ANADOLU ÜNİVERSİTESİ

BİLECİK ŞEYH DEBALİ ÜNİVERSİTESİ

Fen Bilimleri Enstitüsü
Matematik Anabilim Dalı

BİRCH VE SWİNNERTON-DYER KONJEKTÜRÜ ÜZERİNE

Fatih TANRIKULU
Yüksek Lisans

Tez Danışmanı
Doç.Dr. İlker İNAM

BİLECİK, 2017

Ref.No: 10137186

ANADOLU ÜNİVERSİTESİ

BİLECİK ŞEYH DEBALİ ÜNİVERSİTESİ

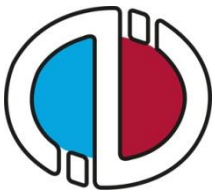
Fen Bilimleri Enstitüsü
Matematik Anabilim Dalı

BİRCH VE SWİNNERTON-DYER KONJEKTÜRÜ ÜZERİNE

Fatih TANRIKULU
Yüksek Lisans

Tez Danışmanı
Doç.Dr. İlker İNAM

BİLECİK, 2017



ANADOLU UNIVERSITY

BILECIK SEYH EDEBALI UNIVERSITY

Graduate School of Sciences
Department of Mathematics

ON THE BIRCH AND SWINNERTON-DYER CONJECTURE

Fatih TANRIKULU
Master's Thesis

Thesis Advisor
Assoc.Prof.Dr. Ilker INAM

BILECIK, 2017

BİLECİK ŞEYH EDEBALİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS
JÜRİ ONAY FORMU

Bilecik Şeyh Edebali Üniversitesi Fen Bilimleri Enstitüsü Yönetim Kurulunun 11.01.2017 tarih ve ....3..... sayılı kararıyla oluşturulan jüri tarafından 27.01.2017 tarihinde tez savunma sınavı yapılan Fatih TANRIKULU'nun "Birch ve Swinnerton-Dyer Konjektürü 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. Özden KORUOĞLU

ÜYE : Doç. Dr. Nülifer ÖZDEMİR

ONAY

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

TEŞEKKÜR

Yüksek Lisans eğitimimin tez hazırlama süreci boyunca yardımlarını benden esirgemeyen, yoğun mesaisine rağmen beni ihmal etmeyen kıymetli hocam, Sayın Doç. Dr. İlker İNAM'a ve destekleri ile sürekli yanımda olduklarını hissettiren aileme ve kurumuma teşekkürlerimi sunarım.

Fatih TANRIKULU

ÖZET

Birch ve Swinnerton-Dyer Konjektürü (BSD-Konjektürü), Matematik'in son yıllardaki en popüler problemlerinden birisi olup, Clay Matematik Enstitüsü'nün çözümü için 1 milyon dolar ödül vaat etmesi probleme olan ilgiyi oldukça arttırmıştır. Sayısal veriler konjektürün doğruluğunu desteklemektedir. Eliptik eğrilerde cebirsel bir objeyle analitik bir objeyi birbirine bağlayan konjektür iki kısımdan oluşmaktadır. İlk kısım rankla ilgili olup, ikinci kısımda ise eliptik eğrilerle ilgili bir formülün doğruluğu iddia edilmektedir. Dört bölümden oluşan bu çalışmada BSD-Konjektürü tanıtılması hedeflenmiştir. İlk bölümde eliptik eğrilerin özelliklerine ayrılmıştır. İkinci bölümde ise BSD-Konjektürü'nün rankla ilgili olan kısmı ifade edilmiş ve literatürdeki güncel sonuçlar tartışılmıştır. Üçüncü bölümde eliptik eğrilerin Tate-Shafarevich grupları tanıtıldıktan sonra BSD-Konjektürü'nün ikinci kısmını oluşturan formül verilmiştir. Dördüncü ve son bölümde ise konjektürü doğrulayan bazı örnekler ele alınmıştır. Çalışma derleme niteliğindedir.

Anahtar Kelimeler

Eliptik eğriler; L-serileri; Birch ve Swinnertıon-Dyer Konjektürü; Eliptik eğrinin rankı; Tate-Shafarevich grupları.

ABSTRACT

Birch and Swinnerton-Dyer Conjecture (BSD-Conjecture) is one of the most popular problems of Mathematics in recent years and it became a more interesting problem with Clay Mathematics Institute's $1 million prize for its solution. Numerical data support this conjecture's validity. The conjecture, which connects an algebraic object and an analytic object in elliptic curves, consists of two parts. The first part is related to rank and the second part claims the validity of a formula related to elliptical curves. The aim of this four-parted study is to introduce the BSD-conjecture. The first part is spared for the properties of elliptic curves. In the second part, the part related to the rank of BSD-Conjecture is stated and current results in the literature review are discussed. In the third part, Tate-Shafarevich groups of elliptic curves are introduced and the formula which composes the second part of BSD- Conjectures is given. In the fourth and the last section, some examples that support the conjecture are discussed. The study is conducted as a compilation.

Key Words

Elliptic curves; L-series; Birch and Swinnerton-Dyer Conjecture; Rank of elliptic curves; Tate-Shafarevich groups.

İÇİNDEKİLER

ŞEKİLLER DİZİNİ

Sayfa No

SİMGELER VE KISALTMALAR

Simgeler

$a\|b$	: a, b yi Böler
$a \nmid b$	: a, b yi Bölmez
$char(\mathbb{K})$	: $\mathbb{K}$ Cisminin Karakteristiği
$\mathbb{C}$	: Kompleks Sayılar Kümesi
c_p	: p Asalına Karşılık Gelen Tamagawa Sayısı
$\mathbb{F}_p$	: p Elemanlı Sonlu Cisim
$G_{\mathbb{Q}}$	: $\mathbb{Q}$'nun Mutlak Galois grubu
$\ker(\gamma_{p,n})$	: $\gamma_{p,n}$ Dönüşümünün Çekirdeği
$L(E,s)$	: E Eliptik Eğrisinin Tam $L-$ Fonksiyonu
$\mathbb{N}$	: Doğal Sayılar Kümesi
$\mathbb{R}$	: Reel Sayılar Kümesi
r	: E Eliptik Eğrisinin Cebirsel Rankı
r_{an}	: E Eliptik Eğrisinin Analitik Rankı r
$Reg(E)$	: E Eliptik Eğrisinin Regülatörü
$S_{\mathbb{Q}}(E)$	: E Eliptik Eğrisinin Selmer Grubu
$\mathbb{Q}$	: Rasyonel Sayılar Kümesi
$\mathbb{Q}_p$	: p-adik Rasyonel Sayıların Kümesi
$\mathbb{Z}$	: Tam Sayılar Kümesi
$Ш(E/\mathbb{Q})$	: E Eliptik Eğrisinin Tate–Shafarevich Grubu
$\Gamma(z)$	: Gama Fonksiyonu
Ω_E	: E Eliptik Eğrisinin Gerçel Periyodu
Δ_E	: Eliptik Eğrinin Diskriminantı

1. ELİPTİK EĞRİLER

1.1. Giriş

Eliptik eğriler uzun yıllardır matematikçilerin ilgisini çeken bir konudur ve halen de popüler olarak çalışılmaya devam etmektedir. Matematikte son yüzyılların en büyük problemlerinden birisi olan Fermat'ın Son Teoremi'nin ispatında kullanılmış olması konunun cazibesini iyice arttırmıştır. Bu ispata ulaşılmasını sağlayan Modülarite Teoremi yardımıyla eliptik eğriler ile modüler formlar arasında bir köprü kurulmuş olması köprünün bir ucundaki problemi köprünün diğer yakasına taşıyıp çözme imkanı vermiştir. Bu köprü iki yönlü olup halen birçok problemin çözümünde iki konunun da yaygın olarak kullanılmasına neden olmaktadır.

Eliptik eğriler ülkemizdeki çipli pasaportlardaki bilgi şifrelemesinde kullanılan Eliptik Eğri Kriptografisi'nin de temelini oluşturmaktadır. Bunun dışında Analiz ve Fonksiyonlar Teorisi'nde, Cebirsel ve Aritmetik Geometri'de de çeşitli problemlerin çözümünde kullanılmaktadır. Bu çalışmada İngiliz matematikçiler Bryan Birch ve Peter Swinnerton-Dyer tarafından bazı bilgisayar hesaplamalarının ardından 1960'larda ortaya atılan ödüllü bir problemin tanıtımı amaçlanmıştır. Öncelikle eliptik eğrileri tanıtmakla işe başlayalım.

Eliptik eğri denince ilk akla gelen şey bu eğrilerin elipsle bir ilgisi olup olmadığıdır. Geometrik olarak elips eğrisiyle eliptik eğri birbirine hiç benzememektedir. Peki "eliptik eğri" ismi nereden gelmektedir?

18. yüzyılın başlarında bir İtalyan matematikçi olan Giulio Fagnano (1682-1766) belirli eğrilerin yay uzunluklarını hesaplamaya çalıştı. Çalışmalarını 1750'de "Produzioni Matematische" isimli iki ciltlik kitapta yayınlamış olup, bu eseri Papa XIV. Benedikt'e adamıştır(Ball, 2010). Kitap kapağında lemninskat eğrisi yer almaktadır. Fagnano, elips eğrilerinin yay uzunluğunu hesaplama işleminde eliptik integrali tanımlamıştır. Buna göre elipsin yay uzunluğu

$$I(x) = \int^{x} \frac{1}{\sqrt{t^3 + at^2 + bt + c}} dt.$$

integrali yardımıyla hesaplanır. Böylece bir elips eğrisinin yay uzunluğunu bulmak isteyen birisi bu integrali hesaplamak durumundadır, buradan hareketle değişken değişiminde ortaya çıkan $y^2 = x^3 + ax^2 + bx + c$ denklemi eliptik eğri adını aldı.

Tanım 1.1.1. $\mathbb{K}$ herhangi bir cisim ve $a_1, \dots, a_6 \in \mathbb{K}$ olmak üzere,

$$E(\mathbb{K}): y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (1.1)$$

eşitliğini sağlayan noktaların geometrik yerine $\mathbb{K}$ cismi üzerinde bir *eliptik eğri* denir. (1.1) eşitliğine *E eliptik eğrisinin Weierstrass eşitliği* adı verilir.

Eliptik eğrinin denklemi afin dönüşümler kullanılarak, *char*($\mathbb{K}$) = 2 olması durumunda

$$y^2 + a_1y = x^3 + a_2x + a_3 \text{ veya } y^2 + xy = x^3 + a_1x^2 + a_2$$

char($\mathbb{K}$) = 3 olması durumunda da

$$y^2 = x^3 + a_1x^2 + a_2x + a_3$$

halini alır. *char*($\mathbb{K}$) $= 2,3$ durumu ile ilgili ayrıntılı bilgi Silverman'da (1986) bulunabilir.

char($\mathbb{K}$) $\neq 2,3$ olması durumunda tam kareye tamamlama metodu ve uygun dönüşümün ardından yapılacak bazı cebirsel işlemler yardımıyla (1.1) eşitliği daha basit bir hal alarak

$$E: y^2 = x^3 + Ax + B \quad (1.2)$$

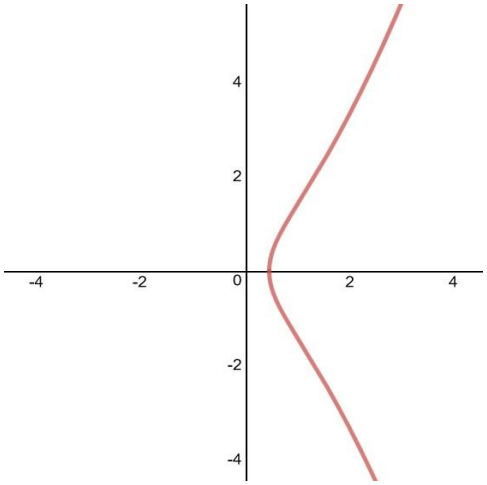
halini alır. (1.2) eşitliğine *Kısa Weierstrass eşitliği* denir.

Weierstrass eşitliğinin kısa haline geçiş aşamaları için ayrıntılı işlemler İnam'da (2011) bulunabilir.

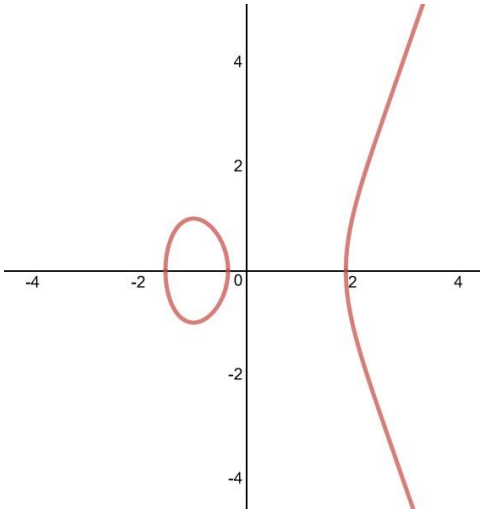
Tanım 1.1.2. $\mathbb{K}$ herhangi bir cisim, $x, y, A, B \in \mathbb{K}$ olmak üzere $E: y^2 = x^3 + Ax + B$, $\mathbb{K}$ cismi üzerinde tanımlı bir eliptik eğri olsun. Bu eliptik eğrinin diskriminantı

$$\Delta = -16(4A^3 + 27B^2) \quad (1.3)$$

olarak tanımlanır. Eğer $\Delta \neq 0$ ise $x^3 + Ax + B = 0$ polinomunun katlı kökü yoktur. Bu durumdaki eliptik eğriye singüler olmayan eliptik eğri adı verilir. Bu özellikteki eliptik eğriler üzerinde özel bir nokta toplamı işlemi tanımlanabileceği için, bu çalışma boyunca aksi belirtilmedikçe eliptik eğri ile singüler olmayan eliptik eğri kastedilecektir.



Şekil 1.1. $y^2 = x^3 + 2x - 1$'in grafiği ($\Delta < 0$).



Şekil 1.2. $y^2 = x^3 - 3x - 1$'in grafiği ($\Delta > 0$).

$\Delta > 0$ olması durumunda eliptik eğrinin grafiği iki parça, $\Delta < 0$ olması durumunda eliptik eğrinin grafiği tek parçadan oluşur.

Tanım 1.1.3. $\mathbb{Q}$ üzerindeki E eliptik eğrisi

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

eşitliği yardımıyla verilsin. Bu durumda E için Weierstrass eşitliklerinin tüm diskriminantlarının mutlak değerleri arasında tüm a_i katsayıları tam sayı olacak şekildeki en küçük $\Delta \in \mathbb{Z}$ diskriminantına sahip olan E eliptik eğrisi bir minimal Weierstrass eşitliği yardımıyla tanımlanır.

Teorem 1.1.4. *E*, $\mathbb{Q}$ üzerinde bir eliptik eğri olsun. Bu durumda her bir *E* eliptik eğrisinin bir minimal modeli vardır.

İspat. Silverman'da (1986) sayfa 244'de Önerme VIII. 8.2.'de yer almaktadır.

Teorem 1.1.5. *E*, $\mathbb{Q}$ üzerinde bir eliptik eğri olsun. Eğer *E* için minimal model mevcut ise bu durumda $a_1, a_3 \in \{0,1\}$ ve $a_2 \in \{-1,0,1\}$ olacak şekilde bir tek indirgenmiş minimal model vardır.

İspat. $\mathbb{Q}$ üzerinde E eliptik eğrisi $b_1, b_2, b_3, b_4, b_6 \in \mathbb{Z}$ olmak üzere

$$y^2 + b_1xy + b_3y = x^3 + b_2x^2 + b_4x + b_6$$

Weierstrass modeli ile verilsin. Silverman (1986) sayfa 59, önerme III.3.1(b) gereği aynı E eliptik eğrisinin farklı iki Weierstrass modeli belli $u \in \mathbb{Q}^*$ ve $r, s, t \in \mathbb{Q}$ için

$$x = u^2X + r, \qquad y = u^3Y + u^2sX + t$$

değişken değişimi yardımıyla birbirine dönüştürülebilir. Silverman, (1986), sayfa 45, Tablo 3.1 gereği, bu değişken değişimi eliptik eğrinin diskriminantında u^{12} çarpanı kadar değişiklik yapar. O halde diskriminantı invaryant bırakan (böylece global minimal modeli koruyan) değişken değişimleri $u = \pm 1$ olanlarıdır.

$a_1, a_3 \in \{0, 1\}$ olmak üzere b_1 ve b_3 katsayıları $b_1 = -2s + a_1$ ve $b_3 = -2t + a_3$ olarak tek türlü yazılıp $X = x$ ve $y = Y + sX + t$ değişken değişimi yardımıyla, belli $c_2, c_4, c_6 \in \mathbb{Z}$ için

$$(Y + sX + t)^2 + b_1X(Y + sX + t) + b_3(Y + sX + t)$$
$$= Y^2 + (b_1 + 2s)XY + (b_3 + 2t)Y$$
$$= Y^2 + a_1XY + a_3Y = X^3 + c_2X^2 + c_4X + c_6$$

yeni global minimal modeli elde edilir.

$a_2 \in \{-1, 0, 1\}$ olmak üzere $c_2 = -3r + a_2$ tek türlü yazılarak, $X = x + r$ ve $y = Y$ değişken değişimi yardımıyla belli $d_4, d_6 \in \mathbb{Z}$ için

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + d_4x + d_6$$

indirgenmiş minimal modeli elde edilir. Böylelikle istenen özellikte indirgenmiş minimal modelin varlığı gösterilmiş oldu. Şimdi ise teklik kısmını gösterelim.

Yukarıdaki biçimde değişken değişimleri a_1 ve a_2'nin modülo 2'deki, a_3'ün modülo 3'teki değerini değiştirmez ve $a_1, a_3 \in \{0, 1\}$ ve $a_2 \in \{-1, 0, 1\}$ kısıtlamaları böylece tek türlü sağlanmış olur. a_1, a_2, a_3 katsayılarını sabit bırakmak için ilk değişken değişiminde $r = t = s = 0$ olmalıdır. Aksi takdirde a_1, a_2, a_3'ten en az birisi değişir. $s = 0$ olduğunda $u = 1$ olur. Aksi takdirde a_1 değişir. Bu ise dönüşümün aşikar olduğunu gösterir. Böylece ispat bitmiş olur.

Magma Hesaplamalı Cebir Sisteminde (Bosma, vd.,1997) bir *E* eliptik eğrisi verildiğinde onun global minimal modeli aşağıdaki gibi kolaylıkla bulunabilir.

Örnek 1.1.6.

```
>E:=EllipticCurve([1,12,132,-5,0]);
>E;
> Elliptic Curve defined by y^2 + x*y + 132*y = x^3 + 12*x^2 - 5*x over Rational
Field
>MinimalModel(E);
> Elliptic Curve defined by y^2 + x*y = x^3 + 11*x + 4244 over Rational Field
```

Bir *E* eliptik eğrisini tanımlayan eşitliğin minimal Weierstrass eşitliği olup olmadığını belirlemek için John Tate'in (1975)'de vermiş olduğu algoritma kullanılabilir.

Şimdi bazı sayı cisimleri üzerinde tanımlı eliptik eğrilerin özelliklerini özetleyelim.

$\mathbb{K} = \mathbb{C}$ olması durumunda, $\mathbb{C}$ üzerindeki tüm eliptik eğriler tora izomorftur (Washington, 2003). Bu nedenle $\mathbb{C}$ üzerinde tanımlı eliptik eğriler için nispeten daha az ilgi çekici sonuçlar elde edilebilir.

p asal olmak üzere $\mathbb{K} = \mathbb{F}_p$ olması durumunda, günümüzün popüler konularından olan eliptik eğri kriptografisi gündeme gelir. Literatürde kısaca ECC (Elliptic Curve Cryptography) olarak geçen konu, eliptik eğriler üzerindeki nokta sayımı ile ilgilidir. Ayrıca $\mathbb{F}_p$ üzerinde tanımlı eliptik eğriler verilen bir sayının asal olup olmadığını test etmeye yarayan "Asallık Testi"nde kullanılır. Konuyla ilgili güncel literatür www.hyperelliptic.org kaynağından takip edilebilir.

$\mathbb{K} = \mathbb{Q}$ durumunda problemler zorlaşır ancak bu kez zengin özellikler söz konusu olur. Bu durumda "eliptik eğrinin rankı" kavramı ortaya çıkar. Buradan da 1 milyon dolar ödüllü Birch ve Swinnerton-Dyer Konjektürü'ne (BSD-Konjektürü) ulaşırız (Clay Mathematics Institute, 2016).

Bu çalışmada BSD-Konjektürü'nü tanıtmak hedeflendiğinden artık problemi ifade etmek için gerekli hazırlıklara başlayabiliriz.

Uyarı 1.1.7. Eliptik eğrilerin grup yapısı bir sonraki kısımda incelenecek olup, eliptik eğri üzerindeki noktaların kümesinin bir grup belirtebilmesi için sonsuzdaki nokta olarak adlandırılan $\mathcal{O} = [0,1,0]$ noktasının eliptik eğri üzerinde olduğu kabul edilecektir.

1.2. Eliptik Eğrilerin Grup Yapısı

Bu kısımda üzerinde tanımlanan özel nokta toplamı işlemi yardımıyla eliptik eğrilerin bir abelyan grup olduğu görülecek ve böylece eliptik eğriler üzerinde aritmetik yapılabilecektir.

Tanım 1.2.1. $\mathbb{K}$, *char*$(\mathbb{K}) \neq 2,3$ özelliğinde bir cisim ve E eliptik eğrisi $\mathbb{K}$ cismi üzerinde

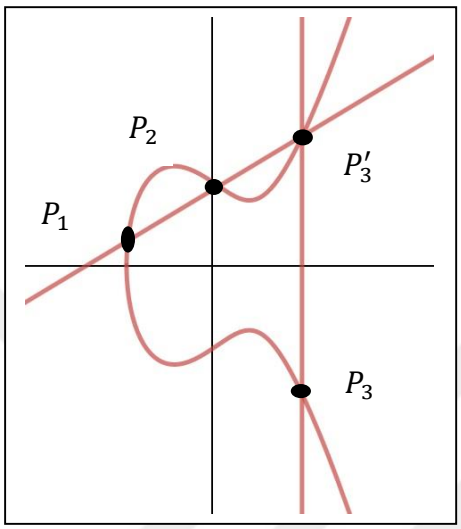
$$E: y^2 = x^3 + Ax + B$$

kısa Weierstrass eşitliğiyle tanımlanmış bir eliptik eğri olsun. Bu durumda, eliptik eğri üzerindeki iki noktanın toplamı şu şekilde tanımlanır:

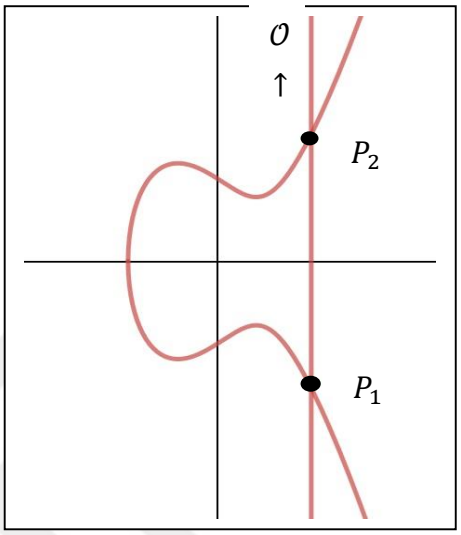
$\mathcal{O} = [0,1,0], P_1, P_2 \in E$ olmak üzere, P_1 ve P_2 noktalarından geçen l doğrusu eliptik eğriyi üçüncü bir noktada keser. Çünkü eliptik eğriyi belirleyen eşitliğin sağ tarafı üçüncü dereceden bir polinomdur. Bu noktayı P_3' ile gösterelim. l' doğrusu P_3' ve $\mathcal{O}$

noktasından geçen doğruyu göstersin. l' doğrusunun eliptik eğriyi kestiği P_3' dışındaki diğer nokta P_3 ile gösterilirse bu nokta P_1 ve P_2 noktalarının toplamı olarak tanımlanır ve $P_1 + P_2$ ile gösterilir.

Başka bir deyişle $P_1 + P_2$, P_1 ve P_2 noktalarından geçen doğrunun eliptik eğriyi kestiği üçüncü noktanın *x*–eksenine göre simetriği olarak tanımlanır.



Şekil 1.3. Eliptik eğrilerde farklı iki noktanın toplamı.



Şekil 1.4. Eliptik eğrilerde *x* eksenine göre simetrik olan iki noktanın toplamı.

Uyarı 1.2.2. $P_1 = P_2$ olması durumunda l doğrusu E eliptik eğrisinin teğet doğrusu olarak alınır. Bu şekilde bir noktanın katları tanımlanabilir.

P_1 ve P_2 noktalarının koordinatları yardımıyla P_3 noktasının koordinatının hesaplanmasındaki farklı durumları inceleyelim.

1. Durum. $P_1 = (x_1, y_1)$ ve $P_2 = (x_2, y_2)$ farklı noktalar ve $x_1 \neq x_2$ olsun. Bu durumda l doğrusunun eğimi

$$m = \frac{y_2 - y_1}{x_2 - x_1}$$

olur, buradan da l doğrusunun denklemi

$$y = m(x - x_1) + y_1 \tag{2.4}$$

olarak elde edilir. $P_3 = (x_3, -y_3)$ noktasının koordinatları hesaplamak için (2.4) eşitliğini kısa Weierstrass eşitliğinde yerine yazarsak

$$(m(x - x_1) + y_1)^2 = x^3 + Ax + B \tag{2.5}$$

elde edilir. Eşitliğin sol tarafını açıp denklemi yeniden düzenlersek

$$x^3 - m^2x^2 + \cdots = 0 \tag{2.6}$$

P_1 ve P_2 noktalarının koordinatlarını bilindiği için

$$x_3 = m^2 - (x_1 + x_2)$$

$$y_3 = m(x_3 - x_1) + y_1$$

olur. Buradan da $m = \frac{y_2 - y_1}{x_2 - x_1}$ iken P_3 noktasının koordinatları

$$(m^2 - (x_1 + x_2), -m(x_3 - x_1) - y_1)$$

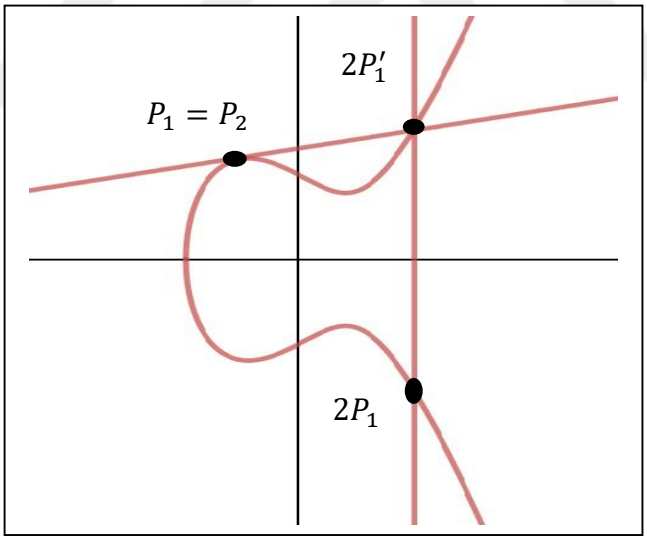
olarak bulunur.

2. Durum. $P_1 = (x_1, y_1)$ ve $P_2 = (x_2, y_2)$ farklı noktalar ve $x_1 = x_2$ olsun. (Grafik 2.2 sağ) Bu durumda verilen iki noktayı birleştirerek l doğrusunu çizdiğimiz zaman dikey bir doğru olduğunu görürüz, bu durumda iki noktanın toplamı

$$P_1 + P_2 = O$$

olarak tanımlanır. Kolayca görülebilir ki $P_1 = (x_1, y_1)$ iken $P_2 = (x_1, -y_1)$ dir.

3. Durum. $P_1 = (x_1, y_1)$ ve $P_2 = (x_2, y_2)$ olmak üzere $P_1 = P_2$ ve $y_1 = y_2 \neq 0$ olsun.



Şekil 1.5. Eliptik eğrilerde ikinci bileşeni sıfırdan farklı olan eşit iki noktanın toplamı.

Bu durumda P_1 noktasından geçen ve eğimi m olan bir teğet doğrusu çizilir. Kapalı fonksiyonunun türevi yardımıyla bu teğetin eğimi

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

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

olarak bulunur.

l doğrusunun denklemi

$$y = m(x - x_1) + y_1$$

iken, P_3 noktasının koordinatları

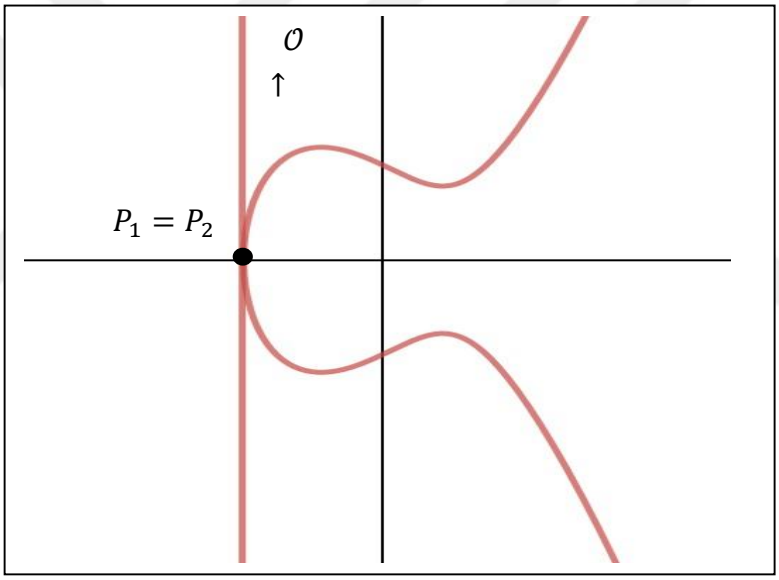
$$(m^2 - 2x_1, -m(x_3 - x_1) - y_1)$$

olarak bulunur. Bu durumda

$$P_1 + P_1 = 2P_1$$

yazılır.

4. Durum. $P_1 = (x_1, y_1)$ ve $P_2 = (x_2, y_2)$ olmak üzere $P_1 = P_2$ ve $y_1 = y_2 = 0$ olsun.



Şekil 1.6. Eliptik eğrilerde ikinci bileşeni sıfır olan eşit iki noktanın toplamı.

P_1 noktasından geçen l teğet doğrusunun E eğrisi ile sonsuzdaki nokta olan $\mathcal{O}$ da kesiştiğini görürüz. Bu 2.Durum ile aynı olup

$$P_1 + P_2 = 2P_1 = \mathcal{O}$$

eşitliğine elde ederiz.

$P + \mathcal{O} = P$ eşitliğinden $\mathcal{O}$'nun etkisiz eleman olduğu görülür.

Teorem 1.2.3. Yukarıdaki toplama işlemi ile birlikte $\mathbb{K}$ cismi üzerinde tanımlı E eliptik eğrisine ait her P_1, P_2 ve P_3 noktaları için aşağıdaki önermeler doğrudur:

i. $P_1 + P_2$ E'nin elemanıdır

ii. $P_1 + P_2 = P_2 + P_1$

iii. $P_1 + \mathcal{O} = \mathcal{O} + P_1 = P_1$

iv. Herhangi P_1 elemanı için $P_1 + P_2 = \mathcal{O}$ olacak şekilde bir $P_2 \in E$ mevcuttur.

v. $P_1 + (P_2 + P_3) = (P_1 + P_2) + P_3$.

Başka bir deyişle E eliptik eğrisi üzerine tanımlı nokta toplamı işlemiyle birlikte bir abelyan grup olur (Silverman, 1986).

İspat. Verilen iki noktanın toplamı ile ilgili farklı durumları incelediğimizde görüldü ki toplama bir ikili işlem olur. P_1 ve P_2 noktasından geçen doğru ile P_2 ve P_1 noktasından geçen doğru aynı doğru olduğu için değişme özelliği de sağlanır. Toplamaya göre etkisiz elemanın $\mathcal{O}$ noktası olduğu görülmüştü. Ters elemanın varlığı 2.Durum'da gösterilmiştir. Birleşme özelliğinin ispatı oldukça uzun olup, rutin işlemler yardımıyla elde edilmektedir. Bu önermelerin tam ispatı Washington (2003), Kısım 2.4., sayfa 20'de bulunabilir.

Uyarı 1.2.4. P noktasının toplamsal tersi $-P$ olarak gösterilse de, $P = (x, y)$ iken $-P \neq (-x, -y)$. Durum 2 de görüldüğü gibi P noktasının tersi $(x, -y)$ dir.

Teorem 1.2.5. (Mordell-Weil) E, bir sayı cismi olan $\mathbb{K}$ üzerinde bir eliptik eğri olsun. Bu durumda $E(\mathbb{K})$ sonlu üreteçli bir abelyan gruptur.

Yukarıdaki teoremde Mordell $\mathbb{K} = \mathbb{Q}$ durumunu ispatlamış (Silverman, 1986), Weil (1967) ise Mordell'in sonucunu herhangi bir $\mathbb{K}$ sayı cismine genişletmiştir.

Sonlu üreteçli abelyan grupların temel teoremi gereğince, $E(\mathbb{Q})$**,** $\mathbb{Z}$**'**nin kopyaları ile sonlu devirli grupların direk çarpımına izomorftur (Asar, vd., 2009). Böylece bir E eliptik eğrisinin cebirsel rankı kavramına ulaşırız.

Tanım 1.2.6. E, $\mathbb{Q}$ üzerinde tanımlı bir eliptik eğri olsun. Mordell-Weil teoremi gereği belli $r \geq 0$ tamsayısı için

$$E(\mathbb{Q}) \cong E_{tors}(\mathbb{Q}) \times \mathbb{Z}^r$$

olur. Buradaki r sayısına E eliptik eğrisinin cebirsel rankı denir. $E_{tors}(\mathbb{Q})$ ise $E(\mathbb{Q})$'nun sonlu mertebeli elemanlarının oluşturduğu büküm altgrubudur.

Şimdi ise eliptik eğri üzerindeki toplama işlemiyle ilgili bazı örnekler ve formülleri verelim.

Örnek 1.2.7. $\mathbb{Q}$ üzerinde tanımlı $E: y^2 = x^3 - 5x + 8$ eliptik eğrisini göz önüne alalım. Kolayca görülebilir ki $P(1,2)$ noktası E eğrisi üzerindedir. Yukarıdaki adımlar takip edilirse

$$2P = P + P = (-\frac{7}{4}, -\frac{27}{8})$$

olarak bulunur. Bu bulduğumuz noktayı $Q = (-\frac{7}{4}, -\frac{27}{8})$ile gösterelim. Aynı işlemler tekrarlanarak

$$3P = P + Q = (\frac{553}{121}, -\frac{11950}{1331})$$

bulunur. Benzer şekilde

$$4P = (\frac{45313}{11664}, -\frac{8655103}{1259712})$$

olarak bulunur. Bu şekilde devam ettikçe koordinatların oldukça karmaşık hale geldiği görülür (Silverman, 2006).

E eliptik eğrisi üzerindeki toplama işlemiyle ilgili yukarıdaki durumları özetleyelim. $E: y^2 = x^3 + Ax + B$ eğrisi üzerinde $P_1 = (x_1, y_1)$ ve $P_2 = (x_2, y_2)$ noktalarını göz önüne alalım. P ve Q noktalarını birleştiren doğruyu $L: y = \lambda x + v$ ile ifade edelim. O halde

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, P_1 \neq P_2 \\ \frac{3x_1^2 + A}{2y_1}, P_1 = P_2 \end{cases} \qquad ve \quad v = y_1 - \lambda x_1$$

olduğu açıktır.

$E: y^2 = x^3 + Ax + B$ eğrisi üzerinde $P_1 = (x_1, y_1)$ ve $P_2 = (x_2, y_2)$ noktalarının toplama işlemini şu şekilde özetleyebiliriz.

- $P_1 \neq P_2$ ve $x_1 = x_2$ ise $P_1 + P_2 = \mathcal{O}$
- $P_1 = P_2$ ve $y_1 = 0$ ise $P_1 + P_2 = 2P_1 = \mathcal{O}$
- $P_1 \neq P_2$ ve $x_1 \neq x_2$ ise

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \quad ve \quad v = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}$$

- $P_1 = P_2$ ve $y_1 \neq 0$ ise

$$\lambda = \frac{3x_1^2 + A}{2y_1} \quad ve \quad v = \frac{-x^3 + Ax + 2B}{2y}$$

böylece $P_1 + P_2 = (\lambda^2 - x_1 - x_2, -\lambda^3 + \lambda(x_1 + x_2) - v)$ olarak bulunur.

Toplama formülü karışık gözükmesine rağmen örnek olarak $P_1 = (x_1, y_1)$ ve $P_2 = (x_2, y_2)$ ayrı noktalar olsun, bu durumda $x(P)$, P noktasının apsisini göstermek üzere

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

olarak bulunur. Eğer $P = (x, y)$ herhangi bir nokta ise, bu durumda

$$x(2P) = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)}$$

dir.

Yukarıdaki gözlem koordinatları özel bir cisimde bulunan noktaların, tüm noktaların oluşturduğu kümelerin bir alt grubunu oluşturduğu sonucuna ulaştırır (Silverman, 2006).

Teorem 1.2.8. $\mathbb{K}$ bir cisim ve E eliptik eğrisi $E: y^2 = x^3 + Ax + B,\ A, B \in \mathbb{K}$ olsun. Koordinatları $\mathbb{K}$'da bulunan E'ye ait noktaların kümesini $E(\mathbb{K})$ ile gösterilmek üzere $E(\mathbb{K}) = \{(x, y) \in E: x, y \in \mathbb{K}\} \cup \mathcal{O}$ olsun. Bu durumda $E(\mathbb{K})$, E'deki tüm noktaların oluşturduğu grubun alt grubudur (Silverman, 1986).

E üzerindeki grup yapısına göre verilen formüller, geometrik resmi bir anlam ifade etmesede, koordinatları herhangi bit cisme ait olan noktalar için de sağlanır. Koordinatları $\mathbb{F}_p$ de bulunan noktaları için aşağıdaki örneğe bakalım.

Örnek 1.2.9. $E: y^2 = x^3 - 5x + 8\ (mod 37)$ ile verilen E eliptik eğrisi $P = (6,3) \in E(\mathbb{F}_{37})$ ve $Q = (9,10) \in E(\mathbb{F}_{37})$ noktalarını içerir. Toplama formülünü kullanarak $E(\mathbb{F}_{37})$ de,

$$2P = (35,11), 3P = (34,25), 4P = (8,6), 5P = (16,19), \ldots$$

$$P + Q = (11,10), \ldots, 3P + 4Q = (31,28) \ldots$$

olarak hesaplanır.

$x = 0,1,2, \ldots, 36$ değerleri teker teker denenerek $x^3 - 5x + 8$'in modülo 37'de tam kare olması halinde listeye ekleyerek, $E(\mathbb{F}_{37})$'nin modülo 37'de aşağıdaki 45 noktadan oluştuğunu buluruz:

$$(1, \pm 2), (5, \pm 21), (6, \pm 3), (8, \pm 6), (9, \pm 27), (10, \pm 25), (11, \pm 27), (12, \pm 23),$$
$$(16, \pm 19), (17, \pm 27),$$
$$(19, \pm 1), (20, \pm 8), (21, \pm 5), (22, \pm 1), (26, \pm 8), (28, \pm 8), (30, \pm 25), (31, \pm 9),$$

$$(33, \pm 1), (34, \pm 25), (35, \pm 26), (36, \pm 7), \mathcal{O}$$

Tam olarak 9 noktanın mertebesi 3'ü böler bu nedenle $E(\mathbb{F}_{37})$ grup yapısı olarak

$$E(\mathbb{F}_{37}) \cong C_3 \times C_{15}$$

Olur (Silverman, 2006).

Teorem 1.2.10. Sonlu bir cisimde $E(\mathbb{F}_p)$ deki noktaların oluşturduğu grup her zaman için ya devirlidir ya da iki devirli grubun çarpımıdır (Washington, 2003).

2. BSD RANK KONJEKTÜRÜ

Bu bölümde Birch ve Swinnertor-Dyer'in eliptik eğrilerin rankları ile ilgili ortaya koyduğu ve BSD'nin ulaşılması zor bölümünü oluşturan BSD rank konjektürü ele alınacaktır.

2.1. Ön Hazırlık.

E, $\mathbb{Q}$ üzerinde bir eliptik eğri ve Δ, E'nin diskriminantı olsun. Bu durumda p asal sayı olmak üzere $p \nmid \Delta$ özelliğindeki p asalları için E, $\mathbb{F}_p$ cismi üzerinde bir eliptik eğri indirger. Dikkat edilirse bu özellikteki p asallarının sayısı sonsuz çokluktadır. Tıpkı diğer $\mathbb{K}$ sayı cisimlerinde olduğu gibi $E(\mathbb{F}_p)$ de bir abelyan grup olur. Bu grubun da sonlu olduğu açıktır.

Sonlu cisim üzerinde tanımlı eliptik eğriler için Hasse 1936'da "Hasse Sınırı" adı verilen aşağıdaki önemli sonucu vermiştir.

Teorem 2.1.1. (Hasse Sınırı) p asal sayı olmak üzere E, $\mathbb{F}_p$ üzerinde tanımlı bir eliptik eğri olsun. Bu durumda

$$\left|p + 1 - \#E(\mathbb{F}_p)\right| \leq 2\sqrt{p} \tag{2.1}$$

olur. (Hasse, 1936)

Uyarı 2.1.2. $a_p := p + 1 - \#E(\mathbb{F}_p)$ olarak tanımlansın. Bu hata terimleri bir araya getirilerek bir üreteç fonksiyonu olarak düşünülebilir.

2.2. Eliptik Eğrilerin L–Fonksiyonu

Bu bölümde ise tüm asallarda $E(\mathbb{F}_p)$ hakkında bilgi veren $L(E,s)$ fonksiyonu tanımlanacaktır. Öte yandan sonsuz noktasının da eklenmesiyle, eliptik eğri üzerinde tanımlanacak olan $\Lambda(E,s)$ fonksiyonu yardımıyla eliptik eğrilerin özelliklerini oldukça geniş anlamda incelemiş olacağız.

E eliptik eğrisi $\mathbb{Q}$ üzerinde

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.2}$$

minimal Weierstrass eşitliği yardımıyla tanımlansın.

Bu durumda E eliptik eğrisinin L −fonksiyonunu tanımlayabilmek için şu adımlar takip edilir:

$p \nmid \Delta$ özelliğindeki her bir p asalı için $\mathbb{F}_p$ sonlu bir cisim olmak üzere, (2.2) eşitliği modülo p'de indirgenerek $\mathbb{F}_p$ üzerinde bir eliptik eğri tanımlar.

Bu özellikteki p asalları için a_p'yi

$$a_p := p + 1 - \#E(\mathbb{F}_p) \tag{2.3}$$

olarak tanımlayalım.

$p|\Delta$ özelliğindeki her bir asal için a_p, kötü indirgemenin çeşidine göre üç şekilde tanımlanır:

Eğer $E_{\mathbb{F}_p}$ singüler eğrisi toplamsal indirgemeye sahipse yani indirgeme cuspidal ise (örneğin $y^2 = x^3$ eğrisi gibi) bu durumda $a_p = 0$ olarak tanımlanır.

Eğer $E_{\mathbb{F}_p}$ singüler eğrisi tıpkı $y^2 = x^3 + x^2$ eğrisinde olduğu gibi parçalanmış çarpımsal indirgemeye sahip ise başka bir deyişle indirgeme düğüm noktası şeklinde olup teğet doğrusu $\mathbb{F}_p$ rasyonel ise (ki bu singüler noktadan geçen teğet doğrunun eğiminin $\mathbb{F}_p$'nin elemanı olduğu anlamına gelir) $a_p = 1$ olarak tanımlanır.

Eğer singüler noktadaki teğetin eğimi $\mathbb{F}_p$'nin elemanı değilse E eliptik eğrisi p'de parçalanmamış çarpımsal indirgemeye sahiptir denir ve $a_p = -1$ olarak tanımlanır.

Tanım 2.2.1. Buna göre kötü p asalları için a_p aşağıdaki gibi tanımlanır:

$$a_p = \begin{cases} 0 : E, p'de\ toplamsal\ indirgemeye\ sahip \\ 1 : E, p'de\ parçalanmış\ çarpımsal\ indirgemeye\ sahip \\ -1 : E, p'de\ parçalanmamış\ çarpımsal\ indirgemeye\ sahip \end{cases}$$

Tanım 2.2.2. a_p sayıları yukarıdaki gibi tanımlansın. Böylece E eliptik eğrisinin tam $L-$ fonksiyonu

$$L_E(s) = \prod_{p|\Delta} (1 - a_p p^{-s})^{-1} \prod_{p\nmid\Delta} (1 - a_p p^{-s} + p^{1-2s})^{-1}$$

olarak tanımlanır.

Uyarı 2.2.3. a_p üzerindeki $|a_p| \leq \sqrt{2p}$ Hasse sınırı yukarıdaki çarpımın $Re(s) > \frac{3}{2}$ özelliğindeki s sayıları için yakınsak olmasını gerektirdiğinden $L_E(s)$ fonksiyonu iyi tanımlıdır (Washington, 2003).

Uyarı 2.2.4. $p|\Delta$ durumunda bile aslında (2.3) eşitliği yani $a_p = p + 1 - \#E(\mathbb{F}_p)$ geçerlidir. Gerçekten de E toplamsal indirgemeye sahip olsun. Bu durumda singüler olmayan noktalar $(\mathbb{F}_p, +)$ grubuna izomorf bir grup oluştururlar, ki dikkat edilirse bu grup p elemanlıdır. Diğer yandan E eliptik eğrisi bir tane singüler noktaya sahip olduğu için eğri üzerinde toplam $p + 1$ tane nokta olur. Bu değer (2.3) eşitliğinde yerine yazılırsa

$$a_p = p + 1 - (p + 1) = 0$$

olarak hesaplanır.

E, p'de parçalanmış indirgemeye sahip olsun. Böyle bir durumda bir singüler nokta dışındaki singüler olmayan noktalar $(\mathbb{F}_p^*,\times)$'ya izomorf bir grup oluştururlar. O halde E üzerinde $1+(p-1)=p$ tane nokta vardır. Bu değer (2.3)'de yerine yazılırsa

$$a_p = p + 1 - p = 1$$

bulunur.

E eliptik eğrisi p'de parçalanmamış indirgemeye sahip olsun. Bu durumda singüler olmayan noktalar $(\mathbb{F}_{p^2}^*/\mathbb{F}_p^*,\times)$ grubuna izomorf bir grup oluştururlar.Dikkat edilirse bu grup $p+1$ elemanlıdır. Singüler nokta da hesaba katılırsa bu durumda E eliptik eğrisi üzerinde $p+2$ tane nokta olduğu görülür. Bu değer (2.3)'de yerine konulursa

$$a_p = p + 1 - (p + 2) = -1$$

bulunur.

Dikkat edilirse $L(E,s)$ fonksiyonu E eliptik eğrisi üzerinde sonsuz noktası için hiç bir şey söylememektedir. Aşağıda tanımlanacak $\Lambda(E,s)$ fonksiyonu yardımıyla $L(E,s)$ fonksiyonu genişletilmiş olacaktır.

Teorem 2.2.5. Her $s \in \mathbb{C}$ için $\Lambda(E,s) = N^{s/2} \cdot (2\pi)^{-s} \cdot \Gamma(s) \cdot L(E,s)$ fonksiyonu $\mathbb{C}$'nin tamamında analitik bir karmaşık fonksiyona genişletilecek ve

$$\Lambda(E, 2-s) = \varepsilon \cdot \Lambda(E,s)$$

fonksiyonel eşitliğini sağlayacak şekilde tek bir $N = N_E$ pozitif tam sayısı ve $\varepsilon = \varepsilon_E \in \{\pm 1\}$ sayısı vardır. Burada $\Gamma(z)$, $z \in \mathbb{C}$ için

$$\Gamma(z) = \int_0^\infty t^{z-1} e^{-t} dt$$

şeklinde tanımlanan $\Gamma-$ fonksiyonudur (Wiles, 1995; Breuil, vd., 2001).

Tanım 2.2.6. Yukarıdaki teoremdeki N sayısına E eliptik eğrisinin *kondüktörü* ve ε sayısına E'nin *kök sayısı* veya E için *fonksiyonel eşitlikteki işaret* adı verilir.

Uyarı 2.2.7. Yukarıda tanımlanan sayılar, E eliptik eğrisi değiştikçe, değişeceği için N_E ve ε_E şeklinde gösterilir.

Bir eliptik eğrinin Δ diskriminantı ile N_E kondüktörü arasında yakın bir ilişki vardır. Kolayca gösterilebilir ki N_E'yi bölen asallar aynı zamanda Δ'yı da böler.

Bir E eliptik eğrisi verildiğinde tüm durumlar için N ve ε'unu hesaplayan geometrik bir algoritma vardır. Bu algoritmaya *Tate algoritması* denir.

Örnek 2.2.8. Verilen bir E eliptik eğrisinin kondüktörü olan N sayısı ve kök sayısı olan ε Magma Hesaplamalı Cebir Sistemi kullanılarak aşağıdaki aşağıdaki komutlar yardımıyla hesaplanır (Bosma, vd.,1997):

```
> E:=EllipticCurve([1,0,23,41,-1]);
> N:=Conductor(E);
> epsilon:=RootNumber(E);
> N;
648165
> epsilon;
1
```

Tanım 2.2.9. E eliptik eğrisinin $\tilde{L} - Fonksiyonu$

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

olarak tanımlanır.

2.3. Birch ve Swinnerton-Dyer Rank Konjektürü İfadesi ve Bazı Sonuçlar

Tanım 2.3.1. E eliptik eğrisinin *analitik rankı* r_{an} ile gösterilir ve $\tilde{L}(E,s)$ fonksiyonunun $s = 1$'deki sıfırının mertebesi olarak tanımlanır, yani

$$\tilde{L}(E,s) = c_{r_{an}}(s-1)^{r_{an}} + \cdots$$

olur.

Aşağıda sayılar teorisinde son yüzyılın en önemli sonuçlarından birisi verilmiştir. BSD-Konjektürü'nün en heyecan veren yanı, analitik bir obje ile cebirsel bir obje arasında bağ kurmasıdır.

Konjektür 2.3.2. (BSD Rank Konjektürü) $E, \mathbb{Q}$ üzerinde bir eliptik eğri olsun. Bu durumda E'nin cebirsel rankı analitik rankına eşittir. Yani

$$r = r_{an}$$

dır.

Bu problem oldukça zordur. Tıpkı ünlü matematikçi Nick KATZ'ın 2001'de BSD-Konjektürü üzerine Arizona'da düzenlenen Arizona Kış Okulu'nda söylediği gibi "bu problemi çözmek için yeni bir fikir gereklidir" (Stein, 2016).

Bu büyük problemin özel halleri uzun süredir çalışılmaktadır. Bu yaklaşım sayesinde A. Wiles, B. Gross, D. Zagier ve V. Kolyvagin konjektürün özel bir durumu olan aşağıdaki sonucu ispatlamıştır.

Teorem 2.3.3. E, $\mathbb{Q}$ üzerinde bir eliptik eğri ve $r_{an} \leq 1$ olsun. Bu durumda

$$r_{an} = r$$

Dir (Wiles, 2000; Gross ve Zagier, 1986; Kolyvagin, 1988).

Uyarı 2.3.4. 2000 yılında Clay Matematik Enstitüsü her birinin çözümüne bir milyon dolar vereceği 7 problemi (web sitesinde) açıklamıştır. BSD konjektürü de bu problemlerden birisidir. Bilim insanları konjektürün ispatı için çeşitli yoğun çalışmalar yapmaya devam etse de bu çalışmanın yapıldığı tarih itibariyle doğrudan konjektür ile ilgili yeni bir sonuç bulunamamıştır.

$\mathbb{Q}$ üzerinde bir eliptik eğrinin rank değerini hesaplamak veya bir rank değerine karşılık gelen eliptik eğri bulmak oldukça zordur. Yine bu çalışmanın yapıldığı tarihi itibariyle $\mathbb{Q}$ üzerinde rankı minimum 28 olan bir eliptik eğri örneği Noam ELKIES tarafından 2006 yılında bulunmuştur (Bober, 2013). Eğri şu şekildedir,

$$y^2 + xy + y = x^3 - x^2 -$$

$$20067762415575526585033208209338542750930230312178956502x + 3448161179503055646703298569039072037485594435931918036126600829629193944873224342 9.$$

Bu eliptik eğri üzerinde sonsuz mertebeli birbirinden bağımsız 28 tane nokta bulunmuştur. Böylece rankın en az 28 olduğu sonucuna ulaşılmıştır.

Aşağıda bir eliptik eğrinin analitik rankıyla ilgili bir sonuç verilmektedir.

Teorem 2.3.5. E, $\mathbb{Q}$ üzerinde bir eliptik eğri, $\varepsilon \in \{\pm 1\}$ E eliptik eğrisinin kök sayısı ve r_{an} E eliptik eğrisinin analitik rankı yani, $r = ord_{s=1}L(E,s)$ olsun. Bu durumda,

$$\varepsilon = (-1)^{r_{an}}$$

dır.

İspat. $s = 1$ için $\Gamma(1) = 1$ olduğundan $ord_{s=1}L(E,s) = ord_{s=1}\Lambda(E,s)$ yazılabilir. O halde teoremi ispatlamak için $L(E,s)$'yi $\Lambda(E,s)$ ile değiştirmek yeterlidir. Diğer yandan $r = r_{an}$ sayısının $\Lambda^{(r)}(E,1) \neq 0$ olacak şekildeki negatif olmayan en küçük r tam sayısı olduğunu biliyoruz. Ardışık türev alınarak herhangi bir $k \geq 0$ tam sayısı için

$$(-1)^k \Lambda^{(k)}(E, 2-s) = \varepsilon \cdot \Lambda^{(k)}(s) \qquad (2.4)$$

olduğu elde edilir. Böylece $s = 1$ ve $k = r$ değerleri yukarıda yerine yazılarak ve $\Lambda^{(r)}(E,1) \neq 0$ argümanı kullanılarak $(-1)^r = \varepsilon$ elde edilir. Böylece teorem ispatlanmış olur.

BSD-Konjektürü'nün doğru olduğu kabul edilirse E eliptik eğrisinin rankını hesaplamak için bir metot bulunabilir.

Teorem 2.3.6. E, $\mathbb{Q}$ üzerinde bir eliptik eğri olsun. Eğer BSD–Konjektürü doğru ise, bu durumda E'nin rankını hesaplamak için bir algoritma vardır. (Stein, 2016)

Teorem 2.3.7. E, $\mathbb{Q}$ üzerinde bir eliptik eğri olsun. Eğer BSD–Konjektürü doğru ise, o zaman $E(\mathbb{Q})$'yu hesaplamak için bir algoritma vardır. (Stein, 2016)

2.4. Parite Konjektürü

Eliptik eğrinin cebirsel ve analitik rankıyla ilgili bir diğer açık problem ise Parite Konjektürü olarak adlandırılır.

Konjektür 2.4.1. (Parite Konjektürü) E, $\mathbb{Q}$ üzerinde bir eliptik eğri olsun. Bu durumda

$$r \equiv r_{an} \pmod 2$$

olur.

Bu problemle ilgili elde edilen güncel sonuçlara bakılacak olursa, bir sonraki bölümde tanımlanacak olan Tate-Shafarevich grubunun sonlu olduğu kabul edilerek T. Dokchitser ve V. Dokchiter oldukça ilgi çekici makalelerinde 2010'da Parite Konjektürü'nün doğru olduğunu ispatlamıştır (Dokchitser ve Dokchitser, 2010). Diğer yandan J. Nekovar yine daha sonra tanımlanacak olan Selmer gruplarını çalışarak Parite Konjektürü boyunca yeni sonuçlar elde etmiştir (Nekovar ve Plater, 2000; Nekovar, 2001; Nekovar, 2007; Nekovar, 2009).

2.5. $L(E,s)$'yi Hesaplamak İçin Çeşitli Metotlar

Bu bölümde s'nin gerçel değerleri için $L(E,s)$'yi hesaplamanın kısa bir yolunu vereceğiz. Dokchitser'de (2004) çok daha ayrıntılı bir hesaplama yöntemi bulunabilir. Aynı kaynakta herhangi bir s karmaşık sayısı için $L(E,s)$'nin Taylor açılımı da bulunabilir.

Teorem 2.5.1 E, $\mathbb{Q}$ üzerinde bir eliptik eğri ve s bir karmaşık sayı olmak üzere $L(E,s)$, E eliptik eğrisinin $L-$ serisi olsun. Bu durumda

$$F_n(t) = \Gamma\left(t+1, \frac{2\pi}{\sqrt{N}}\right) \cdot \left(\frac{\sqrt{N}}{2\pi n}\right)^{t+1}$$

ve

$$\Gamma(z,\alpha)=\int_{\alpha}^{\infty}t^{z-1}e^{-t}dt$$

olmak üzere

$$L(E,s)=N^{-s/2}\cdot(2\pi)^{s}\cdot\Gamma(s)^{-1}\cdot\sum_{n=1}^{\infty}a_n\cdot(F_n(s-1)-\varepsilon F_n(1-s))$$

dir (Lavrik, 1966).

Uyarı 2.5.2. Teorem 2.5.1'de $L(E,s)$ serisi için oldukça hızlı şekilde yakınsayan bir ifade verir. Öte yandan aynı teorem tüm kompleks düzlem üzerinde meremorf şekilde devam ettirilebilen ve belirli bir fonksiyonel eşitliği sağlayan herhangi bir $\sum a_n n^s$ Dirichlet serisi hesaplamaya yarayan bir teoremin özel halidir (Cohen, 2000).

Şimdi ise yaklaşımlar kullanarak rank hesaplama üzerinde duralım. E, $\mathbb{Q}$ üzerinde bir eliptik eğri olsun. Bu durumda bu metot ilk olarak $r=0,1,2,3,\ldots$ için $\mathrm{L}^{(r)}(E,1)$ serisine sürekli şekilde yakınsayan seriyi bulmayı amaçlar. Ardından $\mathrm{L}^{(r)}(E,1)$ türevleri alınarak bu değerlerin 0'dan farklı ilk r değeri bulunur, bu ise E eliptik eğrisinin analitik rankını verir. Dikkat edilirse (2.4) gereği $\mathrm{L}^{(k)}(E,1)$ değerlerinin yarısı otomatik olarak 0 olur. Bu metotla ilgili ayrıntılı bilgi Cremona'da (1997) Bölüm 2.13 ve Dokchitser'de, (2004) bulunabilir.

Bu bölümde biraz daha farklı bir metot kullanılarak $L(E,s)$ serisini hesaplamak için farklı bir metot vereceğiz. Bu metot sadece türev tanımı kullanılarak Teorem 2.5.1 yardımıyla elde edilecektir.

Teorem 2.5.3. $c_r\neq 0$ olmak üzere

$$L(E,s)=c_r(s-1)^r+c_{r+1}(s-1)^{r+1}\ldots$$

olsun. Bu durumda

$$\lim_{s\to 1}(s-1)\cdot\frac{L'(s)}{L(s)}=r.$$

İspat. Doğrudan hesaplama yapılarak

$$\begin{aligned}\lim_{s\to 1}(s-1)\cdot\frac{L'(s)}{L(s)}&=\lim_{s\to 1}(s-1)\cdot\frac{rc_r(s-1)^{r-1}+(r+1)c_{r+1}(s-1)^{r}+\cdots}{c_r(s-1)^r+c_{r+1}(s-1)^{r+1}+\cdots}\\&=r\cdot\lim_{s\to 1}\frac{c_r(s-1)^r+\frac{(r+1)}{r}c_{r+1}(s-1)^{r+1}+\cdots}{c_r(s-1)^r+c_{r+1}(s-1)^{r+1}+\cdots}\\&=r.\end{aligned}$$

bulunur. Bu da ispatı bitirir.

3. BSD FORMÜLÜ ÜZERİNE

3.1 Eliptik Eğrilerin Selmer ve Tate–Shafarevich Grupları

E, $\mathbb{Q}$ üzerinde tanımlı bir eliptik eğri, $\overline{\mathbb{Q}}$, $\mathbb{Q}$'nun cebirsel kapanışı ve

$$G_{\mathbb{Q}} \coloneqq Aut_{\mathbb{Q}}(\overline{\mathbb{Q}})$$

$\mathbb{Q}$'nun mutlak Galois grubu olsun. $m \in \mathbb{N}$ için $H^m(\mathbb{Q}, E)$ ile m. Galois kohomoloji grubu gösterilsin. Böylece her $m \in \mathbb{N}$ için $G_{\mathbb{Q}} -$ modüllerinin

$$0 \longrightarrow E(\overline{\mathbb{Q}})[n] \longrightarrow E(\overline{\mathbb{Q}}) \xrightarrow{\ n\ } E(\overline{\mathbb{Q}}) \longrightarrow 0$$

tam dizisi elde edilir.

Serre'a (1979) göre Galois kohomoloji gruplarının yukarıda belirtilen kısa tam dizi ile eşleşmiş bir uzun tam dizisi vardır. Böylece bu uzun tam dizinin başlangıcı göz önüne alınarak E eliptik eğrisi ile eşleşen

$$0 \longrightarrow E(\mathbb{Q})/nE(\mathbb{Q}) \longrightarrow H^1(G_{\mathbb{Q}}, E(\overline{\mathbb{Q}})[n]) \xrightarrow{\ \alpha\ } H^1(G_{\mathbb{Q}}, E(\overline{\mathbb{Q}})[n]) \longrightarrow 0$$

Kummer dizisi elde edilir.

Tanım 3.1.1. Her bir p asalı için $\mathbb{Q}$ nun p -adik valüasyona karşılık gelen $\overline{\mathbb{Q}}$ genişlemesi seçilsin. G_p, $G_{\mathbb{Q}}$ da karşılık gelen ayrışma grubu, P asal sayıların kümesi ve $\gamma_{p,n}$ dönüşümü

$$\gamma_{p,n}: H^1(G_{\mathbb{Q}}, E(\overline{\mathbb{Q}})[n]) \longrightarrow H^1(G_{\mathbb{Q}}, E(\overline{\mathbb{Q}}))[n]$$

özelliğindeki kısıtlama dönüşümü olsun. Bu durumda E eliptik eğrisinin Tate–Shafarevich grubu $Ш(E/\mathbb{Q})$ ile gösterilir ve

$$Ш(E/\mathbb{Q})[n] \coloneqq \bigcap_{p \in P} \ker(\gamma_{p,n})$$

olmak üzere

$$Ш(E/\mathbb{Q}) \coloneqq \bigcup_{n \in \mathbb{N}} Ш(E/\mathbb{Q})[n]$$

olarak tanımlanır. E eliptik eğrisinin Selmer grubu ise $S_{\mathbb{Q}}(E)$ ile gösterilir ve

$$S_{\mathbb{Q}}(E)[n] \coloneqq \alpha^{-1}(Ш(E/\mathbb{Q})[n])$$

olmak üzere

$$S_{\mathbb{Q}}(E) \coloneqq \bigcup_{n \in \mathbb{N}} S_{\mathbb{Q}}(E)[n]$$

olarak tanımlanır.

3.2 Tate-Shafarevich Grupları Hakkında Bazı Sonuçlar

Eliptik eğriler konusunda ilerleme kaydedebilmek için BSD-Konjektürü'nü ispatlamak, BSD-Konjektürü'nü elde edebilmek için de Tate-Shafarevich gruplarının özelliklerinin çok iyi bilinmesi gerekir. Bu konu matematikte son yılların en popüler konularından birisidir. Özellikle Tate-Shafarevich grubunun sonluluğu hakkındaki gizem sürmektedir. Bu bölümde bu tez çalışması tarihi itibariyle literatürde mevcut sonuçları ve doğruluğu hakkında güçlü kanılara sahip olunan bazı konjektürleri vereceğiz.

İlk olarak Tate ve Shafarevich tarafından 1960'larda ortaya atılan konjektürü verelim.

Konjektür 3.2.1. (Tate-Shafarevich): $\mathbb{K}$ bir sayı cismi ve E, $\mathbb{K}$ üzerinde bir eliptik eğri olsun. Bu durumda $Ш(E/\mathbb{K})$sonludur (Silverman, 1986).

Aşağıda bir eliptik değerinin Tate-Shafarevich grubunun aritmetiği hakkında önemli bir sonuç verilmiştir.

Teorem 3.2.2. $\mathbb{K}$ bir sayı cismi ve E, $\mathbb{K}$ üzerinde bir eliptik eğri olsun. Eğer $Ш(E/\mathbb{K})$ sonlu ise bu takdirde $\#Ш(E/\mathbb{K})$ bir tam karedir (Cassells, 1965).

E, $\mathbb{Q}$ üzerinde tanımlı bir eliptik eğri olsun. Bu durumda $L(E,1)$ değeri ile $Ш(E/\mathbb{Q})$ ve dolayısıyla $E(\mathbb{Q})$ arasında oldukça önemli bir ilişki vardır. Bazı kısıtlamalarla Tate-Shafarevich konjektürü hakkında aşağıdaki ilerlemeler kaydedilmiştir.

Teorem 3.2.3. E, $\mathbb{Q}$ üzerinde üzerinde tanımlı kompleks çarpıma sahip bir eliptik eğri olsun. Eğer $L(E,1) \neq 0$ ise $\#E(\mathbb{Q})$ sonludur (Coates ve Wiles, 1977).

Teorem 3.2.4. E, $\mathbb{Q}$ üzerinde tanımlı bir eliptik eğri olsun. Eğer $L(E,s)$ fonksiyonu $s = 1$ de birinci mertebeden sıfır yerine sahipse bu takdirde E'nin sonsuz mertebeli bir rasyonel noktası vardır (Gross-Zagier, 1986).

Bu iki sonuç kullanılarak Karl Rubin aşağıdaki önemli teoremi vermiştir.

Teorem 3.2.5. E, $\mathbb{Q}$ üzerinde üzerinde tanımlı kompleks çarpıma sahip bir eliptik eğri olsun. Bu durumda $\#Ш(E/\mathbb{Q})$ sonludur (Rubin, 1987).

Aslında Rubin (1987) yukarıdaki teoremle birlikte oldukça derin sonuçlar bulundurmaktadır.

E, $\mathbb{Q}$ üzerinde bir eliptik eğri ve r_{an}, $L(E,s)$ fonksiyonunun $s = 1$'deki sıfırının mertebesi ve r, E eliptik eğrisinin rankını göstersin. Bu koşullar altında Kolyvagin aşağıdaki önemli sonucu vermiştir.

Teorem 3.2.6. Eğer $r_{an} \leq 1$ ise bu takdirde $r_{an} = r$ ve $Ш(E/\mathbb{Q})$ sonludur. (Kolyvagin, 1988)

Tate-Shafarevich grupları halen popüler olarak çalışılan bir konu olup yazarları arasında 2014 Fields madalyası sahibi Manjul Bhargava'nın yer aldığı 2014'de arxiv.org da yer alan makalede aşağıdaki sonuç verilmiştir. Bu sonuç tez çalışması tarihi itibariyle literatürde yer alan en güncel sonuçtur. Bu sonuç kabaca $\mathbb{Q}$ üzerinde eliptik eğrilerin büyük çoğunluğunun ($> \%66$) BSD-Konjektürü'nü sağladığını göstermektedir.

Teorem 3.2.7. $\mathbb{Q}$ üzerinde tanımlı yüksekliğe göre sıralanmış eliptik eğrilerin önemli bir çoğunluğu BSD Rank Konjektürü'nü sağlar (Bhargava, vd., 2014).

Uyarı 3.2.8. 1. Teoremin ifadesinde yer alan "önemli bir çoğunluk" en az yüzde 66,48'i belirtmektedir.

2. Bhargava ve diğerlerinde BSD Rank Konjektürü'nün doğruluğu dışında Tate-Shafarevich grubunun sonluluğu hakkında da önemli bir sonuç verilmektedir.

Teorem 3.2.9. $\mathbb{Q}$ üzerinde tanımlı yüksekliğe göre sıralanmış eliptik eğrilerin önemli bir çoğunluğunun Tate-Shafarevich grubu sonludur (Bhargava, vd., 2014).

Bunlardan başka aynı çalışmada cebirsel ve analitik rankları 0 ile cebirsel ve analitik rankları 1 olan eliptik eğrilerin tüm eliptik eğrilerin içindeki oranı için bazı yeni alt sınırlar verilmiştir.

Teorem 3.2.10. $\mathbb{Q}$ üzerinde tanımlı yüksekliğe göre sıralanmış eliptik eğrilerin en az %16.5'inin cebirsel ve analitik rankı sıfır, en az %20,68'inin cebirsel ve analitik rankı biridir (Bhargava, vd., 2014).

Sonuç 3.2.11. $\mathbb{Q}$ üzerinde tanımlı yüksekliğe göre sıralanmış eliptik eğrilerin cebirsel veya analitik rankının ortalaması 0,2068'dir (Bhargava, vd., 2014).

Örnek 3.2.12. Teorem 3.2.5. kullanılarak $\mathbb{Q}$ üzerinde tanımlı ve kompleks çarpıma sahip kondüktörü 27 olan, $y^2 + y = x^3 - 7$ eliptik eğrisinin Tate-Shafarevich grubunun sonlu olduğu gösterilebilir.

3.3. BSD Formülü

Bu bölümde Birch ve Swinnerton-Dyer tarafından verilen ve eliptik eğrilerin cebirsel ve analitik özelliklerini birleştiren doğruluğun kabul edilmesiyle bir çok önemli hesaplamada faydalı olacak bir formül verilecektir.

Konjektür 3.3.1. (BSD Formülü). E, $\mathbb{Q}$ üzerinde üzerinde rankı r olan bir eliptik eğri olsun. Bu takdirde $r = ord_{s=1}L(E,s)$ ve

$$\frac{\mathrm{L}^{(r)}(E,1)}{r!} = \frac{\Omega_E \cdot Reg(E) \cdot \#Ш(E/\mathbb{Q}) \prod_p c_p}{\#E_{tors}(\mathbb{Q})^2}$$

olur. Burada c_p Tamagawa sayılarını, $Reg(E)$ E eliptik eğrisinin regülatörünü, Ω_E ise E eliptik eğrisinin gerçel periyodunu gösterir (Silverman, 1986).

Şimdi bu konjektürü anlamaya çalışıp bazı örneklerle doğrulayalım.

Tanım 3.3.2.

$$y^2 + \underline{a}_1 xy + \underline{a}_3 y = x^3 + \underline{a}_2 x^2 + \underline{a}_4 x + \underline{a}_6$$

E eliptik eğrisi için minimal Weierstrass eşitliği olsun. Bu durumda E eliptik eğrisinin gerçel periyodu Ω_E ile gösterilir ve

$$\Omega_E = \int_{E(\mathbb{R})} \frac{dx}{2y + \underline{a}_1 x + \underline{a}_3}$$

olarak tanımlanır.

Uyarı 3.3.3. Cremona (1997), Bölüm 3.7'de Gauss aritmetik-geometrik ortalaması kullanılarak Ω_E'yi etkili olarak hesaplamak için bir metot verilmektedir.

Teorem 3.3.4. E, $\mathbb{Q}$ üzerinde bir eliptik eğri olsun. $P_1, \dots, P_n$ "modülo torsiyon"da bir taban olsun ve "$\langle , \rangle$" E eliptik eğrisi için Neron-Tate kanonik yükseklik eşlemesini göstersin. Bu durumda E eliptik eğrisinin regülatörü $Reg(E)$ ile gösterilir ve (i,j)'deki girdisi $\langle P_i, P_j \rangle$ olmak üzere $n \times n$ tipindeki matrisin determinantının mutlak değer olarak tanımlanır.

Tanım 3.3.5. p asal olmak üzere, E, $\mathbb{Q}_p$ p-adik cismi üzerinde tanımlı bir eliptik eğri olsun. Bu durumda E'nin p'deki Tamagawa sayısı c_p ile gösterilir ve

$$c_p \coloneqq [E\left(\mathbb{Q}_p\right) : E^0\left(\mathbb{Q}_p\right)]$$

sonlu indeksi olarak tanımlanır. Burada $E^0\left(\mathbb{Q}_p\right)$ iyi indirgemeye sahip noktaların oluşturduğu alt grubu göstermektedir. Böylece iyi asal p'ler için $c_p = 1$ olur.

Örnek 3.3.6. Bir E eliptik eğrisinin herhangi bir p'de Tamagawa sayısı aşağıdaki şekilde hesaplanır.

```
> E:=EllipticCurve([0,-1,1,-10,-20]);
> E;
>TamagawaNumber(E,11);
>5
```

Uyarı 3.3.7. Cremona (1997), Bölüm 3.2'de Tamagawa sayılarını hesaplamak için etkin bir metot verilmiştir.

Uyarı 3.3.8. E, $\mathbb{Q}$ üzerinde bir eliptik eğri olsun. Bu durumda $Ш(E/\mathbb{Q})$ grubunun sonlu olup olmadığının henüz bir netliğe kavuşmuş olmadığını gördük. $\#Ш(E/\mathbb{Q})$'yu hesaplamak için bilinen genel bir algoritma olmamasına karşın Grigorov, vd., (2005) $\#Ш(E/\mathbb{Q})$'yu pratikte hesaplamaya yarayan bazı metotlar verilmiştir. Gerçekten de BSD Rank Konjektürü'nün doğru olduğu ve $Ш(E/\mathbb{Q})$'nun sonlu olduğu kabul edilse bile hala $\#Ш(E/\mathbb{Q})$'yu hesaplama yarayacak bir yol henüz yoktur.

$Ш(E/\mathbb{Q})$'nun sonlu olduğunu kabul edelim. Bu durumda herhangi bir p asalı için $Ш(E/\mathbb{Q})$'nun p'inci kısmı olan $Ш(E/\mathbb{Q})(p)$ hesaplanabilir. Ancak burada hangi p asalına kadar hesaplama yapacağımızı bilmiyoruz. Dikkat edilirse $r_{E,an} \leq 1$ durumunda Kolyvagin'in sonucu olan Teorem 3.2.6. kullanılarak $\#Ш(E/\mathbb{Q})$ sayısı için kesin bir üst sınır verildiğinden böyle bir durumda $\#Ш(E/\mathbb{Q})$ hesaplanabilirdir.

4. BSD KONJEKTÜRÜ'NÜN UYGULAMALARI

Bu bölümde Magma Hesaplamalı Cebir Sistemi kullanılarak BSD konjektürü için bir önceki bölümde verilen hesaplama formülü ile ilgili konjektürü doğrulayan bazı örnekler verilecektir (Bosma, vd.,1997).

Örnek 4.1. İlk olarak rankı sıfır olan $\mathbb{Q}$ üzerinde tanımlı

$$y^2 + y = x^3 - x^2 - 10x - 20$$

eliptik eğrisini göz önüne alalım. Bu eğri Magma Hesaplamalı Cebir Sisteminde

```
>E:=EllipticCurve([0,-1,1,-10,-20]);
```

komutuyla tanımlanır(Bosma, vd.,1997). Eğrinin doğru tanımlanıp tanımlanmadığını anlamak için E; komutu yazılır. Bu eğrinin diskriminantı, rankı ve kondüktörü sırasıyla

```
> Discriminant(E);
> Rank(E);
> Conductor(E);
```

komutları ile hesaplanır.

Aynı eliptik eğrinin Cremona eliptik eğri veri tabanındaki yerini bulmak için "isogeni sınıfı" ve kondüktör ile etkilendiği eğriyi bulabilmek için "CremonaReference(E);" komutu yazılır (Cremona, 2017). Bu komutlar yardımıyla yukarıda tanımlanan E eliptik eğrisi için yazılan komutların ekran görüntüsü

```
> E:=EllipticCurve([0,-1,1,-10,-20]);
> E;
Elliptic Curve defined by y^2 + y = x^3 - x^2 - 10*x - 20 over Rational Field
> Discriminant(E);
-161051
> Rank(E);
0
> Conductor(E);
11
> CremonaReference(E);
11a1
```

şeklindedir.

E eliptik eğrisinin $L-$fonksiyonun $s = 1$'deki değeri aşağıdaki şekilde hesaplanır;

```
> a:=LSeries(E);
> b:=Evaluate(a,1);
> b;
0.25384186085591068433775892335 1
```

Burada dikkat edilirse transandantal bir sayı olan b sayısı Magma Hesaplamalı Cebir Sisteminde standart hesaplamaya göre 30 haneye kadar hesaplanmıştır (Bosma, vd.,1997). Daha fazla ondalık basamak hesaplayabilmek için örneğin 40 basamak için Magma Hesaplamalı Cebir Sisteminde

```
> a:=LSeries(E: Precision:=40);
> b:=Evaluate(a,1);
> b;
```

şeklinde bir komut yazılabilir (Bosma, vd.,1997). Prensipte $L-$serisi istenilen kadar basamak için hesaplanabilir. Buradaki esas sıkıntı hesaplama süresidir.

BSD formülünde yer alan Ω_E gerçel periyot değerini "RealPeriod(E);" komutuyla hesaplarız. Bu değer de standart komutta 30 haneli hesaplanmakta olup örneğin 100 basamak değeri için

```
> RealPeriod(E);
1.269209304279553421688794616754547305219492241830608667967
> RealPeriod(E: Precision:=100);
1.269209304279553421688794616754547305219492241830608667967
1369212304083386127777226903623059215126 07
```

şeklinde işlem yapılır.

Formülde yer alan E eliptik eğrisinin regülatörü olan $Reg(E)$ ise "Regulator(E);" şekilde hesaplanır. Dikkat edilirse burada $rank(E) = 0$ olduğu için $Reg(E)$ tanım gereği 1 olur.

Tamagawa sayıları ise şu şekilde hesaplanır. E eliptik eğrisinin diskriminantı $\Delta = -161050 = (-11)^5$ olduğundan $p = 11$ dışındaki tüm c_p Tamagawa sayıları tanım gereği 1'dir. $p = 11$ deki Tamagawa sayısı yani c_{11} ise

```
> TamagawaNumber(E,11);
5
> TamagawaNumber(E,13);
1
```

şeklinde hesaplanır.

E eliptik eğrisinin torsiyon alt grubunun mertebesi ise

```
> A:=TorsionSubgroup(E);
> #A;
5
```

şeklinde hesaplanır.

E eliptik eğrisi için $\#Ш(E/\mathbb{Q})$ aşağıdaki şekilde hesaplanır:

```
> E := EllipticCurve("11a1");
> K := RationalsAsNumberField();
> EK := BaseChange(E,K);
> ConjecturalSha(EK,[]);
1.00000
```

Tüm bu veriler eşliğinde BSD formülünün doğruluğunu bu örnek için sayısal olarak test edelim. $r = 0$ olduğundan

$$\frac{\mathrm{L}^{(r)}(E,1)}{r!} = \frac{L(E,1)}{1} = L(E,1) = 0.25384186085591068433775892335 1 \quad (4.1)$$

$$\frac{\Omega_E \cdot Reg(E) \cdot \#Ш(E/\mathbb{Q}) \prod_p c_p}{\#E_{tors}(\mathbb{Q})^2} = \frac{1.26920930427955342168879461675 \cdot 1 \cdot 1 \cdot 5}{5^2}$$

$$= 0.25384186085591068433775892335 1 \quad (4.2)$$

(4.1) ve (4.2) ifadeleri birbirine eşit olduğundan BSD formülü bu değerler için sağlanır.

Uyarı 4.2. 1. Yukarıdaki #Ш("11a1") değeri BSD'nin doğru olduğu kabul edilerek (*) formülünden hesaplanan değerdir. Burada analitik rankın sıfır olması nedeniyle bu hesap Magma Hesaplamalı Cebir Sisteminde kolaylıkla yapılmıştır (Bosma, vd.,1997).

2. Burada konjektürel #Ш("11a1") değeri 1 çıktığı için eliptik eğri "11a1" aşikar Tate-Shafarevich grubuna sahiptir denir.

3. BSD formülünde yer alan Ω_E, eğri tek parça iken yani $\Delta < 0$ olduğunda "RealPeriod(E);" değerine eşit, eğri iki parça iken yani $\Delta > 0$ olduğunda "RealPeriod(E);" değerinin iki katına eşit olur. Bundan sonraki örneklerde "p:=(Discriminant(E) gt 0 select 2 else 1) * RealPeriod(E);" komutu yazılarak her iki duruma da uygun hesaplama yapılacaktır ve $\#Ш(E/\mathbb{Q})$ değeri BSD formülünün doğruluğu kabul edilerek Magma Hesaplamalı Cebir Sisteminde yazılan kod ile hesaplanacaktır (Bosma, vd.,1997).

Örnek 4.3. Şimdi de rankı sıfır ancak, aşikar olmayan Tate-Shafarevich grubuna sahip bir eliptik eğri için BSD Konjektür Formülü'nü doğrulayalım. $\mathbb{Q}$ üzerindeki E eliptik eğrisi

$$y^2 + xy = x^3 + x^2 - 1154x - 15345$$

olsun. Bu eğri Magma Hesaplamalı Cebir Sisteminde

```
> E:=EllipticCurve([1,1,0,-1154,-15345]);
> E;
```

şeklinde ifade edilir (Bosma, vd.,1997). Verilen eliptik eğrinin diskriminantı, rankı, kondüktörü, Cremona referansı, gerçel periyodu ve regülatörü bir önceki örnekteki gibi

hesaplanabilir. Bu örnek için diskriminant 3042735921 olduğundan, Tamagawa sayılarını bulmak için önce hangi p asalı için işlem yapacağımızı bulmalıyız. Bunun için diskriminantı bölen p asallarını belirlemek amacıyla

```
> Factorization(3042735921);
```

kodu Magma Hesaplamalı Cebir Sistemi ekranına yazılır (Bosma, vd.,1997). 3 ve 227 sayıları bulunur. $p = 3$ ve $p = 227$ deki Tamagawa sayıları c_3 ve c_{227} hesaplanarak çarpılır. Verilen eliptik eğrinin BSD formülünde geçen ifadelerin hesaplanması için girilen komutlar ve ekran çıktıları ise şu şekilde olur;

```
> E:=EllipticCurve([1,1,0,-1154,-15345]);
> E;
Elliptic Curve defined by y^2 + x*y = x^3 + x^2 - 1154*x - 15345 over Rational
Field
> d:=Discriminant(E);
> Rank(E);
0
> Conductor(E);
681
> Factorization(3042735921);
[ <3, 10>, <227, 2> ]
> CremonaReference(E);
681b1
> a:=LSeries(E);
> b:=Evaluate(a,1);
> b;
1.844815206126820716928527729 16
> p:=(Discriminant(E) gt 0 select 2 else 1) * RealPeriod(E);
> p;
0.819917869389698096412678990738
> rg:=Regulator(E);
> c_3:=TamagawaNumber(E,3);
> c_227:=TamagawaNumber(E,227);
> c:=c_3 * c_227;
> A:=TorsionSubgroup(E);
> e:=#A;
> ConjSha:=(b*e^2)/(p*rg * c );
> ConjSha;
9.000000000000000000000000000
```

Dikkat edilirse $\#Ш(E/\mathbb{Q})$ değeri BSD formülünün doğruluğu kabul edilerek hesaplanmıştır.

Örnek 4.4. Bu örnekte rankı bir olan $\mathbb{Q}$ üzerinde tanımlı

$$y^2 + y = x^3 - x$$

eliptik eğrisi için BSD formülünü doğrulayalım. Dikkat edilirse bu örnek için rank 1 olduğundan L- fonksiyonunun birinci mertebeden türevini hesaplamamız gerekecek. Bunun için Magma Hesaplamalı Cebir Sisteminde

```
> a:=LSeries(E);
> b:=Evaluate(a,1 : Derivative:=1);
> b;
```

kodlarını yazmamız yeterlidir(Bosma, vd.,1997). Formülde geçen diğer bileşenler için önceki örneklerdeki gibi hesaplamalar yapılır. Girilen kodlar ve ekran çıktısı şu şekildedir;

```
> E:=EllipticCurve([0,0,1,-1,0]);
> E;
Elliptic Curve defined by y^2 + y = x^3 - x over Rational Field
> d:=Discriminant(E);
> Rank(E);
1
> Conductor(E);
37
> CremonaReference(E);
37a1
> a:=LSeries(E);
> b:=Evaluate(a,1 : Derivative:=1);
> b;
0.30599977383405230182048368 3322
> p:=(Discriminant(E) gt 0 select 2 else 1) * RealPeriod(E);
> p;
5.98691729246391925966401995891
> rg:=Regulator(E);
> c_37:=TamagawaNumber(E,37);
> c:=c_37;
> A:=TorsionSubgroup(E);
> e:=#A;
> ConjSha:=(b*e^2)/(p*rg * c );
> ConjSha;
1.00000000000000000000000000000
```

Örnek 4.5. Bu örnekte rankı 2 olan $\mathbb{Q}$ üzerinde tanımlı

$$y^2 + y = x^3 + x^2 - 2x$$

eliptik eğrisini göz önüne alalım. Bu örnek için rank 2 olduğundan BSD formülü

kullanarak $\#Ш(E/\mathbb{Q})$ değerini hesaplarken bu kez ikinci türev alınırken payda kısmına da 2! geldiğini göz önünde bulundurmalıyız. Magma Hesaplamalı Cebir Sisteminde kodları ve ekran çıktısı şu şekildedir (Bosma, vd.,1997);

```
> E:=EllipticCurve([0,1,1,-2,0]);
> E;
Elliptic Curve defined by y^2 + y = x^3 + x^2 - 2*x over Rational Field
> d:=Discriminant(E);
> Rank(E);
2
> Conductor(E);
389
> CremonaReference(E);
389a1
> a:=LSeries(E);
> b:=Evaluate(a,1 : Derivative:=2);
> b;
1.5186330005768535404603852157 9
> p:=(Discriminant(E) gt 0 select 2 else 1) * RealPeriod(E);
> p;
4.9804251217101101506427155838 8
> rg:=Regulator(E);
> c_389:=TamagawaNumber(E,389);
> c:=c_389;
> A:=TorsionSubgroup(E);
> e:=#A;
> ConjSha:=(b*e^2)/(p*rg * c*2 );
> ConjSha;
1.0000000000000000000000000000 0
```

Örnek 4.6. Bu örnekte rankı üç olan $\mathbb{Q}$ üzerinde tanımlı

$$y^2 + y = x^3 - 7x + 6$$

eliptik eğrisini göz önüne alalım. Magma Hesaplamalı Cebir Sisteminde çıktısı şu şekildedir (Bosma, vd.,1997);

```
> E:=EllipticCurve([0,0,1,-7,6]);
> E;
Elliptic Curve defined by y^2 + y = x^3 - 7*x + 6 over Rational Field
> d:=Discriminant(E);
> Rank(E);
3
> Conductor(E);
5077
> CremonaReference(E);
5077a1
> a:=LSeries(E);
```

```
> b:=Evaluate(a,1 : Derivative:=3);
> b;
10.391099400715804138751850 5104
> p:=(Discriminant(E) gt 0 select 2 else 1) * RealPeriod(E);
> p;
4.151687983086933049884175683 51
> rg:=Regulator(E);
> c_5077:=TamagawaNumber(E,5077);
> c:=c_5077;
> A:=TorsionSubgroup(E);
> e:=#A;
> ConjSha:=(b*e^2)/(p*rg * c*6 );
> ConjSha;
1.000000000000000000000000000 00
```

Örnek 4.7. Bu örnekte ise rankı 6 olan $\mathbb{Q}$ üzerinde tanımlı

$$y^2 + xy = x^3 - x^2 - 79x + 289$$

eliptik eğrisini inceleyelim. Bu eğri için Magma Hesaplamalı Cebir Sistemi ekranı şu şekildedir(Bosma, vd.,1997);

```
> E:=EllipticCurve([1,-1,0,-79,289]);
> E;
Elliptic Curve defined by y^2 + x*y = x^3 - x^2 - 79*x + 289 over Rational Field
> d:=Discriminant(E);
> Rank(E);
4
> Conductor(E);
234446
> CremonaReference(E);
234446a1
> a:=LSeries(E);
> b:=Evaluate(a,1 : Derivative:=4);
> b;
214.652337501621337114022200403
> p:=(Discriminant(E) gt 0 select 2 else 1) * RealPeriod(E);
> p;
2.972671847263335536001777300 80
> rg:=Regulator(E);
> c_2:=TamagawaNumber(E,2);
> c_117223:=TamagawaNumber(E,117223);
> c:=c_2*c_117223;
> A:=TorsionSubgroup(E);
> e:=#A;
> ConjSha:=(b*e^2)/(p*rg * c*24 );
> ConjSha;
1.000000000000000000000000000 00
```

KAYNAKLAR

Asar, A. O., Arıkan, A., Arıkan, A., "Cebir" , ***Eflatun Yayın Evi***, Maltepe-Ankara (2009).

Ball., W. W.R., "A Short Account of the History of Mathematics" , ***Dover Books on Mathematics***, The UK, (2010).

Breuil, C., Conrad, B., Diamond, F., Taylor, R., "On The Modularity Of Elliptic Curves Over Q: Wild 3-Adic Exercises", ***J. Amer. Math. Soc.***, 14 (4): 843–939 (2001).

Bober, J. W., "Proceedings of the Tenth Algorithmic Number Theory Symposium", http://msp.org/obs/2013/1-1/obs-v1-n1-p07-s.pdf (2013).

Bosma, W.,Cannon, J., Playoust, C.,"The Magma AlgebraSystem. I: The User Language"***Journal of SymbolicComputation***, 24(3-4): 235-265 (1997).

Cassells, J. W. S.."Arithmetic on Curvesgenus 1", ***VII on conjectures of BirchandSwinnerton–Dyer,*** Cambridge, ENGLAND, 180–199. (1965).

Clay Mathematics Institute, Birch and Swinnerton-Dyer Conjecture, http://www.claymath.org/millennium-problems/birch-and-swinnerton-dyer-conjecture (Ziyaret edilme tarihi: 31.12.2016).

Cohen, H., "Advanced Topics in Computational Number Theory Graduate Texts in Mathematics", ***Springer-Verlag***, New York, (2000).

Coates, J., Wiles, A. "On the conjecture of Birch and Swinnerton-Dyer." ***Invent. Math.***, 39(3): 223–251 (1977)

Cremona, J., E., "Algorithms For Modular Elliptic Curves", ***Cambridge University Press***, Cambridge (1997).

Cremona, J., E., Algorithms for Modular Elliptic Curves, Online Edition , http://homepages.warwick.ac.uk/staff/J.E.Cremona/book/fulltext/index.html (Ziyaret edilme tarihi: 01.01.2017).

Dokchitser, T., "Computing special values of motivic L-functions", ***Experiment. Math.*** 13(2): 137-149 (2004).

Dokchitser, T.,Dokchitser, V., "On theBirch-Swinnerton-Dyer Quotients Modulo Squares" ***Annals of Math. (2)*** 172 (1): 567–596 (2010).

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

Hasse, H., , "Zur Theorie Der Abstrakten Elliptischen Funktionenkörper. I, II & III", ***Crelle's Journal***, 1936 (175): 149 (1936).

KAYNAKLAR (devam ediyor)

hyperelliptic.org, http://www.hyperelliptic.org/ (Ziyaret edilme tarihi: 31.12.2016).

İnam, İ., "Modüler Formlar, Eliptik Eğriler Ve Uygulamaları", Doktora Tezi, ***Uludağ Üniversitesi Fen Bilimleri Enstitüsü***, Bursa (2011).

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

Lavrik, A. F., "The Functional Equation For Dirichlet L-Functions And The Problem Of Divisors İn Arithmetic Progressions" ***Izv. Akad. Nauk SSSR Ser. Mat.***, 30: 433-448 (1966).

Nekovář, J., Plater, A., "On the parity of ranks of Selmer Groups", ***Asian J. Math***., 4(2): 437–497 (2000).

Nekovář, J., "On The Parity of Ranks of Selmer Groups. II." ***C. R. Acad. Sci. Paris Sér. I Math***. 332(2): 99–104 (2001).

Nekovář, J., "On The Parity of Ranks of Selmergroups. III", ***Documenta Mathematica***, 12 : 243–274 (2007).

Nekovář, J., "On The Parity Of Ranks Of Selmer Groups. IV.", ***Compos. Math***.,145(6): 1351–1359 (2009).

Rubin, K., "Tate-Shafarevich Groups and L-Functions of Elliptic Curves With Complex Multiplication", ***Inventiones Mathematicae***, 89: 527-560 (1987).

Silverman, J., H., "TheArithmetic of EllipticCurves". **Springer-Verlag**, USA (1986).

Silverman, J., H., An Introduction to the Theory of Elliptic Curves https://www.math.brown.edu/~jhs/Presentations/WyomingEllipticCurve.pdf (2006).

Stein, A. W., The Birch and Swinnerton-Dyer Conjecture, a Computational Approach, https://github.com/williamstein/bsd (Ziyaret edilme tarihi: 31.12.2016).

Tate, J., "AlgorithmForDeterminingTheType of A Singular Fiber in an EllipticPencil", ***Modular Functions of OneVariable IV, LectureNotes in Mathematics, Berlin / Heidelberg: Springer***, 476:33–52 (1975).

Washington, J., L., "Elliptic Curves",***Chapman&Hall/C*****RC**, Florida, USA (2003).

Weil, A., "Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen." ***Mathematische Annalen***, 168: 149–156 (1967).

KAYNAKLAR (devam ediyor)

Wiles, A. "Modular Elliptic Curves And Fermat's Last Theorem" ***Annals of Math. (2)***, 141(3); 443–551(1995).

Wiles, A., "Twenty Years Of Number Theory" Mathematics: frontiers and perspectives, Vladimir Igorevich Arnol′d, ***Amer. Math. Soc***., Providence, 329–342 (2000).

ÖZGEÇMİŞ

Fotoğraf

Kişisel Bilgiler

Adı Soyadı : Fatih TANRIKULU

Doğum Yeri ve Tarihi : Bünyan / 1984

Eğitim Durumu

Lisans Öğrenimi : Gazi Üniversitesi, Matematik

Bildiği Yabancı Diller : İngilizce

Bilimsel Faaliyetleri :

İş Deneyimi

Stajlar :

Projeler :

Çalıştığı Kurumlar : TSK

İletişim

Adres : TSK

Tel : 0(212) 663 24 90

E-Posta Adresi : fatih_84@mynet.com

Akademik Çalışmaları

i. ……

Yabancı Dil Bilgisi **:** İngilizce (Orta Seviye)

Tarih: 09.01.2017