}{8993}, \frac{5783298}{2468041}$
61471349610	6	Rogers (2000)	$\frac{779}{134}, \frac{52441}{31691}, \frac{228001}{931}, \frac{21033}{10658}, \frac{56416}{32761}, \frac{4427538}{2255}$

Çizelge 6.2. $dy^2 = x^3 - x$ ailesi için ranklar.

Tanım 6.2.1. $E: y^2 = x^3 + ax + b$ eliptik eğrisi $a, b \in \mathbb{Q}$ olsun ve d sıfırdan farklı bir rasyonel sayı olsun. d tamsayısı ile oluşturulan eliptik eğri yani quadratik twisti $E_d: y^2 = x^3 + ad^2x + bd^3$ olur. Bu eğride $(x, y) \rightarrow (dx, d^2y)$ değişkenleri ile değiştirildiğinde, E_d eğrisi tekrar yazılabilir ve bu eğri

$$E_d: dy^2 = x^3 + ax + b$$

eğrisi ile izomorfiktir yani diğer bir deyişle eşittir (Rubin ve Silverberg 2002).

Değişkenler değiştirildiğinde kuadratik twist denklemi $dy^2 = x^3 + ax + b$ olarak yazılabilir ve burada d tamsayısının içinde tam kare bulunmayan tam sayı olduğu farzedilir. E ve E_d rasyonel sayılar üzerinde izomorfik olmadıklarından dolayı $E(\mathbb{Q})$ ve $E_d(\mathbb{Q})$ çok farklı olabilir. Bu bölümde d rasyonel sayısı değişirken $rank\,(E_d)$'nin davranışı incelenecektir. E_{dt^2} eğrisi her $t \in \mathbb{Q}^x$ için E_d eğrisine izomorfik olduğundan dolayı d içinde tam kare bulunmayan tamsayıları üzerinde düşünülmesi yeterlidir.

$y^2 = x^3 - x$ eğrisi için geniş bir şekilde çalışıldığından dolayı bu bölümün diğer kısımlarında bu eliptik eğri alınarak ve bu eliptik eğrinin quadratik twisti üzerinde durularak çalışmalar yapılmıştır. Bu $dy^2 = x^3 - x$ ailesi üç kenarının uzunlukları rasyonel sayı ve alanı tamsayı olan dik üçgenlerin varlığı problemi olan "Denk Sayı Problemi" ile yakından bağlantılıdır. Bu problem ile bu kuadratik twist ailesinin arasındaki ilişki ise "$rank(E_d) > 0$ ancak ve ancak d bir denk sayıdır" olmasıdır.

Ayrıca, eliptik eğride $(x, y) \to (-x, y)$ ile değiştirildiğinde E_d ve E_{-d} eliptik eğrilerinin izomorfik olduğu açıkça görüldüğünden dolayı d rasyonel sayısı sınırlandırılıp $d > 0$ olarak ele alınsın.

E_{157} eliptik eğrisi ele alındığında sonsuz mertebeli en sade noktası

$$\left(-\frac{277487787329244632169121}{609760250665615167250729}, \frac{228266305682897166312876541591264 20}{476144382506163554005382044222449067}\right).$$

Teorem 6.2.2. (Rubin ve Silverberg 2002) Eğer d asal sayı ise, E_d'nin rankının üst sınırı d sayısının tek asal bölenlerinin ikişer kez olanlarından verilir ve bir C mutlak sabit vardır öyle ki $|d| > 2$ şartı ile bütün içinde tam kare bulunmayan d sayıları için

$$rank\ (E_d) \leq C\,\frac{\log|d|}{\log\log|d|}$$

olur ve bu eşitsizlik E_d eliptik eğrisinin rankı için aşikar sınır olarak bilinir.

Ayrıca E_d eliptik eğrisi büyük ranka sahipse aynı zamanda d sayısı da bir çok asal bölene sahiptir. Tablo 2'de en son verilen d ele alınırsa $61471349610 = 2 \cdot 3 \cdot 5 \cdot 11 \cdot 19 \cdot 41 \cdot 43 \cdot 67 \cdot 83$ olur.

6.3. Kuadratik Twist Ailesinin Ranklarının Değişimi

Bu bölümde eliptik eğrilerden oluşturulmuş olan kuadratik twistlerin ranklarının dağılımları konusuna değinilecek yani E eliptik eğrimiz sabit olsun. d tamsayısı değişirken $rank\ (E_d)$ nin dağılımı üzerinde çalışmak istiyoruz.

Tanım 6.3.1. $S(X) = \{\, d \in \mathbb{Z}\ içinde\ tam\ kare\ bulunmasın : |d| \leq X\}$ olsun. Böylelikle aşağıdakiler tanımlansın:

i) Ortalama rank eğer limit varsa

$$Avg\ (E) = A(E) = \lim_{X\to\infty} \frac{\sum_{d\in S(X)} rank\ (E_d)}{\#S(X)}$$

olarak tanımlanır. Ayrıca üst ve alt ortalama rank sırasıyla $\bar{A}(E)$ ve $\underline{A}(E)$ olarak ifade edilir ve bunlarda sırasıyla lim sup ve lim inf e karşılık gelir.

ii) * sembolü "2", "tek", "$\geq$ 3" gibi olduğu yerlerde

$$N_*(E, X) = \#\{d \in S(X) : rank\ (E_d) * dır$$

şeklinde tanımlanır ve burada kısalık açısından $N(X) = N_{\geq 0}(X) = \#S(X)$ olarak yazılsın.

iii) Yoğunluk eğer limit varsa, $Dens_*(E) = D_*(E) = \lim_{X\to\infty} N(X)$ şeklinde tanımlansın. Ayrıca $\overline{D}_*(E)$ ve $\underline{D}_*(E)$ olarak ifade edilir ve bunlarda sırasıyla lim sup ve lim inf e karşılık gelir (Rubin ve Silverberg 2002).

Teorem 6.3.4. (Rubin ve Silverberg 2002) Parite Konjektürü sağlandığı kabul edilsin. Bu takdirde

(i) $Dens_{çift}(E) = {}^{1}/_{2}$ ve $Dens_{tek}(E) = {}^{1}/_{2}$.

(ii) $Avg\ (E) \geq {}^{1}/_{2}$.

Konjektür 6.3.5. (Goldfeld 1979) $Avg\ (E) = A(E) = \lim_{X\to\infty} \frac{\sum_{d\in S(X)} rank\ (E_d)}{\#S(X)} = {}^{1}/_{2}$ olur.

Goldfeld Konjektürü ortalama rankın Parite Konjektürü'nün izin verdiği ranktan daha küçük olduğunu söyler ve Goldfeld konjektürü ile Parite Konjektürü birleştirildiğinde aşağıdaki konjektür bulunur ve daha kolay bir sonuç olur.

Konjektür 6.3.6. (Rubin ve Silverberg 2002) (Yoğunluk Konjektürü)

$Dens_0(E) = Dens_1(E) = {}^{1}/_{2}$, $Dens_{\geq 2}(E) = 0$

Ek olarak, $N(X) \sim \frac{2}{\zeta(2)} X = \frac{12}{\pi^2} X$. Yoğunluk konjektürü

$N_0(X) \sim N_1(X) \sim \frac{6}{\pi^2} X$, $N_{\geq 2}(X) = o(X)$

olduğunu belirtir.

Konjektür 6.3.7. (Rubin ve Silverberg 2002) $b_E \neq 0$ şartı ile b_E ve e_E tamsayıları vardır öyle ki

$\lim_{X\to\infty} \frac{N_{\geq 2, çift}(X)}{X^{3/4} \log(X)^{e_E}} = b_E$.

Heath-Brown eğer $y^2 = x^3 - x$ eliptik eğrisi ele alınır ve d tek tamsayıları ile twistler kısıtlanırsa, en azından r rankı ile twistler yoğunluğu r ile en azından üstsel olarak sıfıra gider. Bundan dolayı, r nin küçük değerleri için ortalama rank için bir üst sınır ve yoğunluklar $\underline{D_r}(E)$ için alt sınırların sonuçları çıkarılabilir.

Teorem 6.3.8. (Heath-Brown 1994) E eğrisini sabitleyip $y^2 = x^3 - x$ olsun. $Avg^0(E)$ ve $Dens_*{}^0(E)$ ifadeleri ortalama ve yoğunluğun tek sayıların d ye kısıtlanışını ifade ediyor olsun. Bu takdirde

(i) $\overline{Avg}^0(E) \leq 1{,}2645$

(ii) $r \geq 0$ için $\overline{Dens}_r(E) \leq 1{,}7313 \cdot 2^{-(r^2-r)/2}$

(iii) $\underline{Dens}_0(E) > 0{,}044$

(iv) Üstelik Parite Konjektürü sağlanıyorsa, bu takdirde $\underline{Dens}_1(E) > 0{,}26$ olur.

KAYNAKLAR

Asar, A.O., Arıkan, A. ve Arıkan, A., "Cebir", ***Gazi Kitapevi***, (2012).

Birch, B., Swinnerton–Dyer, H., P., F., Notes on elliptic curves II. ***J. Reine Angew. Math.***, 218: 79–108, (1965),

E. Lutz, Sur l'equation $y^2 = x^3 - Ax - B$ dans les corps p-adic, ***J. Reine Angew. Math.*** 177, 238-247, (1937),

Goldfeld, D., In Number theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979), 751,108-118. ***Springer, Berlin***, (1979),

Gross, B., H., Zagier, D., B., H., "Points and Derivatives of L-Series." ***Invent. Math***. 84(2): 225–320 (1986).

Heath Brown, R., The size of Selmer groups for the congruent number problem, II, ***Invent. Math.***, 118 331-370. (1994),

Kaya, R. , Projektif Geometri, ***Osmangazi Üniversitesi Yayınları***, Eskişehir(2005)

Koblitz, N. , Introduction to Elliptic Curves and Modular Forms, ***Springer***, USA (1993),

Kolyvagin, V., A., "The Mordell-Weil and Shafarevich-Tate groups for Weil Elliptic Curves" ***Izv. Akad. Nauk SSSR Ser. Math.,*** 52(6): 1154-1180 (1988),

Mordell, L. J., On the rational solutions of the indeterminate equation of the third and fourth degrees, ***Proc. Cambridge Philos. Soc.*** 21, 179-192, (1922),

Mazur, B., Modular curves and the Eisenstein ideal, ***Publ. Math. IHES***, 47, 33-186, (1977),

Nagell, T., Solution de quelque problèmes dans la théorie arithmétique des cubiques planes du premier genre, ***Wid. Akad. Skrifter Oslo*** I No.1, 1-25, (1935),

Rubin ve Silverberg 2002, "Ranks of Elliptic Curves", ***Bulletin of the American Mathematical Society***, 39, 4, 455-474, (2002),

Silverman, J. H. , Tate , J. , "Rational Points on Elliptic Curves", ***Springer***, USA(1992),

Silverman, J.H. , The Aritmetic of Elliptic Curves, ***Springer***, USA(2016),

Washington, L. C. , Elliptic Curves: Number Theory and Cryptography (Discrete Mathematics and Its Applications) , ***Chapman and Hall/CRC***, Florida, USA(2003).

ÖZGEÇMİŞ

Kişisel Bilgiler

Adı Soyadı : Ayşe Gör

Doğum Yeri ve Tarihi : Rize / 1990

Eğitim Durumu

Lisans Öğrenimi :Abant İzzet Baysal Üniversitesi, Matematik

Bildiği Yabancı Diller : İngilizce

İş Deneyimi

Stajlar :

Projeler :

Çalıştığı Kurumlar :

İletişim:

Adres : İlkadım/Samsun

Tel :

E-posta Adresi : aysegor2973@gmail.com

Yabancı Dil Bilgisi

İngilizce, 82.5/100, YDS

Tarih: 29.01.2019