T.C.

BURSA ULUDAĞ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

CEBİRSEL EĞRİLER ÜZERİNDEKİ RASYONEL DİZİLER

Gamze SAVAŞ ÇELİK
0000-0002-6609-1713

Prof. Dr. Gökhan SOYDAN
(Danışman)

DOKTORA TEZİ
MATEMATİK ANABİLİM DALI

BURSA – 2022

TEZ ONAYI

Gamze SAVAŞ ÇELİK tarafından hazırlanan "Cebirsel Eğriler Üzerindeki Rasyonel Diziler" adlı tez çalışması aşağıdaki jüri tarafından oy birliği/oy çokluğu ile Bursa Uludağ Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı'nda **DOKTORA TEZİ** olarak kabul edilmiştir.

Danışman **:** Prof. Dr. Gökhan SOYDAN

Üye: Prof. Dr. Gökhan SOYDAN İmza
0000-0002-6321-4132
Bursa Uludağ Üniversitesi Fen Edebiyat Fakültesi,
Matematik Anabilim Dalı

Üye: Prof. Dr. İ. Naci CANGÜL İmza
0000-0002-0700-5774
Bursa Uludağ Üniversitesi Fen Edebiyat Fakültesi,
Matematik Anabilim Dalı

Üye: Prof. Dr. A. Muhammed ULUDAĞ İmza
0000-0001-7761-8472
Galatasaray Üniversitesi Fen Edebiyat Fakültesi,
Matematik Anabilim Dalı

Üye: Doç. Dr. Alp BASSA İmza
0000-0002-9685-7361
Boğaziçi Üniversitesi Fen Edebiyat Fakültesi,
Matematik Anabilim Dalı

Üye: Prof. Dr. S. Kemal AKAY İmza
0000-0002-7597-1528
Bursa Uludağ Üniversitesi Fen Edebiyat Fakültesi,
Fizik Anabilim Dalı

Yukarıdaki sonucu onaylarım

Prof. Dr. Hüseyin Aksel EREN
Ensititü Müdürü
/ 01 / 2022

B. U. Ü. Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu,
- başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- atıfta bulunduğum eserlerin tümünü kaynak olarak gösterdiğimi,
- kullanılan verilerde herhangi bir tahrifat yapmadığımı,
- ve bu tezin herhangi bir bölümünü bu üniversite veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı

beyan ederim.

07 / 01 / 2022

İmza

Gamze SAVAŞ ÇELİK

Bu tez çalışması Bursa Uludağ Üniversitesi Bilimsel Araştırma Projeleri Birimi tarafından F-2020/8 nolu proje ile desteklenmiştir.

TEZ YAYINLANMA
FİKRİ MÜLKİYET HAKLARI BEYANI

Enstitü tarafından onaylanan lisansüstü tezin tamamını veya herhangi bir kısmını, basılı (kâğıt) ve elektronik formatta arşivleme ve aşağıda verilen koşullarla kullanıma açma izni Bursa Uludağ Üniversitesi'ne aittir. Bu izinle Üniversiteye verilen kullanım hakları dışındaki tüm fikri mülkiyet hakları ile tezin tamamının ya da bir bölümünün gelecekteki çalışmalarda (makale, kitap, lisans ve patent vb.) kullanım hakları tarafımıza ait olacaktır. Tezde yer alan telif hakkı bulunan ve sahiplerinden yazılı izin alınarak kullanılması zorunlu metinlerin yazılı izin alınarak kullandığını ve istenildiğinde suretlerini Üniversiteye teslim etmeyi taahhüt ederiz.

Yükseköğretim Kurulu tarafından yayınlanan "**Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge** " kapsamında, yönerge tarafından belirtilen kısıtlamalar olmadığı takdirde tezin YÖK Ulusal Tez Merkezi / B.U.Ü. Kütüphanesi Açık Erişim Sistemi ve üye olunan diğer veri tabanlarının (Proquest veri tabanı gibi) erişimine açılması uygundur.

Prof. Dr. Gökhan SOYDAN	Gamze SAVAŞ ÇELİK
07 / 01 / 2022	07 / 01 / 2022

ÖZET

Doktora Tezi

CEBİRSEL EĞRİLER ÜZERİNDEKİ RASYONEL DİZİLER

Gamze SAVAŞ ÇELİK

Bursa Uludağ Üniversitesi
Fen Bilimleri Enstitüsü
Matematik Anabilim Dalı

Danışman: Prof. Dr. Gökhan SOYDAN

Tez yedi bölümden oluşmaktadır. İlk üç bölümde cebirsel ve eliptik eğriler ile ilgili temel bilgiler ve bazı önemli teoremlere yer verilmiştir.

$K, L \in \mathbb{Q}$ iken $\mathbb{Q}$'da $y^2 = x^3 + Kx + L$ ile verilen E eliptik eğrisi olsun. $i = 1, \ldots, k$ iken noktaların x-bileşenleri x_i'ler ardışık küplerden oluşursa $(x_i, y_i) \in E(\mathbb{Q})$ rasyonel noktalar kümesinin E üzerinde ardışık küplerin bir dizisi olduğu söylenir. Tezin dördüncü bölümünde ardışık küplerin 5-terimli dizilerini içeren eliptik eğrilerin sonsuz bir ailesinin varlığını gösteriyoruz. Ayrıca bu beş rasyonel noktanın $E(\mathbb{Q})$'da lineer bağımsız ve dolayısıyla $E(\mathbb{Q})$'nun rankı en az 5 olduğunu gösterdik.

Tezin beşinci bölümünde, bir $\mathbb{F}$ sayı cismindeki elemanların bir S alt kümesi verildiğinde x-bileşenleri S'nin elemanları olan rasyonel noktalara sahip $\mathbb{F}$ cismi üzerindeki düzlem cebirsel eğrilerin varlığını tartışıyoruz. S-dizisinin eleman sayısı $|S| = 4, 5$ veya 6 iken üzerindeki rasyonel noktaların x-bileşenlerinin S'de bulunduğu (bükülmüş) Edwards eğrileri ve (genel) Huff eğrilerinin sonsuz ailelerini sergiliyoruz. Bu, bazı cebirsel eğriler üzerindeki belirli tipteki diziler hakkında yapılmış önceki çalışmaları geneller.

Bir düzlem cebirsel eğri üzerindeki rasyonel noktaların x veya y-bileşenleri ortak çarpanı r olacak şekilde bir geometrik dizi oluşturursa bu eğri üzerindeki rasyonel noktaların dizisi bir r-geometrik dizisi olarak adlandırılır. Tezin altıncı bölümünde $x^2 + y^2 = 1$ birim çember denklemi üzerinde en az 3-terimli r-geometrik dizilerini bulunduran sonsuz çoklukta r-rasyonel sayısının varlığını ispatlıyoruz.

Son bölümde tezdeki sonuçlar tartışılmıştır ve tez sonrası gelecek çalışmalardan bahsedilmiştir.

Anahtar Kelimeler: Birim çember, Edwards eğrisi, eliptik eğri, geometrik dizi, Huff eğrisi, rasyonel nokta, rasyonel dizi

2022, viii + 126 sayfa.

ABSTRACT

Ph. D. Thesis

RATIONAL SEQUENCES ON ALGEBRAIC CURVES

Gamze SAVAŞ ÇELİK

Bursa Uludağ University
Graduate School of Natural and Applied Sciences
Department of Mathematics

Supervisor: Prof. Dr. Gökhan SOYDAN

The thesis consists of seven chapters. In the first three chapters, the fundamental notions and some important theorems are given concerning algebraic and elliptic curves.

Let E be an elliptic curve over $\mathbb{Q}$ described by $y^2 = x^3 + Kx + L$ where $K, L \in \mathbb{Q}$. A set of rational points $(x_i, y_i) \in E(\mathbb{Q})$ for $i = 1, 2, \ldots, k$, is said to be a sequence of consecutive cubes on E if the x-coordinates x_i's of these points for $i = 1, 2, \ldots$ form consecutive cubes. In the fourth chapter of the thesis, we show the existence of an infinite family of elliptic curves containing a length-5-term sequence of consecutive cubes. Morever, it has been proved that these five rational points in $E(\mathbb{Q})$ are linearly independent and hence the rank r of $E(\mathbb{Q})$ is at least 5.

In the fifth chapter of the thesis, given a set S of elements in a number field $\mathbb{F}$, we discuss the existence of planar algebraic curves over $\mathbb{F}$ which possess rational points whose x-coordinates are exactly the elements of S. If the size $|S|$ of S is either $4, 5$, or 6, we exhibit infinite families of (twisted) Edwards curves and (general) Huff curves for which the elements of S are realized as the x-coordinates of rational points on these curves. This generalizes earlier work on progressions of certain types on some algebraic curves.

A sequence of rational points on an algebraic planar curve is said to form an r-geometric progression sequence if either the abscissae or the ordinates of these points form a geometric progression sequence with ratio r. In the sixth chapter of the thesis, we prove the existence of infinitely many rational numbers r such that for each r there exist infinitely many r-geometric progression sequences on the unit circle $x^2+y^2 = 1$ of length at least 3.

In the final chapter, the results of the thesis are discussed and some problems for the future work are given.

Key Words: unit circle, Edwards curve, elliptic curve, geometric progression, Huff curve, rational point, rational progression

2022, viii + 126 pages.

TEŞEKKÜR

Doktora öğrencisi yetiştirmek petekten bal süzmek kadar özen ve sabır gösteren bir süreç olup bu çalışma sürecinde, sabrı, bilgi ve deneyimleri ile bana yol gösteren, güler yüzü ve destek veren sözleriyle çalışma azmimi arttıran, tez çalışmasının planlanmasında, araştırılmasında, yürütülmesinde ve düzenlenmesinde ilgi ve desteğini esirgemeyen, değerli zamanını ayırmaktan çekinmeyen, engin birikimiyle yardımına ihtiyaç duyduğum her zaman kapısını açık bulma bahtiyarlığını hissettiğim, birlikte çalışmaktan onur duyduğum değerli tez danışmanım sayın Prof. Dr. Gökhan SOYDAN'a teşekkürlerimi sunarım.

Tezime F-2020/8 numaralı araştırma projesi ile destek veren Bursa Uludağ Üniversitesi Bilimsel Araştırma Projeleri Birimine teşekkür ederim.

Yaşamım boyunca vermiş olduğu destekle gücüme güç katan ve hala kahrımı çeken canım annem Saniye SAVAŞ'a ve SAVAŞ ailesinin her bir üyesine; maddi ve manevi olarak her zaman yanımda olan desteklerini esirgemeyen sevgili annem Asiye ÇELİK ve sevgili babam Metin ÇELİK'e teşekkürü borç bilirim.

Tam tez dönemimde güneş gibi doğup hayatımı aydınlatan, bir gülüşüyle bütün dertlerimi unuttuğum, moral kaynağım, hayatımın neşesi, bazen kendisine ayırmam gereken vakitten feragatta bulunarak ihmal ettiğim en kıymetlim, biricik yavrum Metin Ali ÇELİK'e bütün kalbimle teşekkür ederim.

Son olarak, hayatımın her alanında olduğu gibi bu zorlu yolculuğun yükünü paylaşıp beni hafifleten, anlayışı, güveni ve hissettirdiği sevgisi ile birçok fedakarlıklar gösterip beni destekleyerek, yapabileceklerim için beni yüreklendiren, hayatıma huzur katan sevgili eşim Fatih ÇELİK'e en derin duygularımla teşekkür ederim.

Bu çalışmayı, bedenen yanımda olamasa da benimle hep gurur duyduğunu bildiğim, çok küçük yaşta kaybettiğim rahmetli canım babam Ali SAVAŞ'a ithaf ediyorum.

Gamze SAVAŞ ÇELİK
07 / 01 / 2022

İçindekiler

SİMGELER ve KISALTMALAR DİZİNİ

Simgeler	**Açıklama**
$\mathbb{C}$	Kompleks sayılar kümesi
$\mathbb{R}$	Reel sayılar kümesi
$\mathbb{Q}$	Rasyonel sayılar kümesi
$\mathbb{Z}$	Tamsayılar kümesi
$\mathbb{N}$	Doğal sayılar kümesi
$\mathbb{F}$	Cisim
$\overline{\mathbb{F}}$	$\mathbb{F}$ cisminin cebirsel kapanışı
$\overline{\mathbb{F}}[V]_p$	V'nin P noktasındaki lokal halkası
$\mathbb{P}^n$	n-boyutlu projektif uzay
E	Weierstrass eğrisi
E_d	Edwards eğrisi
$E_{a,d}$	(twisted) Bükülmüş Edwards eğrisi
$\hat{E}_d$	Bükülmüş Huff eğrisi
$H_{a,b}$	Huff eğrisi
$G_{a,b}$	Genel Huff eğrisi
$E/\mathbb{F}$	Katsayıları $\mathbb{F}$ cisminden alınan E eğrisi
$E(\mathbb{F})$	$\mathbb{F}$ cismindeki E eğrisi üzerindeki noktaların kümesi
$E(\mathbb{Q})$	$\mathbb{Q}$ cismi üzerindeki E eğrisinin noktalarının kümesi
$E_{tors}(\mathbb{F})$	$\mathbb{F}$ cismi üzerindeki E eğrisinin büküm noktalarının kümesi
$E[m]$	E eğrisi üzerindeki $m.$ mertebeden büküm noktalarının kümesi
$E_{ns}(\mathbb{F})$	E eğrisi üzerindeki tekil olmayan noktaların oluşturduğu küme
$Kar(\mathbb{F})$	$\mathbb{F}$ cisminin karakteristiği
$\mathbb{F}[x]$	Katsayıları $\mathbb{F}$ cisminden alınan x'in polinomlar halkası
$j(E)$	E eğrisinin j değişmezi
$dim(V)$	V'nin boyutu
$Div(C)$	C'nin bölen grubu
Δ	Weierstrass denkleminin diskriminantı
$0_{\mathbb{F}}$	$\mathbb{F}$ cisminin sıfır elemanı
$M_{\mathbb{F}}$	$\mathbb{F}$'nin değerlemelerinin kümesi
ord_P	(normalleştirilmiş) değerleme
r	E eliptik eğrisinin rankı
V	Projektif varyete

ŞEKİLLER DİZİNİ

Sayfa

ÇİZELGELER DİZİNİ

Sayfa

GİRİŞ

Mertebesi d olan bir $f(x, y)$ polinomu verilsin. $\mathbb{F}$ cismi üzerinde d. dereceden bir C cebirsel düzlem eğrisi

$$\{(x, y) \in \mathbb{F}^2 : f(x, y) = 0\}$$

şeklinde tanımlanır. C cebirsel düzlem eğrisi polinomların homojen koordinatlarda ifade edilişi yardımıyla da projektif koordinatlara genişletilebilir. $S = \{x_1, x_2, \ldots, x_n\} \subset \mathbb{F}$ kümesi verilsin. Eğer $i = 1, 2, \ldots, n$ için (x_i, y_i) noktaları C cebirsel eğrisi üzerinde birer $\mathbb{F}$-rasyonel nokta ise, bu rasyonel noktalar n *uzunluklu bir* S *dizisi* olarak adlandırılır. Eğri üzerindeki $P = (x, y)$ noktası için $x = x(P)$ ve $y = y(P)$ şeklinde gösterelim.

C üzerindeki $\mathbb{F}$-rasyonel noktaların $C(\mathbb{F})$ kümesini çalışmak, aritmetik geometri ve sayılar teorisi konusunda geniş araştırma sahasına sahiptir. Örneğin, f polinomunun derecesi 2 ise C'nin cinsinin 0 olduğu bilinir ve bu durumda eğri bir rasyonel noktaya sahip ise sonsuz çoklukta rasyonel nokta içerir. Eğer f polinomunun derecesi 3 ve düzgün bir eğri ise C'nin cinsi 1'dir. Böyle bir $C(\mathbb{F})$, rasyonel nokta içeriyorsa *eliptik eğri* adını alır. Bu durumda Mordell-Weil teoremine göre $C(\mathbb{F})$ sonlu üreteçli bir abelyan gruptur. Yani, $C(\mathbb{F})$'nin grup yapısı, $T \times \mathbb{Z}^r$ şeklinde yazılabilir. Burada T, sonlu mertebeli noktaların alt grubudur ve $r \geq 0$, C'nin $\mathbb{F}$'deki rankıdır.

Aritmetik geometride şu soru sorulabilir: $\mathbb{F}^2$'de S noktalarının bir kümesi verildiğinde kaç tane d dereceli C cebirsel düzlem eğrisi $S \subseteq C(\mathbb{F})$ şartını sağlar? Bazen cevap basittir. Örneğin, $\mathbb{F}^2$'de 10 tane nokta verildiğinde, bu noktalardan bir kübik eğrinin geçmesi için şart

$$a_1x^3 + a_2x^2y + a_3x^2 + a_4xy^2 + a_5xy + a_6x + a_7y^3 + a_8y^2 + a_9y + a_{10} = 0$$

eşitliğinde S noktalarının yerine konulduğunda 10 tane doğrusal denklemden oluşan bir sistemin çözülebilmesidir. Böylece, karşılık gelen katsayı matrisinin determinantı sıfır ise, sistemin aşikar olmayan bir çözümü vardır ve dolayısıyla bu eğri S noktalarından geçen kübik bir eğridir. Bu nedenle $\mathbb{F}^2$'de belli noktalardan geçen belirli bir derecedeki cebirsel

eğrilerin varlığının kontrol edilmesi için doğrusal cebire ihtiyacı var.

Şimdi başka bir soru ele alalım: $S \subset \mathbb{F}$ verildiğinde, her $x \in S$ ve herhangi $P \in C(\mathbb{F})$ için $x = x(P)$ olacak şekilde d.dereceden C cebirsel eğrileri var mıdır? (Diğer bir soru, x-bileşenleri yerine $y = y(P)$ bileşenleri göz önüne alınırsa böyle cebirsel eğriler var mıdır?)

Sonlu bir $S = \{x_1, x_2, \ldots, x_n\} \subset \mathbb{F}$ kümesi verildiğinde, eğer (x_i, y_i) $(i = 1, \ldots, n)$ $\mathbb{F}$-rasyonel noktaları C cebirsel eğrisi üzerinde ise bu rasyonel noktaların *n-uzunluğunda S-dizisi* oluşturduğu söylenir. İlk olarak 1992'de Lee ve Vélez tarafından $n = 4$ uzunluğundaki S-aritmetik dizisini içeren sonsuz çoklukta $y^2 = x^3 + a$ eğrisi olduğu gösterilmiştir (Lee ve Vélez 1992). 1992'den bugüne çeşitli yazarlar tarafından maksimum uzunlukta S-dizilerini (aritmetik dizi, geometrik dizi veya herhangi rasyonel dizi) bulunduran eliptik eğriler, eliptik eğrilerin farklı modelleri (Edwards eğrisi, Huff eğrisi) ve konikler göz önüne alınmıştır.

Bu tez çalışmasında bazı düzlem cebirsel eğriler üzerindeki maksimum uzunluklu rasyonel dizilerin bulunması amaçlanmıştır. Bu amaca ulaşmak için eliptik eğriler, eliptik eğrilerin farklı modelleri ((twisted) bükülmüş Edwards eğrisi, Edwards eğrisi, Huff eğrisi, genel Huff eğrisi) ve birim çember üzerindeki rasyonel noktaların x-bileşenlerin oluşturduğu rasyonel diziler incelenmiştir ve bazı sonuçlar elde edilmiştir.

Bu tezde elde edilen ana sonuçlar şu şekildedir:

Teorem 1 $n = 5$ uzunluklu ardışık küplerin bir S-dizisi olsun. Bu durumda x-bileşenleri bu ardışık küpler olan sonsuz çoklukta Weierstrass formunda eliptik eğri vardır. Ayrıca bu beş rasyonel nokta lineer bağımsızdır.

Teorem 2 $n = 4, 5$ veya 6 uzunluklu S-dizileri olsun. Bu durumda x-bileşenleri (herhangi bir kısıtlama olmaksızın) bu dizilerin elemanları olan sonsuz çoklukta eliptik eğrilerin farklı modelleri vardır.

Teorem 3 Geometrik bir dizinin ortak çarpanı r olmak üzere, her bir $r \in \mathbb{Q}$ için birim çember üzerinde x-bileşenleri geometrik dizi oluşturan $n = 3$ uzunluklu sonsuz çoklukta S-geometrik dizisi vardır.

Daha ayrıntılı olarak, tezin ilk bölümünde cebirsel varyeteler ve cebirsel eğriler ile ilgili temel tanım ve teoremler verilmiştir. İkinci bölümde cebirsel eğri ailesinin bir üyesi olan eliptik eğriler ile ilgili literatürden iyi bilinen temel tanımlar ve bazı önemli teoremler ifade edilmiştir. Üçüncü bölümde ise eliptik eğrilerin farklı modelleri olan Edwards ve Huff eğrileri tanıtıldı ve bu eğrilerin aritmetiği hakkında bazı temel bilgiler verildi. Tezin dördüncü bölümünde Teorem 1'in ispatı yapıldı ve ana adımlar açıkça belirtildi.

Beşinci bölümde Teorem 2 her bir eliptik eğri modeli için ayrı ayrı ispatlandı. Bu vesile ile literatürde var olan eliptik eğri modelleri üzerindeki S-dizileri ile ilgili önceki bazı sonuçlar genellenmiş oldu. Tezin altıncı bölümünde Teorem 3'ün ispatı yapıldı. Böylece birim çember üzerindeki geometrik diziler ile ilgili ilk sonuç literatüre kazandırılmış oldu.

Son bölümde ise tezde verilen tüm sonuçlar özetlendi ve tez sonrası yapılacak çalışmalardan bahsedildi.

1. CEBİRSEL VARYETELER VE CEBİRSEL EĞRİLER

1.1 Cisim Teorisinden Bazı Temel Kavramlar

Bu bölümde cisim teoriden iyi bilinen bazı temel tanım ve teoremler verilecektir.

Tanım 1.1.1 $\mathbb{F}$ bir küme ve bu kümenin elemanları arasında "+" ve "." ile göstereceğimiz iki tane ikili işlem tanımlanmış olsun.

i) $a, b \in \mathbb{F}$ ise $a + b = b + a$ ve $a.b = b.a$.

ii) $a, b, c \in \mathbb{F}$ ise $a + (b + c) = (a + b) + c$ ve $a.(b.c) = (a.b).c$.

iii) $a, b, c \in \mathbb{F}$ ise $a.(b + c) = (a.b) + (a.c)$.

iv) Her $a \in \mathbb{F}$ için $a + 0_{\mathbb{F}} = a$ olacak şekilde $0_{\mathbb{F}} \in \mathbb{F}$ vardır.

v) Her $a \in \mathbb{F}$ için $a.1 = a$ olacak şekilde $1 \in \mathbb{F}$ vardır.

vi) Her $a \in \mathbb{F}$ için $a + (-a) = 0_{\mathbb{F}}$ olacak şekilde $-a \in \mathbb{F}$ vardır.

vii) Her $0 \neq a \in \mathbb{F}$ için $a.a^{-1} = 1$ olacak şekilde $a^{-1} \in \mathbb{F}$ vardır.

şartlarını sağlayan $(\mathbb{F}, +, .)$ üçlüsüne *cisim* adı verilir.

Tanım 1.1.2 $\mathbb{F}$ bir cisim $E, \mathbb{F}$'nin bir cisim genişlemesi olsun. O zaman E'nin $\mathbb{F}$ uzayı olarak boyutuna E'nin $\mathbb{F}$ üzerindeki *derecesi* denir ve $[E : \mathbb{F}]$ ile gösterilir. $[E : \mathbb{F}]$'nin sonlu ya da sonsuz olmasına göre E'ye $\mathbb{F}$'nin *sonlu cisim genişlemesi* ya da bir *sonsuz cisim genişlemesi* denir (Asar ve ark. 2012).

Örnek 1.1.3 $\mathbb{R}$, $\mathbb{Q}$'nun sonsuz bir cisim genişlemesi, $\mathbb{C}$, $\mathbb{R}$'nin sonlu bir cisim genişlemesidir. $\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}\}$ ve $\{1, i\}$, $\mathbb{C}$ üzerinde lineer bağımsız olduğundan $[\mathbb{C} : \mathbb{R}] = 2$ dir. Öte yandan e sayısı hiçbir $g(x) \in \mathbb{Q}[x]$ polinomunun kökü değildir. Dolayısıyla $\{e^i \mid i \geq 0\}$ sonsuz kümesi $\mathbb{Q}$ üzerinde lineer bağımsızdır ve $[\mathbb{R} : \mathbb{Q}]$ sonsuzdur (Asar ve ark. 2012).

Tanım 1.1.4 $\mathbb{F}$ bir cisim ve $E, \mathbb{F}$'nin bir cisim genişlemesi olsun. $u \in E$ olsun. Eğer $\mathbb{F}[x]$'in sıfırdan farklı bir $f(x)$ polinomu için $f(u) = 0_{\mathbb{F}}$ ise u'ya $\mathbb{F}$ *üzerinde bir cebirsel sayı*, cebirsel olmayan sayıya da *transandant sayı* denir (Asar ve ark. 2012).

Örnek 1.1.5 $\mathbb{C}, \mathbb{Q}$'nun bir cisim genişlemesidir. $\sqrt{2},\ x^2-2$'nin bir kökü olduğundan $\mathbb{Q}$ üzerinde bir cebirsel elemandır. Aynı zamanda $\sqrt{-1}=i$'de x^2+1'in bir kökü olduğundan $\mathbb{Q}$ üzerinde cebirsel bir elemandır.

Örnek 1.1.6 π ve e, $\mathbb{Q}$ üzerinde transandanttır. e doğal logaritmanın tabanıdır (Asar ve ark. 2012).

Tanım 1.1.7 $\mathbb{F}$ bir cisim $E, \mathbb{F}$'nin bir cisim genişlemesi olsun. Eğer E'nin her elemanı $\mathbb{F}$ üzerinde en çok $n.$ dereceden bir cebirsel sayı ise E cismine $\mathbb{F}$'nin bir *cebirsel cisim genişlemesi* denir ve $\mathbb{F}(u)$ ile gösterilir. Dolayısıyla

$$\mathbb{F}(u)=\{c_0 1+c_1 u+\cdots+c_{n-1}u^{n-1}|0\leqslant i\leqslant n-1, c_i\in\mathbb{F}\}$$

dir.

Örnek 1.1.8 $f(x)=x^3-3x-1$ polinomu $\mathbb{Q}$'da indirgenemez, yani $\mathbb{Q}$'da kökü yoktur. $f(x)$'in bir kökü u olmak üzere

$$\mathbb{Q}(u)=\{c_0 1+c_1 u+c_2 u^2|c_0,c_1,c_2\in\mathbb{Q}\}$$

olarak alınırsa $\mathbb{Q}(u), \mathbb{Q}$'nun bir cisim genişlemesidir.

Tanım 1.1.9 $E, \mathbb{F}$'nin bir cisim genişlemesi olsun.

$$\overline{\mathbb{F}}_E=\{c : c\in E \text{ ve } c, \mathbb{F} \text{ üzerinde cebirseldir}\}$$

kümesine $\mathbb{F}$'nin E içindeki *cebirsel kapanışı* denir (Asar ve ark. 2012).

Bilindiği gibi katsayıları kompleks sayılar olan ve sabit olmayan her polinomun bir kompleks kökü vardır. Bu sonuç cebirin temel teoremi olarak bilinir. Bu sonucun ispatı için birçok matematikçi uğraştığı halde ancak 1799'da Gauss doktora tezinde bu sonucun hatasız ispatını vermiştir. Bu özelliğe sahip olan cisimleri diğerlerinden ayırt etmek amacıyla aşağıdaki tanım verilebilir.

Tanım 1.1.10 $\mathbb{F}$ bir cisim olsun. Eğer $\mathbb{F}[x]$'in sabit olmayan her elemanının $\mathbb{F}$ içinde bir kökü varsa $\mathbb{F}$'ye *cebirsel kapalı* bir cisim denir (Asar ve ark. 2012).

Yukarıda belirtildiği gibi $\mathbb{C}$ cebirsel kapalıdır fakat ne $\mathbb{Q}$ ne de $\mathbb{R}$ cebirsel kapalıdır. Böylece $\mathbb{R}$ cebirsel kapalı değil fakat $\mathbb{R}$'nin cebirsel genişlemesi olan $\mathbb{C}$ cebirsel kapalıdır. Bu durumda $\mathbb{C}$'ye $\mathbb{R}$'nin cebirsel kapanışı denir. Buradan hareketle aşağıdaki tanım verilebilir.

Tanım 1.1.11 Bir $\mathbb{F}$ cisminin cebirsel kapalı bir cebirsel genişlemesine $\mathbb{F}$'nin bir *cebirsel kapanışı* denir (Asar ve ark. 2012).

1.2 Afin Varyeteler

Tanım 1.2.1 $\mathbb{F}$ cismi üzerindeki afin n uzayı

$$\mathbb{A}^n = \mathbb{A}^n(\overline{\mathbb{F}}) = \{P = (x_1, \ldots, x_n) : x_i \in \overline{\mathbb{F}}\}$$

ile tanımlanır. Benzer şekilde $\mathbb{A}^n$'nin $\mathbb{F}$ rasyonel noktalarının kümesi

$$\mathbb{A}^n(\mathbb{F}) = \{P = (x_1, \ldots, x_n) \in \mathbb{A}^n : x_i \in \mathbb{F}\}$$

şeklinde tanımlanır (Silverman 2009).

$\overline{\mathbb{F}}[X] = \overline{\mathbb{F}}[X_1, \ldots, X_n]$, n değişkenli bir polinom halkası ve $I \subset \overline{\mathbb{F}}[X]$ bir ideal olsun. Bu tür herhangi bir I ideali ile $\mathbb{A}^n$'nin bir alt kümesi

$$V_I = \{P \in \mathbb{A}^n : f(P) = 0 : \forall f \in I\}$$

şeklinde ilişkilendirilebilir.

Tanım 1.2.2 Bir (afin) cebirsel küme V_I biçimindeki herhangi bir kümedir. V bir cebirsel küme ise, V'nin ideali

$$I(V) = \{f \in \overline{\mathbb{F}}[X] : f(P) = 0, \forall P \in V\}$$

ile verilir. Eğer $I(V)$ ideali $\mathbb{F}[X]$'teki polinomlar tarafından üretilebiliyorsa bir cebirsel küme $\mathbb{F}$ cismi üzerinde tanımlanır ve $V/\mathbb{F}$ ile gösterilir. Eğer $V, \mathbb{F}$ cismi üzerinde tanımlı ise V'nin $\mathbb{F}$-rasyonel noktaların kümesi

$$V(\mathbb{F}) = V \cap \mathbb{A}^n(\mathbb{F})$$

ile gösterilir (Silverman 2009).

Şimdi V'nin $\mathbb{F}$ cismi üzerinde tanımlı olduğunu ve $f_1, \ldots, f_m \in \mathbb{F}[X]$'in $I(V/\mathbb{F})$ idealinin üreteçleri olduğunu varsayalım. O halde $V(\mathbb{F})$ kümesi tam olarak

$$f_1(X) = \ldots = f_m(X) = 0, \quad x_1, \ldots, x_n \in \mathbb{F}$$

polinom denklemlerinin $(x_1, \ldots, x_n)$ çözümlerinin kümesidir.

Örnek 1.2.3 $\mathbb{F}$ bir cisim ve $kar(\mathbb{F}) \neq 2$ olsun.

$$X^2 - Y^2 = 1$$

denklemi ile verilen $\mathbb{A}^2$'deki cebirsel küme V olsun.

$$\begin{aligned} \mathbb{A}^1(\mathbb{F})\backslash\{0\} &\to V(\mathbb{F}) \\ t &\mapsto \Big(\frac{t^2+1}{2t}, \frac{t^2-1}{2t}\Big) \end{aligned}$$

dönüşümü altında $V(\mathbb{F})$ kümesi $\mathbb{A}^1(\mathbb{F})\backslash\{0\}$ kümesine birebir karşılık gelir (Silverman 2009).

Örnek 1.2.4 $\mathbb{Q}$ cismi üzerinde

$$V : X^n + Y^n = 1$$

cebirsel kümesi tanımlansın. 1995'te Andrew Wiles tarafından ispatlanan Fermat'nın son

teoremi gereği $n \geq 3$ olmak üzere

$$V(\mathbb{Q}) = \begin{cases} (1,0),(0,1), & n \text{ tek ise} \\ (\pm 1,0),(0,\pm 1), & n \text{ çift ise} \end{cases}$$

şeklindedir (Silverman 2009).

Tanım 1.2.5 $I(V)$ ideali $\overline{\mathbb{F}}[X]$'te bir asal ideal ise o zaman V afin cebirsel kümesi *(afin) varyete* olarak adlandırılır (Silverman 2009).

$V/\mathbb{F}$ bir varyete yani $V, \mathbb{F}$ cismi üzerinde tanımlanmış bir varyete olsun. O halde $V/\mathbb{F}$'nin afin koordinat halkası

$$\mathbb{F}[V] = \frac{\mathbb{F}[X]}{I(V/\mathbb{F})}$$

olarak tanımlanır. $\mathbb{F}[V]$ halkası bir tamlık bölgesidir ve bunun bölüm cismi (kesirler cismi) $\mathbb{F}(V)$ ile gösterilip $V/\mathbb{F}$'nin *fonksiyon cismi* olarak adlandırılır. Benzer şekilde $\overline{\mathbb{F}}[V]$ ve $\overline{\mathbb{F}}(V)$, $\mathbb{F}$'nin $\overline{\mathbb{F}}$ ile değiştirilmesiyle tanımlanır.

Tanım 1.2.6 $\mathbb{F}$ bir cisim ve V bir varyete olsun. V'nin boyutu, $\overline{\mathbb{F}}(V)$'nin $\overline{\mathbb{F}}$'ye göre aşkınlık derecesi olup $dim(V)$ ile gösterilir (Silverman 2009).

Örnek 1.2.7 $\overline{\mathbb{F}}(\mathbb{A}^n) = \overline{\mathbb{F}}(X_1, \ldots, X_n)$ olduğundan $\mathbb{A}^n$'nin boyutu n'dir. Benzer şekilde $V \subset \mathbb{A}^n$ sabit olmayan tek bir

$$f(X_1, \ldots, X_n)$$

polinom denklemiyle verilirse o zaman $dim(V) = n - 1$ olur (Silverman 2009).

Tanım 1.2.8 V bir varyete, $P \in V$ ve $f_1, \ldots, f_m \in \overline{\mathbb{F}}[X]$ $I[V]$ idealinin üreteçlerinin bir kümesi olsun. Eğer

$$\left(\frac{\partial f_i}{\partial X_j}\right)_{1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant n}$$

$m \times n$ matrisinin rankı $n - dimV$ ise o zaman V, P noktasında *tekil (singüler) değildir (veya düzgündür)* denir. Eğer V her noktada tekil değilse o zaman V *düzgündür (smooth)* denir (Silverman 2009).

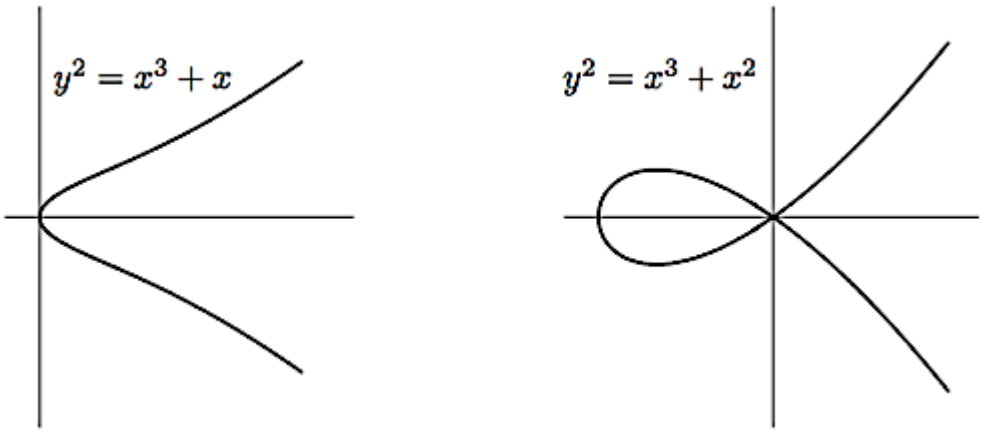
Örnek 1.2.9 V, sabit olmayan tek bir polinom denklemi

$$f(X_1, \ldots, X_n) = 0$$

ile verilsin. O zaman $dim(V) = n-1$'dir. $P \in V$ noktasının tekil nokta olması için gerek ve yeter şart

$$\frac{\partial f}{\partial X_1}(P) = \ldots = \frac{\partial f}{\partial X_n}(P) = 0$$

olmalıdır. Tekil noktaları olmayan bir eğri *düzgün eğri* olarak adlandırılır (Silverman 2009).



Şekil 1.2.1. Düzgün eğri ve tekil eğri

Örnek 1.2.10 $V_1 : Y^2 = X^3 + X$ ve $V_2 : Y^2 = X^3 + X^2$ varyetelerini göz önüne alalım. Örnek 1.2.9'u kullanarak V_1 ve V_2 üzerindeki herhangi bir tekil noktanın sırasıyla

$$V_1^{sing} : 3X^2 + 1 = 2Y = 0 \quad \text{ve} \quad V_2^{sing} : 3X^2 + 2X = 2Y = 0$$

eşitliklerini sağladığını görüyoruz. Böylece V_1 düzgündür, V_2 ise bir $(0, 0)$ tekil noktaya sahiptir (Silverman 2009).

1.3 Projektif Varyeteler

Tarihsel olarak projektif uzay, afin uzaya "sonsuzdaki noktaları" ekleme süreciyle ortaya çıkmıştır. Projektif uzay, bir boyuttan daha büyük afin uzayda, orjinden geçen doğruların

kolleksiyonu olarak tanımlanır.

Tanım 1.3.1 x_i'lerden en az biri sıfırdan farklı olmak üzere tüm

$$(x_0, \ldots, x_n) \in \mathbb{A}^{n+1}$$

$(n+1)$-bileşenlilerin kümesi üzerinde, eğer her i için $x_i = \lambda y_i$ olacak şekilde $\lambda \in \overline{\mathbb{F}}^*$ var iken

$$(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n)$$

denklik bağıntısı gerçeklenirse bu $(n+1)$-lilerin kümesine *n-boyutlu projektif uzay* denir ve $\mathbb{P}^n$ veya $\mathbb{P}^n(\overline{\mathbb{F}})$ ile gösterilir.

Bu denklik bağıntısında

$$\{(\lambda x_0, \ldots, \lambda x_n) : \lambda \in \overline{\mathbb{F}}^*\}$$

denklik sınıfı $[x_0, \ldots, x_n]$ ile gösterilir. $x_0, \ldots, x_n$ bileşenleri $\mathbb{P}^n$'de karşılık gelen nokta için *homojen koordinatlar* olarak adlandırılır. $\mathbb{P}^n$'de $\mathbb{F}$-rasyonel noktaların kümesi

$$\mathbb{P}^n(\mathbb{F}) = \{[x_0, \ldots, x_n] \in \mathbb{P}^n : \forall x_i \in \mathbb{F}\}$$

ile verilir (Silverman 2009).

Uyarı 1.3.2 Eğer $P = [x_0, \ldots, x_n] \in \mathbb{P}^n(\mathbb{F})$ ise buradan her $x_i \in \mathbb{F}$ sonucu gelmez. Ancak $x_i \neq 0$ olacak şekilde i seçildiğinde her j için $x_j/x_i \in \mathbb{F}$ olur (Silverman 2009).

Tanım 1.3.3 Her $\lambda \in \overline{\mathbb{F}}$ için

$$f(\lambda x_0, \ldots, \lambda x_n) = \lambda^d f(x_0, \ldots, x_n)$$

ise $f \in \overline{\mathbb{F}}[X] = \overline{\mathbb{F}}[X_0, \ldots X_n]$ polinomu d. *dereceden homojen bir polinom* olarak adlandırılır. $I \subset \overline{\mathbb{F}}[X]$ olacak şekilde bir I ideali eğer homojen polinomlar tarafından üretili-

yorsa bu ideal *homojendir*.

f homojen bir polinom ve $P \in \mathbb{P}^n$ olsun. Her homojen I ideali için

$$V_I = \{P \in \mathbb{P}^n : f(P) = 0 : \forall f \in I \quad \text{homojen polinom}\}$$

kuralı ile $\mathbb{P}^n$'nin bir alt kümesi ilişkilendirilir (Silverman 2009).

Tanım 1.3.4 Bir (projektif) cebirsel küme, homojen bir I ideali için V_I biçimindeki herhangi bir kümedir. Eğer V bir projektif cebirsel küme ise $I(V)$ ile gösterilen V'nin homojen ideali

$$\{f \in \overline{\mathbb{F}}[X] : f \text{ homojen ve } \forall P \in V \text{ için } f(P) = 0\}$$

tarafından üretilen $\overline{\mathbb{F}}[X]$'in idealidir. $\mathbb{F}$ cismi üzerinde tanımlanan böyle bir V'nin $I(V)$ ideali $\mathbb{F}[X]$'teki homojen polinomlar tarafından üretilebiliyorsa $V/\mathbb{F}$ ile gösterilir. Eğer V, $\mathbb{F}$ cismi üzerinde tanımlıysa

$$V(\mathbb{F}) = V \cap \mathbb{P}^n(\mathbb{F})$$

kümesi V'nin $\mathbb{F}$-rasyonel noktalarının kümesidir (Silverman 2009).

Örnek 1.3.5 Hepsi birden sıfır olmayan $a, b, c \in \overline{\mathbb{F}}$ için $\mathbb{P}^2$'deki bir doğru

$$aX + bY + cZ = 0$$

lineer denklemiyle verilen cebirsel bir kümedir. Eğer $c \neq 0$ ise o zaman böyle bir doğru $\frac{a}{c}$ ve $\frac{b}{c}$'yi içeren herhangi bir cisim üzerinde tanımlıdır. Daha genel olarak $\mathbb{P}^n$'deki bir hiperdüzlem, hepsi birden sıfır olmayan $a_i \in \overline{\mathbb{F}}$ için

$$a_0X_0 + \cdots + a_nX_n = 0$$

denklemi ile tanımlanır (Silverman 2009).

Örnek 1.3.6 $\mathbb{P}^2$'deki bir cebirsel küme

$$V : X^2 + Y^2 = Z^2$$

ile verilsin. $Kar(\mathbb{F}) \neq 2$ iken

$$\mathbb{P}^1(\mathbb{F}) \to V(\mathbb{F}), \qquad [s,t] \mapsto [s^2 - t^2, 2st, s^2 + t^2]$$

dönüşümü altında $V(\mathbb{F})$ kümesi ile $\mathbb{P}^1(\mathbb{F})$ izomorftur (Burada İzomorf tanımı için Örnek 1.4.6'ya bakınız) (Silverman 2009).

Tanım 1.3.7 Bir projektif cebirsel küme eğer $I(V)$ homojen ideali $\overline{\mathbb{F}}[X]$'te bir asal ideal ise bu cebirsel küme *(projektif) varyete* olarak adlandırılır (Silverman 2009).

$\mathbb{P}^n$, $\mathbb{A}^n$'nin bir çok kopyasını içerir. Örneğin $0 \leq i \leq n$ için

$$\phi_i : \mathbb{A}^n \to \mathbb{P}^n$$

$$(y_1, \ldots, y_n) \mapsto [y_1, y_2, \ldots, y_{i-1}, 1, y_i, \ldots, y_n]$$

olacak şekilde bir ϕ_i dönüşümü vardır. Burada

$$H_i = \{P = [x_0, \ldots, x_n] \in \mathbb{P}^n : x_i = 0\}$$

kümesi $X_i = 0$ ile verilen $\mathbb{P}^n$'deki hiperdüzlemi göstersin ve

$$U_i = \{P = [x_0, \ldots, x_n] \in \mathbb{P}^n : x_i \neq 0\} = \mathbb{P}^n \backslash H_i$$

kümesi H_i'nin tümleyeni olsun. Dolayısıyla

$$\phi_i^{-1} : U_i \to \mathbb{A}^n$$
$$[x_0, \ldots, x_n] \mapsto \left[\frac{x_0}{x_i}, \frac{x_1}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i} \ldots, \frac{x_n}{x_i}\right]$$

birebir-örten fonksiyonu vardır.

Sabit bir i için, $\mathbb{A}^n$'yi, ϕ_i dönüşümü ile $\mathbb{P}^n$'deki U_i kümesiyle tanımlayacağız.

Şimdi $I(V) \subset \overline{\mathbb{F}}[X]$ olacak şekilde $I(V)$ ideali ile V projektif cebirsel küme olsun. Bu durumda bazı sabir i değerleri için $I(V \cap \mathbb{A}^n) \subset \overline{\mathbb{F}}[Y]$ olmak üzere $V \cap \mathbb{A}^n$ kümesi

$$I(V \cap \mathbb{A}^n) = \{f(Y_1, \ldots, Y_{i-1}, 1, Y_{i+1}, \ldots, Y_n) : f(X_0, \ldots, X_n) \in I(V)\}$$

ideali ile verilen afin cebirsel bir kümedir. Şunu da belirtelim ki $U_0, \ldots, U_n$ kümeleri $\mathbb{P}^n$'nin tümünü örter. Böylece herhangi bir V projektif varyetesi $V \cap U_0, \ldots, V \cap U_n$ alt kümeleri tarafından örtülür. Bu alt kümelerin her biri uygun ϕ_i^{-1} dönüşümüyle bir afin varyetedir. $f(X_0, \ldots, X_n)$ polinomunun $f(Y_1, \ldots, Y_{i-1}, 1, Y_{i+1}, \ldots, Y_n)$ polinomu ile değiştirme işlemine X_i'ye göre *dehomojenizasyon* denir.

Bu işlem tersine çevrilebilir. Herhangi bir $f(Y) \in \overline{\mathbb{F}}[Y]$ için $d = deg(f)$, f^* ın bir polinom olduğu en küçük tamsayı olmak üzere

$$f^*(X_0, \ldots, X_n) = X^d f\left(\frac{X_0}{X_i}, \frac{X_1}{X_i}, \ldots, \frac{X_{i-1}}{X_i}, \frac{X_{i+1}}{X_i} \ldots, \frac{X_n}{X_i}\right)$$

şeklinde tanımlanır. Burada f^*, f'nin X_i'ye göre *homojenleştirilmesi* denir.

Tanım 1.3.8 $V \subset \mathbb{A}^n$ iken V bir afin cebirsel küme ve V'nin ideali $I(V)$ olsun. V'yi

$$\phi_i : V \subset \mathbb{A}^n \to \mathbb{P}^n$$

aracılığı ile $\mathbb{P}^n$'nin bir alt kümesi olarak göz önüne alınsın. V'nin projektif kapanışı $\overline{V}$ ile gösterilir. $\overline{V}$ homojen ideali $I(\overline{V})$olan ve

$$\{f^*(X) : f \in I(V)\}$$

tarafından üretilen bir projektif cebirsel kümedir (Silverman 2009).

Önerme 1.3.9 $a)$ V bir afin varyete olsun. O zaman $\overline{V}$ bir projektif varyetedir ve

$$V = \overline{V} \cap \mathbb{A}^n$$

eşitliği sağlanır.

$b)$ V bir projektif varyete olsun. O zaman $V \cap \mathbb{A}^n$ bir afin varyetedir ve

$$\text{ya } V \cap \mathbb{A}^n = \emptyset \quad \text{ya da } V = \overline{V \cap \mathbb{A}^n}$$

olur.

$c)$ Eğer $\mathbb{F}$ cismi üzerinde bir afin V varyetesi tanımlanırsa $\overline{V}$'de $\mathbb{F}$ üzerinde tanımlanır. Eğer ki V projektif varyete ise $V \cap \mathbb{A}^n$'de $\mathbb{F}$ üzerinde tanımlanır (Silverman 2009).

Not 1.3.10 Önerme 1.3.9'a göre her afin varyete, bir tek projektif varyete ile tanımlanabilir. Afin koordinatlarla ilgilenmek daha kolay olduğu için "V bir projektif varyete olsun" dediğimizde ve bazı homojen olmayan denklemler yazdığımızda belirtilen bir W afin varyetenin projektif kapanışının V olduğunu düşüneceğiz. $V \backslash W$'nin noktaları V *üzerindeki sonsuzdaki noktalar* olarak adlandırılır (Silverman 2009).

Örnek 1.3.11 V bir projektif varyete olsun ve

$$V : Y^2 = X^3 + 17$$

denklemi ile verilsin. $X = \overline{X}/\overline{Z}, Y = \overline{Y}/\overline{Z}$ olmak üzere V varyetesi $\mathbb{P}^2$'de homojen koordinatlarda

$$\overline{Y}^2\overline{Z} = \overline{X}^3 + 17$$

denklemi ile verilir. Bu varyete sonsuzda tek bir noktaya sahiptir. Yani $\overline{Z} = 0$ olduğunda sonsuzdaki noktası $[0, 1, 0]$ şeklindedir. Örneğin

$$V(\mathbb{Q}) = \{(x, y) \in \mathbb{A}^2(\mathbb{Q}) : y^2 = x^3 + 17\} \cup \{[0, 1, 0]\}$$

ile verilir (Silverman 2009).

Tanım 1.3.12 $V/\mathbb{F}$ projektif varyete ve $V \cap \mathbb{A}^n \neq \emptyset$ olacak şekilde $\mathbb{A}^n \subset \mathbb{P}^n$ seçelim. V'nin boyutu $V \cap \mathbb{A}^n$'nin boyutudur. V'nin fonksiyon cismi $\mathbb{F}(V)$ ile gösterilir ve $V \cap \mathbb{A}^n$'nin fonksiyon cismidir.

Benzer şekilde $\overline{\mathbb{F}}(V)$ içinde geçerlidir (Silverman 2009).

Tanım 1.3.13 V bir projektif varyete ve $P \in V$ olsun. $P \in \mathbb{A}^n$ olmak üzere $\mathbb{A}^n \subset \mathbb{P}^n$ seçelim. Eğer $V \cap \mathbb{A}^n$, P noktasında düzgün bir eğri ise V'de P noktasında düzgün bir eğridir.

V'nin P noktasındaki lokal halkası $\overline{\mathbb{F}}[V]_P$ ile gösterilir. Bu lokal aynı zamanda $V \cap \mathbb{A}^n$'ın P noktasındaki halkasıdır. Bir $F \in \overline{\mathbb{F}}(V)$ fonksiyonu $\mathbb{F}[V]_P$'de ise P'de regülerdir (Silverman 2009).

Uyarı 1.3.14 $\mathbb{P}^n$'nin fonksiyon cismi, f ve g'nin aynı dereceden homojen polinomlar olduğu $F(X) = f(X)/g(X)$ rasyonel fonksiyonlarından oluşan $\overline{\mathbb{F}}[X_0, \ldots, X_n]$'in alt cismi olarak da tanımlanabilir. Böyle bir ifade, her P için $g(P) \neq 0$ iken $\mathbb{P}^n$ üzerinde iyi tanımlanmış bir fonksiyon verir. Benzer şekilde, bir projektif varyete olan V'nin fonksiyon cismi $F(X) = f(X)/g(X)$ rasyonel fonksiyonların cismidir. Bu durumda aşağıdaki şartlar sağlanır:
(i) f ve g aynı derecede homojendir,
(ii) $g \notin I(V)$,
(iii) $f_1 g_2 - f_2 g_1 \in I(V)$ ise $\frac{f_1}{g_1}$ ve $\frac{f_2}{g_2}$ fonksiyonları tanımlanır (Silverman 2009).

1.4 Varyeteler Arasında Dönüşümler

Bu bölümde projektif varyeteler arasındaki cebirsel dönüşümler ele alınacaktır. Bunlar rasyonel fonksiyonlarla tanımlanan dönüşümlerdir.

Tanım 1.4.1 V_1 ve $V_2 \subset \mathbb{P}^n$ projektif varyeteler olsun. V_1'den V_2'ye rasyonel bir dönüşüm

$$f : V_1 \to V_2, \quad \phi = [f_0, \ldots, f_n]$$

biçimindeki bir dönüşümdür; burada $f_0, \ldots, f_n \in \overline{\mathbb{F}}(V_1)$ fonksiyonları $f_0, \ldots, f_n$'nin tümünün tanımlı olduğu her $P \in V_1$ noktası için

$$\phi(P) = [f_0(P), \ldots, f_n(P)] \in V_2$$

özelliğine sahiptir (Silverman 2009).

Tanım 1.4.2

$$\phi = [f_0, \ldots, f_n] : V_1 \to V_2$$

rasyonel dönüşümünün $P \in V_1$'de düzgün (regüler) olması için $g \in \overline{\mathbb{F}}(V_1)$ iken aşağıdaki şartlar sağlanmalıdır:

(i) Her gf_i, P'de regülerdir.

(ii) $(gf_i)(P) \neq 0$ olacak şekilde i ler vardır.

Eğer böyle bir g varsa o zaman

$$\phi(P) = [(gf_0)(P), \ldots, (gf_n)(P)]$$

olur (Silverman 2009).

Not 1.4.3 Farklı noktalar için farklı g'ler almak gerekebilir. Her noktada düzgün olan rasyonel bir dönüşüme *morfizm* denir.

Uyarı 1.4.4 $V_1 \subset \mathbb{P}^m$ ve $V_2 \subset \mathbb{P}^n$ projektif varyeteler olsun. $\overline{\mathbb{F}}(V_1)$'deki fonksiyonların aynı dereceye sahip $\overline{\mathbb{F}}[X_0, \ldots, X_m]$'deki homojen polinomların bölümleri olarak tanımlanabileceğini Uyarı 1.3.14'ten hatırlayınız. Böylece $\phi = [f_0, \ldots, f_n]$ rasyonel dönüşümünü f_i'lerin "paydalarını yok eden" homojen polinomla çarparak aşağıdaki alternatif tanımı elde ederiz:

$\phi : V_1 \to V_2$ rasyonel dönüşümü,

(i) $\phi_i(X) \in \overline{\mathbb{F}}[X] = \overline{\mathbb{F}}[X_0, \ldots, X_n]$ olup hepsi $I(V_1)$'de olmayan aynı dereceye sahip homojen polinomlar,

(ii) her $f \in I(V_2)$ için

$$f(\phi_0(X), \ldots, \phi_n(X)) \in I(V_1)$$

olmak üzere

$$\phi = [\phi_0(X), \ldots, \phi_n(X)]$$

formunda bir dönüşümdür (Silverman 2009).

Açıkçası bazı $\phi_i(P) \neq 0$ olması koşuluyla $\phi(P)$ iyi tanımlıdır. Ancak tüm i'ler için $\phi_i(P) = 0$ olsa bile $\phi(P)$'yi anlamlandırmak için ϕ'yi değiştirmek mümkün olabilir. Bunu şu şekilde kesinleştiriyoruz:

(i) $\psi_0, \ldots, \psi_n$ aynı dereceye sahip polinomlar,

(ii) Her $0 \leq i, j \leq n$ için $\phi_i\psi_j \equiv \phi_j\psi_i(\mod I(V_1))$,

(iii) Bazı i'ler için $\psi(P) \neq 0$

olacak şekilde homojen $\psi_0, \ldots, \psi_n \in \overline{\mathbb{F}}[X]$ polinomları varsa yukarıdaki gibi bir rasyonel $\phi = [\phi_0, \ldots, \phi_n] : V_1 \to V_2$ dönüşümü $P \in V_1$ noktasında düzgündür.

Eğer bu gerçekleşirse

$$\phi(P) = [\psi_0(P), \ldots, \psi_n(P)]$$

olur.

Yukarıdaki gibi her yerde düzgün olan rasyonel bir dönüşüme *morfizm* denir.

Tanım 1.4.5 V_1 ve V_2 varyeteler olsun. $\psi o \phi$ ve $\phi o \psi$ sırasıyla V_1 ve V_2 üzerindeki birim dönüşümler olmak üzere $\phi : V_1 \to V_2$ ve $\psi : V_2 \to V_1$ morfizmleri varsa V_1 ve V_2 izomorfiktir ve $V_1 \cong V_2$ şeklinde gösterilir. Eğer ϕ ve ψ, $\mathbb{F}$ cismi üzerinde tanımlanabiliyorsa $V_1/\mathbb{F}$ ve $V_2/\mathbb{F}$'nin $\mathbb{F}$ üzerinde izomorf olduğu söylenebilir. Hem ϕ hem de ψ'nin sadece rasyonel dönüşümler değil, morfizmler olması gerektiğine dikkat edin (Silverman 2009).

Örnek 1.4.6 $Kar(\mathbb{F}) \neq 2$ ve V örnek 1.3.6'da

$$V : X^2 + Y^2 = Z^2$$

ile verilen varyete olsun. $\phi : V \to \mathbb{P}^1, \phi = [X + Z, Y]$ rasyonel dönüşümünü göz önüne alalım. Açıkçası ϕ dönüşümü muhtemelen $[1, 0, -1]$ noktası dışında, yani $X+Z = Y = 0$ olduğu noktada V'nin her noktasında düzgündür. Ancak $(X + Z)(X - Z) = -Y^2$ ($\mod I(V)$) kullanarak

$$\phi = [X + Z, Y] = [X^2 - Z^2, Y(X - Z)] = [-Y^2, Y(X - Z)] = [-Y, X - Z]$$

elde edilir. Böylece $\phi([1, 0, -1]) = [0, 2] = [0, 1]$ olur. Bu durumda ϕ, V'nin her noktasında düzgündür, yani ϕ bir morfizmdir.

$$\psi : \mathbb{P}^1 \to V, \quad \psi = [S^2 - T^2, 2ST, S^2 + T^2]$$

dönüşümü bir morfizm olduğu kolaylıkla kontrol edilebilir ve ϕ'nin tersini sağlar. Dolayısıyla V ve $\mathbb{P}^1$ izomorftur (Silverman 2009).

Örnek 1.4.7

$$\phi : \mathbb{P}^2 \to \mathbb{P}^2 \quad \phi = [X^2, XY, Z^2]$$

rasyonel dönüşümü $[0, 1, 0]$ noktası dışında her yerde düzgündür (Silverman 2009).

Örnek 1.4.8 V

$$V : Y^2Z = X^3 + X^2Z$$

şeklinde bir varyete olsun ve

$$\psi : \mathbb{P}^1 \to V, \quad \psi = [(S^2 - T^2)T, (S^2 - T^2)S, T^3]$$

$$\phi : V \to \mathbb{P}^1, \quad \phi = [Y, X]$$

rasyonel dönüşümleri göz önüne alalım. Burada ψ bir morfizmdir, ϕ ise $[0, 0, 1]$'de düzgün değildir. $[0, 0, 1]$ noktası V'nin tekil noktası olması tesadüf değildir.
$\phi \circ \psi$ ve $\psi \circ \phi$ dönüşümleri tanımlandıkları her yerde birim dönüşüm olmasına rağmen, ϕ ve ψ dönüşümleri izomorf değildir. Çünkü ϕ bir morfizm değildir (Silverman 2009).

Örnek 1.4.9

$$V_1 : X^2 + Y^2 = Z^2 \text{ ve } \quad V_2 : X^2 + Y^2 = 3Z^2$$

varyetelerini göz önüne alalım. $V_2(\mathbb{Q}) \neq \emptyset$ olduğundan $V_1(\mathbb{Q})$ çok sayıda nokta içerdiğinden, bu varyeteler $\mathbb{Q}$ üzerinde izomorf değildirler. Bununla birlikte V_1 ve V_2 varyeteleri $\mathbb{Q}(\sqrt{3})$ üzerinde izomorf olup bu varyeteler arasında

$$\phi : V_2 \to V_1, \quad \phi = [X, Y, \sqrt{3}Z]$$

izomorfizması vardır (Silverman 2009).

Şimdi eliptik eğrileri çalışmamız için gerekli olacak, cebirsel eğriler hakkında yani boyutu bir olan projektif varyeteler hakkındaki temel bilgiler verilecektir.

1.5 Eğriler

Bir eğri denildiğinde her zaman boyutu 1 olan projektif varyete düşünülecektir. Genel anlamda düzgün eğrilerle ilgileneceğiz. $\mathbb{P}^1$'de düzgün eğri örnekleri olarak 1.3.6-1.3.11 örnekleri verilebilir. Düzgün bir eğri üzerindeki noktalarda lokal halkaları tanımlayarak başlayalım.

Önerme 1.5.1 C bir eğri ve $P \in C$ düzgün bir nokta olsun. O zaman $\overline{\mathbb{F}}[C]_P$ bir ayrık değerleme halkasıdır (Silverman 2009).

Tanım 1.5.2 C bir eğri ve $P \in C$ düzgün bir nokta olsun. $\overline{\mathbb{F}}[C]_P$ üzerinde (normalleştirilmiş) değerleme

$$ord_P : \overline{\mathbb{F}}[C]_P \to \{0, 1, 2, \dots\} \cup \{\infty\}$$

$$ord_P(f) = \sup\{d \in \mathbb{Z} : f \in M_P^d\}$$

ile verilir.

$ord_P(f/g) = ord_P(f) - ord_P(g)$ kullanılarak

$$ord_P : \overline{\mathbb{F}}(C) \to \mathbb{Z} \cup \infty$$

dönüşümü ile ord_P'yi $\overline{\mathbb{F}}[C]$'ye genişletiriz.

P noktasında C eğrisi için bir düzgünleştirici (uniformizer), $ord_P(t) = 1$ olacak şekilde herhangi bir $t \in \overline{\mathbb{F}}(C)$ fonksiyonudur, yani M_P ideali için bir üreteçtir (Silverman 2009).

Tanım 1.5.3 C bir eğri, $P \in C$ düzgün bir nokta (yukarıdaki gibi) ve $f \in \overline{\mathbb{F}}(C)$ olsun. f'nin P'deki mertebesi $ord_P(f)$ ile gösterilir. Eğer $ord_P(f) > 0$ ise o zaman f'nin P'de bir sıfırı vardır. Eğer $ord_P(f) < 0$ ise o zaman f'nin P'de bir kutbu vardır. Eğer $ord_P(f) \geq 0$ ise f, P'de regülerdir ve $f(P)$'yi değerlendirebilir. Aksi takdirde P'de bir kutbu vardır ve $f(P) = \infty$'dur (Silverman 2009).

Önerme 1.5.4 C düzgün bir eğri ve $f \neq 0$ olmak üzere $f \in \overline{\mathbb{F}}(C)$ olsun. O zaman f'nin bir kutup noktası veya kök olan sonlu çoklukta C noktası vardır. Ayrıca f'nin hiç kutbu yoksa o zaman $f \in \overline{\mathbb{F}}$'tır (Silverman 2009).

Örnek 1.5.5

$$C_1 : Y^2 = X^3 + X \quad \text{ve} \quad C_2 : Y^2 = X^3 + X^2$$

eğrilerini göz önüne alalım (Projektif varyeteler için afin denklemlerle ilgili Not 1.3.10'u hatırlayalım. C_1 ve C_2 eğrilerinin her birinin sonsuzda bir tek noktası vardır). $P = (0, 0)$ olsun. O zaman C_1, P'de düzgün bir eğridir, ancak C_2, P'de düzgün bir eğri değildir. Örnek 1.2.10'a bakılabilir.

$\overline{\mathbb{F}}[C_1]_P$'nin M_P maksimal idealini ele alırsak M_P/M_P^2, Y tarafından üretilir. Örneğin;

$$ord_P(Y) = 1, \quad ord_P(X) = 2, \quad ord_P(2Y^2 - X) = 2$$

olur. (Son olarak $2Y^2 - X = 2X^3 + X$ olduğuna dikkat edin) Öte yandan $\overline{\mathbb{F}}[C_2]_P$ ayrık bir değerleme halkası değildir (Silverman 2009).

1.6 Eğriler Arasında Dönüşümler

Düzgün eğriler için her noktada rasyonel bir dönüşümün tanımlandığı temel sonuç ile başlayalım.

Önerme 1.6.1 C bir eğri V, $V \subset \mathbb{P}^N$ olacak şekilde bir varyete, $P \in C$ düzgün nokta ve $\phi : C \to V$ rasyonel bir dönüşüm olsun. O zaman ϕ, P'de regülerdir. Özellikle eğer C düzgün bir eğri ise ϕ bir morfizmdir (Silverman 2009).

Örnek 1.6.2 $C/\mathbb{F}$ düzgün eğri ve $f \in \mathbb{F}(C)$ bir fonksiyon olsun. Bu durumda f fonksiyonu

$$f : C \to \mathbb{P}^1, \quad P \mapsto [f(P), 1]$$

şeklinde rasyonel bir dönüşüm tanımlar. Bu dönüşüm morfizmdir ve

$$f(P) = \begin{cases} [f(P), 1], & \text{f, P'de regüler ise} \\ [1, 0], & \text{f'nin P'de kutbu var ise} \end{cases}$$

ile verilir (Silverman 2009).

Teorem 1.6.3 $\phi : C_1 \to C_2$ eğrilerin morfizmi olsun. O halde ϕ, ya sabit bir fonksiyon ya da örten bir fonksiyondur.

$C_1/\mathbb{F}$ ve $C_2/\mathbb{F}$ eğrileri ve $\mathbb{F}$ üzerinde tanımlanan $\phi : C_1 \to C_2$ sabit olmayan rasyonel bir dönüşüm olsun. O zaman ϕ dönüşümü ile bileşkesi

$$\phi^* : \mathbb{F}(C_2) \to \mathbb{F}(C_1), \quad \phi^* f = f o \phi$$

$\mathbb{F}$'yi sabitleyen fonksiyon cisimlerinin birebir fonksiyonunu içerir (Silverman 2009).

Teorem 1.6.4 $C_1/\mathbb{F}$ ve $C_2/\mathbb{F}$ eğriler olsun.

$a)$ $\mathbb{F}$ cismi üzerinde tanımlanan sabit olmayan $\phi : C_1 \to C_2$ dönüşümü olsun. O halde $\mathbb{F}(C_1), \phi^*(\mathbb{F}(C_2))$'nin sonlu bir genişlemesidir.

$b)$ ß : $\mathbb{F}(C_2) \to \mathbb{F}(C_1)$ fonksiyonu $\mathbb{F}$'yi sabit bırakan fonksiyon cisimlerinin birebir fonksiyonu olsun. O zaman $\mathbb{F}$ cismi üzerinde $\mathbb{Q}^* = $ ß olmak üzere sabit olmayan tek bir $\phi : C_1 \to C_2$ dönüşümü vardır.

$c)$ $\mathbb{K} \subset \mathbb{F}(C_1)$ olacak şekilde $\mathbb{K}$'yı içeren sonlu indeksli bir alt cismi olsun. O zaman

$\mathbb{F}$ izomorfizmine kadar tek bir düzgün $C'/\mathbb{F}$ eğrisi ve $\mathbb{F}$ üzerinde $\phi^*\mathbb{F}(C') = \mathbb{K}$ olacak şekilde tanımlanmış sabit olmayan bir $\phi : C_1 \to C'$ dönüşümü vardır (Silverman 2009).

Tanım 1.6.5 $\mathbb{F}$ cismi üzerinde tanımlanan eğrilerin bir $\phi : C_1 \to C_2$ dönüşümü olsun. Eğer ϕ sabit ise ϕ'nin derecesi 0 olarak tanımlanır. Aksi takdirde ϕ'nin sonlu bir dönüşüm olduğu söylenir ve derecesi

$$\deg \phi = [\mathbb{F}(C_1) : \phi^*\mathbb{F}(C_2)]$$

ile tanımlanır.
Eğer $\mathbb{F}(C_1)/\phi^*\mathbb{F}(C_2)$ cisim genişlemesi, karşılık gelen özelliğe sahipse ϕ ayrılabilir, ayrılamaz ya da tamamen ayrılamaz (purely inseparable) olduğu söylenir ve genişlemenin ayrılabilir veya ayrılamazlık dereceleri sırasıyla $deg_s\chi$ ve $deg_i\phi$ ile gösterilir (Silverman 2009).

Sonuç 1.6.6 C_1 ve C_2 düzgün eğriler ve $\phi : C_1 \to C_2$ birinci dereceden bir dönüşüm olsun. O zaman ϕ bir izomorfizmdir (Silverman 2009).

Tanım 1.6.7 $Kar(\mathbb{F}) \neq 2$ olsun. $f(x) \in \mathbb{F}$ polinomu $d.$ dereceden olmak üzere

$$C_0 : y^2 = f(x) = a_0x^d + a_1x^{d-1} + \cdots + a_d$$

ile verilen $C_0/\mathbb{F}$ afin eğrisini ele alalım. $P = (x_0, y_0) \in C_0$ noktasının tekil olduğunu varsayalım. O zaman

$$2y_0 = f'(x_0) = 0$$

olur. Yani $y_0 = 0$ ve $x_0 = 0, f(x)$'in çift katlı köküdür. Dolayısıyla $\Delta(f) \neq 0$ olduğunu varsayarsak o zaman $y^2 = f(x)$ afin eğrisi düzgün bir eğridir. Bu C_0 eğrisi *hipereliptik eğri* olarak adlandırılır (Silverman 2009).

Eğer C_0'ın afin denklemini homojenleştirerek $\mathbb{P}^2$'de bir eğri olarak ele alırsak, $d \geq 4$ olduğunda sonsuzdaki nokta(lar)ın tekil olduğu kolayca kontrol edilebilir. Öte yandan

Teorem 1.6.4 c) maddesi $\mathbb{F}(C_0) = \mathbb{F}(x, y)$ fonksiyon cismine eşit olan herhangi düzgün projektif $C/\mathbb{F}$ eğrisinin varlığını garanti eder.

Örneğin $d = 4$ durumunu göz önüne alalım. C_0 afin denklemi

$$C_0 : y^2 = a_0x^4 + a_1x^3 + a_2x^2 + a_3x + a_4$$

olsun.

$$[1, x, y, x^2] : C_0 \to \mathbb{P}^3$$

dönüşümü tanımlansın. $[X_0, X_1, X_2, X_3] = [1, x, y, x^2]$ verildiğinde görüntü kümesinin ideali açıkça

$$F = X_3X_0 - X_1^2$$
$$G = X_2^2X_0^2 - a_0X_1^4 - a_1X_1^3X_0 - a_2X_1^2X_0^2 - a_3X_1X_0^3 - a_4X_0^4$$

iki homojen polinomunu içerir. Ancak bu iki polinomun sıfır kümesi $X_0 = X_1 = 0$ doğrusunu içerdiğinden istenilen C eğrisi olamaz. Bu yüzden, ikinci dereceden

$$H = X_2^2 - a_0X_3^2 - a_1X_1X_3 - a_2X_0X_3 - a_3X_0X_1 - a_4X_0^2$$

polinomu elde etmek için G polinomunda $X_1^2 = X_0X_3$ yazılır ve X_0^2 yok edilir. F ve H tarafından üretilen ideal, düzgün bir C eğrisi verdiğini iddia ediyoruz.

Bunu görmek için öncelikle $X_0 \neq 0$ ise X_0'a göre homojenleştirirsek ($x = X_1/X_0, y = X_2/X_0, z = X_3/X_0$) eşitliklerini kullanarak,

$$z = x^2 \quad \text{ve} \quad y^2 = a_0z^2 + a_1xz + a_2z + a_3x + a_4$$

afin eğrisini elde ederiz.

İlk denklem ikinci denklemde yerine yazıldığında orjinal C_0 eğrisi elde edilir. Böylece $C_0 \cong C \cap \{X_0 \neq 0\}$ olur. Eğer $X_0 = 0$ ise o zaman $X_1 = 0$ olur ve $X_2 = \pm\sqrt{a_0}X_3$ olur.

Böylece $X_0 = 0$ hiper düzleminde C'nin $[0, 0, \pm\sqrt{a_0}, 1]$ olmak üzere iki noktası vardır ($f(x)$'in derecesini 4 olarak varsaydığımız için $a_0 \neq 0$ olduğuna dikkat edin). Bu iki noktada C'nin düzgün olduğunu kontrol etmek için $u = \frac{X_0}{X_3}, v = \frac{X_1}{X_3}$ ve $w = \frac{X_2}{X_3}$ olarak X_3'e göre homojenleştiririz. Böylece

$$w^2 = a_0 + a_1 v + a_2 v^2 + a_3 v^3 + a_4 v^4$$

tek afin denkleminden

$$u = v^2 \quad w^2 = a_0 + a_1 v + a_2 u + a_3 uv + a_4 u^2$$

denklemleri elde edilir. Böylece $f(x)$ polinomunun çift katlı kökü olmadığını varsayarak $(v, w) = (0, \pm\sqrt{a_0})$ noktasının tekil olmayan bir nokta olduğu görülür.

1.6.1 Frobenius Dönüşümü

$Kar(\mathbb{F}) = p > 0$ olduğunu varsayalım ve $q = p^r$ olsun. Herhangi bir $f \in \mathbb{F}[X]$ polinomu için f'nin her katsayısını q. kuvvete artırarak elde edilen polinom $f^{(q)}$ olsun. O zaman herhangi bir $C/\mathbb{F}$ eğrisi için, homojen ideali

$$I(C^{(q)}) = \{f^{(q)} : f \in I(C)\}$$

ile verilen eğri olarak yeni bir $C^{(q)}/\mathbb{F}$ eğrisi tanımlanabilir. Ayrıca

$$\phi : C \to C^{(q)}, \quad \phi([x_0, \ldots, x_n]) = [x_0^q, \ldots, x_n^q]$$

ile tanımlanan, q. *kuvvet Frobenius morfizmi* olarak adlandırılan C'den $C^{(q)}$'ya doğal bir dönüşüm vardır. ϕ'nin C'yi $C^{(q)}$'ya resmettiğini görmek için her

$$P = [x_0, \ldots, x_n] \in C$$

noktası için $\phi(P)$ görüntüsünün $I(C^{(q)})$'nun her $f^{(q)}$ üretecinin bir sıfırı olduğunu göstermek yeterlidir.

$$\begin{aligned} f^{(q)}(\phi(P)) &= f^{(q)}(x_0^q, \ldots, x_n^q) \\ &= (f(x_0, \ldots, x_n))^q, \qquad (kar(\mathbb{F}) = p \quad \text{iken}) \\ &= 0 \qquad\qquad\qquad , \qquad (f(P) = 0 \quad \text{iken}) \end{aligned}$$

şeklinde hesaplanır.

Örnek 1.6.8 $\mathbb{P}^2$'deki bir C eğrisi

$$C : Y^2Z = X^2 + aXZ^2 + bZ^3$$

denklemi ile verilsin. O zaman $C^{(q)}$ eğrisi

$$C^{(q)} : Y^2Z = X^2 + a^qXZ^2 + b^qZ^3$$

denklemi ile verilir (Silverman 2009).

Aşağıdaki önerme, Frobenius dönüşümünün temel özelliklerini tanımlar.

Önerme 1.6.9 $\mathbb{F}$ bir cisim $kar(\mathbb{F}) = p > 0, q = p^r, C/\mathbb{F}$ bir eğri ve $\phi : C \to C^{(q)}$ dönüşümü q. kuvvetten Frobenius morfizmi olsun.

$a)$ $\phi^*\mathbb{F}(C)^{(q)} = \mathbb{F}(C)^q = \{f^q : f \in \mathbb{F}(C)\}$,

$b)$ ϕ tamamen ayrılmaz,

$c)$ $\deg \phi = q$

olarak tanımlanır (Silverman 2009).

Sonuç 1.6.10 $q = deg_i(\psi)$ iken karakteristiği p olan bir cisim üzerindeki düzgün eğrilerin her $\psi : C_1 \to C_2$ dönüşümü

$$C_1 \xrightarrow{\phi} C_1^{(q)} \xrightarrow{\lambda} C_2$$

şeklinde ifade edilir. ϕ dönüşümü q. kuvvet Frobenius dönüşümüdür ve λ dönüşümü ayrılabilirdir (Silverman 2009).

1.7 Bölenler (Divisors)

C eğrisinin bölen grubu $Div(C)$ ile gösterilir. Bu grup C noktaları ile üretilen serbest değişmeli gruptur. Böylece bir $D \in Div(C)$ böleni, sonlu sayıda $P \in C$ noktaları için $n_P = 0$ ve $n_P \in \mathbb{Z}$ olmak üzere

$$D = \sum_{P \in C} n_P(P)$$

şeklinde ifade edilen bir toplamdır. D'nin derecesi

$$\deg D = \sum_{P \in C} n_P$$

ile tanımlanır. Derecesi 0 olan bölenler, $Div(C)$'nin bir alt grubunu oluşturur ve

$$Div^0(C) = \{D \in Div(C) : \deg D = 0\}$$

ile gösterilir.

Şimdi C eğrisinin düzgün olduğunu farzedelim ve $f \in \overline{\mathbb{F}}(C)^*$ olsun. O zaman

$$div(f) = \sum_{P \in C} ord_P(f)(P)$$

olarak verilen $div(f)$ bölenini f ile ilişkilendirebiliriz.

Her ord_P bir değerleme olduğundan

$$div : \overline{\mathbb{F}}(C)^* \to Div(C)$$

dönüşümü değişmeli grupların bir homomorfizmidir.

Tanım 1.7.1 Bir $D \in Div(C)$ böleni, bazı $f \in \overline{\mathbb{F}}(C)$ için $D = div(f)$ formundaysa temel bölendir (principal divisor). $D_1 - D_2$ temel bölen ise iki bölen doğrusal olarak denktir ve $D_1 \sim D_2$ olarak gösterilir. C'nin $Pic(C)$ ile gösterilen bölen sınıfı grubu (veya Picard grubu), $Div(C)$'nin temel bölenlerin alt grubu ile bölümüdür (Silverman 2009).

Önerme 1.7.2 C düzgün bir eğri ve $f \in \overline{\mathbb{F}}(C)^*$ olsun.

$a)$ $div(f) = 0$ olması için gerek ve yeter şart $f \in \mathbb{F}^*$ olmasıdır.

$b)$ $\deg(div(f)) = 0$'dır (Silverman 2009).

Örnek 1.7.3 $\mathbb{P}^1$'de derecesi 0 olan her bölen temel bölendir. Bunu görmek için $D = \sum n_P(P)$'nin derecesinin 0 olduğunu varsayalım. $P = [\alpha_P, \beta_P] \in \mathbb{P}^1$ yazarak D'nin

$$\prod_{P \in \mathbb{P}^1} (\beta_P X - \alpha_P Y)^{n_P}$$

fonksiyonunun böleni olduğunu görürüz. $\sum n_P = 0$ oluşunun, bu fonksiyonun $\mathbb{F}(\mathbb{P}^1)$'de kalmasını sağladığına dikkat edin. Dolayısıyla $deg : Pic(\mathbb{P}^1) \to \mathbb{Z}$ dönüşümünün bir izomorfizm olduğu ortaya çıkar. Bunun tersi de doğrudur. Yani C düzgün bir eğriyse ve $Pic(C) \cong \mathbb{Z}$ ise o zaman C'de $\mathbb{P}^1$'e izomorftur (Silverman 2009).

Örnek 1.7.4 $Kar(\mathbb{F}) \neq 2$ olduğunu varsayalım. Birbirinden farklı $e_1, e_2, e_3 \in \overline{\mathbb{F}}$ olmak üzere

$$C : y^2 = (x - e_1)(x - e_2)(x - e_3)$$

eğrisini göz önüne alalım. C'nin düzgün bir eğri olduğu ve P_∞ ile gösterdiğimiz sonsuzda tek bir noktaya sahip olduğu kontrol edilebilir. $i = 1, 2, 3$ için $P_i = (e_i, 0) \in C$ olsun. O zaman

$$div(x - e_i) = 2(P_i) - 2(P_\infty)$$

$$div(y) = (P_1) + (P_2) + (P_3) - 3(P_\infty)$$

olur (Silverman 2009).

Tanım 1.7.5 C bir eğri olsun. Ω_C ile gösterilen C üzerindeki (meromorfik) diferansiyel formların uzayı, $x \in \overline{\mathbb{F}}(C)$ için dx formundaki semboller tarafından üretilen $\mathbb{F}$-vektör

uzayıdır ve

(i) $\forall x, y \in \overline{\mathbb{F}}(C)$ için $d(x+y) = dx + dy$,

(ii) $\forall x, y \in \overline{\mathbb{F}}(C)$ için $d(xy) = xdy + ydx$,

(iii) $\forall a \in \overline{\mathbb{F}}$ için $da = 0$

özellikleri sağlanır (Silverman 2009).

Tanım 1.7.6 $w \in \Omega_C$ olsun. w ile ilişkili bir bölen

$$div(w) = \sum_{P \in C} ord_P(w)(P) \in Div(C)$$

dir. Eğer her $P \in C$ için

$$ord_P(w) \geq 0$$

ise $w \in \Omega_C$ diferansiyeli regüler (veya holomorfik) olur. Eğer her $P \in C$ için

$$ord_P(w) \leq 0$$

ise $w \in \Omega_C$ yok olmayandır (nonvanishing) (Silverman 2009).

Tanım 1.7.7 C'deki kanonik bölen sınıfı, sıfırdan farklı herhangi bir $w \in \Omega_C$ diferansiyeli için $div(w)$'nin $Pic(C)$'deki görüntüsüdür. Bu bölen sınıfındaki herhangi bir bölen *kanonik bölen* olarak adlandırılır (Silverman 2009).

Örnek 1.7.8 $C : y^2 = (x-e_1)(x-e_2)(x-e_3)$ eğrisini göz önüne alalım. O zaman $div(dx) = (P_1)+(P_2)+(P_3)-3(P_\infty), \quad (dx = d(x-e_1) = -x^2 d(1/x))$ olur. Dolayısıyla $div(dx/y) = 0$ olduğu görülür. Böylece dx/y diferansiyeli hem holomorfiktir hem de yok olmayandır (Silverman 2009).

1.8 Riemann-Roch Teoremi

C bir eğri olsun. $Div(C)$ üzerindeki kısmi mertebe aşağıdaki gibi tanımlanmaktadır.

Tanım 1.8.1 Eğer $P \in C$ için $n_P \geq 0$ ise $D = \sum n_P(P)$ böleni pozitif (veya etkili) olup

$$D \geq 0$$

ile gösterilir. Benzer şekilde herhangi iki $D_1, D_2 \in Div(C)$ böleni için $D_1 - D_2$'nin pozitif olduğunu belirtmek için

$$D_1 \geq D_2$$

yazılır (Silverman 2009).

Örnek 1.8.2 $f \in \overline{\mathbb{F}}(C)^*$, bir $P \in C$ noktası dışında her yerde regüler olan bir fonksiyon olsun ve P noktasında en fazla n mertebeli bir kutbu olsun. f fonksiyonu ile ilgili

$$div(f) \geq -n(P)$$

eşitsizliği ifade edilebilir. Ayrıca benzer şekilde

$$div(f) \geq (Q) - n(P)$$

eşitsizliği f'nin Q'da sıfırı olduğunu ifade eder. Bu nedenle bölen ile eşitsizlikleri, fonksiyonların kutuplarını ve/ veya sıfırlarını ifade etmek için kullanışlı bir yoldur (Silverman 2009).

Tanım 1.8.3 $D \in Div(C)$ olsun.

$$\mathbb{L}(D) = \{f \in \overline{\mathbb{F}}(C)^* : div(f) \geq -D\} \cup \{0\}$$

kümesi sonlu boyutlu $\overline{\mathbb{F}}$ vektör uzayıdır ve boyutu

$$\ell(D) = dim_{\overline{\mathbb{F}}}\mathbb{L}(D)$$

ile gösterilir. Artık cebirsel eğri geometrisinde çok önemli temel bir sonuç ifade edilebilir

(Silverman 2009).

Teorem 1.8.4 (Riemann-Roch) C düzgün bir eğri ve $\mathbb{F}_C, C$ üzerinde kanonik bir bölen olsun. $\forall\ D \in Div(C)$ böleni için

$$\ell(D) - \ell(\mathbb{F}_C - D) = degD - g + 1$$

bağıntısı ile bir $g \geq 0$ tamsayısı bulunabilir. Bu g sayısına C *eğrisinin cinsi* denir (Silverman 2009).

Sonuç 1.8.5 Aşağıdaki özellikler sağlanır.

$a)$ $\ell(\mathbb{F}_C) = g$,

$b)$ $\deg \mathbb{F}_C = 2g - 2$,

$c)$ $\deg D > 2g - 2$ ise o zaman $\ell(D) = \deg D - g + 1$

olur (Silverman 2009).

Örnek 1.8.6 $C = \mathbb{P}^1$ olsun. C üzerinde hiçbir holomorf diferansiyel yoktur. Böylece $\ell(\mathbb{F}_C) = 0$ olur. Dolayısıyla Sonuç 1.8.5 ile $\mathbb{P}^1$'in cinsi 0 olur ve Riemann-Roch teoremine göre

$$\ell(D) - \ell(-2(\infty) - D) = \deg D + 1$$

olur. Özellikle eğer $\deg D \geq -1$ ise

$$\ell(D) = \deg D + 1$$

olur (Silverman 2009).

Aritmetik geometride, cebirsel eğriler üzerindeki rasyonel noktaların sonluluğu hakkında aşağıdaki teorem 1910'da Mordell tarafından "sanı" olarak verilmiştir.

Teorem 1.8.7 δ, cinsi $g \geq 2$ olacak şekilde $\mathbb{F}$ cismi üzerinde bir cebirsel eğri olsun. Bu durumda δ üzerinde sonlu çoklukta rasyonel nokta vardır. Başka bir deyişle $\mathbb{F}$-rasyonel noktaların $\delta(\mathbb{F})$ kümesi sonludur (Faltings 1983).

2. ELİPTİK EĞRİLER

Bu bölümde eliptik eğriler ile ilgili temel kavramlar ve bazı önemli teoremler verilecektir.

2.1 Weierstrass Denklemler

Eliptik eğriler belirli bir taban noktasına sahip cinsi 1 olan düzgün cebirsel eğrilerdir. Bu özellikteki her eğri, sonsuzdaki doğru üzerinde bulunan sadece bir taban noktası ile kübik bir denklemin $\mathbb{P}^2$'deki yeri olarak yazılabilir. Yani X ve Y uygun bir şekilde ölçeklendirildikten sonra $a_1, a_2, a_3, a_4, a_6 \in \overline{\mathbb{F}}$ ve $\mathcal{O} = [0, 1, 0]$ taban noktası olmak üzere bir eliptik eğri

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{2.1.1}$$

formundaki denklem ile verilir. Bu tipteki denklemler *Weierstrass denklemleri* olarak adlandırılır. (2.1.1) eğrisini göz önüne alalım. Bu homojen eğride $Z = 0$ olması $X = 0$ demektir ve Y sıfırdan farklı herhangi bir elemandır. Böylece $Z = 0$ olduğunda (2.1.1) üzerindeki *sonsuzdaki nokta* $\mathcal{O} = (0 : 1 : 0)$ şeklinde elde edilir.

Notasyonu kolaylaştırmak için homojen olmayan $x = X/Z$ ve $y = Y/Z$ koordinatları kullanarak (2.1.1)'deki Weierstrass denkleminden aşağıdaki cebirsel düzlemsel eğri elde edilir.

Tanım 2.1.1 $\mathbb{F}$ bir cisim ve $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}$ olmak üzere

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.1.2}$$

biçimindeki E eğrisi, sonsuzdaki $\mathcal{O} = [0, 1, 0]$ noktası ile birlikte *uzun Weierstrass normal formunda eğri* olarak adlandırılır (Schmitt ve Zimmer 2003).

$Kar(\overline{\mathbb{F}}) \neq 2$ ise o zaman kareye tamamlayarak denklemi sadeleştirebiliriz.

$$y \longrightarrow \frac{1}{2}(y - a_1x - a_3)$$

yazıldığında

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= a_1a_3 + 2a_4 \\ b_6 &= a_3^2 + 4a_6 \end{aligned} \tag{2.1.3}$$

olmak üzere

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$

formunda bir denklem elde edilir. Ayrıca

$$\begin{aligned} b_8 &= a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2 \\ c_4 &= b_2^2 - 24b_4 \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6 \end{aligned} \tag{2.1.4}$$

olarak tanımlanır. (2.1.3) ve (2.1.4)'te ifade edilen değerler *Tate değerleri* olarak adlandırılır. E eğrisinin diskriminantı, j *değişmezi* ve w*-diferansiyel değişmezi* sırası ile

$$\begin{aligned} \Delta(E) &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\ j &= \frac{c_4^3}{\Delta} \\ w &= \frac{dx}{2ya_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y} \end{aligned}$$

şeklinde tanımlanır. Dolayısıyla

$$4b_8 = b_2b_6 - b_4^2 \quad \text{ve} \quad 1728\Delta = c_4^3 - c_6^2$$

bağıntıları kolayca sağlanır. Eğer $Kar(\overline{\mathbb{F}}) \neq 2, 3$ ise o zaman

$$(x, y) = \left(\frac{x - 3b_2}{36}, \frac{y}{108} \right)$$

dönüşümü ile x^2'li terimi yok ederek daha basit hali olan

$$E : y^2 = x^3 - 27c_4x - 56c_6$$

denklemi elde edilir.

Tanım 2.1.2 C cebirsel düzlem eğri

$$C : f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$$

Weierstrass denklemi ile verilsin. $P = (x_0, y_0) \in C$ olmak üzere P'nin *tekil nokta* olması için gerek ve yeter şart

$$\frac{\partial f}{\partial x}(x_0, y_0) = 0 \quad ve \quad \frac{\partial f}{\partial y}(x_0, y_0) = 0$$

olmalıdır (Silverman 2009).

Eğer birinci kısmi türevler $P = (x_0, y_0)$ noktasında sıfır ise, tekil nokta katlı bir noktadır. Bu katlı noktanın iki farklı teğeti varsa *düğüm (node)*, iki teğetinin çakışması durumunda *çıkıntı (cusp)* olarak adlandırılır. Tekil noktaları olan eğriye *tekil eğri*, tekil noktaları olmayan bir eğri *düzgün eğri* olarak adlandırılır (Schmitt ve Zimmer 2003).

Önerme 2.1.3 Uzun Weierstrass formunda verilen eğriler aşağıdaki gibi sınıflandırılabilir:

i. Eğri düzgündür $\Leftrightarrow \Delta \neq 0$ dır.

ii. Eğrinin bir *düğümü* vardır $\Leftrightarrow \Delta = 0$ ve $c_4 \neq 0$.

iii. Eğrinin bir *çıkıntısı* vardır $\Leftrightarrow \Delta = 0$ ve $c_4 = 0$.

(ii) ve (iii) durumlarında eğri tek tekil noktaya sahiptir (Silverman 2009).

Tanım 2.1.4 Diskriminantı sıfırdan farklı (2.1.2) uzun Weierstrass normal formundaki eğri, (sonsuzdaki nokta ile birlikte) $\mathbb{F}$ cismi üzerinde bir *eliptik eğri* olarak adlandırılır.

Tanım 2.1.5 $\mathbb{F}$ cismi üzerinde tanımlı E ve E' eliptik eğrileri

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$
$$E' : y'^2 + a'_1x'y' + a'_3y' = x'^3 + a'_2x'^2 + a'_4x' + a'_6$$

olarak verilsin. Bu durumda E eğrisini E' eğrisine dönüştüren

$$x = u^2x' + r, \quad y = u^3y' + u^2sx' + t \quad (u, r, s, t \in \mathbb{F}, u \neq 0)$$

dönüşümleri varsa böyle dönüşümlere *birasyonel dönüşümler*, E ve E' eliptik eğrilerine $\mathbb{F}$ cismi üzerinde *birasyonel denktir* denir.

Bu dönüşümlerin ters dönüşümü de

$$x' = \frac{1}{u^2}(x - r), \quad y' = \frac{1}{u^3(y - sx + sr - t)}$$

şeklindedir. Bu sonuçlar aşağıdaki tabloda düzenlenmiştir (Silverman 2009).

Çizelge 2.1.1. Weierstrass denklemleri için değişken değiştirme formülleri

$ua_1' = a_1 + 2s$
$u^2a_2' = a_2 - sa_1 + 3r - s^2$
$u^3a_3' = a_3 + ra_1 + 2t$
$u^4a_4' = a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st$
$u^6a_6' = a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1$
$u^2b_2' = b_2 + 12r$
$u^4b_4' = b_4 + rb_2 + 6r^2$
$u^6b_6' = b_6 + 2rb_4 + r^2b_2 + 4r^3$
$u^8b_8' = b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4$
$u^4c_4' = c_4$
$u^6c_6' = c_6$
$u^12\Delta' = \Delta$
$j' = j$
$u^{-1}w' = w$

Tanım 2.1.6 $Kar(\mathbb{F}) \neq 2, 3$ iken $E, \mathbb{F}$'de bir eliptik eğrisi olsun. Bu durumda $A, B \in \mathbb{F}$ olmak üzere E'yi $\mathbb{F}$ cisminde

$$E' : y^2 = x^3 + Ax + B \tag{2.1.5}$$

formundaki E''ne resmeden bir $\phi : E \to E'$ birasyonel dönüşümü vardır. Bu durumda E' eğrisi *basitleştirilmiş (veya kısa) Weierstrass normal formunda bir eliptik eğri* olarak adlandırılır (Schmitt ve Zimmer 2003).

Yukarıda ifade edilen basitleştirilmiş Weierstrass normal formundaki bir eğri için diskriminant ve j-değişmezi

$$\Delta(E) = -16(4A^3 + 27B^2), \quad j(E) = \frac{-12^3(4A)^3}{\Delta}$$

şeklindedir.

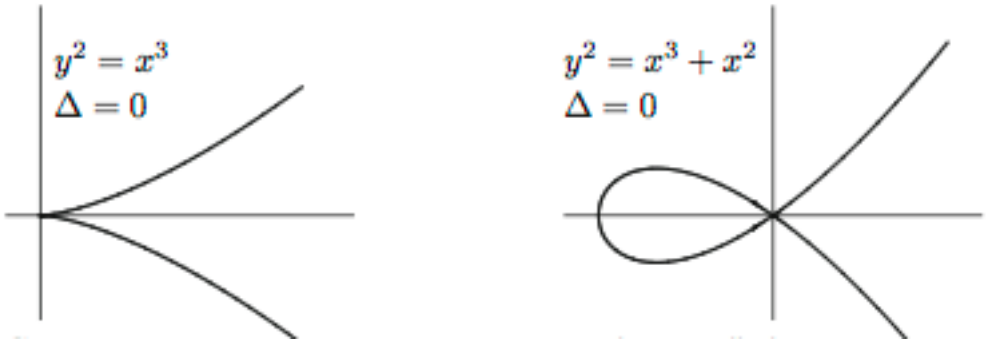
j değişmezi iki eliptik eğrinin birbirinin ne zaman izomorf olduğunu belirlemek için kullanılır. Aşağıdaki teorem basitleştirilmiş Weierstrass normal formunda verilen iki eliptik eğrinin birbirine ne zaman izomorf olduğunu belirtmektedir.

Teorem 2.1.7 $\mathbb{F}$ bir cisim E ve E' eğrileri $\mathbb{F}$ cismi üzerinde tanımlı basitleştirilmiş Weierstrass normal formunda verilen iki eliptik eğri olsun. Bu iki eğrinin $\mathbb{F}$ cismi üzerinde izomorf olmaları için gerek ve yeter şart E ve E' eğrilerinin j-değişmezlerinin aynı olmasıdır (Schmitt ve Zimmer 2003).

Aşağıdaki örnekte düzgün eğriler ve tekil eğrilerin grafiği yer almaktadır.

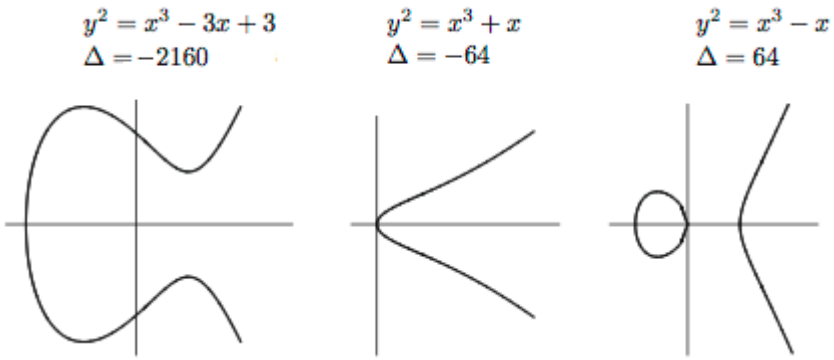
Örnek 2.1.8

- $y^2 = x^3$ eğrisi için $\Delta = 0$ olup $x = 0$ katlı bir kök olduğundan bir eliptik eğri değildir.
- $y^2 = x^3 + x^2$ eğrisi için $\Delta = 0$ olup $x = 0$ katlı bir kök olduğundan bir (tekil eğri) eliptik eğri değildir.
- $y^2 = x^3 - 3x + 3$ eğrisi için $\Delta = 2160$ olup bir (düzgün eğri) eliptik eğridir.
- $y^2 = x^3 + x$ eğrisi için $\Delta = -64$ olup bir eliptik eğridir.
- $y^2 = x^3 - x$ eğrisi için $\Delta = 64$ olup bir eliptik eğridir.



Çıkıntı Düğüm

Şekil 2.1.1. Tekil Eğriler



Şekil 2.1.2. Düzgün Eğriler

Eliptik eğriler sonlu ya da sonsuz çoklukta rasyonel çözüme sahiptir. Daha önce tanımlanan $\mathcal{O}$ noktası eliptik eğriler teorisi için oldukça önemlidir. Eliptik eğriler üzerindeki noktalar $\mathcal{O}$ noktası ile birlikte bir (toplamsal) abelyan grup oluşturur.

Paralel olan herhangi iki doğrunun $\mathbb{R}^2$'de kesişmedikleri bilinmektedir, fakat bu iki doğru $\mathbb{P}^2$'de sonsuzda kesişirler. Bu da, eliptik eğriler üzerindeki noktaların oluşturduğu küme üzerinde tanımlanacak olan toplama işleminde kullanılacaktır.

2.2 Eliptik Eğriler Üzerinde Toplama Kuralı

E, (2.1.2) formunda bir eliptik eğri olsun. $E \subset \mathbb{P}^2$ eliptik eğrisi üzerindeki $P = (x, y)$ rasyonel noktalar, sonsuzdaki $\mathcal{O} = [0, 1, 0]$ noktası ile birlikte

$$E(\mathbb{F}) = \{(x, y) \in E : x, y \in \mathbb{F}\} \cup \{\mathcal{O}\}$$

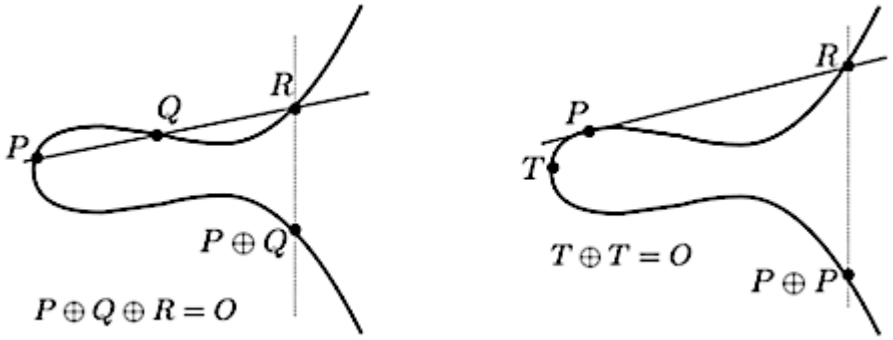
kümesini oluşturur. $L \subset \mathbb{P}^2$ bir doğru olsun. O zaman denklemin derecesi 3 olduğundan L doğrusu E eğrisi ile tam olarak üç noktada kesişir. Bu noktalar P, Q, R olsun. Tabi ki eğer L, E'ye teğet ise P, Q ve R noktalarının farklı olması gerekmez. Katlılıkları ile birlikte alınan $L \cap E$ tam olarak 3 noktadan oluşur. Bu da Bézout teoreminin özel bir halidir.

Teorem 2.2.1 Bir doğru ile bir eliptik eğri katlılıkları ile birlikte tam olarak 3 noktada kesişir (Schmitt ve Zimmer 2003).

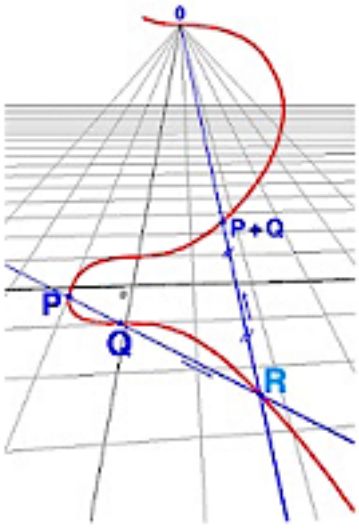
Teorem 2.2.2 (Bézout Teoremi) $m.$ dereceden bir düzlem eğri ile $n.$ dereceden bir düzlem eğri en çok $m.n$ tane noktada kesişir (Silverman 2009).

Aşağıdaki tanımda E üzerindeki toplama işlemi kuralı $\oplus$ sembolü ile tanımlanır.

Tanım 2.2.3 (Toplama Kuralı) P ve Q, (2.1.2) formundaki E eliptik eğrisi üzerindeki farklı iki nokta olsun. P ve Q noktalarından geçen l doğrusu, eliptik eğriyi üçüncü bir $R = (x, y)$ noktasında kessin. l', R ve $\mathcal{O}$'dan geçen bir doğru olsun. Bu durumda l', E'yi R, $\mathcal{O}$ ve üçüncü bir noktada keser. Üçüncü noktayı $P \oplus Q$ ile gösteririz. (Eğer $P = Q$ ise bu durumda l doğrusu E eliptik eğrisine P noktasında teğettir) (Silverman 2009).



Şekil 2.2.1.



Şekil 2.2.2.

Önerme 2.2.4 Toplama kuralı $\oplus$ aşağıdaki özellikleri sağlar:

i. Bir l doğrusu E'yi (farklı olması gerekli olmayan) P, Q, R noktalarında keserse o zaman $(P \oplus Q) \oplus R = \mathcal{O}$ olur.

ii. Toplama kuralının değişme özelliği: $P \oplus Q = Q \oplus P$.

iii. Toplama kuralının birleşme özelliği: $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$.

iv. $\mathcal{O}$ noktası birim elemandır : $P \oplus \mathcal{O} = P = \mathcal{O} \oplus P$.

v. P noktasının tersi $\ominus P$ dir : $P \oplus (\ominus P) = \mathcal{O} = (\ominus P) \oplus P$

(Silverman 2009).

Yukarıda verilenlere göre *E eliptik eğrisi üzerindeki noktaların kümesi toplama kuralına göre (sonsuzdaki $\mathcal{O}$ noktası dahil) değişmeli bir gruptur* denir.

Not 2.2.5 Buradan itibaren E eliptik eğrisi üzerindeki grup işlemleri için $\oplus$ ve $\ominus$ özel sembolleri yerine daha basit olan $+$ ve $-$ kullanılacaktır. $m \in \mathbb{Z}$ ve $P \in E$ için

$$[m]P = \underbrace{P + \cdots + P}_{m>0 \text{ ise m terim}}, \quad [m]P = \underbrace{-P - \cdots - P}_{m<0 \text{ ise } |m| \text{ terim}}, \quad [0]P = \mathcal{O}$$

olur (Silverman 2009).

Teorem 2.2.6 $P_1 = (x_1, y_1)$ ve $P_2 = (x_2, y_2)$ noktaları (2.1.2) uzun Weierstrass normal formunda eğri üzerindeki noktalar olsun. Bu durumda

$a)$ $-P_1 = (x_1, -y_1 - a_1x_1 - a_3)$ olur.

$b)$ Eğer $x_1 = x_2$ ve $y_1 + y_2 + a_1x_2 + a_3 = 0$ ise $P_1 + P_2 = \mathcal{O}$ olur. Aksi takdirde λ ve ν aşağıdaki formüller ile tanımlanır:

Çizelge 2.2.1.

	λ	ν
$x_1 \neq x_2$	$\frac{y_2-y_1}{x_2-x_1}$	$\frac{y_1x_2-y_2x_1}{x_2-x_1}$
$x_1 = x_2$	$\frac{3x_1+2a_2x_1+a_4-a_1y_1}{2y_1+a_1x_1+a_3}$	$\frac{-x_1^3+a_4x_1+2a_6-a_3y_1}{2y_1+a_1x_1+a_3}$

şeklindedir.

O halde $y = \lambda x + \nu, P_1$ ve P_2'den geçen doğrudur veya $P_1 = P_2$ ise E'ye teğettir.

Yukarıdaki gösterimlerle $P_1 + P_2 = P_3 = (x_3, y_3)$ noktasının bileşenleri

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$$

$$y_3 = -(\lambda + a_1)x_3 - \nu - a_3$$

ile verilir.

$c)$ $P_1 \neq \pm P_2$ ise

$$x(P_1 + P_2) = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 + a_1\left(\frac{y_2 - y_1}{x_2 - x_1}\right) - a_2 - x_1 - x_2$$

ve $P = (x, y) \in E$ için "ikiye katlama formülü"

$$x(2P) = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6} \tag{2.2.1}$$

olup b_2, b_4, b_6 ve b_8 değerleri daha önce verilen değerlerdir (Silverman 2009).

Şimdi sayısal hesaplamalar yapmada kolaylık sağlamak için (2.1.5) basitleştirilmiş Weierstrass normal formunda eğriler için toplam formülünü vereceğiz.

Önerme 2.2.7 $P_1 = (x_1, y_1)$ ve $P_2 = (x_2, y_2)$ noktaları (2.1.5) basitleştirilmiş Weierstrass normal formunda eğri üzerindeki noktalar olsun. O zaman $P_1 + P_2 = (x_3, y_3)$ olmak üzere

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & P_1 \neq P_2 \text{ ise} \\ \\ \frac{3x_1^2 + A}{2y_1}, & P_1 = P_2 \text{ ise} \end{cases}$$

iken

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = \lambda(x_1 - x_3) - y_1$$

şeklinde tanımlanır (Mollin 2001).

$2P_1$ noktasının bileşenleri Önerme 2.2.7 kullanılarak bulunur.

Örnek 2.2.8 $\mathbb{Q}$ cismi üzerinde $y^2 = x^3+4x+4$ eliptik eğrisini alalım. Bu eğri üzerindeki $P_1 = (1,3)$ ve $P_2 = (0,2)$ noktaları olmak üzere $P_1 + P_2$'yi hesaplayalım. Bunun için öncelikle bu noktalardan geçen doğrunun eğimini bulmalıyız.
$\lambda = \frac{2-3}{0-1} = 1$ ve böylece $x_3 = 1^2 - 1 - 0 = 0$ ve $y = 1(1-0) - 3 = -2$ olup $P_1 + P_2 = (0,-2)$ bulunur.

2.3 Weierstrass Denklemler İçin Başka Formlar

2.3.1 Legendre Form

Bazen uygun olan başka bir Weierstrass denklem biçimi vardır.

Tanım 2.3.1 Bir Weierstrass denklemi

$$y^2 = x(x-1)(x-\lambda)$$

formunda yazılabiliyorsa *Legendre formunda* olarak adlandırılır (Silverman 2009).

Önerme 2.3.2 $Kar(\mathbb{F}) \neq 2$ iken $e_1, e_2, e_3 \in \mathbb{F}$ olmak üzere

$$E : y^2 = x^3 + ax^2 + bx + c = (x-e_1)(x-e_2)(x-e_3) \tag{2.3.1}$$

olsun.

$$x_1 = (e_2-e_1)^{-1}(x-e_1), \quad y_1 = (e_2-e_1)^{-3/2}y, \quad \lambda = \frac{e_3-e_1}{e_2-e_1}$$

olarak alındığında

$$E : y_1^2 = x_1(x_1-1)(x_1-\lambda) \tag{2.3.2}$$

elde edilir (Washington 2008).

2.3.2 Üçüncü Derece Denklemler

Burada üçüncü dereceden denklemler ile eliptik eğriler arasındaki ilişki ifade edilecektir. $Kar(\mathbb{F}) \neq 2, 3$ olsun. $x, y \in \mathbb{F}$ olmak üzere Weierstrass formuna dönüştürülen ($4A^3 + 27B^2 = 0$ olsa bile), $C(x, y) = 0$ kübik bir denklem, örneğin:

$$x^3 + y^3 + z^3 = 0 \tag{2.3.3}$$

kübik Fermat denklemini ele alalım. $xyz \neq 0$ olmak üzere bu denklemin hiçbir rasyonel çözümü olmadığı 900'lü yıllarda Araplar tarafından sanı olarak verilmişti. Bu denklem Fermat'ın son teoreminin özel bir halini temsil eder. 1673'de Fermat $n \geq 3$ tamsayısı için

$$x^n + y^n = z^n$$

denkleminin sıfırdan farklı tamsayı çözümü olmayacağını iddia etmişti. Bu iddia 1995 yılında Andrew Wiles ve öğrencisi Richard Taylor tarafından ispatlandı (Taylor ve Wiles 1995). $n = 3$ durumundaki ilk ispat, muhtemelen Fermat tarafından yapılmıştı. $xyz \neq 0$ olmak üzere (2.3.3) denklemini göz önüne alalım. $x^3 + y^3 = (x + y)(x^2 - xy + y^2)$ şeklinde yazılabileceğinden $x + y \neq 0$ dır.

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

yazalım. O zaman $(u + v)^3 + (u - v)^3 + 1 = 0$ eşitliğinden $2u^3 + 6uv^2 + 1 = 0$ olur. Her tarafı u^3 ile bölündüğünde ($x + y \neq 0$ olduğundan $u \neq 0$)

$$6(v/u)^2 = -(1/u)^3 - 2$$

elde edilir.

$$x_1 = -\frac{6}{u} = -12\frac{z}{x + y}, \qquad y_1 = \frac{36v}{u} = 36\frac{x - y}{x + y}$$

olsun. Bu durumda (2.3.3) denklemi

$$y_1^2 = x_1^3 - 432$$

eliptik eğrisine dönüşür. Bu eşitliğin çözümleri $(x_1, y_1) = (12, 36), (12, -36)$ ve $\mathcal{O}$ dur. $y_1 = 36$ olması durumunda $x - y = x + y$ ve dolayısıyla $y = 0$ olur. Benzer şekilde $y_1 = -36$ ise $x = 0$ olur. $(x_1, y_1) = \mathcal{O}$ olması durumunda $x = -y$ olup $z = 0$ olur. O halde $xyz \neq 0$ olmak üzere $x^3 + y^3 + z^3 = 0$ denkleminin çözümü yoktur. Sonuç olarak (2.3.3) denklemi eliptik eğri teorisinden yararlanılarak çözülmüş olur.

2.3.3 Dördüncü Derece Denklemler

$a \neq 0$ ve $a, b, c, d, e \in \mathbb{F}$ iken

$$v^2 = au^4 + bu^3 + cu^2 + du + e \tag{2.3.4}$$

formundaki eğrileri göz önüne alalım. $p, q \in \mathbb{F}$ olmak üzere (p, q) noktası (2.3.4) eğrisi üzerindeki bir nokta ise o zaman (tekil olmadığından) (2.3.4) formundaki eğri bazı değişken dönüşümleri yardımıyla Weierstrass formunda bir eliptik eğriye dönüşür. $\mathbb{F}$ cismi üzerinde tanımlanan bir E eliptik eğrisinin her zaman $E(\mathbb{F})$'de bir $\mathcal{O}$ noktası vardır ($(0, 1, 0)$ projektif koordinatları mutlaka $\mathbb{F}$'dedir). Dolayısıyla eğer bir C eğrisini, tüm katsayılar $\mathbb{F}$'de olacak şekilde Weierstrass formuna dönüştürürsek, o zaman C üzerindeki koordinatları $\mathbb{F}$'de olan bir nokta ile başlamak gerekir. Şimdi (p, q) noktası (2.3.4) denklemi üzerinde olduğunu varsayalım. Dolayısıyla u yerine $u + p$ yazdığımızda $p = 0$ olduğunu varsayabiliriz. Böylece (p, q) noktası $(0, q)$ olur. İlk olarak $q = 0$ olduğunu varsayalım. Eğer $d = 0$ ise o zaman eğrinin $(u, v) = (0, 0)$ tekil noktası vardır. O halde $d \neq 0$ varsayalım. Böylece

$$\left(\frac{v}{u^2}\right)^2 = d\left(\frac{1}{u}\right)^3 + c\left(\frac{1}{u}\right)^2 + b\left(\frac{1}{u}\right) + a$$

elde edilir. Bu da kolayca Weierstrass forma dönüşebilir. Zor olan durum $q \neq 0$ olduğunda ise aşağıdaki sonuca ulaşırız.

Teorem 2.3.3 $Kar(\mathbb{F}) \neq 2$ ve $a, b, c, d, q \in \mathbb{F}$ olmak üzere

$$v^2 = au^4 + bu^3 + cu^2 + du + q^2 \tag{2.3.5}$$

olsun.

$$x = \frac{2q(v+q) + du}{u^2}, \quad y = \frac{4q^2(v+q) + 2q(du + cu^2) - (d^2u^2/2q)}{u^3}$$

alalım.

$$a_1 = \frac{d}{q}, \quad a_2 = c - \left(\frac{d^2}{4q^2}\right), \quad a_3 = 2qb, \quad a_4 = -4q^2a, \quad a_6 = a_2a_4$$

olarak tanımlansın. O zaman (2.3.5) eğrisi (2.1.2) uzun Weierstrass normal formunda eğriye dönüşür. Ters dönüşüm ise

$$u = \frac{2q(x+c) - (d^2/2q)}{y}, \quad v = -q + \frac{u(ux - d)}{2q}$$

şeklindedir. $(u, v) = (0, q)$ noktası $(x, y) = \mathcal{O}$ noktasına ve $(u, v) = (0, -q)$ noktası $(x, y) = (-a_2, a_1a_2 - a_3)$ noktasına karşılık gelir (Washington 2008).

Örnek 2.3.4

$$v^2 = u^4 + 1 \tag{2.3.6}$$

eğrisini ele alalım. $a = 1, b = c = d = 0$ ve $q = 1$'dir.

$$x = \frac{2(v+1)}{u^2}, \quad \frac{4(v+1)}{u^3}$$

ise o zaman $E : y^2 = x^3 - 4x$ eliptik eğrisi elde edilir. Bu dönüşümün tersi ise

$$u = 2x/y, \quad v = -1 + (2x^3/y^2)$$

şeklindedir. $(u, v) = (0, 1)$ noktası E üzerinde $\mathcal{O}$ noktasına, $(u, v) = (0, -1)$ noktası da $(0, 0)$ noktasına karşılık gelir. E üzerindeki tüm rasyonel noktalar

$$E(\mathbb{Q}) = \{\mathcal{O}, (0, 0), (2, 0), (-2, 0)\}$$

olur. Bu noktalar $(u, v) = (0, 1), (0, -1)$ ve sonsuzdaki noktalara karşılık gelir. Böylece dördüncü dereceden eğri üzerindeki tek sonlu rasyonel nokta $(u, v) = (0, \pm 1)$'dir. Buradan $a^4+b^4 = c^2$ nin sadece tamsayı çözümlerinin $ab = 0$'ı sağlar. Dolayısıyla bu denklem de Fermat'nın son teoreminin $n = 4$ durumuna karşılık gelir.

Şimdi $u, v \to \infty$ durumunu ele alalım. Eğer (2.3.6) denklemini homojen hale getirmek istersek

$$F(u, v, w) = v^2w^2 - u^4 - w^4 = 0$$

elde edilir. Sonsuzdaki noktalar $w = 0$'dır. Bu noktaları bulabilmek için $w = 0$ olarak alınırsa $u^4 = 0$ olup $u = 0$ elde edilir. Böylece $(u : v : w) = (0 : 1 : 0)$ noktası bulunur. Ancak karşılık gelen Weierstrass modelinde $(2, 0)$ ve $(-2, 0)$ olmak üzere iki nokta vardır. $(u : v : w) = (0 : 1 : 0)$ noktasının 4. derece eğri üzerinde tekil nokta olması bir sorundur. Dolayısıyla bu noktada

$$F_u = F_v = F_w = 0$$

olur. Böylece eğri kendisini $(u : v : w) = (0 : 1 : 0)$ noktasında keser. Eğrinin bir dalı $v = u^2\sqrt{1 + (1/u)^4}$ ve diğeri $v = -u^2\sqrt{1 + (1/u)^4}$ olur.

Daha basit olarak gerçek veya kompleks sayılarla çalışalım. Bu ifadelerden ikincisini $x = 2(v + 1)/u^2$ de yerine yazarsak ve $u \to \infty$ olarak alınırsa

$$x = \frac{2(v+1)}{u^2} = \frac{2(1 - u^2\sqrt{1 + (1/u)^4})}{u^2} \to -2$$

elde edilir. Eğrinin diğer dalı için $x \to +2$ bulunur. Böylece dördüncü derece denklemi Weierstrass denklemine dönüştüren dönüşüm, tekil noktada eğriyi iki dala ayırdı (Washington 2008).

Şimdi aşağıdaki önemli sonucu verelim:

Teorem 2.3.5 $K, L, M, N, P \in \mathbb{Q}$ olmak üzere

$$t^2 = Ku^4 + Lu^3 + Mu^2 + Nu + P \tag{2.3.7}$$

formundaki eğri

$$I = 12KP - 3LN + M^2 \tag{2.3.8}$$

ve

$$J = 72KMP + 9LMN - 27KN^2 - 27L^2P - 2M^3 \tag{2.3.9}$$

dönüşümleri yardımıyla

$$\chi : V^2 = U^3 - 27IU - 27J \tag{2.3.10}$$

formundaki bir χ eğrisine birasyonel denktir.

χ'nin $\Delta(\chi)$ diskriminantı $(4I^3 - J^2)/27$'dir, ve χ'nin tekil olması için gerek ve yeter şart $\Delta(\chi) = 0$ olmasıdır. Üstelik K bir tam kare olduğunda

$$R = \left(3\frac{3L^2 - 8KM}{4K}, 27\frac{L^3 + 8K^2N - 4KLM}{8K^{3/2}}\right) \tag{2.3.11}$$

noktası $\chi(\mathbb{Q})$ üzerindedir (Cremona 1997).

2.3.4 İki Kuadratik Yüzeyin Kesişimi

Üç boyutlu uzayda iki tane ikinci dereceden yüzeyin kesişimi, bu kesişim noktasındaki bir nokta ile birlikte genellikle bir eliptik eğridir. $Kar(\mathbb{F}) \neq 2$ ve a, b, c, d, e, f katsayıları

sıfırdan farklı ve $\mathbb{F}$ cisminde olmak üzere

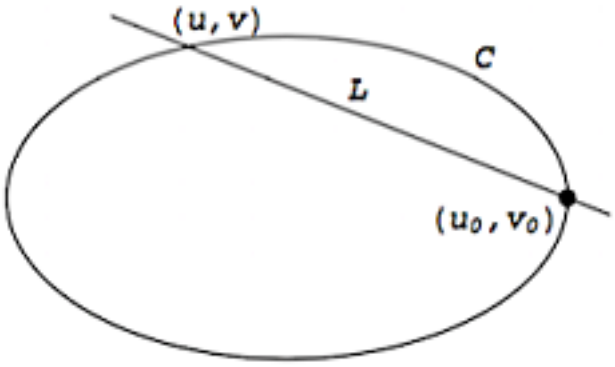
$$au^2 + bv^2 = e, \quad cu^2 + dw^2 = f \tag{2.3.12}$$

formundaki denklemleri göz önüne alalım. Her iki denklem, uvw- uzayında bir yüzeydir ve kesişimleri bir eğridir. Bu iki eğri bir P noktasında kesişirse (2.3.12) eğrisi Weierstrass formundaki bir eliptik eğriye dönüştürülebilir.

Bu iki yüzeyin kesişimini analiz etmeden (2.3.12)'deki ilk denklemi ele alalım. Bu eğriye uv-düzleminde $C : au^2 + bv^2 = e$ eğrisi diyelim. $P = (u_0, v_0)$ noktası C eğrisi üzerinde olsun. P noktasından geçen doğrunun eğimi m, $t \in \mathbb{Q}$ parametresine bağlı olarak

$$u = u_0 + t \quad v = v_0 + mt \tag{2.3.13}$$

şeklinde yazılabilir. L'nin C ile kesiştiği diğer nokta bulunmak istenirse:



Şekil 2.3.1

(2.3.13), C eğrisinde yerine yazıldığında

$$a(2u_0t + t^2) + b(2v_0mt + m^2t^2) = 0$$

elde edilir. $t = 0$ olması (u_0, v_0)'a karşılık geldiğinden

$$t = -\frac{2au_0 + 2bv_0m}{a + bm^2}$$

elde edilir. Böylece

$$u = u_0 - \frac{2au_0 + 2bv_0m}{a + bm^2} \quad v = v_0 - \frac{2au_0m + 2bv_0m^2}{a + bm^2}$$

olur.

Eğer $u, v \in \mathbb{F}$ olmak üzere (u, v) noktası C üzerindeki herhangi bir nokta ise (u, v) ve P'den geçen doğrunun eğimi m, $\mathbb{F}$'dedir (veya sonsuzdur).

Şimdi uvw-uzayında bir "silindir" olarak kabul edilen C'yi $cu^2 + dw^2 = f$ yüzeyiyle kesiştirelim. u yerine yazıldığında

$$dw^2 = f - c\left(u_0 - \frac{2au_0 + 2bv_0m}{a + bm^2}\right)$$

olup düzenlendiğinde

$$\begin{aligned} d(w(a + bm^2))^2 =& (a + bm^2)^2 f - c(bu_0m^2 - 2bv_0m - au_0)^2 \\ =& (b^2f - cb^2u_0^2)m^4 + 4cb^2v_0u_0m^3 + (2abf - c(-2au_0^2b + 4b^2v_0^2))m^2 \\ & - 4cau_0bv_0m + a^2f - ca^2u_0^2 \end{aligned}$$

elde edilir. m^4'ün baş katsayısı $b^2f - cb^2u_0^2$'dır ve bu $b^2dw_0^2$'ye eşittir. Eğer $w_0 = 0$ ise dördüncü dereceden polinom kübik bir polinom haline gelir ve böylece yeni elde edilen denklem kolayca Weierstrass formuna getirilebilir . Bu kübik polinomun başkatsayısının yok olması için gerek ve şart $v_0 = 0$ olmasıdır. Fakat bu durumda $(u_0, v_0, w_0) = (u_0, 0, 0)$ noktasının uvw-eğrisinin tekil noktası olması demektir. Bu da kaçınmamız gereken bir durumdur (Washington 2008).

Örnek 2.3.6

$$u^2 + v^2 = 2 \qquad u^2 + 4w^2 = 5$$

kuadratik yüzeylerinin kesişimini düşünelim. $(u_0, v_0, w_0) = (1, 1, 1)$ olsun. İlk olarak $u^2 + v^2 = 2$ yüzeyinin çözümlerini parametrik ifade edelim. $u = 1 + t$ ve $v = 1 + mt$ olsun. Bu değerler yerine yazıldığında $(1 + t)^2 + (1 + mt)^2 = 2$ olup düzenleme

yapıldığında $t(2+2m)+t^2(1+m^2)=0$ elde edilir. $t=0$ çözümünü göz ardı edersek $t=-(2+2m)/(1+m^2)$ olup böylece

$$u=1-\frac{2+2m}{1+m^2}=\frac{m^2-2m-1}{1+m^2} \quad v=1-m\frac{2+2m}{1+m^2}=\frac{1-2m-m^2}{1+m^2}$$

elde edilir. $m=-1$ olması $(u,v)=(1,1)$ noktasına karşılık gelir (bunun nedeni, bu noktada teğetinin eğiminin $m=-1$ olmasıdır). Bulunan u ve v değerleri $u^2+4w^2=5$'te yerine yazıldığında

$$4(w(1+m^2))^2=5(1+m^2)^2-(m^2-2m-1)^2=4m^4+4m^3+8m^2-4m+4$$

elde edilir. $r=w(1+m^2)$ olarak alındığında

$$r^2=m^4+m^3+2m^2-m+1$$

olur. Teorem 2.3.3'ten $q=1$ olup dördüncü dereceden eğri

$$y^2-xy+2y=x^3+\frac{7}{4}x^2-4x-7$$

genelleştirilmiş Weierstrass denklemine dönüşür. Sol taraf kareye tamamlandığında $y_1=y+1-\frac{1}{2}x$ olup

$$y_1^2=x^3+2x^2-5x-6$$

eliptik eğrisine dönüşür (Washington 2008).

2.4 İzojeniler

Şimdi eğriler arasındaki dönüşümlerini göz önüne alalım.

Tanım 2.4.1 E_1 ve E_2 eliptik eğriler olsun. E_1'den E_2'ye bir izojeni

$$\phi: E_1 \to E_2, \quad \phi(\mathcal{O})=\mathcal{O}$$

şeklinde bir morfizmdir. $\phi(E_1) \neq \{\mathcal{O}\}$ olmak üzere E_1'den E_2'ye bir izojeni varsa, E_1 ve E_2 eğrileri izojendirler (Silverman 2009).

Eliptik eğriler üzerindeki noktalar kümesi toplama işlemine göre değişmeli gruptur. Dolayısıyla bu gruplar arasındaki dönüşümler grup oluşturur. E_1'den E_2'ye olan izojeniler kümesi

$$Hom(E_1, E_2) = \{E_1 \to E_2 \text{ izojenileri}\}$$

ile gösterilir. İki izojeninin de toplamı

$$(\phi + \psi)(P) = \phi(P) + \psi(P)$$

ile gösterilir ve $\phi + \psi$ bir morfizm olup bir izojenidir. Böylece $Hom(E_1, E_2)$ bir gruptur.

Eğer $E_1 = E_2$ ise de izojeniler oluşturulabilir. Böylece, E bir eliptik eğri ise

$$End(E) = Hom(E, E)$$

yukarıda verilen toplama kuralı ve

$$(\phi\psi)(P) = \phi(\psi(P))$$

çarpma kuralı ile bir halka olur. $End(E)$ halkası, E'nin *endomorfizm halkası* olarak adlandırılır. $End(E)$'nin tersinir elemanları, $Aut(E)$ ile gösterilen E'nin otomorfizm grubunu oluşturur.

Tanım 2.4.2 E bir eliptik eğri ve $m \geq 1$ olmak üzere $m \in \mathbb{Z}$ olsun. E'nin m-torsiyon (büküm) alt grubu $E[m]$ olmak üzere

$$E[m] = \{P \in E : [m]P = \mathcal{O}\}$$

kümesi E'nin m mertebeli noktaların kümesidir.

$$E_{tors} = \cup_{m=1}^{\infty} E[m]$$

sonlu mertebeli noktaların kümesidir. Eğer E, $\mathbb{F}$ cismi üzerinde tanımlı ise $E(\mathbb{F})$'deki sonlu mertebeli noktalar kümesi $E_{tors}(\mathbb{F})$ ile gösterilir (Silverman 2009).

Not 2.4.3 $\mathcal{O}$ noktası aşikar nokta olarak adlandırılır. P büküm noktası değilse *sonsuz mertebeli nokta* olarak adlandırılır (Mollin 2001).

Örnek 2.4.4 $Kar(\mathbb{F}) \neq 2$ ve $i \in \overline{\mathbb{F}}$ 4. dereceden ilkel kök, yani $i^2 = -1$ olsun.

$$E : y^2 = x^3 - x$$

eliptik eğrisi $End(E)$ endomorfizm halkasına sahiptir. Bu eğrinin üzerindeki noktalar arasında

$$[i] : (x, y) \to (-x, iy)$$

ile verilen $[i]$ dönüşüm olduğundan $End(E)$, $\mathbb{Z}$'den kesinlikle büyüktür. Böylece E, karmaşık çarpmaya (complex multiplication) sahiptir. $[i], \mathbb{F}$ cismi üzerinde tanımlı olması için gerek ve yeter şart $i \in \mathbb{F}$ olmasıdır. Dolayısıyla $E, \mathbb{F}$ üzerinde tanımlansa bile $End_{\mathbb{F}}(E)$, $End(E)$'den daha küçük olabilir.

Bu örnekle devam edersek

$$[i]o[i](x, y) = [i](-x, iy) = (x, -y) = -(x, y)$$

olup $[i]o[i] = -1$'dir. Böylece

$$\mathbb{Z}[i] \to End(E), \quad m + ni \mapsto [m] + [n]o[i]$$

bir halka homomorfizmi vardır. Eğer $kar(\mathbb{F}) = 0$ ise bu dönüşüm bir izomorfizm olup

$\mathbb{Z}[i] \cong End(E)$ olur. Bu durumda

$$Aut(E) \cong \mathbb{Z}[i]^* = \{\pm 1, \pm i\}$$

mertebesi 4 olan bir devirli gruptur (Silverman 2009).

Örnek 2.4.5 $Kar(\mathbb{F}) \neq 2, a, b \in \mathbb{F}, b \neq 0$ ve $r = a^2 - 4b \neq 0$ olsun.

$$E_1 : y^2 = x^3 + ax^2 + bx$$
$$E_2 : Y^2 = X^3 - 2aX^2 + rX$$

eliptik eğrilerini göz önüne alalım. Bu eğriler arasında derecesi 2 olan

$$\phi : E_1 \to E_2 \qquad \phi' : E_2 \to E_1$$
$$(x, y) \mapsto \left(\frac{y^2}{x^2}, \frac{y(b - x^2)}{x^2}\right) \qquad (X, Y) \mapsto \left(\frac{Y^2}{4X^2}, \frac{Y(r - X^2)}{8X^2}\right)$$

izojenileri vardır.

Kolay bir hesaplama ile E_1'de $\phi' o \phi = [2]$ ve E_2'de $\phi o \phi' = [2]$ olduğunu görülür (Silverman 2009).

Teorem 2.4.6 (İki ve Üç Mertebeli Noktalar)

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

düzgün bir eğri ve $P(x, y) \neq \mathcal{O} \in C$ olsun.

- P noktasının mertebesi $2 \Leftrightarrow y = 0$ dır.
- P noktasının mertebesi $3 \Leftrightarrow x, \omega(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + 4ac - b^2$ polinomunun bir köküdür.

Örnek 2.4.7 $\mathbb{Q}$ cismi üzerinde

$$y^2 = x^3 + 1$$

eliptik eğrisini ele alalım. $P = (-1, 0), R = (2, -3) \in E(\mathbb{Q})$ olsun.

P noktasının mertebesi, $2P = \mathcal{O}$ olduğundan 2'dir.

R noktasının mertebesi, $2R = (0, -1), 3R = (-1, 0), 4R = (0, 1), 5R = (2, 3)$ yani $5R = -R$ olup böylece $6R = \mathcal{O}$ olduğundan 6'dır.

Eliptik eğriler üzerinde iki ve üç mertebeli noktaların oluşturduğu grubun yapısı aşağıdaki teoremler ile verilmiştir.

Teorem 2.4.8 E, $\mathbb{F}$ cismi üzerinde tanımlı bir eliptik eğri olsun. $Kar(\mathbb{F}) \neq 2$ ise

$$E[2] \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

olup $Kar(\mathbb{F}) = 2$ ise

$$E[2] \cong \mathcal{O} \text{ veya } \mathbb{Z}_2$$

dir (Washington 2008).

Teorem 2.4.9 E, $\mathbb{F}$ cismi üzerinde tanımlı bir eliptik eğri olsun. $Kar(\mathbb{F}) \neq 2$ ise

$$E[3] \cong \mathbb{Z}_3 \times \mathbb{Z}_3$$

dir (Washington 2008).

Daha genel bir durum olarak bir eliptik eğri üzerindeki n mertebeli noktaların oluşturduğu grubun yapısı aşağıda verilmiştir.

Teorem 2.4.10 E, $\mathbb{F}$ cismi üzerinde tanımlı bir eliptik eğri , $n \in \mathbb{N}$ olsun. Eğer $\mathbb{F}$'nin karakteristiği n'yi bölmüyor veya sıfır ise

$$E[n] \cong \mathbb{Z}_n \times \mathbb{Z}_n$$

olup $\mathbb{F}$'nin karakteristiği $p > 0$ ve $p \mid n$ ise $p \nmid m$ olacak şekilde $n = mp^r$ için

$$E[n] \cong \mathbb{Z}_m \times \mathbb{Z}_m \text{ veya } E[n] \cong \mathbb{Z}_n \times \mathbb{Z}_m$$

ile verilir (Washington 2008).

2.5 Bölüm Polinomları

(2.1.2) uzun Weierstrass normal formunda bir E eğrisi verilsin. (2.1.3) ve (2.1.4)'teki b_2, b_4, b_6 ve b_8 değerlerini alalım ($Kar(\mathbb{F}) \neq 2, 3$ ise (2.1.5) basitleştirilmiş Weierstrass normal formunda eğri kullanılabilir).

$\psi_m \in \mathbb{Z}[a_1, \ldots, a_6, x, y]$ bölüm polinomları,

$$\begin{aligned}
&\psi_1 = 1,\\
&\psi_2 = 2y + a_1x + a_3,\\
&\psi_3 = 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8,\\
&\psi_4 = \psi_2(2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + (b_4b_8 - b_6^2)),\\
&\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, \quad m \geq 2,\\
&\psi_2\psi_{2m} = \psi_{m-1}^2\psi_m\psi_{m+2} - \psi_{m-2}\psi_m\psi_{m+1}^2, \quad m \geq 3
\end{aligned} \tag{2.5.1}$$

ile tanımlanır. Her $m \geq 1$ için ϕ_m ve ω_m polinomları

$$\begin{aligned}
\phi_m &= x\psi_m^2 - \psi_{m+1}\psi_{m-1},\\
\omega_m &= (4y)^{-1}(\psi_{m-1}^2\psi_{m+2} + \psi_{m-2}\psi_{m+1}^2)
\end{aligned} \tag{2.5.2}$$

bağıntıları ile verilir.

(2.5.1) ve (2.5.2) polinomları ile $P = (x_0, y_0) \in E$ noktası için

$$mP = \left(\frac{\phi_m(P)}{\psi_m(P)^2}, \frac{\omega_m(P)}{\psi_m(P)^3}\right) \tag{2.5.3}$$

formülü verilir.

2.6 $\mathbb{Q}$ Üzerindeki Eliptik Eğriler

Bu alt bölümde $\mathbb{Q}$'daki eliptik eğriler ile ilgili literatürden iyi bilinen bazı önemli teoremler ifade edilecektir.

Aşağıdaki teorem 1930'larda Nagell ve Lutz tarafından bağımsız olarak ispatlanmıştır. Bu teorem, $\mathbb{Q}$'da tanımlanan bir eliptik eğri üzerindeki büküm noktalarının hızlı bir şekilde belirlenmesini sağlar.

Teorem 2.6.1 (Nagell-Lutz) $E, \mathbb{Q}$ üzerinde (2.1.5) basitleştirilmiş Weierstrass normal formunda bir eğri ve $(x, y) \in E(\mathbb{Q})$ olsun. $P = (x, y) \in E(\mathbb{Q})$ noktası sonlu mertebeli olsun. Bu durumda $x, y \in \mathbb{Z}$'dir ve $y \neq 0$ olması halinde $y^2 | 4A^3 + 27B^2$ olur ($y = 0$ olması halinde P'nin mertebesi 2'dir) (Washington 2008).

Örnek 2.6.2 $\mathbb{Q}$ cismi üzerinde $E : y^2 = x^3 + 4$ eliptik eğrisi olsun. $4A^3 + 27B^2 = 432$ olduğundan $y^2 | 432$ olacak şekilde y değerlerini belirleyelim . $P(x, y), E(\mathbb{Q})$'da sonlu mertebeli bir nokta olsun. $0 = x^3 + 4$ denkleminin rasyonel çözümleri olmadığından $y = 0$ olamaz. O halde $y = \pm 1, \pm 2, \pm 3, \pm 4, \pm 12$ olabilir. Fakat sadece $y = \pm 2$ için x'in rasyonel bir değeri olduğundan eğri üzerindeki sonlu mertebeli noktalar $(0, 2), (0, -2)$ olur. Kolay bir hesaplama ile $3(0, \pm 2) = \mathcal{O}$ olduğu bulunur. Buradan $E(\mathbb{Q})$'nun büküm (torsion) alt grubu 3 mertebeli devirli bir gruptur (Washington 2008).

Teorem 2.6.3 (Mazur) $E, \mathbb{Q}$ üzerinde tanımlı bir eliptik eğri olsun. Bu durum

$$E_{tors}(\mathbb{Q}) \cong \begin{cases} \mathbb{Z}_n, & 1 \leq n \leq 10 \text{ ya da } n = 12 \\ \\ \mathbb{Z}_n \times \mathbb{Z}_n, & 1 \leq n \leq 4 \end{cases}$$

olur (Washington 2008).

Şimdi $\mathbb{Q}$ cismi üzerindeki bir eliptik eğrinin $E(\mathbb{Q})$ grup yapısına örnekler verelim.

Örnek 2.6.4 $\mathbb{Q}$ cismi üzerinde $E : y^2 = x^3 - x$ eliptik eğrisi olmak üzere bu eğri üzerindeki sonlu mertebeli noktaların kümesi $E_{tors}(\mathbb{Q}) = \{\mathcal{O}, (0, 0), (\pm 1, 0)\}$ şeklindedir. Bu

kümenin her bir elemanı $2P = \mathcal{O}$ olduğundan $E_{tors}(\mathbb{Q})$'nun grup yapısı $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$'dir (Kato ve ark. 2000).

Örnek 2.6.5 $\mathbb{Q}$ cismi üzerinde $E : y^2 = x^3 + 1$ eliptik eğrisi ve bu eğri üzerinde $P = (2, 3)$ verilsin. $2P = (0, 1), 3P = (-1, 0), 4P = (0, -1), 5P = (2, -3)$ yani $5P = -P$ olup böylece $6P = \mathcal{O}$ olduğundan P noktasının mertebesi 6'dır. Buradan $E(\mathbb{Q})$'nun grup yapısı

$$E(\mathbb{Q}) \cong \mathbb{Z}/6\mathbb{Z}$$

olarak bulunur (Kato ve ark. 2000).

Örnek 2.6.6 $E : y^2 = x^3 - 4$ eliptik eğrisi ve bu eğri üzerinde $P = (2, 2)$ verilsin. $2P = (5, -11), 3P = (\frac{106}{9}, \frac{1090}{27})$ olup sonlu mertebeli olmadığından $E(\mathbb{Q})$'nun grup yapısı

$$E(\mathbb{Q}) \cong \mathbb{Z}$$

olup serbest bir gruptur (Kato ve ark. 2000).

$\mathbb{Q}$ cismi için $E(\mathbb{Q})$'nun grup yapısıyla ilgili olarak verilenler, herhangi bir $\mathbb{F}$ sayı cismi üzerinde de geçerlidir.

Şimdi eliptik eğriler üzerindeki rasyonel noktaların grubu ile ilgili iki önemli sonucu verelim.

Teorem 2.6.7 (Zayıf-Mordell Weil) $\mathbb{Q}$ cismi üzerinde tanımlı E eliptik eğrisi olsun. O zaman $E(\mathbb{Q})/2E(\mathbb{Q})$ sonludur (Washington 2008).

Teorem 2.6.8 (Mordell-Weil Teoremi) $A, B \in \mathbb{Q}$ olmak üzere E eliptik eğrisi

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

denklemiyle verilsin. $E(\mathbb{Q})$'daki her P noktası için $n_1, \ldots, n_r \in \mathbb{Z}$ iken

$$P = n_1P_1 + \cdots + n_rP_r$$

olacak şekilde $\{P_1, \ldots, P_r\}$ sonlu kümesi vardır. Başka bir ifade ile $E(\mathbb{Q})$ sonlu üreteçli bir abelyan gruptur (Mollin 2001).

Aşağıdaki teorem ise kısa Weierstrass normal formunda eğri üzerindeki tamsayı noktalar kümesinin sonlu olduğunu ifade eder.

Teorem 2.6.9 (Siegel Teoremi) $A, B \in \mathbb{Z}$ ve $\Delta = 4A^3 + 27B^2 \neq 0$ olmak üzere

$$E : y^2 = x^3 + Ax + B \in \mathbb{Z}[x]$$

eliptik eğrisi olsun. E üzerinde sadece sonlu sayıda tamsayı bileşenli $P = (x, y)$ noktası vardır (Mollin 2001).

Şimdi sonlu üreteçli abelyan (değişmeli) grupların yapısı ile ilgili iyi bilinen iki sonucu ifade edelim.

Teorem 2.6.10 $i = 1, 2, \ldots, s-1$ ve $n_i | n_{i+1}$ olmak üzere sonlu değişmeli grup

$$\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s}$$

formundaki bir gruba izomorftur. n_i tamsayıları G grubu tarafından tek bir şekilde belirlenir (Cangül 2016).

G grubunun sonlu bir alt kümesi $g_1, g_2, \ldots, g_k$ ile G'nin her elemanı

$$m_1 g_1 + \cdots + m_k g_k, \qquad (m_i \in \mathbb{Z})$$

formunda yazılabiliyorsa (tek bir şekilde olması gerekmez), *G sonlu üreteçli bir abelyan grup* olarak adlandırılır.

Teorem 2.6.11 Sonlu üreteçli bir abelyan grup $i = 1, 2, \ldots, s-1$ için $n_i | n_{i+1}$ ve $r \geq 0$ olmak üzere

$$\mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s}$$

formundaki bir gruba izomorftur (Fraleigh 2003).

r ve n_i tamsayıları, G tarafından tek bir şekilde belirlenir.

G'nin altgrubu

$$\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s}$$

grubuna izormorftur. Bu grup G'nin *torsiyon (büküm) alt grubu* olarak, r tam sayısı ise G'nin *rankı* olarak adlandırılır.

Mordell-Weil teoremine göre $E, \mathbb{Q}$ üzerinde bir eliptik eğri ise $E(\mathbb{Q})$ sonlu üreteçli bir değişmeli gruptur. Teorem 2.6.10 ve Teorem 2.6.11 ile $\mathbb{Q}$'daki bir eliptik eğrinin Mordell-Weil grubu

$$E[\mathbb{Q}] \cong T \times \mathbb{Z}^r \tag{2.6.1}$$

ile temsil edilir. Burada T torsiyon altgrubu iken, $E(\mathbb{Q})$'nun rankı $r \geq 0$ tam sayısıdır (Washington 2008)

Örnek 2.6.12 E eliptik eğrisi

$$y^2 = x^3 - 4x$$

olsun. $E(\mathbb{Q})/2E(\mathbb{Q}) = \{\mathcal{O}, (0,0), (2,0), (-2,0)\}$'dır. Ayrıca Nagell-Lutz teoremini kullanarak kolay bir hesaplama ile $E(\mathbb{Q})$'nun büküm alt grubu

$$T = E[2]$$

olduğunu gösterir. Teorem 2.6.7'den $E(\mathbb{Q}) \cong T \times \mathbb{Z}^r$ ve böylece

$$E(\mathbb{Q})/2E(\mathbb{Q}) \cong (T/2T) \times \mathbb{Z}_2^r = T \times \mathbb{Z}_2^r$$

olur. Dolayısıyla $E(\mathbb{Q})/2E(\mathbb{Q})$'nun mertebesi 4 olduğundan E'nin rankı sıfırdır (yani $r = 0$). Sonuç olarak

$$E(\mathbb{Q}) = E[2] = \{\mathcal{O}, (0,0), (2,0), (-2,0)\}$$

dır (Washington 2008).

(2.6.1)'daki temsilde sonsuz kısım için bir taban, $E(\mathbb{Q})$'nun tabanı olarak adlandırılır. $\mathbb{Q}$ üzerinde bir E eliptik eğrisinin Mordell-Weil grubu $E(\mathbb{Q})$'yu belirlemek zor bir problemdir. $E(\mathbb{Q})_{tors}$ büküm grubunu hesaplamak zor değildir, ancak sorun $E(\mathbb{Q})$ grubunun serbest $E(\mathbb{Q})_{fr}$ kısmını belirlemektir.

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

olduğunu biliyoruz. Ancak $\mathbb{Q}$ üzerinde bir E eliptik eğrisinin r rankını belirlemek için henüz genel bir yöntem yok. Ayrıca $\mathbb{F}$ cismi üzerindeki E eliptik eğrisinin r tane lineer bağımsız noktasının $P_1, \ldots, P_r$ olduğu biliniyorsa $E(\mathbb{Q})_{fr}$ için bir taban oluşturup oluşturmadıklarına karar vermek de kolay değildir.

İleriki bölümler için gerekli olan Silverman'ın Özelleştirme teoremini verelim:

Teorem 2.6.13 E_t, $\mathbb{Q}(t)$ üzerinde sabit olmayan bir eliptik eğri ise bu durumda sadece sonlu çoklukta $s \in \mathbb{Q}$ için $E_t(\mathbb{Q}(t)) \to E_s(\mathbb{Q})$ homomorfizmi birebirdir. Böylece

$$rank(E_s(\mathbb{Q})) \geq rank(E_t(\mathbb{Q}(t)))$$

olur (Silverman 1994).

2.7 Yükseklik Fonksiyonları ve Lineer Bağımsız Noktalar

Bu alt bölümde bir $\mathbb{F}$ sayı cisminde tanımlı eliptik eğrinin üzerindeki $E(\mathbb{F})$ noktalar kümesinde lineer bağımsız noktaların nasıl bulunacağı ile ilgili teoremi vereceğiz. İlk olarak yükseklik fonksiyonlarını tanımlayacağız ve sonrasında bunlarla ilgili literatürden iyi bilinen bazı sonuçları ifade edeceğiz.

$M_{\mathbb{F}}, \mathbb{F}$'nin değerlemeleri kümesi ve $v \in M_{\mathbb{F}}$ iken n_v, v'deki lokal derece olsun. x sayı cismi elemanı olmak üzere

$$v(x) = -\log |x|_v$$

şeklinde yazılır. Eğer $v, \wp_v$ asal idealine karşılık gelen arşimedyan olmayan bir mutlak değer ise o zaman $\aleph(\wp_v), \wp_v$ idealinin normu iken normalleştirilmiş ayrık toplamsal değerlendirmesi

$$|x|_v = \aleph(\wp_v)^{ord_v(x)/n_v}$$

formülü ile verilir. Burada $\mathbb{F}$'nin ayrık değerlemelerinin kümesi $M_{\mathbb{F}}^0$ ile gösterilir.

Tanım 2.7.1 $\mathbb{F}$ bir cisim olsun.

$a)$ $P = [x_0 : \ldots : x_N] \in \mathbb{P}^N(\mathbb{F}), \mathbb{F}$ cismi üzerinde bir projektif nokta olsun. $v \in M_{\mathbb{F}}$ için P'nin v'deki lokal $\mathbb{F}$-yüksekliği

$$H_{\mathbb{F},v}(P) = \max\{|x_0|_v, \ldots, |x_N|_v\}$$

dir. P'nin global $\mathbb{F}$-yüksekliği

$$H_{\mathbb{F}}(P) = \prod_{v \in M_{\mathbb{F}}} H_{\mathbb{F},v}(P)^{n_v}$$

ile verilir. P'nin global mutlak yüksekliği

$$H(P) = H_{\mathbb{F}}(P)^{1/[\mathbb{F}:\mathbb{Q}]}$$

ile verilir.

$b)$ Eğer $x \in \mathbb{F}$ ise $v \in M_{\mathbb{F}}$'de x'in lokal $\mathbb{F}$-yüksekliği

$$H_{\mathbb{F},v}(x) = H_{\mathbb{F},v}([1 : x]) = \max\{1, |x|_v\}$$

x'in global $\mathbb{F}$-yüksekliği

$$H_{\mathbb{F}}(x) = \prod_{v \in M_{\mathbb{F}}} H_{\mathbb{F},v}(x)^{n_v}$$

olup x'in global mutlak yüksekliği

$$H(x) = H_{\mathbb{F}}(x)^{1/[\mathbb{F}:\mathbb{Q}]}$$

şeklindedir.

c) $x \in \mathbb{F}$ olsun. $v \in M_{\mathbb{F}}$ için x'in v noktasındaki sıradan logaritmik lokal $\mathbb{F}$-yüksekliği

$$h_{\mathbb{F},v}(x) = -\min\{0, v(x)\} = \log H_{\mathbb{F},v}(x)$$

olur. x'in (global) mutlak ya da sıradan logaritmik yüksekliği

$$h(x) = \frac{1}{[\mathbb{F}:\mathbb{Q}]} \sum_{v \in M_{\mathbb{F}}} n_v h_{\mathbb{F},v}(x)$$

olup x'in sonsuzdaki (global) mutlak ya da sıradan logaritmik yüksekliği

$$h_{\infty}(x) = \frac{1}{[\mathbb{F}:\mathbb{Q}]} \sum_{v \in M_{\mathbb{F}}^{\infty}} n_v h_{\mathbb{F},v}(x)$$

ile verilir (Schmitt ve Zimmer 2003).

Tanım 2.7.2 $E/\mathbb{F}$ (2.1.2) formunda bir eliptik eğri, $P = (x, y) \in E(\mathbb{F})$ ve $v \in M_{\mathbb{F}}$ olsun. O zaman v'de P'nin sıradan logaritmik lokal yüksekliği

$$h_v(P) = -\frac{1}{2}\min\{0, v(x)\} = \frac{1}{2}\log(H_{\mathbb{F},v}(x)) = \frac{1}{2}h_{\mathbb{F},v}(x)$$

şeklindedir (Schmitt ve Zimmer 2003).

Tanım 2.7.3 $E/\mathbb{F}$ (2.1.2) formunda bir eliptik eğri ve $P = (x, y) \in E(\mathbb{F})$ olsun. P'nin *sıradan (logaritmik) lokal yüksekliği*

$$h(P) = \log(H(x)) = \frac{1}{[\mathbb{F}:\mathbb{Q}]} \sum_{v \in M_{\mathbb{F}}^{\infty}} n_v h_v(P)$$

olup $h(\mathcal{O}) = 0$ dır (Schmitt ve Zimmer 2003).

Tanım 2.7.4 (global) Néron-Tate $\hat{h}(P)$ yüksekliği (ya da kanuni yükseklik)

$$\hat{h}(P) = \lim_{n\to\infty} \frac{h(2^n P)}{2^{2n}}$$

ile verilir (Schmitt ve Zimmer 2003).

Uyarı 2.7.5 Herhangi $m \in \mathbb{N}, m \geq 2$ için kanuni yükseklik

$$\hat{h}(P) = \lim_{n\to\infty} \frac{h(m^n P)}{m^{2n}}$$

ile de tanımlanabilir (Schmitt ve Zimmer 2003).

Önerme 2.7.6 Bir $E/\mathbb{F}$ bir eliptik eğrisi için aşağıdaki özellikler sağlanır:

$a)$ $P, Q \in E$ olsun. Bu durumda

$$\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q)$$

dir.

$b)$ Her $P \in E$ ve $m \in \mathbb{Z}$ için $\hat{h}(mP) = m^2\hat{h}(P)$'dir.

$c)$ $P \in E$ olsun. Bu durumda $\hat{h}(P) \geq 0$ ve

$$h(P) = 0 \quad \Leftrightarrow \quad P \in E(\overline{\mathbb{F}})_{tors}$$

olur.

$d)$ $\hat{h}$, ikinci dereceden formdur, yani $\hat{h}$ çift ve

$$<,>: E(\overline{\mathbb{F}}) \times E(\overline{\mathbb{F}}) \to \mathbb{R}$$

$$< P, Q >= \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)$$

eşleştirmesi (pairing) simetrik ve bilineerdir. Bu eşleşme *Néron-Tate eşleşmesi* olarak adlandırılır.
(Bazen sağ tarafın önüne $1/2$ çarpanı yerleştirilir. Bunun avantajı ise $\hat{h}(P) =< P, P >$ olmasıdır)(Schmitt ve Zimmer 2003).

Kanuni yükseklik bu lokal yükseklik fonksiyonlarının toplamı olarak ifade edilebilir.

Teorem 2.7.7 $E/\mathbb{F}$ bir eliptik eğri olsun. $v \in M_{\mathbb{F}}$ için $\hat{h}_v$ local yükseklik fonksiyonu olsun. O halde $P \in E(\mathbb{F})$ için kanuni yükseklik

$$\hat{h}(P) = \frac{1}{[\mathbb{F} : \mathbb{Q}]} \sum_{v \in M_{\mathbb{F}}} n_v \hat{h}_v(P)$$

şeklindedir (Schmitt ve Zimmer 2003).

Tanım 2.7.8 $E/\mathbb{F}$ bir eliptik eğri olsun.
$a)$ $n > 0$ olmak üzere $P_1, \ldots, P_n \in E(\mathbb{F})$ noktalarının regülatörü

$$R_{P_1,\ldots,P_n} = det(< P_i, P_j >)_{1 \leq i,j \leq n}$$

ile verilir.
$b)$ $\{P_1, \ldots, P_n\}$, $E(\mathbb{F})$'nin bir bazı olsun. $E(\mathbb{F})$'nin regülatörü $r > 0$ ($E/\mathbb{F}$'nin rankı) $P_1, \ldots, P_n \in E(\mathbb{F})$ noktalarının regülatörü ise

$$R_{E/\mathbb{F}} = R_{P_1,\ldots,P_r}$$

olur. $E/\mathbb{F}$'nin regülatör matrisi $det(\Re_{E/\mathbb{F}}) = R_{E/\mathbb{F}}$ olmak üzere

$$\Re_{E/\mathbb{F}} = (\langle P_i, P_j \rangle)_{1 \leq i,j \leq r}$$

matrisidir. Eğer $r = 0$ ise $R_{E/\mathbb{F}} = 1$'dir (Schmitt ve Zimmer 2003).

Yükseklik fonksiyonları ile ilgili gerekli hazırlıkları tamamladıktan sonra $E/\mathbb{F}$ üzerindeki lineer bağımsız noktaların nasıl bulunacağını ifade eden aşağıdaki teoremi ifade

edelim. Bu teorem ileriki bölümlerde kullanılacaktır.

Teorem 2.7.9 $E/\mathbb{F}$ bir eliptik eğri olsun.

$a)$ $n > 0$ olmak üzere $E(\mathbb{F})$'deki noktalarının bir kümesi $\{P_1, \ldots, P_n\}$ olsun. Bu noktaların regülatörünün $R_{P_1,\ldots,P_n} = 0$ eşitliğini sağlaması için gerek ve yeter şart $P_1, \ldots, P_n$ noktalarının lineer bağımsız olmasıdır.

$b)$ $E(\mathbb{F})$'deki lineer bağımsız noktaların maksimal kümesi $\{P_1, \ldots, P_r\}$, yani $r = rank(E(\mathbb{F})) > 0$ olsun. O zaman $P_1, \ldots, P_r$ noktaları ya $E(\mathbb{F})$'nin bir tabanıdır ya da $R_{E/\mathbb{F}}$, $E/\mathbb{F}$'nin regülatörü iken üzere

$$R_{P_1,\ldots,P_r} = m^2 R_{E/\mathbb{F}}$$

olacak şekilde bir $m \geq 2, (m \in \mathbb{N})$ tamsayısı vardır (Schmitt ve Zimmer 2003).

3. ELİPTİK EĞRİLERİN FARKLI MODELLERİ

3.1 Edwards Eğrileri

2007 yılında, Harold Edwards (2007) "Eliptik eğriler için normal form" isimli makalesi ile eliptik eğrilerin farklı bir modeli olan "Edwards eğrilerini" literatüre kazandırdı. Eliptik fonksiyonlar (eğriler) Euler zamanından beri çalışılır. Bu yeni eğri üzerinde grup işlemi kuralları tanımlamak için Abel, Euler ve Gauss tarafından verilen eliptik fonksiyon (eğri) tanımını kullandı. Günümüzde eliptik eğri kübik bir eğri olarak göz önüne alınır ve eğriyi kesen bir doğru üzerindeki üç nokta yardımıyla da bu eğri üzerindeki noktaların grup toplama işlemi kuralları belirlenir. Bu kurallar iyi bilinir ve yaygın bir şekilde öğretilir. Bu grup kuralları ile Euler'in "Cebirsel integrasyonu" (Euler de Abel'den ilham almıştır) arasında bağlantı birbirinden uzaktır. Ama aslında aynı kavramların farklı ifadeleridir.

Abel tarafından geliştirilen olguya başka bir yaklaşım, yine Abel tarafından grup yapısının bir genellemesi olarak tasarlanmıştı. Burada fikir şuydu: Kübik eğriyi doğru ile kesiştirmek yerine keyfi bir eğriyi yardımcı eğrilerin keyfi bir ailesi ile kesiştirmek. Yardımcı eğrinin denklemindeki parametreler değiştiğinde verilen eğri ile kesişim noktaları da değişir. Abel, uygun koşullar altında, N tane kesişim noktasının $N - g$ serbest dereceleriyle bu yolda hareket ettiğini keşfetti. Burada g (eğrinin cinsi), N'ye veya kullanılan yardımcı eğri ailesine değil yalnızca verilen keyfi bir eğriye bağlıdır. Eğri düzgün kübik bir eğri ve yardımcı eğriler doğrular olduğunda $N = 3$ tane kesişim noktası vardır ve bu noktalar $N - g = 2$ serbest derece ile hareket eder. Böylece $g = 1$'dir. Edwards yaptığı çalışma ile Abel'in yaklaşımını içeren olguya yeni bir bakış açısı sundu.

Euler eliptik fonksiyonlar teorisinde

$$x^2 + y^2 + x^2y^2 = 1$$

eliptik eğrisinin özel bir durumu için bir "toplama formülü" önermişti. Bu formül sonra-

sında Gauss tarafından aşağıdaki şekilde ifade edildi:

$$S = \frac{s_1c_2 + s_2c_1}{1 - s_1s_2c_1c_2}, \quad C = \frac{c_1c_2 - s_1s_2}{1 + s_1s_2c_1c_2}. \tag{3.1.1}$$

Gauss'un harf seçiminde s ve c harflerini kullanması, sinüs ve kosinüs için toplama formülleri ile benzer bir formül ortaya koyar (Paylar sinüs ve kosinüsün toplam formülündeki ifadeleridir). Aslında Gauss, $s(t)$ ve $c(t)$ transandantal fonksiyonları ile (3.1.1)'i şöyle ifade eder:

$(S, C) = (s(t + t'), c(t + t')), (s, c) = (s(t), c(t)), (s', c') = (s(t'), c(t'))$ iken $s(t)$'nin tanımı $t = \int_0^{\sin t} \frac{dx}{\sqrt{1-x^2}}$'ye benzer olarak $t = \int_0^{s(t)} \frac{dx}{\sqrt{1-x^4}}$ ile $c(t)$'nin tanımı ise $\cos t = \sqrt{1 - (\sin t)^2}$ $(\cos 0 = 1)$ ifadesine benzer olarak $c(t) = \sqrt{\frac{1-s(t)^2}{1+s(t)^2}}$ $(c(0) = 1)$ ile verilir.

Bu dikkat çekici Euler-Gauss formülleri sadece $s^2+c^2+s^2c^2 = 1$ eğrisine uygulanabilir. Ancak bunlar keyfi bir eliptik eğrisinin grup toplama kuralını ifade eden bir formülün özel bir durumudur. Edwards'ın makalesinde bu eğri

$$x^2 + y^2 = a^2(1 + x^2y^2) \tag{3.1.2}$$

ile, toplama kuralı ise eğer a sıfırdan farklı bir sabit ve $a^5 \neq a$ iken

$$X = \frac{x_1y_2 + x_2y_1}{a(1 + x_1x_2y_1y_2)}, \quad Y = \frac{y_1y_2 - x_1x_2}{a(1 - x_1x_2y_1y_2)} \tag{3.1.3}$$

bağıntıları ile verilir.

(Burada (3.1.2) formülü $a = \sqrt{i}, x = s\sqrt{i}$ ve $y = c\sqrt{i}$ durumudur.) Aslında (3.1.2) denkleminin eliptik eğri olması için $a \neq a^5$ olmalıdır. Abel'in çalışmasına göre f, farklı köklere sahip 3 veya 4 dereceli bir polinom olmak üzere bir eliptik eğri $z^2 = f(x)$ biçimindedir (g cinsi 1'dir, burada $f, 2g-1$ veya $2g-2$ dereceli bir polinom). $z = (1-a^2x^2)$ olarak alınırsa (3.1.2) denklemi $z^2 = (a^2 - x^2)(1 - a^2x^2)$ biçiminde olur. Polinomun sağ tarafı 4. derecedendir. Bu nedenle $(a^2 - x^2)(1 - a^2x^2) = a^2x^4 - (a^4 + 1)x^2 + a^2$ polinomunun farklı köklere sahip olması koşuluyla bir eliptik eğri tanımlaması için gerek

ve yeter şart diskriminantının

$$\Delta = (a^4 + 1)^2 - 4a^4 = (a^4 - 1)^2$$

sıfırdan farklı olmasıdır. Dolayısıyla, $(a^4 - 1)^2$ sıfırdan farklı olmalıdır veya eşdeğer şekilde ifade edilen $a^5 \neq a$ olmalıdır.
Harold M. Edwards'tan sonra, Bernstein ve Lange (2007) tarafından (3.1.2) eğrisinin daha genel bir hali göz önüne alındı ve aşağıdaki tanım verildi.

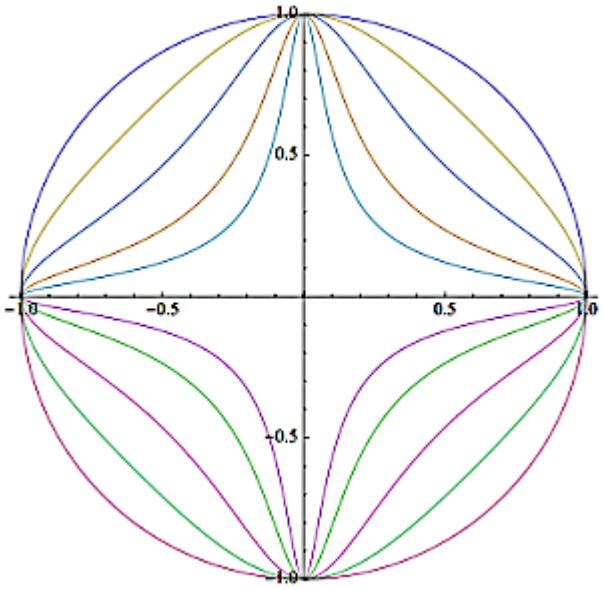
Tanım 3.1.1 $\mathbb{F}$ bir cisim ve $kar(\mathbb{F}) \neq 2$ olmak üzere

$$E_d : x^2 + y^2 = 1 + dx^2y^2 \qquad d \in \mathbb{F}\backslash\{0, 1\} \tag{3.1.4}$$

tipindeki eğriye *Edwards eğrisi* denir. $c, d \in \mathbb{F}$ ve $cd(1 - c^4d) \neq 0$ olmak üzere

$$x^2 + y^2 = c^2(1 + dx^2y^2)$$

formundaki eğri de *Edwards eğrisi* olarak adlandırılır.



Şekil 3.1.1. $d = 0, -2, -10, -50, -200$ için Edwards eğrileri

d değişkenini 0 alırsak (3.1.4) birim çembere karşılık gelen d değişkeni negatif yönde

arttığında eğri bir Denizyıldızı gibi görünür .

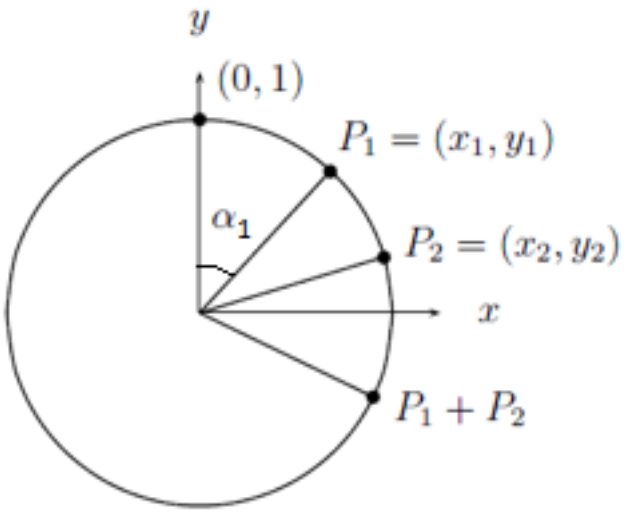
Uyarı 3.1.2 Tanım 3.1.1'deki Edwards eğrileri için verilen iki form birbirine izomorftur. Eğer $d = \bar{d}\bar{c}^4$ ise $\bar{x} = \bar{c}x$ ve $\bar{y} = \bar{c}y$ tanımlanırsa $x^2 + y^2 = 1 + dx^2y^2$ ve $\bar{x}^2 + \bar{y}^2 = \bar{c}^2(1 + \bar{d}\bar{x}^2\bar{y}^2)$ formundaki eğrilerin birbirine izomorf olduğu açıkça görülür.

3.2 Edwards Eğrileri Üzerinde Grup Toplam Kuralı

Edwards eğrileri üzerinde toplama kuralı da tanımlanabilir, ancak bu Weierstrass eğrileri kuralından farklıdır. Bu toplama kuralı aynı zamanda geometrik olarak da yorumlanabilir. Bunu yapmak için, Şekil 3.2.1.'deki birim çemberi göz önüne alınsın ve bu çember üzerinde bir saat varmış gibi açılar eklensin. Öyleyse, birim elemanı $(0, 1)$ olur (genellikle birim çember üzerinde, $(1, 0)$ ile başlanır). Bu nedenle $x_1 = \sin(\alpha_1), y_1 = \cos(\alpha_1)$ ve $x_2 = \sin(\alpha_2), y_2 = \cos(\alpha_2)$ alalım. Bir çember üzerine düzenli açıların eklenmesiyle, şu sonuç alınır:

$$\begin{aligned} x_3 &= \sin(\alpha_1 + \alpha_2) \\ &= \sin(\alpha_1)cos(\alpha_2) + \cos(\alpha_1)sin(\alpha_2) \\ &= x_1y_2 + x_2y_1 \\ y_3 &= \cos(\alpha_1 + \alpha_2) \\ &= \cos(\alpha_1)\cos(\alpha_2) + \sin(\alpha_1)\sin(\alpha_2) \\ &= y_1y_2 - x_1x_2 \end{aligned}$$

Bu bir grup tanımlar ve *saat grup* olarak adlandırılır. Ancak birim çember eliptik bir eğri değildir. Bu nedenle, dx^2y^2 terimi eklenir. Böylece bir eliptik eğri elde edilir.



Şekil 3.2.1. $P_1 + P_2 = P_3$

Yukarıda ifade edildiği gibi, $dx_1x_2y_1y_2 \neq \pm 1$ olduğunda, Edwards eğrileriyle ilgili grup toplama kuralı aşağıda verilir:

Tanım 3.2.1 (Grup Toplam Kuralı) (3.1.4) ile verilen E_d Edwards eğrisini alalım. $P_0 = (x_0, y_0) \in E_d$ ise o zaman $-P_0 = (-x_0, y_0)$ olur. $i = 1, 2, 3$ için $P_i = (x_i, y_i) \in E_d$ iken $P_1 + P_2 = P_3$ olsun. O zaman

$$(x_1, y_1) + (x_2 + y_2) = (x_3, y_3) = \left(\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right)$$

olur. Burada $(0, 1)$ noktası birim elemandır ve $-(x_1, y_1) = (-x_1, y_1)$ olup birim elemandan farklıdır. Edwards eğrisi üzerindeki bir noktanın iki katı

$$2(x_1, y_1) = \left(\frac{2x_1y_1}{1 + dx_1^2y_1^2}, \frac{y_1^2 - x_1^2}{1 - dx_1^2y_1^2} \right)$$

şeklinde verilir (Bernstein ve Lange 2007).

Bu toplama kuralının gerçekten bir grup kuralı tanımladığını görmek için, herhangi iki noktanın toplamının, Edwards eğrisi üzerinde bir nokta olup olmadığı kontrol etmek yeterlidir.

Teorem 3.2.2 $\mathbb{F}$ bir cisim, $kar(\mathbb{F}) \neq 2$ ve $d \in \mathbb{F}\backslash\{0,1\}$ olsun. $x_1, y_1, x_2, y_2 \in \mathbb{F}$ olmak üzere $x_1^2+y_1^2 = 1+dx_1^2y_1^2$ ve $x_2^2+y_2^2 = 1+dx_2^2y_2^2$ eğrilerini alalım. $dx_1x_2y_1y_2 \neq \{-1,1\}$ olduğunu varsayalım. $x_3 = \dfrac{x_1y_2+x_2y_1}{1+dx_1x_2y_1y_2}, y_3 = \dfrac{y_1y_2-x_1x_2}{1-dx_1x_2y_1y_2}$ tanımlayalım. O zaman $x_3^2+y_3^2 = 1+dx_3^2y_3^2$ olur (Bernstein ve Lange 2007).

Söylendiği gibi grup toplamı $dx_1x_2y_1y_2 \neq \{-1,1\}$ olduğunda tamamlanır. Sonraki teoremde belirtildiği gibi, d'nin $\mathbb{F}$ cisminde bir kare olmadığı durumdur:

Teorem 3.2.3 $Kar(\mathbb{F}) \neq 2$ ve E_d (3.1.4) formunda Edwards eğrisi olsun. Varsayalım d, $\mathbb{F}$'de kare olmasın. $x_1, y_1, x_2, y_2 \in \mathbb{F}$ olmak üzere $x_1^2 + y_1^2 = 1 + dx_1^2y_1^2$ ve $x_2^2 + y_2^2 = 1 + dx_2^2y_2^2$ eşitlikleri sağlanacak şekilde seçilsin. Bu durumda $dx_1x_2y_1y_2 \neq \{-1,1\}$'dir (Bernstein ve Lange 2007).

Sonuç 3.2.4 Edwards eğrisi üzerindeki noktalar Tanım 3.2.1 grup toplam kuralı ile birlikte d, $\mathbb{F}$'de bir kare olmadığında bir değişmeli gruptur.

Teorem 3.2.5 $Kar(\mathbb{F}) \neq 2$ iken E eliptik eğrisi $\mathbb{F}$ cismi üzerinde tanımlı olsun. Eğri üzerinde en az bir tane 4. mertebeden nokta olsun. Bu durumda E eliptik eğrisi ya $\mathbb{F}$ üzerinde ya da $\mathbb{F}$'nin uygun bir cisim genişlemesi üzerinde tanımlı bir Edwards eğrisine dönüştürülebilir (Edwards 2007).

3.3 Dört Özel Nokta

Bir Edwards eğrisinin denklemi göz önüne alındığında eğer bir (x, y) çözümü varsa, $(\pm x, \pm y)$ ve $(\pm y, \pm x)$ de çözümler olacaktır. (3.1.4) eğrisinin dört çözümü

$$(0,1), (0,-1), (1,0) \text{ ve } (-1,0) \tag{3.3.1}$$

kolaylıkla bulunur. Bu dört nokta ile

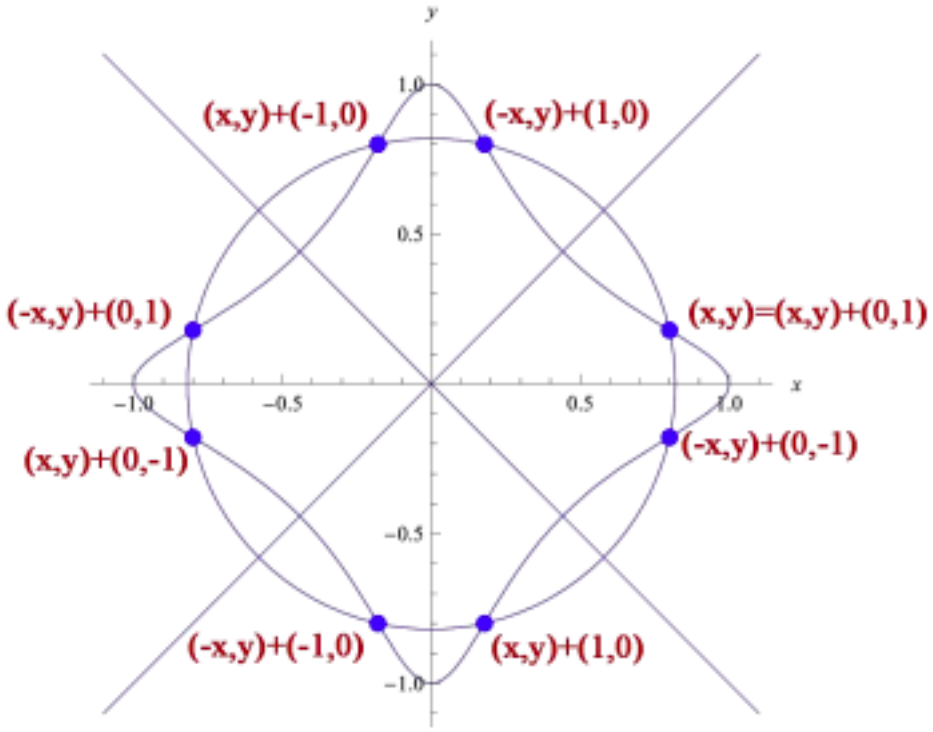
$$S : P \longmapsto \pm P + Q,\ Q \in \{(0,1), (0,-1), (1,0), (-1,0)\}$$

ile verilen D_4 otomorfizmlerinin bir grubu oluşturulabilir.

Bu grup $(0,0)$ ve Q noktalarından geçen doğrulara ayrıca $y = x$ ve $x = -y$ doğrularına göre yansımalarında ve $0 \leq k < 4$ için $\frac{k\pi}{2}$ radyanlık dönmelerden oluşur. Böylece D_4, 8 elemandan oluşur.

S dönüşümü altında D_4'ün elemanları aşağıdaki gibidir:

- $(x,y) + (0,1) = (x,y)$ ve $(-x,y) + (0,1) = (-x,y)$
- $(x,y) + (0,-1) = (-x,-y)$ ve $(-x,y) + (0,-1) = (x,-y)$
- $(x,y) + (1,0) = (y,-x)$ ve $(-x,y) + (1,0) = (y,x)$
- $(x,y) + (-1,0) = (-y,x)$ ve $(-x,y) + (-1,0) = (-y,-x)$.



Şekil 3.3.1 $d = -16$ için Edwards eğrisi üzerindeki sekiz nokta (x,y)'nin y ve x-eksenine göre ve $y = x$ ve $y = -x$ doğrularına göre yansımalarından ve (x,y)'nin $0 \leq k < 4$ için $\frac{k\pi}{2}$ radyanlık dönmesinden elde edilmiştir.

Önceki bölümde $(0,1)$ noktasının birim eleman olduğu söylenmişti. Bununla birlikte, Q'nun dört noktasından herhangi biri birim eleman olarak seçilebilir. Eğri üzerindeki

her noktaya yeni birim elemanı ekleyerek, toplama kuralı biraz değişecektir ancak eğri üzerindeki noktalar yine bir değişmeli grup oluşturur. Özellikle

$$\{(0,1),(0,-1),(1,0),(-1,0)\} \subset \{E_d(\mathbb{Q})\}$$

kümesi 4. mertebeden devirli bir grup oluşturur, grubun üreteci $(-1,0)$ veya $(1,0)$ dir.

$(1,0)$ noktası için

$$2(1,0) = (1,0) + (1,0) = (0,-1)$$
$$3(1,0) = (1,0) + (0,-1) = (-1,0)$$
$$4(1,0) = (1,0) + (-1,0) = (0,1)$$
$$5(1,0) = (1,0) + (0,1) = (1,0)$$

şeklindedir. $(-1,0)$ için de aynı şekilde gösterilir .

Sonuç olarak, bir Edwards eğrisinin 4. mertebeden noktalara sahip olduğu gösterilmiştir. Bu ise bir Edwards eğrisi üzerindeki noktaları bir Weierstrass eğrisi üzerindeki noktalara (veya tersi) eşleyen bir dönüşüm oluşturmak için temel anahtardır (Dam 2012).

3.4 Bükülmüş (Twisted) Edwards Eğrileri

Bu bölümde yine literatürden iyi bilinen (3.1.4) formundaki Edwards eğrisinin daha geneli olan bükülmüş Edwards eğrisi hakkında bazı bilgiler verilir. Edwards eğrisi üzerinde 4. mertebeden noktaların varlığı Edwards eğrisi formundaki eliptik eğrilerin sayısını kısıtlar. Bu nedenle bükülmüş Edwards eğrileri tanımlanarak Edwards eğrileri kümesi daha büyük eliptik eğri ailesi içine dahil edilir. Edwards eğrileri kriptografide önemli bir uygulama alanına sahiptir. Ayrıca bükülmüş Edwards eğrilerinin kriptografik uygulamaları hesaplamalar açısından daha hızlı olduğundan Edwards eğrilerine göre daha avantajlıdır. 2008'de Bernstein ve ark. (2008) tarafından bükülmüş Edwards eğrileri aşağıdaki gibi tanımlanır.

Tanım 3.4.1 $Kar(\mathbb{F}) \neq 2$ ve $a, d \in \mathbb{F}\backslash\{0\}$ olsun. Bu durumda

$$E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2 \tag{3.4.1}$$

tipindeki eğri *bükülmüş Edwards eğrisi* olarak adlandırılır (Bernstein ve ark. 2008).

Uyarı 3.4.2 $a = 1$ olması halinde klasik Edwards eğrisi elde edilir.

Teorem 3.4.3 $E_{a,d}$ bükülmüş Edwards eğrisi üzerindeki nokta toplamı her $(x_1, y_1), (x_2, y_2)$ $\in E_{a,d}(\mathbb{F})$ için

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2} \right)$$

ile verilir. Birim eleman $(0, 1)$ ve (x_1, y_1)'in tersi $(-x_1, y_1)$'dir (Bernstein ve ark. 2008).

Tanım 3.4.4 $\mathbb{F}$ bir cisim $a, b \in \mathbb{F}$ ve $b(a^2 - 4) \neq 0$ eşitsizliği sağlanıyorken

$$M_{a,b} : by^2 = x^3 + ax^2 + x$$

eğrisi *Montgomery eğrisi* olarak adlandırılır ki bir eliptik eğriye dönüştürülebilir. Tersi de doğrudur (Montgomery 1987).

Teorem 3.4.5 Her bir Twisted Edwards eğrisi Montgomery formundaki bir eliptik eğriye dönüştürülebilir. Tersi de doğrudur (Bernstein ve ark. 2008).

3.5 Edwards Eğrisinden Weierstrass Formundaki Eğriye Dönüşüm

Bu bölümün amacı bir Edwards eğrisine karşılık gelen Weierstrass eğrisini bulmaktır. Bunu yapmak için Cassels (1991)'de 8.bölümde ifade edilen yöntem kullanılır.

$$E_d : x^2 + y^2 = 1 + dx^2y^2 \tag{3.5.1}$$

Edwards eğrisini

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

şeklinde düzenleyelim. Eşitliğin her iki tarafı (dx^2-1) ile çarpılırsa

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

elde edilir. Burada $z = (dx^2-1)y$ dönüşümü yapıldığında

$$z^2 = dx^4 - (d+1)x^2 + 1$$

elde edilir. Şimdi $n = \frac{1}{x}$ ve $m = \frac{z}{x^2}$ olsun (bunun rasyonel bir dönüşüm olduğuna dikkat edin). O halde

$$\begin{aligned} m^2 &= n^4 - (d+1)n^2 + d \\ &= \left(n^2 - \frac{d+1}{2}\right)^2 + d - \left(\frac{d+1}{2}\right)^2 \\ &= P(n)^2 + R(n) \end{aligned}$$

elde edilir. Burada $P(n) = n^2 - \frac{d+1}{2}$ ve $R(n) = d - (\frac{d+1}{2})^2$ şeklindedir. Şimdi eğrinin denklemi

$$(m + P(n))(m - P(n)) = R(n)$$

olur. Burada $m + P(n) = \beta$ olarak alınırsa

$$\begin{aligned} m - P(n) &= \frac{R(n)}{\beta} \\ 2P(n) &= \beta - \frac{R(n)}{\beta} \end{aligned}$$

elde edilir. Eşitliği β^2 ile çarpıp $\beta n = \alpha$ yazıldığında

$$2\alpha^2 = \beta^3 + (d+1)\beta^2 - \left(d - \left(\frac{d+1}{2}\right)^2\right)\beta$$

elde edilir ve bu neredeyse Weierstrass formundadır. Her iki taraf 8 ile çarpıldığında $2\alpha^2$ terimi kaybolur ve dolayısıyla

$$16\alpha^2 = 8\beta^3 + 8(d+1)\beta^2 - 8\left(d - \left(\frac{d+1}{2}\right)^2\right)\beta$$

$$(4\alpha)^2 = (2\beta)^3 + 2(d+1)(2\beta)^2 - (4d - (d+1)^2)(2\beta)$$

elde edilir. Burada $(v, w) = (2\beta, 4\alpha)$ verdiliğinde

$$E : w^2 = v^3 + 2(d+1)v^2 + (d-1)^2 v \tag{3.5.2}$$

Weierstrass formundaki eğri elde edilir (Dam 2012).

Şimdi Edwards eğrisine karşılık gelen (3.5.2) Weierstrass eğrisinin, Legendre formundaki bir eliptik eğri ile ilişkili olduğu gösterilecektir. Bunun için Silverman ve Tate (1992) sayfa 79'da tanımlanan Önermedeki homomorfizmi kullanalım.
$a' = -2a = -4(d+1)$ ve $b' = a^2 - 4b = 4(d+1)^2 - 4(d-1)^2$ olmak üzere E ile $E' : w^2 = v^3 + a'v^2 + b'v$ arasında bir homomorfizm vardır. Böylece

$$E' : w^2 = v^3 - 4(1+d)v^2 + (4(d+1)^2 - 4(d-1)^2)v \tag{3.5.3}$$

elde edilir. E''nün birim elemanı $\mathcal{O}'$ olmak üzere, bu homomorfizm, E''deki $\mathcal{O}$ ve $(0,0)$ noktalarını E''ündeki $\mathcal{O}'$ noktasına resmeder. E''ündeki diğer elemanlar $E' \backslash \mathcal{O}'$ ile eşleştirilir. (3.5.3)'deki eşitliğin sağ tarafı çarpanlarına ayrılırsa

$$E' : w^2 = v(v-4)(v-4d)$$

elde edilir. Her iki taraf 64 ile bölündüğünde

$$\left(\frac{w}{8}\right)^2 = \frac{v}{4}\left(\frac{v}{4} - 1\right)\left(\frac{v}{4} - d\right)$$

olur. Burada $w' = \frac{w}{8}$ ve $v' = \frac{v}{4}$ olarak değiştirildiğinde

$$E'_d : w'^2 = v'(v'-1)(v'-d) \tag{3.5.4}$$

Legendre tipinde eliptik eğri elde edilir. Özetlemek gerekirse, (3.5.1) formundaki Edwards eğrisi, (3.5.2) ve (3.5.4) formlarındaki Weierstrass eğrilerine birasyonel denktir.

Uyarı 3.5.1 (3.5.4) eliptik eğrisinin diskriminantı $\Delta = 16(1-2d+d^2)(d-2d^2+d^3)$'tür. $\Delta = 0 \Leftrightarrow d = 0$ veya $d = 1$ dir. Bu durumda birim çember elde edilir; birim çember ise eliptik eğri değildir. Ancak Tanım 3.1.1 kullanılarak ve $Kar(\mathbb{F}) \neq 2$ olmak üzere $\mathbb{F}$ cismi üzerinde bir Edwards eğrisinin $d \in \mathbb{F}\backslash\{0,1\}$ iken bir eliptik eğriye karşılık geldiği açıktır.

Edwards eğrisinin karşılık geldiği Weierstrass eğrisi aşağıdaki dönüşümler yardımıyla verilir:

$$(x,y) \mapsto (x,z) = (x,(dx^2-1)y)$$
$$(x,z) \mapsto (n,m) = (1/x, z/x^2)$$
$$(n,m) \mapsto (n,\beta) = (n, m+n^2-(d+1)/2)$$
$$(n,\beta) \mapsto (\beta,\alpha) = (\beta, n\beta)$$
$$(\beta,\alpha) \mapsto (v,w) = (2\beta, 4\alpha)$$

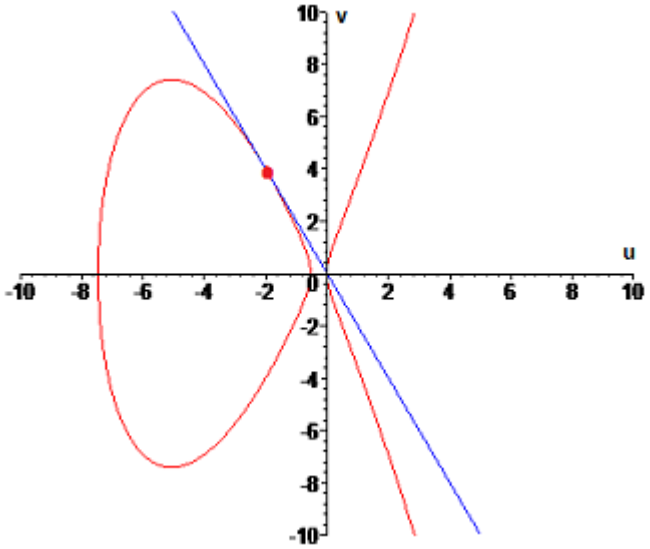
Edwards eğrisi üzerindeki her (x,y) için

$$(x,y) \to (x,y) + (0,-1) = (-x,-y)$$

dönüşümü kullanılır. Bu, eğrinin birim elemanının diğer eğrinin birim elemanı ile düzgün bir şekilde eşleştirildiğinden emin olmak için yapılmalıdır. Son durumda Edwards eğrisi ile bu eğrinin Weierstrass formu arasındaki geçişler aşağıdaki dönüşümler yardımıyla yapılır:

$$(x,y) \mapsto (v,w) = \left(\frac{A}{x^2}, \frac{-2A}{x^3}\right), \quad A = 2y - (2dy + d + 1)x^2 + 2$$
$$(v,w) \mapsto (x,y) = \left(-\frac{2v}{w}, \frac{w^2 - (2+2d)v^2 - 2v^3}{4dv^2 - w^2}\right)$$

Örnek 3.5.2 Bir Edwards eğrisi üzerindeki $(x,y) = (-1,0)$ noktası (3.5.2) eğrisi üzerindeki $(v,w) = (1-d, 2(d-1))$ noktasına dönüşür. $d = 3$ seçilirse $(v,w) = (-2,4)$ olup $w^2 = v^3 + 8v^2 + 4v$ Weierstrass eğrisi üzerindedir. $(v,w) = (-2,4)$ noktasından Weierstrass eğrisine çizilen teğet $(u,v) = (0,0)$ noktasından geçer. Böylece $4(-2,4) = (0,1)$ olduğundan bu nokta 4. mertebedendir. O halde $(-1,0)$ noktası Edwards eğrisi üzerinde 4. mertebeden nokta olup Weierstrass eğrisi üzerindeki $(-2,4)$ noktasına karşılık gelir.



Şekil 3.5.1.

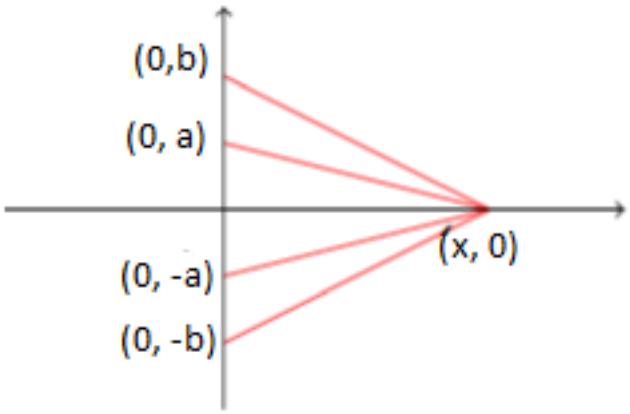
3.6 Huff Eğrileri ve Bir Diophant Problem

1948'de G.B. Huff tarafından aşağıdaki Diophant problemi göz önüne alındı (Huff 1948):

$\forall s,t \in S$ için s ve t arasındaki uzaklık bir rasyonel sayı olmak üzere $S, \mathbb{R}^2$ düzleminin altkümesi ve S rasyonel uzaklıklar kümesini göstersin. Farklı $a,b \in \mathbb{Q}$ verildiğinde S kümesi y-ekseni üzerinde $(0,\pm a)$ ve $(0,\pm b)$ noktalarını ve herhangi $x \in \mathbb{Q}$ için x-ekseni üzerinde $(x,0)$ noktasını içersin. Böyle bir $(x,0)$ noktası

$$x^2 + a^2 = u^2 \quad \text{ve} \quad x^2 + b^2 = v^2 \quad (u,v \in \mathbb{Q}) \tag{3.6.1}$$

denklemlerini sağlamak zorundadır.



Şekil 3.6.1.

Örnek 3.6.1 $a = 2, b = 5$ ise $(\frac{8}{3}, 0)$ noktası iyi bir seçimdir, çünkü iki mesafe $\frac{10}{3}$ ve $\frac{17}{3}$ tür.

(3.6.1)'deki denklemler homojenleştirilirse

$$x^2 + a^2z^2 = u^2 \quad \text{ve} \quad x^2 + b^2z^2 = v^2 \tag{3.6.2}$$

şeklinde olur. (3.6.2)'deki sistem $\mathbb{P}^3$'te cinsi 1 olan bir eğri tanımlar. Huff ve sonrasında öğrencisi Peeples bu eğrinin $\mathbb{Q}$'da pozitif ranklı bazı örneklerini incelemiştir. Bu vesile ile k, keyfi büyüklükteki rasyonel uzaklıklar kümesinin kardinalitesini göstermek üzere $k > 4$ iken tam $k - 4$ tane noktanın bir doğru üzerinde olduğunu Peeples tarafından gösterilmiştir (Peeples 1954).

Yukarıda bahsedilen cinsi 1 olan eğri $a, b \in \mathbb{Q}$ olmak üzere

$$H_{a,b} : ax(y^2 - 1) = by(x^2 - 1) \tag{3.6.3}$$

eğrisine birasyonel denktir. Kolaylıkla görülür ki tek karakteristiğe sahip herhangi bir cisim üzerinde (3.6.3) eğrisi $a^2 \neq b^2$ ve $a, b \neq 0$ iken bir eliptik eğriye karşılık gelir.

2010'da Joye, Tibouchi ve Vergnaud 1948'de Huff tarafından tanıtılan Diophant problemini incelemek için bir eliptik eğri modeli geliştirdiler ve az önce bahsedilen durumu

genelleyerek aşağıdaki tanımı verdiler (Joye ve ark. 2010).

Tanım 3.6.2 $\mathbb{F}$ bir cisim ve $Kar(\mathbb{F}) \neq 2$ olsun. $ab(a-b) \neq 0$ iken

$$H_{a,b} : ax(y^2 - 1) = by(x^2 - 1) \tag{3.6.4}$$

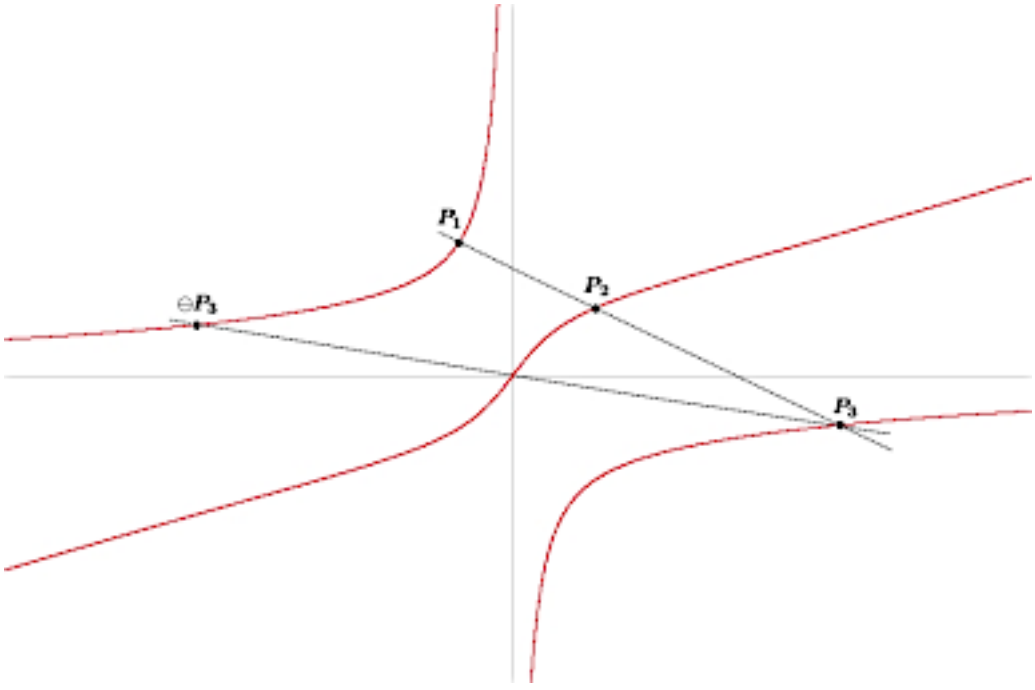
formundaki eğri *Huff eğrisi* olarak adlandırılır (Joye ve ark. 2010).

Huff eğrisinin projektif koordinatlardaki tanımı ise aynı yazarlar tarafından şöyle verildi:

Tanım 3.6.3 $Kar(\mathbb{F}) \neq 2$ olsun.

$$H'_{a,b} : aX(Y^2 - Z^2) = bY(X^2 - Z^2) \tag{3.6.5}$$

denklemini sağlayan $(X : Y : Z) \in \mathbb{P}^2(\mathbb{F})$ projektif noktaların kümesi $a, b \in \mathbb{F}^*$ ve $a^2 \neq b^2$ iken bir eliptik eğriye karşılık gelir. Bu eğri, eliptik eğrinin *Huff modeli* olarak adlandırılır (Joye ve ark. 2010).



Şekil 3.6.2. Huff Eğrisi

$(0 : 0 : 1)$'deki teğet $aX = bY$ doğrusudur. Bu doğru eğriyi 3 noktada keser. $\mathcal{O} = (0 : 0 : 1)$ noktası H''nün bir kıvrılma noktasıdır. $\mathcal{O}$ birim eleman olmak üzere H' üzerinde $\oplus$

toplama işlemini tanımlayalım. H' eğrisini üç noktada kesen bir doğru olsun. Bu noktalara P_1, P_2 ve P_3 diyelim. $P_1 \oplus P_2 \oplus P_3 = \mathcal{O}$ şeklinde tanımlanır. $P_1 = (X_1 : Y_1 : Z_1)$ noktasının tersi $\ominus P_1 = (X_1 : Y_1 : -Z_1)$ ile verilir ve $P_1 \oplus P_2 = \ominus P_3$ şeklindedir. Sonsuzdaki noktasının tersi de (bu gruptaki işleme göre) kendisidir. Böylece sonsuzdaki üç nokta $(1:0:0), (0:1:0)$ ve $(a:b:0)$ H''nün 2 mertebeli noktalarıdır. Bu noktalar $\mathbb{P}^2$'de $Z = 0$ doğrusu üzerindedir. Bu noktaların herhangi ikisinin toplamı üçüncüsüne eşittir. Daha genel bir ifade ile $(X_1 : Y_1 : Z_1)$'den geçen x-eksenine paralel bir doğrunun H''nü kestiği noktanın tersi $(X_1 : Y_1 : Z_1) \oplus (1:0:0)$ ifadesine eşittir.

$Z_1 \neq 0$ olduğunda

$$(X_1 : Y_1 : Z_1) \oplus (1:0:0) = (Z_1^2 : -X_1Y_1 : X_1Z_1)$$

ve benzer şekilde

$$(X_1 : Y_1 : Z_1) \oplus (0:1:0) = (-X_1Y_1 : Z_1^2 : Y_1Z_1)$$

dir.

$Z_1 \neq 0$ iken

$$(a:b:0) = (1:0:0) \oplus (0:1:0)$$

eşitliğinden $(X_1 : Y_1 : Z_1) \oplus (a:b:0) = (Z_1^2 : -X_1Y_1 : X_1Z_1) \oplus (0:1:0)$ ve böylece

$$(X_1 : Y_1 : Z_1) \oplus (a:b:0) = \begin{cases} (a:b:0), & (X_1 : Y_1 : Z_1) = (0:0:1) \text{ ise} \\ (Y_1Z_1 : X_1Z_1 : -X_1Y_1), & \text{aksi takdirde} \end{cases}$$

şeklinde ifade edilir.

Uyarı 3.6.4 (Huff 1948)'deki kaynakta

$\gamma : \mathbb{P}^2(\mathbb{F}) \to \mathbb{P}^2(\mathbb{F})$

$(X:Y:Z) \mapsto (U:V:W) = (ab(bX - aY) : ab(b^2 - a^2)Z : -aX + bY)$

ve

$\gamma^{-1} : \mathbb{P}^2(\mathbb{F}) \to \mathbb{P}^2(\mathbb{F})$

$(U : V : W) \mapsto (X : Y : Z) = (b(U + a^2W) : a(U + b^2W) : V)$ ters projektif dönüşümleri yardımıyla (3.6.5) eğrisi

$$V^2W = U(U + a^2W)(U + b^2W) \tag{3.6.6}$$

Weierstrass denklemine indirgenir. Burada Weierstrass eğrisi üzerindeki $(0 : 1 : 0)$ sonsuzdaki noktasına γ^{-1} dönüşümü ile karşılık gelir. Ayrıca (3.6.6) eşitliğinden Huff eğrisinin afin koordinatlarda

$$V^2 = U(U + a^2)(U + b^2)$$

eliptik eğrisine izomorf olduğu da açıktır (Joye ve ark. 2010).

3.7 Huff Eğrisi için Afin Formül ve Projektif Formüller

(3.6.4) eğrisini göz önüne alalım. Bu eğri üzerinde $P_1 = (x_1, y_1)$ ve $P_2 = (x_2, y_2)$ noktalarından geçen doğru $y = \lambda x + \mu$ olsun. Bu doğru eğriyi üçüncü bir noktada yani $\ominus P_3 = (-x_3, y_3)$ noktasında keser. Bu doğruyu (3.6.4) denkleminde yerine yazarsak, bazı ara işlemlerden sonra üçüncü noktanın afin koordinatları

$$x_3 = \frac{(x_1 + x_2)(1 + y_1y_2)}{(1 + x_1x_2)(1 - y_1y_2)}, \quad y_3 = \frac{(y_1 + y_2)(1 + x_1x_2)}{(1 - x_1x_2)(1 + y_1y_2)} \tag{3.7.1}$$

ile verilir (Joye ve ark. 2010).

Huff eğrileri eliptik eğrilerin farklı bir modeli olduğundan kriptografik uygulamalarda hız açısından oldukça avantajlıdır. Hatta bu eğrilerde afin koordinatlar yerine projektif koordinatlarda daha hızlı aritmetik (noktaların toplama işlemi, noktanın katını alma) yapılır.

(3.7.1)'deki formüllerin projektif versiyonu

$$\begin{aligned} X_3 &= (X_1Z_2 + X_2Z_1)(Y_1Y_2 + Z_1Z_2)^2(Z_1Z_2 - X_1X_2) \\ Y_3 &= (Y_1Z_2 + Y_2Z_1)(Y_1Y_2 + Z_1Z_2)^2(Z_1Z_2 - Y_1Y_2) \\ Z_3 &= (Z_1^2Z_2^2 - X_1^2X_2^2)(Z_1^2Z_2^2 - Y_1^2Y_2^2) \end{aligned} \tag{3.7.2}$$

bağıntıları ile verilir (Joye ve ark. 2010).

Teorem 3.7.1 $Kar(\mathbb{F}) \neq 2$ olsun. $P_1 = (X_1 : Y_1 : Z_1),\ P_2 = (X_2 : Y_2 : Z_2)$ noktaları $\mathbb{F}$ cisminde tanımlı bir Huff eğrisi üzerinde noktalar olsun. Bu durumda (3.7.2) formülleri ile verilen toplama işlemi $X_1X_2 \neq \pm Z_1Z_2$ ve $Y_1Y_2 \neq \pm Z_1Z_2$ şartlarını sağladığında geçerlidir (Joye ve ark. 2010).

3.8 Bükülmüş Huff Eğrisi

Bir Huff eğrisi üzerindeki noktaların torsiyon grubu $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ dir. $\mathcal{P} \in \mathbb{F}(t)$ ikinci dereceden monik bir polinomu göstersin ve bu polinom diskriminantı sıfırdan farklı ve $\mathcal{P} \neq 0$ olsun. Bu durumda $a, b \in \mathbb{F}^*$ iken

$$ax\mathcal{P}(y) = by\mathcal{P}(x)$$

kübik eğrisini tanıtabiliriz. $\{(0:0:1),(0:1:0),(1:0:0),(a:b:0)\} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ noktaların kümesi yukarıdaki eğriye aittir. Dahası $\mathcal{P}, \mathbb{F}$'te çarpanlarına ayrılırsa, yani $\mathcal{P}(t) = (t - w_1)(t - w_2)\ \ (w_1, w_2 \in \mathbb{F}^*)$ olduğunda $(\pm w_1 : \pm w_2 : 1)$ noktaları da eğri üzerindedir.

$Kar(\mathbb{F}) \neq 2$ iken $\mathcal{P}(t) = t^2 - d\ \ (d \in \mathbb{F}^*)$ polinomunu göz önüne alalım. Böylece $a, b, d \in \mathbb{F}^*$ ve $a^2 \neq b^2$ iken düzgün

$$\hat{E}_d : aX(Y^2 - dZ^2) = bY(X^2 - dZ^2) \tag{3.8.1}$$

kübik denklemini sağlayan $(X : Y : Z) \in \mathbb{P}^2(\mathbb{F})$ projektif noktaların kümesi ile ilgilene-

ceğiz. (3.8.1) denklemi Weierstrass formundaki

$$V^2W = U(U + \frac{a^2}{d}W)(U + \frac{b^2}{d}W) \tag{3.8.2}$$

denklemine karşılık gelir. (3.8.1) ve (3.8.2) arasında

$$\begin{aligned}(X : Y : Z) &= (b(dU + a^2W) : a(dU + b^2W) : dV)\\ (U : V : W) &= (ab(bX - aY) : ab(b^2 - a^2)Z : d(-aX + bY))\end{aligned} \tag{3.8.3}$$

dönüşümleri tanımlıdır. $(X : Y : Z) \leftarrow (X : Y : Z\sqrt{d})$ dönüşümü $E = \hat{E}_1$'den $\hat{E}_d$'ye ($\mathbb{F}(\sqrt{d})$ üzerinde) bir izomorfizmaya indirgenir. $\hat{E}_d$ eğrileri *ikinci dereceden bükülmüş Huff eğrileri* olarak adlandırılır.

Huff eğrileri ile ilgili detaylı bilgi için Joye ve ark. (2010) kaynağına bakılabilir.

3.9 Genel Huff Eğrisi

Joye ve ark. (2010), Huff tarafından tanıtılan (3.6.4) eğrisinin bir eliptik eğri modeli olduğunu gösterdikten sonra, yine aynı yıl Wu ve Feng tarafından aşağıdaki eğri ailesi tanıtıldı.

Tanım 3.9.1 $\mathbb{F}$ bir cisim $Kar(\mathbb{F}) \neq 2$ olsun. $a, b \in \mathbb{F}$ ve $ab(a - b) \neq 0$ iken

$$G_{a,b} : x(ay^2 - 1) = y(bx^2 - 1) \tag{3.9.1}$$

formundaki eğri *Genel Huff eğrisi* olarak adlandırılır. Bu eğri ailesi (3.6.4)'teki eğri ailesini içerir (Wu ve Feng 2010).

Şimdi de bu eğri ile ilgili aşağıdaki teoremi ifade edelim.

Teorem 3.9.2 $Kar(\mathbb{F}) \neq 2$ olsun. $a, b \in \mathbb{F}$ ve $a \neq b$ iken (3.9.1) eğrisi projektif koordinatlarda

$$G'_{a,b} : X(aY^2 - Z^2) = Y(bX^2 - Z^2)$$

formundadır. Bu eğri

$$U = bX - aY, \quad V = (b-a)Z, \quad W = Y - X$$

iken $\varphi(X, Y, Z) = (U, V, W)$ dönüşümü ile

$$V^2W = U(U + aW)(U + bW) \tag{3.9.2}$$

eliptik eğrisine izomorftur. Ayrıca

$$X = U + aW, \quad Y = U + bW, \; Z = V$$

iken ters dönüşüm bağıntısı $\psi(U, V, W) = (X, Y, Z)$ ile verilir (Wu ve Feng 2010).

(3.9.1) $G_{a,b}$ genel Huff eğrisi ve aritmetiği hakkında detaylı bilgi için Wu ve Feng (2010) makaleye bakılabilir.

4. ARDIŞIK KÜP DİZİLERİNİ BULUNDURAN ELİPTİK EĞRİLER

4.1 Giriş

Katsayıları $\mathbb{Q}$'dan alınan (2.1.2) uzun Weierstrass normal formundaki rasyonel eliptik eğrisini göz önüne alalım. $i = 1, 2, \ldots, n$ için $x_1, x_2, \ldots, x_n$ bileşenleri aritmetik bir dizi oluşturursa bu dizi n-*uzunluklu aritmetik dizi* olarak adlandırılır.

$S \subset \mathbb{Q}$ olacak şekilde n-uzunluklu S-aritmetik dizilerini göz önüne alalım. Bu konu ile ilgili ilk çalışma 1992'de Lee ve Vélez tarafından yapılmıştır. Bu yazarlar tarafından $n = 4$ uzunluklu S-dizisini içeren sonsuz çoklukta $y^2 = x^3 + a$ eğrisi olduğu gösterilmiştir (Lee ve Vélez 1992). 7 yıl sonra Bremner tarafından $n = 7$ ve $n = 8$ uzunluklu S-dizisini içeren sonsuz çoklukta eliptik eğri olduğu gösterildi (Bremner 1999). 2003'te $n = 7$ ve $n = 8$ uzunluklu S-dizisini içeren eliptik eğrilerin sonsuz ailesini üretmek için farklı bir metot Campbell tarafından geliştirildi. Buna ilave olarak, yine aynı yazar tarafından $n = 9$ uzunluklu S-dizisini içeren dördüncü dereceden eliptik eğrilerin sonsuz ailesini elde etmek için bir metot tanımlandı ve $n = 12$ uzunluklu bir S-dizisini içeren dördüncü derecen bir eliptik eğri örneği verildi (Campbell 2003). 2 yıl sonra Ulas tarafından, ilk olarak $n = 10$ uzunluklu bir S-dizisini içeren sonsuz çoklukta dördüncü dereceden eliptik eğri ailesini üretecek bir metot verildi ve sonrasında da $n = 12$ uzunluklu S-dizisini içeren dördüncü dereceden eğrilerin sonsuz ailesinin varlığı gösterildi (Ulas 2005). 2006'da, Ulas'ın yaklaşımı basitleştirilerek, yeni bir yöntem $n = 14$ uzunluklu S-dizileri ile ilgili bir kaç tane dördüncü dereceden eğri örneğinin elde edilebileceği Macleod tarafından gösterildi (Macleod 2006). 3 yıl sonra Ulas tarafından, $n = 11$ uzunluklu S-dizilerini içeren, cinsi 2, $der(f(x)) = 5$ olan $y^2 = f(x)$ şeklinde sonsuz çoklukta eğri ailesi bulundu (Ulas 2009). 2009'da, $n = 12$ uzunluklu S-dizilerini bulunduracak eğrilerin sonsuz bir ailesinin varlığı Alvarado tarafından gösterildi (Alvarado 2009).

x-bileşenlerinin oluşturduğu S-dizisinin geometrik dizi oluşturma durumu 6. bölümde ele alınacaktır.

Şimdi $k, l, m \in \mathbb{Q}$ olmak üzere $\mathbb{Q}$ cismi üzerinde

$$E: \ y^2 = kx^3 + lx + m \tag{4.1.1}$$

eliptik eğrisini göz önüne alalım. $i = 1, 2, \ldots, n$ iken $(x_i, y_i) \in E(\mathbb{Q})$ rasyonel noktalarının x_i-bileşenleri ardışık kareler olacak şekilde bir S-dizisinin $(S \subset \mathbb{Q})$ elemanları olsun. 2017'de Kamel ve Sadek tarafından $n = 5$ uzunluklu bu özellikteki S-dizisini bulunduran sonsuz çoklukta (4.1.1) tipinde eğri bulunabileceği gösterildi. Ayrıca bu özellikteki 5 rasyonel noktanın $E(\mathbb{Q})$'da lineer bağımsız olduğu ispatlanarak rankı en az 5 olan eliptik eğrilerin sonsuz bir ailesi literatüre tanıtıldı (Kamel ve Sadek 2017).

Tezin bu bölümü orjinal sonuçlar içermektedir. Bu bölümde eliptik eğriler üzerindeki rasyonel noktaların x-bileşenlerinin ardışık küplerin bir dizisini oluşturma durumu ele alınacaktır. Burada (4.1.1) tipindeki eliptik eğriler (yani kısa Weierstrass formunda eğriler) göz önüne alınır. Kamel ve Sadek (2017) makalesindeki yöntem kullanılarak, literatüre yeni sonuçlar kazandırılır.

4.2 Apsisleri Ardışık Küpler Olan Dizileri Bulunduran Eliptik Eğriler

Tanım 4.2.1 $\mathbb{F}$ cismi üzerinde (2.1.2) formundaki E eliptik eğrisi verilsin. $i = 1, 2, \ldots$ iken $x_i = (c+i)^3$ olacak şekilde $c \in \mathbb{F}$ varsa $(x_i, y_i) \in E(\mathbb{F})$ noktaları E üzerinde *ardışık küplerin bir dizisini* oluşturur.

Şimdi Teorem 1.8.7'yi kullanarak, bir eliptik eğri üzerinde ardışık küplerin sonluluğuyla ilgili aşağıdaki önermeyi verelim.

Önerme 4.2.2 $\mathbb{F}$ cismi üzerinde (2.1.2) formundaki E eliptik eğrisini göz önüne alalım. E üzerindeki ardışık küplerin bir dizisi $(x_i, y_i) \in E(\mathbb{F})$ olsun. Bu durumda (x_i, y_i) dizisi sonludur.

İspat. Genelliği kaybetmeden varsayalım ki $i = 1, 2, \ldots, n \in \mathbb{F}$ iken $x_i = (c+i)^3$ olsun.

Bu eşitlik (2.1.2) formundaki E eliptik eğrisi üzerinde yerine konulursa cinsi 5 olan

$$E' : y^2 + a_1x^3y + a_3y = x^9 + a_2x^6 + a_4x^3 + a_6$$

hipereliptik eğrisi elde edilir. Böylece $(c+i, y) \in E'(\mathbb{F})$ olur. Faltings Teoremine göre $E'(\mathbb{F})$, yani ardışık küpleri bulunduran dizi sonlu elemanlıdır. ■

Tanım 4.2.3 E, (2.1.2) formunda $\mathbb{Q}$ üzerinde bir eliptik eğri olsun. $i = 1, 2, \ldots, n$ olmak üzere $(x_i, y_i) \in E(\mathbb{Q})$, E üzerinde ardışık küplerin bir dizisi olsun. Bu diziye *n-uzunluklu ardışık küplerin dizisi* denir.

4.3 5 Uzunluklu Ardışık Küp Dizilerini Bulunduran Eliptik Eğriler

Bu bölümde, $\mathbb{Q}$ üzerinde (4.1.1) tipindeki eliptik eğrilerinin bir ailesini keşfediyoruz. Burada 5-uzunluklu ardışık küp dizilerini içeren sonsuz çoklukta eliptik eğrinin var olduğunu göstereceğiz.

3-uzunluklu ardışık küplerin dizisini göz önüne alalım. $c \in \mathbb{Q}$ iken $((c-1)^3, p), (c^3, q)$, ve $((c+1)^3, r)$ noktaları (4.1.1) eğrisi üzerinde olursa bu rasyonel noktalar 3-uzunluklu ardışık küplerin dizisini oluşturur. Bu noktaların (4.1.1) eğrisi üzerinde oluşu

$$\begin{aligned} p^2 &= k(c-1)^9 + l(c-1)^3 + m, \\ q^2 &= kc^9 + lc^3 + m, \\ r^2 &= k(c+1)^9 + l(c+1)^3 + m \end{aligned}$$

denklem sistemini ortaya çıkarır. Bu denklem sistemi çözülürse

$$\begin{aligned} k =& [(3c^2+3c+1)p^2 + (-6c^2-2)q^2 + (3c^2-3c+1)r^2]/6c(27c^8+54c^6+c^2+2), \\ l =& [-(9c^8+36c^7+84c^6+126c^5+126c^4+84c^3+36c^2+9c+1)p^2 + (18c^8, \\ & + 168c^6+252c^4+72c^2+2)q^2 - (9c^8-36c^7+84c^6-126c^5+126c^4-84c^3, \\ & + 36c^2-9c+1)r^2]/6(3c^2-3c+1)(9c^6+9c^5+24c^4+21c^3+13c^2+6c+2)c, \end{aligned}$$

$$
\begin{aligned}
m =&[(6c^{10}+33c^9+83c^8+126c^7+126c^6+84c^5+36c^4+9c^3+c^2)p^2 \\
&+(-12c^{10}-4c^8+72c^6-72c^4+4c^2+12)q^2+(6c^{10}-33c^9+83c^8-126c^7 \\
&+126c^6-84c^5+36c^4-9c^3+c^2)r^2]/6(3c^2-3c+1)(9c^6+9c^5+24c^4 \\
&+21c^3+13c^2+6c+2)
\end{aligned}
\tag{4.3.1}
$$

bulunur. Böylece aşağıdaki sonuç elde edilir.

Uyarı 4.3.1 $p,q,r \in \mathbb{Q}(c)$ yukarıdaki gibi verilirse $((c-1)^3,p),(c^3,q)$ ve $((c+1)^3,r)$ rasyonel noktalarını (4.1.1) üzerinde bulunduracak $k,l,m \in \mathbb{Q}(c)$'nin varlığını biliyoruz.

Şimdi bu üç noktaya ilave olarak varsayalım ki $((c+2)^3,s)$ noktası (4.1.1) eğrisi üzerinde olsun. Böylece (4.1.1) eğrisi üzerinde 4 uzunluklu ardışık küplerin dizisini elde ederiz. k,l,m ve $((c+2)^3,s)$ değerleri (4.1.1) eğrisinde yerine yazıldığında

$$
\begin{aligned}
s^2 =&[(84+2109c^2+626c+243c^8+27c^9+1026c^7+2646c^6+4536c^5+5292c^4 \\
&+4159c^3)p^2+(-1674c^7-1950c^2-762c-3951c^3-5544c^4-486c^8 \\
&-3780c^6-5544c^5-168-81c^9)q^2+(702c^7+1134c^6+138c-159c^2 \\
&+243c^8+81c^9+252c^4+1008c^5+84-207c^3)r^2]/(3c^2-3c+1)(3c^2+1) \\
&(1+3c^2+3c)(c^2+2)c
\end{aligned}
\tag{4.3.2}
$$

elde edilir.

Bu nedenle, $\mathbb{Q}(c)$'de (4.3.2) denklemini sağlayan p,q,r ve s elemanlarını bulmamız gerekir.

Şimdi (4.3.2) denklemi için (p,q,r,s) genel çözümlerinin nasıl bulunacağını açıklayalım. $\mathbb{Q}$ üzerinde

$$
S: a_1x^2+a_2y^2+a_3z^2+a_4t^2=0 \tag{4.3.3}
$$

kuadratik yüzeyini göz önüne alalım. $Q_1=(1:1:1:1)$ noktası S kuadratik yüzeyi üzerindedir ve bu yüzey üzerinde başka bir $Q_2=(u_1:v_1:w_1:0)$ rasyonel noktası

olsun. Üç boyutlu $\mathbb{P}^3$ projektif uzayında bu noktaları üzerinde bulunduran projektif doğru

$$aQ_1 + bQ_2 = (a + bu_1 : a + bv_1 : a + bw_1 : a)$$

olur. S yüzeyi ile $aQ_1 + bQ_2$ projektif doğrusunun kesişimi

$$(a_1 + a_2 + a_3 + a_4)a^2 + (a_1u_1^2 + a_2v_1^2 + a_3w_1^2)b^2 + (2a_1u_1 + 2a_2v_1 + 2a_3w_1)ab = 0$$

ikinci dereceden denklemini verir. Buradan

$$\begin{aligned} a &= a_1u_1^2 + a_2v_1^2 + a_3w_1^2, \\ b &= -2(a_1u_1 + a_2v_1 + a_3w_1) \end{aligned}$$

elde edilir. Dolayısıyla S-yüzeyinin (x, y, z, t) çözümleri parametrik olarak

$$\begin{aligned} x &= a + bu_1 = -a_1u_1^2 + a_2v_1^2 + a_3w_1^2 - 2a_2u_1v_1 - 2a_3u_1w_1, \\ y &= a + bv_1 = a_1u_1^2 - a_2v_1^2 + a_3w_1^2 - 2a_1u_1v_1 - 2a_3v_1w_1, \\ z &= a + bw_1 = a_1u_1^2 + a_2v_1^2 - a_3w_1^2 - 2a_1u_1w_1 - 2a_2v_1w_1, \\ t &= a = a_1u_1^2 + a_2v_1^2 + a_3w_1^2 \end{aligned} \tag{4.3.4}$$

şeklinde bulunur.

Şimdi $Q_1 = (p, q, r, s) = (1 : 1 : 1 : 1)$ noktası (4.3.2) denklemi için özel bir çözümü olup, bu yüzey üzerinde başka bir $Q_2 = (p, q, r, s) = (u : v : w : 0)$ rasyonel noktası alalım. (4.3.3)'daki kuadratik yüzeyin çözümleri için verilen (4.3.4) formülleri kullanılarak (4.3.2)'nin çözümleri aşağıdaki gibi verilir:

$$\begin{aligned} p = {} & (c+1)\left(3\,c^2+3\,c+1\right)\left(3\,c^2+6\,c+4\right)\left(3\,c^2+9\,c+7\right)\left(c^2+2\,c+3\right)u^2 \\ & +3\,\left(c^2+c+1\right)\left(3\,c^2+1\right)\left(3\,c^2+9\,c+7\right)\left(3\,c^3+6\,c^2+18\,c+8\right)v^2 \\ & -3\,\left(c^2+c+1\right)\left(3\,c^2-3\,c+1\right)\left(3\,c^2+6\,c+4\right)\left(3\,c^3+3\,c^2+15\,c+7\right)w^2 \end{aligned}$$

$$
\begin{aligned}
&- 6\,\left(c^2+c+1\right)\left(3\,c^2+1\right)\left(3\,c^2+9\,c+7\right)\left(3\,c^3+6\,c^2+18\,c+8\right)vu\\
&+ 6\,\left(c^2+c+1\right)\left(3\,c^2-3\,c+1\right)\left(3\,c^2+6\,c+4\right)\left(3\,c^3+3\,c^2+15\,c+7\right)wu,
\end{aligned}
$$

$$
\begin{aligned}
q = &-\left(c+1\right)\left(3\,c^2+3\,c+1\right)\left(3\,c^2+6\,c+4\right)\left(3\,c^2+9\,c+7\right)\left(c^2+2\,c+3\right)u^2\\
&- 3\,\left(c^2+c+1\right)\left(3\,c^2+1\right)\left(3\,c^2+9\,c+7\right)\left(3\,c^3+6\,c^2+18\,c+8\right)v^2\\
&- 3\,\left(c^2+c+1\right)\left(3\,c^2-3\,c+1\right)\left(3\,c^2+6\,c+4\right)\left(3\,c^3+3\,c^2+15\,c+7\right)w^2\\
&+ 2\,\left(c+1\right)\left(3\,c^2+3\,c+1\right)\left(3\,c^2+6\,c+4\right)\left(3\,c^2+9\,c+7\right)\left(c^2+2\,c+3\right)vu\\
&+ 6\,\left(c^2+c+1\right)\left(3\,c^2-3\,c+1\right)\left(3\,c^2+6\,c+4\right)\left(3\,c^3+3\,c^2+15\,c+7\right)wv,
\end{aligned}
$$

$$
\begin{aligned}
r = &-\left(c+1\right)\left(3\,c^2+3\,c+1\right)\left(3\,c^2+6\,c+4\right)\left(3\,c^2+9\,c+7\right)\left(c^2+2\,c+3\right)u^2\\
&+ 3\,\left(c^2+c+1\right)\left(3\,c^2+1\right)\left(3\,c^2+9\,c+7\right)\left(3\,c^3+6\,c^2+18\,c+8\right)v^2\\
&+ 3\,\left(c^2+c+1\right)\left(3\,c^2-3\,c+1\right)\left(3\,c^2+6\,c+4\right)\left(3\,c^3+3\,c^2+15\,c+7\right)w^2\\
&+ 2\,\left(c+1\right)\left(3\,c^2+3\,c+1\right)\left(3\,c^2+6\,c+4\right)\left(3\,c^2+9\,c+7\right)\left(c^2+2\,c+3\right)wu\\
&- 6\,\left(c^2+c+1\right)\left(3\,c^2+1\right)\left(3\,c^2+9\,c+7\right)\left(3\,c^3+6\,c^2+18\,c+8\right)wv,
\end{aligned}
$$

$$
\begin{aligned}
s = &-\left(c+1\right)\left(3\,c^2+3\,c+1\right)\left(3\,c^2+6\,c+4\right)\left(3\,c^2+9\,c+7\right)\left(c^2+2\,c+3\right)u^2\\
&+ 3\,\left(c^2+c+1\right)\left(3\,c^2+1\right)\left(3\,c^2+9\,c+7\right)\left(3\,c^3+6\,c^2+18\,c+8\right)v^2\\
&- 3\,\left(c^2+c+1\right)\left(3\,c^2-3\,c+1\right)\left(3\,c^2+6\,c+4\right)\left(3\,c^3+3\,c^2+15\,c+7\right)w^2.
\end{aligned}
\tag{4.3.5}
$$

Uyarı 4.3.2 Yukarıdaki argüman şunu gösterir: $p, q, r, s \in \mathbb{Q}(c, u, v, w)$ değişkenleri bilindiğinde dört rasyonel nokta $((c-1)^3, p), (c^3, q), ((c+1)^3, r), ((c+2)^3, s)$'nin (4.1.1) eğrisi üzerinde oluşu $k, l, m \in \mathbb{Q}(c)$'nin var olması demektir.

Şimdi $((c-2)^3, t) \in E(\mathbb{Q})$ olduğunu varsayalım. Bu durumda (4.1.1) eğrisi üzerinde 5-uzunluklu ardışık küplerin dizisi elde edilmiş olur. Böylece

$$
t^2 = Ku^4 + Lu^3 + Mu^2 + Nu + P \tag{4.3.6}
$$

elde edilir. Burada

$$K = [(c+1)\left(3\,c^2+3\,c+1\right)\left(3\,c^2+6\,c+4\right)\left(3\,c^2+9\,c+7\right)\left(c^2+2\,c+3\right)]^2,$$

$$\begin{aligned}L =& -24\ (c+1)\left(c^2+2\,c+3\right)\left(3\,c^2+3\,c+1\right)\left(3\,c^2+4\right)\left(3\,c^2+6\,c+4\right)(3\,c^2\\&+9\,c+7)^2\left(c^2-c+1\right)\left(3\,c^3+3\,c^2+27\,c+1\right)v+32c\ (c+1)\left(c^2+2\,c+3\right)\\&(3\,c^2+3\,c+1)\left(3\,c^2+4\right)\left(3\,c^2+6\,c+4\right)^2\left(3\,c^2+9\,c+7\right)\left(c^2+8\right)(3\,c^2-6\,c\\&+4)w,\end{aligned}$$

$$\begin{aligned}M =& 6\,(1215\,c^{14}+4131\,c^{13}+24543\,c^{12}+49383\,c^{11}+134460\,c^{10}+152118\,c^9\\&+263619\,c^8+229491\,c^7+297153\,c^6+223859\,c^5+208374\,c^4+123018\,c^3\\&+52116\,c^2+16504\,c+480)\left(3\,c^2+9\,c+7\right)^2v^2-24\ \left(c^2+c+1\right)\left(3\,c^2+4\right)\\&\left(3\,c^2+6\,c+4\right)\left(3\,c^2+9\,c+7\right)(189\,c^{10}+2340\,c^8-1530\,c^7+7383\,c^6\\&-9918\,c^5+7365\,c^4+740\,c^3-246\,c^2+1552\,c+21)wv+2\,(2835\,c^{14}\\&-8424\,c^{13}+37881\,c^{12}-109188\,c^{11}+156276\,c^{10}-373032\,c^9+395718\,c^8\\&-344976\,c^7+374198\,c^6-336324\,c^5-98956\,c^4-407760\,c^3-243937\,c^2\\&+2688\,c+441)\left(3\,c^2+6\,c+4\right)^2w^2,\end{aligned}$$

$$\begin{aligned}N =& -72\,(c^2+c+1)(3\,c^2+4)(c^2-c+1)(3\,c^2+1)(3\,c^3+6\,c^2+18\,c+8)\\&(3\,c^3+3\,c^2+27\,c+1)(3\,c^2+9\,c+7)^2v^3+48\,(c^2+c+1)(3\,c^2+4)\\&(3\,c^2+6\,c+4)(3\,c^2+9\,c+7)(27\,c^{10}+450\,c^8-450\,c^7+2019\,c^6-1494\,c^5\\&+2325\,c^4-1180\,c^3-1398\,c^2+16\,c+21)v^2w+24\,(c^2+c+1)(3\,c^2+4)\\&(3\,c^2+6\,c+4)(3\,c^2+9\,c+7)(135\,c^{10}+1440\,c^8-630\,c^7+3345\,c^6-6930\,c^5\\&+2715\,c^4+3100\,c^3+2550\,c^2+1520\,c-21)vw^2-96c\,(c^2+c+1)(3\,c^2+4)\\&(3\,c^2-3\,c+1)(3\,c^2-6\,c+4)(3\,c^3+3\,c^2+15\,c+7)(c^2+8)(3\,c^2+6\,c+4)^2w^3,\end{aligned}$$

$$
\begin{aligned}
P =&[3(c^2+c+1)\left(3\,c^2-3\,c+1\right)\left(3\,c^2+6\,c+4\right)(3\,c^3+3\,c^2+15\,c+7)]^2w^4\\
&+72\,\left(3\,c^2-3\,c+1\right)\left(3\,c^2+4\right)\left(3\,c^2+6\,c+4\right)\left(3\,c^2-9\,c+7\right)(3\,c^3+3\,c^2\\
&+15\,c+7)\left(3\,c^3-3\,c^2+27\,c-1\right)\left(c^2+c+1\right)^2w^3v-18\,(6561c^{14}+2187c^{13}\\
&+91125c^{12}+42039c^{11}+287712c^{10}-5994c^9-224127c^8+6399c^7\\
&+316035c^6+232191c^5+1581642c^4+299082c^3+294228c^2+248472c\\
&-7840)(c^2+c+1)^2w^2v^2+72\,\left(3\,c^2+1\right)\left(3\,c^2+4\right)\left(3\,c^2+9\,c+7\right)(3\,c^2\\
&-9\,c+7)(3\,c^3-3\,c^2+27\,c-1)\left(3\,c^3+6\,c^2+18\,c+8\right)\left(c^2+c+1\right)^2wv^3\\
&+[3\,\left(c^2+c+1\right)\left(3\,c^2+1\right)\left(3\,c^2+9\,c+7\right)\left(3\,c^3+6\,c^2+18\,c+8\right)]^2v^4
\end{aligned}
$$

şeklinde olur.

K, L, M, N ve P'nin v ve w cinsinden dördüncü dereceden homojen denklem oldukları görülmektedir. Böylece, $w = 1$ olduğunu varsayabiliriz.

Şimdi $\mathbb{Q}(c, v)$ cismi üzerinde

$$H : Y^2 = KX^4 + LX^3 + MX^2 + NX + P \tag{4.3.7}$$

eğrisini düşünelim.

(4.3.7) formundaki eğri Teorem 2.3.5 yardımıyla bir χ eğrisine birasyonel denk olup, χ eğrisi üzerinde bir R noktası kolaylıkla bulunabilir.

Şimdi Teorem 2.6.13 (Silverman Özelleştirme Teoremi) kullanılarak aşağıdaki teoremi verebiliriz.

Teorem 4.3.3 $\mathbb{Q}(c, v)$ üzerindeki (4.3.7) eğrisi rankı en az 1 olan χ eğrisine birasyonel denktir (Çelik ve Soydan 2018).

İspat. (4.3.7) eğrisi homojen formda yazılırsa $Y^2 = KX^4+LX^3Z+MX^2Z^2+NXZ^3+PZ^4$ şeklinde olup bu eğrinin rasyonel noktaları $T = (X : Y : Z) = (1 : (c+1)(3c^2+3c+1)(3c^2+6c+4)(3c^2+9c+7)(c^2+2c+3) : 0)$ şeklindedir. Teorem 2.3.5'in adımları kullanılarak (4.3.7) eğrisinin (2.3.10) eğrisine birasyonel denk olduğu görülür.

(2.3.8)-(2.3.11) eşitlikleri kullanılarak $c = 3$, $v = \frac{3094}{5795}$ değerleri alınarak

$$\psi : Y^2 = X^3 - \frac{19155688278708494907117216280017764352}{81450625}X + \frac{3047612503727941445407183938385383023426294144093808 2304}{735091890625}$$

özelleştirilmiş eğrisi ve bu eğri üzerindeki R noktasının özelleştirilmişi olan $\tilde{R}$=$(\frac{4692656977319420928}{9025}, \frac{697619129064490002577858 56}{9025})$ noktası bulunur. MAGMA (Bosma ve ark. 1997) paket programı yardımıyla $\tilde{R}$ noktasının ψ üzerinde sonsuz mertebeli nokta olduğu belirlenir. Böylece Teorem 2.6.13 yardımıyla R noktasının χ üzerinde sonsuz mertebeli olduğu görülür. ■

Sonuç 4.3.4 $c_0 \in \mathbb{Q}$ iken ardışık küplerin aşikar olmayan bir dizisi $\{(c_0-2)^3, (c_0-1)^3, c_0^3, (c_0+1)^3, (c_0+2)^3\}$ olsun. Bu durumda $i = -2, -1, 0, 1, 2$ iken x-bileşeni $(c_0+i)^3$ olan sonsuz çoklukta

$$E_j : y^2 = k_j x^3 + l_j x + m_j, 0 \neq j \in \mathbb{Z}$$

eliptik eğrisi vardır. Üstelik bu beş rasyonel nokta lineer bağımsızdır (Çelik ve Soydan 2018).

İspat. (4.3.5)'deki formüllerde $c = c_0, v = v_0$ ve $w = 1$ olarak seçilirse $K, L, M, N, P \in \mathbb{Q}$ iken

$$\chi_{c_0,v_0,1} : t^2 = Ku^4 + Lu^3 + Mu^2 + Nu + P \tag{4.3.8}$$

eliptik eğrisi elde edilir ve Teorem 4.3.3'e göre bu eğrinin rankı pozitiftir. O zaman $\chi_{c_0,v_0,1}(\mathbb{Q})$'de sonsuz mertebeli $R = (u, t)$ noktası bulunur. $\chi_{c_0,v_0,1}(\mathbb{Q})$'de R noktasının j katı olması için $0 \neq j \in \mathbb{Z}$ iken $jR = (u_j, t_j)$ alınır.

Şimdi (4.3.1)'de $p, q, r, s \in \mathbb{Q}(c, u, v, w)$ için $c = c_0, v = v_0, w = 1$ and $u = u_j$ değerleri yerine yazıldığında sırasıyla p_j, q_j, r_j, s_j sayıları elde edilir. O zaman (4.3.1)'de $k, l, m \in \mathbb{Q}(c, p, q, r)$ için p_j, q_j, r_j, s_j değerleri yerine yazıldığında sırasıyla k_j, l_j, m_j değerleri elde edilir.

Böylece $0 \neq j \in \mathbb{Z}$ iken $E_j : y^2 = k_j x^3 + l_j x + m_j$ eliptik eğrisinin sonsuz bir ailesini inşa etmiş oluruz. Eliptik eğrilerin bu sonsuz E_j ailesi $((c_0-1)^3, p_j), (c_0^3, q_j), ((c_0+1)^3, r_j), ((c_0+2)^3, s_j), ((c_0-2)^3, t_j) \in E_j(\mathbb{Q})$ noktalarını üzerinde bulundurur. Bu ise x-bileşenleri $\mathbb{Q}$'da ardışık küpler olan 5-uzunluklu rasyonel diziyi bulunduran eliptik eğrilerin sonsuz bir ailesini elde ettiğimiz anlamına gelir.

Şimdi $((c_0-1)^3, p_j), (c_0^3, q_j), ((c_0+1)^3, r_j), ((c_0+2)^3, s_j), ((c_0-2)^3, t_j) \in E_j(\mathbb{Q})$ noktalarının lineer bağımsız olduğunu göstereceğiz. Bunun için (4.3.8) eğrisi üzerinde bir (u, t) noktası bulmalıyız .

(4.3.8) denklemini göz önüne alalım. $c = 3, v = \frac{3094}{5795}, w = 1$ alındığında

$$t^2 = 63404527588416\, u^4 - \frac{782109496219903488}{9025}\, u^2 + \frac{19793578415844699648}{550525}\, u + \frac{4781724178941965835740 16}{303077775625} \tag{4.3.9}$$

eğrisi elde edilir. (4.3.9)'nin sağ tarafı tam kareye tamamlandığında

$$(u, t) = (\frac{60547}{77653}, \frac{78134116669224}{130068775}) \in \chi_{3,\frac{3094}{5795},1}(\mathbb{Q})$$

sonsuz mertebeli bir nokta elde edilir.

Böylece $c = 3$, $v = \frac{3094}{5795}$, $w = 1$, $u = \frac{60547}{77653}$ alındığında

$$E : y^2 = \frac{10193176476045327287 04}{50501152925375} x^3 + \frac{17064086301085936686 0672}{2657955417125} x + \frac{5018469623203840351296469056}{16917886230000625}$$

özelleştirilmiş eliptik eğrisi elde edilir. Bu eğri üzerinde bulunan x-bileşenleri ardışık küpler olan 5 nokta

$$E(\mathbb{Q}) = \left(1, \frac{78134116669224}{130068775}\right), \left(2^3, \frac{117823324221624}{130068775}\right), \left(3^3, \frac{202645347682344}{130068775}\right), \left(4^3, \frac{405025200935544}{130068775}\right), (5^3, \frac{898732973533416}{130068775})$$

şeklindedir. Teorem 2.7.9 kullanılarak bu rasyonel noktaların lineer bağımsız olduğu gös-

terilebilir. Teorem 2.7.9'daki uzun prosedür MAGMA (Bosma ve ark. 1997) paket programı ile kolay bir şekilde hesaplanabilir. Dolayısıyla MAGMA programı yardımıyla bu rasyonel noktaların lineer bağımsız olduğu belirlendi.

Silverman'ın Özelleştirme teoremiyle de, $\mathbb{Q}(c, v, u_j)$'de tanımlıE_j eğrisi üzerindeki $((c-1)^3, p_j), (c^3, q_j), ((c+1)^3, r_j), ((c+2)^3, s_j), ((c-2)^3, t_j)$ noktaları lineer bağımsızdır. Böylece ispat tamamlanır. ■

Uyarı 4.3.5 Sonuç 4.3.4, rankı $r \geq 5$ olan eliptik eğrilerin sonsuz bir ailesinin varlığını gerektirir (Çelik ve Soydan 2018).

Son olarak, eğer ardışık küplerin 6-uzunluklu dizisini inşa etmek istersek $((c+3)^3, z)$ noktasının (4.1.1) eğrisi üzerinde olduğunu varsaymalıyız. Böylece $K', L', M', N', P' \in \mathbb{Q}(c, v)$ olmak üzere

$$z^2 = K'u^4 + L'u^3 + M'u^2 + N'u + P'$$

eğrisini elde ederiz. O halde aşağıdaki uyarıyı verelim.

Uyarı 4.3.6 Eliptik eğri üzerindeki 6-uzunluklu ardışık küplerin bir dizisinin varlığı

$$C : t^2 = Ku^4 + Lu^3 + Mu^2 + Nu + P, \quad z^2 = K'u^4 + L'u^3 + M'u^2 + N'u + P'$$

eğrilerinin ara kesiti olan cebirsel eğrinin üzerindeki rasyonel bir (u, t, z) noktasının varlığına bağlıdır. Bu C arakesit eğrisinin cinsi 5'tir. Teorem 1.8.7'e göre verilen bir $c \in \mathbb{Q}$ ve $j = -2, -1, 0, 1, 2, 3$ için $(c + j)^3$ ardışık küplerin 6 uzunluklu dizisini bulunduran $\mathbb{Q}$ üzerinde sonlu tane $y^2 = kx^3 + lx + m$ eliptik eğrisi vardır (Çelik ve Soydan 2018).

Çelik ve Soydan (2018) çalışması yayınlandıktan 3 yıl sonra Uyarı 4.3.6'deki problem yani ardışık küplerin 6 uzunluklu dizisini bulunduran ve rankı en az 5 olan $y^2 = kx^3 + lx^2 + mx + n$ eliptik eğri ailesinin varlığı gösterilmiştir (Salami ve Zargar 2021).

5. ELİPTİK EĞRİLERİN FARKLI MODELLERİ ÜZERİNDEKİ RASYONEL DİZİLER

5.1 Giriş

Eliptik eğrilerin farklı modellerinden Edwards eğrisi, bükülmüş Edwards eğrisi, Huff eğrisi ve genel Huff eğrisi hakkında detaylı bilgiler 3. bölümde verildi. Şimdi bu eğriler üzerindeki rasyonel diziler ile ilgili çalışmaların literatür bilgisini tarihsel sıra ile verelim. İlk olarak yukarıda bahsedilen eğriler üzerindeki $S \subset \mathbb{Q}$ olacak şekilde n-uzunluklu S-aritmetik dizileri hakkındaki çalışmaları ele alalım. Edwards ve Huff eğrileri üzerindeki S-aritmetik dizileri hakkında ilk iki çalışma Moody tarafından yapıldı. Moody bu çalışmalarında $n = 9$ uzunluklu S-aritmetik dizisini içeren sonsuz çoklukta Edwards eğrisi ve Huff eğrisi olduğunu gösterdi (Moody 2011). Ayrıca Moody $n \geqslant 10$ uzunluklu S-aritmetik dizisini içeren Edwards eğrisi bulunup bulunmayacağını açık problem olarak bıraktı. 2013 yılında Bremner tarafından $n = 11$ uzunluklu S-aritmetik dizisini bulunduracak Edwards eğrisinin mümkün olmadığı gösterildi (Bremner 2013).

2 yıl sonra Choudhry, $n = 11$ uzunluğunda S-aritmetik dizilerini içeren Huff eğrilerinin bulunduğunu göstererek Moody'nin 2011'deki ikinci çalışmasını genişletti (Choudhry 2015).

Şimdi, S'nin elemanlarının geometrik dizi oluşturduğu durumu göz önüne alalım. 2017'de Ciss ve Moody tarafından $n = 4$ uzunluklu S-geometrik dizilerini bulunduran sonsuz çoklukta Edwards eğrisi ve $n = 5$ uzunluklu S-geometrik dizilerini bulunduran sonsuz çoklukta bükülmüş Edwards eğrisi olduğu gösterildi (Ciss ve Moody 2017).

Tezin bu bölümü orjinal sonuçlar içermektedir. Burada, giriş bölümünde bahsettiğimiz "$S \subset \mathbb{F}$ verildiğinde, her $x \in S$ ve herhangi $P \in C(\mathbb{F})$ için $x = x(P)$ olacak şekilde d. dereceden C cebirsel eğrileri var mıdır ?" sorusuna cevap bulmak için (bükülmüş) Edwards eğrileri ve (genel) Huff eğrileri göz önüne alınır. $\mathbb{F}$ sayı cisminin keyfi bir S altkümesi, yukarıda verilen cebirsel eğrilerin üzerindeki noktaların x-bileşenlerinden oluşan bir dizi olarak düşünülür. Üzerinde herhangi bir kısıtlama olmayan S-rasyonel dizilerin

uzunluğu $|S| = 4, 5$ veya 6 iken bu S-dizilerini bulunduran (bükülmüş) Edwards eğrileri ve (genel) Huff eğrilerinin sonsuz ailelerinin varlığı ispatlanır. Böylelikle bu bölümdeki sonuçlar bu cebirsel eğriler üzerindeki rasyonel diziler hakkında önceden yapılan bazı çalışmaları geneller. Elde edilen sonuçların ispatında yöntem olarak kuadratik ve eliptik yüzeyler üzerindeki rasyonel noktaların varlığı hakkındaki literatürden iyi bilinen sonuçlar kullanılır.

5.2 6 Uzunluklu Dizileri Bulunduran Edwards Eğrileri

(3.1.4) formunda tanımlı Edwards eğrisini göz önüne alalım. Bu eğri üzerindeki noktaların kümesi $E_d(\mathbb{F})$ ile gösterilsin. (3.3.1)'den dolayı $(x, y) = (-1, 0), (0, \pm 1), (1, 0) \in E_d(\mathbb{F})$ olduğu açıktır. $i \neq j$ iken $s_i \neq s_j$ ve $-1 \leq i \leq 4$ olsun. Bu bölümde, herhangi bir $S = \{s_{-1} = -1, s_0 = 0, s_1 = 1, s_2, s_3, s_4\} \subset \mathbb{F}$ kümesi verildiğinde x-bileşenleri s_i'ler olan rasyonel noktaları bulunduran sonsuz sayıda Edwards eğrisi olduğu gösterilecektir. s_2'yi $E_d(\mathbb{F})$ kümesinde bir noktanın x-bileşeni olduğunu varsayarak başlayalım. Bu durumda herhangi $p = \frac{1}{y} \in \mathbb{F}$ için

$$y^2 = \frac{s_2^2 - 1}{s_2^2 d - 1} \text{ veya } s_2^2 d - 1 = (s_2^2 - 1)p^2$$

olur. Benzer şekilde s_3, $E_d(\mathbb{F})$'deki bir noktanın x-bileşeni ise

$$y^2 = \frac{s_3^2 - 1}{s_3^2 d - 1} \text{ veya } s_3^2 d - 1 = (s_3^2 - 1)q^2$$

olur. Buradan

$$d = \frac{(s_2^2 - 1)p^2 + 1}{s_2^2} = \frac{(s_3^2 - 1)q^2 + 1}{s_3^2}$$

olup

$$s_3^2((s_2^2 - 1)p^2 + 1) - s_2^2((s_3^2 - 1)q^2 + 1) = 0 \tag{5.2.1}$$

kuadratik yüzeyi elde edilir ve $(p,q)=(1,1)$ noktası yüzey üzerindedir. Yüzey üzerinde $(p,q)=(1,1)$ noktasından geçen bir ℓ doğrusu, eğriyi ikinci bir

$$(p,q)=(1+m,1+mt) \tag{5.2.2}$$

noktasında kesecektir. Dolayısıyla (5.2.2) noktasının (5.2.1) yüzeyi üzerinde olması

$$s_3^2((s_2^2-1)(1+m)^2+1)-s_2^2((s_3^2-1)(1+mt)^2+1)=0$$

olmasını gerektirir. Buradan

$$m=\frac{{s_3}^2\left(2\,{s_2}^2-2\right)-2\,{s_2}^2\left({s_3}^2-1\right)t}{-{s_3}^2\left({s_2}^2-1\right)+{s_2}^2\left({s_3}^2-1\right)t^2}$$

olarak bulunur. Bulunan m değeri (5.2.2)'de yerine yazıldığında, kuadratik yüzey üzerindeki rasyonel noktaların parametrik çözümleri

$$\begin{aligned}p=&\frac{2ts_2^2-t^2s_2^2-s_3^2+s_2^2s_3^2-2ts_2^2s_3^2+t^2s_2^2s_3^2}{-t^2s_2^2+s_3^2-s_2^2s_3^2+t^2s_2^2s_3^2},\\ q=&-\frac{(-1+s_2^2)s_3^2-2t(-1+s_2^2)s_3^2+t^2s_2^2(-1+s_3^2)}{-(-1+s_2^2)s_3^2+t^2s_2^2(-1+s_3^2)}\end{aligned}$$

şeklinde bulunur.

Böylece s_2 ve s_3 değerleri $\mathbb{F}$ cisminde sabit bırakılarak p ve q değerlerinin $\mathbb{F}(t)$'de olduğu görülür.

Öncelikle Teorem 5.2.2 ve Teorem 5.3.1'ün ispatında kullanacağımız aşağıdaki önermeyi verelim:

Önerme 5.2.1 $x^2+y^2=a^2+a^2x^2y^2$ ile tanımlanan eğri, $i=\sqrt{-1}$ ve $0\leqslant\epsilon\leqslant 3$ olmak üzere b'nin

$$i^\epsilon,\quad \frac{i^\epsilon}{a},\quad i^\epsilon\frac{a-1}{a+1},\quad i^\epsilon\frac{a+1}{a-1},\quad i^\epsilon\frac{a-i}{a+i},\quad i^\epsilon\frac{a+i}{a-i}$$

24 değerden biri olması durumunda $x^2+y^2=b^2+b^2x^2y^2$ ile belirlenen eğriye birasyonel denktir (Edwards 2007, Önerme 6.1).

Şimdi sonucu verelim.

Teorem 5.2.2 $\mathbb{Z}$'de

$$h(s_2, s_3) = -3 + 4s_3^2 + s_2^4 s_3^4 + s_2^2(4 - 6s_3^2) \neq 0$$

bağıntısına sahip bir dizinin terimleri $s_{-1} = -1, s_0 = 0, s_1 = 1, s_2, s_3, s_4$ ve $i \neq j$ iken $s_i \neq s_j$ ile verilsin. g_1 ve g_2 (5.2.4) ile tanımlanırken, ya $\frac{g_1(s_2,s_3)}{h(s_2,s_3)^2}$ ya da $\frac{g_2(s_2,s_3)}{h(s_2,s_3)^3}$ tamsayı değildir. Bu durumda $-1 \leqslant i \leqslant 4$ ve s_i, $E_d(\mathbb{Q})$'daki rasyonel noktaların x-bileşenleri iken

$$E_d : x^2 + y^2 = 1 + dx^2y^2, \qquad d \in \mathbb{Q}$$

bağıntısıyla ifade edilen sonsuz sayıda Edwards eğrisi vardır. Başka bir ifadeyle $S = \{s_i : -1 \leq i \leq 4\}$ şeklindeki bir S-dizisine sahip sonsuz sayıda Edwards eğrisi vardır (Çelik ve ark. 2019).

İspat. $d = \frac{(s_2^2-1)p^2+1}{s_2^2}$ ifadesinde p değerinin yerine yazılmasıyla

$$\begin{aligned}(-t^2s_2^2 + s_3^2 - s_2^2s_3^2 + t^2s_2^2s_3^2)^2 d =& (s_3^4 - 2s_2^2s_3^4 + s_2^4s_3^4) + (4s_3^2 - 8s_2^2s_3^2 + 4s_2^4s_3^2 \\ & - 4s_3^4 + 8s_2^2s_3^4 - 4s_2^4s_3^4)t + (-4s_2^2 + 4s_2^4 - 4s_3^2 \\ & + 14s_2^2s_3^2 - 10s_2^4s_3^2 + 4s_3^4 - 10s_2^2s_3^4 + 6s_2^4s_3^4)t^2 \\ & + (4s_2^2 - 4s_2^4 - 8s_2^2s_3^2 + 8s_2^4s_3^2 + 4s_2^2s_3^4 \\ & - 4s_2^4s_3^4)t^3 + (s_2^4 - 2s_2^4s_3^2 + s_2^4s_3^4)t^4\end{aligned}$$

olur. Böylece s_2 ve s_3 sabit değerleri için $d \in \mathbb{Q}(t)$ olur.

Şimdi s_4'ün E_d'deki bir rasyonel noktanın x-bileşeni iken t'nin sonsuz çoklukta değerinin var olduğunu göstereceğiz. Aslında t'nin pozitif Mordell-Weil rankına sahip eliptik eğri üzerindeki rasyonel bir noktanın x-bileşeni olarak seçilebileceğini göstereceğiz. Dolayısıyla t için mümkün olan değerlerin sonsuz sayıda olduğunu göstereceğiz. $(s_4, r), E_d$

üzerinde bir nokta olsun. Bu durumda

$$r^2 = \frac{s_4^2 - 1}{s_4^2 d - 1} = (A_0 + A_1 t + A_2 t^2 + A_3 t^3 + A_4 t^4)/B(t)^2, \tag{5.2.3}$$

olur. Burada $A_i \in \mathbb{Z}$ ve $B(t) = -t^2 s_2^2 + t^2 s_2^2 s_3^2 + s_3^2 - s_2^2 s_3^2$ olup $A_0 + A_1 t + A_2 t^2 + A_3 t^3 + A_4 t^4$ rasyonel kare olmak zorundadır.

Buradan

$$z^2 = A_0 + A_1 t + A_2 t^2 + A_3 t^3 + A_4 t^4$$

bağıntısına sahip C eliptik eğrisi elde edilir.

$$(t, z) = \big(0, s_3^2(s_2^2 - 1)\big)$$

noktası da bu eğri üzerindedir. Bu eğri Teorem 2.3.5'e göre $E_{I,J} : y^2 = x^3 - 27Ix - 27J$ Weierstrass denklemi ile tanımlanan eliptik eğriye izomorftur. Ayrıca bu eğri

$$P = \big(-12(-1 + s_2^2)(-1 + s_3^2)(-3 + s_2^2 + s_3^2), -216(-1 + s_2^2)^2(-1 + s_3^2)^2\big)$$

rasyonel noktasına sahiptir. $3P$ noktasının koordinatları ise rasyonel fonksiyonlardır. (2.5.1)-(2.5.3)'teki bağıntılar yardımıyla

$$3P = \left(\frac{g_1(s_2, s_3)}{h(s_2, s_3)^2}, \frac{g_2(s_2, s_3)}{h(s_2, s_3)^3}\right), \qquad g_1, g_2 \in \mathbb{Q}[s_2, s_3] \tag{5.2.4}$$

ve

$$h(s_2, s_3) = -3 + 4s_3^2 + s_2^4 s_3^4 + s_2^2(4 - 6s_3^2)$$

şeklindedir. Böylece $h(s_2, s_3) \neq 0$ ve $g_1/h^2 \notin \mathbb{Z}$ veya $g_2/h^3 \notin \mathbb{Z}$ olduğu sürece Teorem 2.6.1 (Nagell-Lutz teoremi)'e göre $3P$ noktası sonsuz mertebeli bir noktadır. Böylece P'de sonsuz mertebeli bir noktadır. Buradan da $E_{I,J}$'nin Mordell-Weil rankının pozitif olduğu görülür. C, $E_{I,J}$'ye izomorf olduğundan da C eğrisi pozitif Mordell-Weil rankına sahiptir. Bu yüzden (5.2.3)'te bir d değeri yerine konulduğunda sonsuz sayıda

$(t, z) \in C(\mathbb{Q})$ rasyonel noktası bulunur. Böylece yukarıda belirtilen rasyonel noktalara sahip olan bir E_d Edwards eğrisi vardır. Önerme 5.2.1 gereği sonsuz sayıdaki bu eğrilerden biri diğerine $\mathbb{Q}$'da izomorf değildir. ■

5.3 4 Uzunluklu Dizileri Bulunduran Bükülmüş (twisted) Edwards Eğrileri

(3.4.1) formuyla tanımlı $E_{a,d}$ bükülmüş Edwards eğrisini göz önüne alalım. $(x, y) = (0, \pm 1) \in E_{a,d}(\mathbb{F})$ olduğu açıktır. $\{u_0 = 0, u_1, u_2, u_3\} \subset \mathbb{F}$ dizisi verilsin. Burada $i \neq j$ iken $u_i \neq u_j$ ise S, $E_{a,d}$ eğrisi üzerindeki rasyonel noktaların x-bileşenlerinin dizisine sahip sonsuz sayıda $E_{a,d}$ bükülmüş Edwards eğrisi olduğu ispatlanır.

Varsayalım ki $E_{a,d}(\mathbb{F})$ kümesindeki bir noktanın x-bileşeni u_1 olsun. O zaman bazı $i \in \mathbb{F}$ için $y^2 = \dfrac{au_1^2 - 1}{u_1^2 d - 1}$ ya da $u_1^2 d - 1 = (au_1^2 - 1)i^2$ olur.

Şimdi u_2, $E_{a,d}(k)$ eğrisi üzerinde bir noktanın x-bileşeni ise $y^2 = \frac{au_2^2 - 1}{u_2^2 d - 1}$ ya da $u_2^2 d - 1 = (au_2^2 - 1)j^2$ olur. Böylece

$$d = \frac{(au_1^2 - 1)i^2 + 1}{u_1^2} = \frac{(au_2^2 - 1)j^2 + 1}{u_2^2}$$

olup

$$u_2^2 \left[(au_1^2 - 1)i^2 + 1\right] - u_1^2 \left[(au_2^2 - 1)j^2 + 1\right] = 0,$$

kuadratik yüzeyi elde edilir ve $(i, j) = (1, 1)$ bu yüzey üzerinde bir noktadır. Bu kuadratik yüzey üzerindeki noktalar

$$\begin{aligned} i &= \frac{-au_1^2u_2^2 + u_2^2 + 2tau_1^2u_2^2 - 2tu_1^2 - at^2u_1^2u_2^2 + u_1^2t^2}{au_1^2u_2^2 - u_2^2 - at^2u_1^2u_2^2 + u_1^2t^2}, \\ j &= \frac{-2atu_1^2u_2^2 + 2tu_2^2 + at^2u_1^2u_2^2 - u_1^2t^2 + au_1^2u_2^2 - u_2^2}{au_1^2u_2^2 - u_2^2 - at^2u_1^2u_2^2 + u_1^2t^2} \end{aligned} \tag{5.3.1}$$

parametrik bağıntıları ile verilir. Şimdi aşağıdaki sonucu verelim.

Teorem 5.3.1 $\mathbb{Z}$'de

$$\begin{aligned}h(u_1,u_2) =& -27-72u_1^2+36u_1^4+18u_1^2u_2^2-12u_1^4u_2^2-18u_2^4+12u_1^2u_2^4+u_1^4u_2^4\\&-2u_1^2u_2^6+u_2^8+a(36u_1^2-12u_1^4-24u_1^2(-3+u_1^2)+36u_2^2+72u_1^2u_2^2\\&-24u_1^4u_2^2-12u_1^2u_2^4+4u_1^4u_2^4-4(-3+u_1^2)u_2^6)+a^2(-144u_1^2u_2^2\\&+36u_1^4u_2^2+18u_2^4-36u_1^2u_2^4+4u_1^4u_2^4+2u_1^2u_2^6-2u_2^8)+a^3(36u_1^2u_2^4\\&+4(-3+u_1^2)u_2^6)+a^4u_2^8 \qquad (5.3.2)\end{aligned}$$

bağıntısına sahip bir dizinin terimleri $u_0=0, u_1, u_2, u_3$ ve $i\neq j$ iken $u_i\neq u_j$ ile verilsin. g_1 ve g_2 (5.3.4) ile tanımlanırken, $h(u_1,u_2)\neq 0$ ve g_1/h^2 ya da g_2/h^3 tamsayı olmasın.

Bu durumda $0\leq i\leq 3$ ve u_i, $E_{a,d}(\mathbb{Q})$'daki rasyonel noktaların x-bileşenleri iken

$$E_{a,d}: ax^2+y^2=1+dx^2y^2, \quad d\in\mathbb{Q},\ a\in\mathbb{Q}^*$$

bağıntısıyla ifade edilen sonsuz sayıda bükülmüş Edwards eğrisi vardır. Başka bir deyişle $S=\{u_i: 0\leq i\leq 3\}$ şeklindeki bir S-dizisine sahip sonsuz sayıda bükülmüş Edwards eğrisi vardır (Çelik ve ark. 2019).

İspat. $d=\dfrac{(au_1^2-1)i^2+1}{u_1^2}$ ifadesinde i'nin yerine (5.3.1)'teki formül yazılırsa

$$\begin{aligned}(au_1^2u_2^2-u_2^2-at^2u_1^2u_2^2+u_1^2t^2)^2d =&(u_1^4a^3u_2^4-2u_1^4a^2u_2^2+u_1^4a)t^4+(-8au_1^2u_2^2\\&+4u_1^2+4u_1^2a^2u_2^4-4u_1^4a-4u_1^4a^3u_2^4\\&+8u_1^4a^2u_2^2)t^3+(-4u_1^2-10u_1^2a^2u_2^4+14au_1^2u_2^2\\&+6u_1^4a^3u_2^4-4u_2^2-10u_1^4a^2u_2^2+4u_1^4a+4au_2^4)t^2\\&+(4u_2^2+8u_1^2a^2u_2^4-8au_1^2u_2^2+4u_1^4a^2u_2^2-4au_2^4\\&-4u_1^4a^3u_2^4)t+u_1^4a^3u_2^4-2u_1^2a^2u_2^4+au_2^4\end{aligned}$$

olur. Böylece u_1 ve u_2 sabit değerleri için $d\in\mathbb{Q}(t)$ olur.

Şimdi u_3'ün $E_{a,d}$ eğrisindeki bir rasyonel noktanın x-bileşeni iken t'nin sonsuz çok-

lukta değerinin var olduğunu göstereceğiz. Aslında t'nin pozitif Mordell-Weil rankına sahip eliptik eğri üzerindeki rasyonel bir noktanın x-bileşeni olarak seçilebileceğini göstereceğiz. Dolayısıyla t için mümkün olan değerlerin sonsuz sayıda olduğunu göstereceğiz. (u_3, ℓ), $E_{a,d}$ üzerinde bir nokta olsun. Bu durumda

$$\ell^2 = \frac{au_3^2 - 1}{du_3^2 - 1} = (C_0 + C_1 t + C_2 t^2 + C_3 t^3 + C_4 t^4)/D(t)^2 \tag{5.3.3}$$

olur. Burada $C_i \in \mathbb{Q}$ ve $D(t) = au_1^2u_2^2 - u_2^2 - at^2u_1^2u_2^2 + u_1^2t^2$ rasyonel kare olmak zorundadır.

Buradan

$$z^2 = C_0 + C_1 t + C_2 t^2 + C_3 t^3 + C_4 t^4$$

bağıntısına sahip C' eliptik eğrisi elde edilir.

$$(t, z) = \left(0, u_2^2(au_1^2 - 1)\right)$$

noktası da bu eğri üzerindedir. Bu eğri Teorem 2.3.5'e göre

$$\begin{aligned} I &= 12C_0C_4 - 3C_1C_3 + C_2^2, \\ J &= 72C_0C_2C_4 + 9C_1C_2C_3 - 27C_1^2C_4 - 27C_0C_3^2 - 2C_2^3 \end{aligned}$$

olmak üzere $E_{I,J} : y^2 = x^3 - 27Ix - 27J$ Weierstrass denklemi ile tanımlanan eliptik eğriye izomorftur. Ayrıca bu eğri

$$Q = (-12(-1 + au_2^2)(-1 + au_1^2)(-3 + au_2^2 + u_1^2), -216(-1 + au_2^2)^2(-1 + au_1^2)^2)$$

rasyonel noktasına sahiptir.

Aslında

$$3Q = \left(\frac{g_1(u_1, u_2)}{h(u_1, u_2)^2}, \frac{g_2(u_1, u_2)}{h(u_1, u_2)^3}\right), \qquad g_1, g_2 \in \mathbb{Q}[u_1, u_2] \tag{5.3.4}$$

olup

$$\begin{aligned}h(u_1,u_2) = &-27-72u_1^2+36u_1^4+18u_1^2u_2^2-12u_1^4u_2^2-18u_2^4+12u_1^2u_2^4+u_1^4u_2^4\\&-2u_1^2u_2^6+u_2^8+a(36u_1^2-12u_1^4-24u_1^2(-3+u_1^2)+36u_2^2+72u_1^2u_2^2\\&-24u_1^4u_2^2-12u_1^2u_2^4+4u_1^4u_2^4-4(-3+u_1^2)u_2^6)+a^2(-144u_1^2u_2^2\\&+36u_1^4u_2^2+18u_2^4-36u_1^2u_2^4+4u_1^4u_2^4+2u_1^2u_2^6-2u_2^8)+a^3(36u_1^2u_2^4\\&+4(-3+u_1^2)u_2^6)+a^4u_2^8\end{aligned}$$

şeklindedir.

Bu nedenle $h(u_1,u_2)\neq 0$ ve $g_1/h^2\notin\mathbb{Z}$ ya da $g_2/h^3\notin\mathbb{Z}$ olduğu sürece $E_{I,J}$ üzerindeki Q noktası, sonsuz mertebeli olduğundan pozitif Mordell-Weil rankına sahiptir. C', $E_{I,J}$ izomorf olduğundan C' eğrisi de pozitif Mordell-Weil ranka sahiptir.

Bu yüzden (5.3.3)'de bir d değeri yerine konulduğunda sonsuz sayıda $(t,z)\in C'(\mathbb{Q})$ rasyonel noktası bulunur. Böylece yukarıda belirtilen rasyonel noktalara sahip olan bir $E_{a,d}$ bükülmüş Edwards eğrisi vardır. Önerme 5.2.1 gereği sonsuz sayıdaki bu eğrilerden biri diğerine $\mathbb{Q}$'da izomorf değildir. ■

Uyarı 5.3.2 $(0,-1),(0,1)$ bükülmüş Edwards eğrisi üzerinde herhangi bir rasyonel nokta olduğundan $\mathbb{Z}$'de dizinin terimleri $u_{-1}=-1$, $u_1=1$, u_2, u_3, u_4 ve $i\neq j$ iken $u_i\neq u_j$ ile verilsin. Bu durumda $i\in\{-1,1,2,3,4\}$ ve u_i, $E_{a,d}(\mathbb{Q})$'daki rasyonel noktaların y-bileşenleri olduğundan sonsuz sayıda bükülmüş Edwards eğrisi vardır (Çelik ve ark. 2019).

5.4 5 Uzunluklu Dizileri Bulunduran Huff Eğrileri

(3.6.4) formuyla verilen $H_{a,b}$ Huff eğrisini göz önüne alalım. $(x,y)=(-1,\pm1),(0,0)$, $(1,\pm1)$ noktaları $H_{a,b}(\mathbb{F})$ kümesine aittir.

Dizinin terimleri $s_{-1}=-1$, $s_0=0$, $s_1=1$, s_2, s_3 ve $i\neq j$ iken $s_i\neq s_j$ ile verilsin. Bu durumda $-1\leq i\leq 3$ ve s_i, $H_{a,b}(\mathbb{F})$ eğrisi üzerindeki rasyonel noktaların x-bileşenleri olduğundan sonsuz sayıda Huff eğrisi vardır.

Varsayalım ki (s_2, p) ve (s_3, q), $H_{a,b}$ üzerinde iki nokta olsun. Böylece

$$as_2(p^2-1) = bp(s_2^2-1), \tag{5.4.1}$$

$$as_3(q^2-1) = bq(s_3^2-1) \tag{5.4.2}$$

elde edilir. (5.4.1) ve (5.4.2) eşitlikleri ile

$$\frac{s_2(p^2-1)}{s_3(q^2-1)} = \frac{p(s_2^2-1)}{q(s_3^2-1)}$$

bulunur. Böylece

$$C' : Apq^2 - Ap - Bqp^2 + Bq = 0$$

eğrisini göz önüne almalıyız. Burada $A = s_3s_2^2 - s_2$ ve $B = s_2s_3^2 - s_2$ dir. Yukarıdaki eşitlikte her iki taraf q^3 ile bölünürse

$$A\frac{p}{q} - A\frac{p}{q}\frac{1}{q^2} - B(\frac{p}{q})^2 + B\frac{1}{q^2} = 0$$

elde edilir. Burada $x = \frac{p}{q}$ ve $y = \frac{1}{q^2}$ yazıldığında

$$Ax - Axy - Bx^2 + By = 0$$

ikinci derece eğrisi elde edilir. $(x, y) = (1, 1)$ noktası bu eğri üzerindedir. Bu kuadratik yüzeyin rasyonel çözümleri

$$x = \frac{Bt - B}{At + B}, \tag{5.4.3}$$

$$y = \frac{At(1-t) + B(1-t)^2}{At + B} \tag{5.4.4}$$

parametrik bağıntıları ile verilir. Böylece aşağıdaki sonuç elde edilir.

Teorem 5.4.1 $\mathbb{Z}$'de $A = s_3s_2^2 - s_2$ ve $B = s_2s_3^2 - s_2$ olmak üzere

$$h = -4 + A^2 - 3AB + B^2 \neq 0$$

bağıntısına sahip bir dizinin terimleri $s_{-1} = -1, s_0 = 0, s_1 = 1, s_2, s_3$, ve $m \neq n$ iken $s_m \neq s_n$ ile verilsin. g_1 ve g_2 (5.4.5) denklemi ile tanımlanırken ya $\frac{g_1}{h^2}$ ya da $\frac{g_2}{h^3}$ tamsayı olmasın. Bu durumda $-1 \leq m \leq 3$ ve s_m, $H_{a,b}(\mathbb{Q})$'daki rasyonel noktaların x-bileşenleri iken

$$H_{a,b} : ax(y^2 - 1) = by(x^2 - 1) \qquad a, b \in \mathbb{Q}, \quad a^2 \neq b^2$$

bağıntısıyla ifade edilen sonsuz sayıda Huff eğrisi vardır. Başka bir deyişle $S = \{s_i : -1 \leq i \leq 3\}$ şeklindeki bir S-dizisine sahip sonsuz sayıda Huff eğrisi vardır (Çelik ve ark. 2019).

İspat. (5.4.3) ve (5.4.4) eşitlikleri kullanılarak

$$\begin{aligned} p^2 &= \frac{x^2}{y} = \frac{B^2(-1+t)}{(B(-1+t) - At)(B + At)}, \\ q^2 &= \frac{1}{y} = \frac{(B + At)}{(-1+t)(B(-1+t) - At)} \end{aligned}$$

elde edilir. Her iki durumda da $(B + At)(-1 + t)(B(-1 + t) - At)$ ifadesinin bir kare olması ya da başka bir ifade ile $(t, z) = (0, B)$ noktasına sahip C'' ile tanımlanan

$$z^2 = (At + B)(t - 1)(t(B - A) - B)$$

eliptik eğrisi üzerindeki rasyonel bir noktanın x-bileşeninin t olması gerekir. Teorem 2.3.5'e göre bu eğri, $A(B - A)t = X$ ve $A(B - A)z = Y$ iken

$$Y^2 = X^3 + ((B - A)^2 - AB)X^2 - 2AB(B - A)^2X + A^2B^2(B - A)^2$$

eliptik eğrisine izomorftur. Ayrıca bu eğri üzerindeki bir rasyonel nokta

$$R = (X, Y) = (0, AB(B - A))$$

ile verilir. (2.5.1)- (2.5.3) formülleri kullanılarak $3R$ aşağıdaki gibi olur.

$$3R = \left(\frac{g_1(A,B)}{h(A,B)^2}, \frac{g_2(A,B)}{h(A,B)^3} \right) \tag{5.4.5}$$

burada $h(A,B) = -4 + A^2 - 3AB + B^2$ olur. Burada Teorem 5.3.1'teki benzer adımlar kullanılarak ispat tamamlanır. ■

5.5 4 Uzunluklu Dizileri Bulunduran Genel Huff Eğrileri

(3.9.1) formuyla verilen $G_{a,b}$ genel Huff eğrisini göz önüne alalım.
$(x,y) = (0,0) \in G_{a,b}(\mathbb{F})$ olduğundan $\mathbb{F}$'de dizinin terimleri $u_0 = 0, u_1, u_2, u_3$, ve $i \neq j$ iken $u_i \neq u_j$ ile verilsin. Bu durumda $i \in \{0,1,2,3\}$ ve u_i, $G_{a,b}(\mathbb{F})$'deki rasyonel noktaların x-bileşenleri olduğundan sonsuz sayıda genel Huff eğrisi vardır. u_1, $G_{a,b}(\mathbb{F})$'deki bir noktanın x-bileşeni ise

$$\frac{ay^2 - 1}{y} = \frac{bu_1^2 - 1}{u_1}$$

ya da

$$\frac{a - i^2}{i} = \frac{bu_1^2 - 1}{u_1}, \quad i \in k \tag{5.5.1}$$

elde edilir.

Benzer şekilde u_2, $G_{a,b}(\mathbb{F})$'deki bir noktanın x-bileşeni ise

$$\frac{ay^2 - 1}{y} = \frac{bu_2^2 - 1}{u_2}$$

ya da

$$\frac{a - j^2}{j} = \frac{bu_2^2 - 1}{u_2}, \quad j \in \mathbb{F} \tag{5.5.2}$$

elde edilir. (5.5.1) ve (5.5.2) ile

$$a = \frac{(bu_1^2 - 1)i + u_1 i^2}{u_1} = \frac{(bu_2^2 - 1)j + u_2 j^2}{u_2}$$

bulunur. Böylece

$$S : Ai^2 + Bj^2 + Ciz + Djz = 0 \tag{5.5.3}$$

eğrisini göz önüne almalıyız. Burada $A = -u_1u_2$, $B = u_1u_2$, $C = -u_1^2u_2b + u_2$, $D = bu_1u_2^2 - u_1$'dir. Bu durumda $S \subset \mathbb{P}^2$ üzerindeki $P = (i : j : z) = (0 : 0 : 1)$ ve $Q = (p : q : r)$ noktalarından geçen

$$mP + nQ = (np : nq : m + nr)$$

doğrusunu göz önüne alalım. S yüzeyi ile $mP + nQ$ doğrusunun kesişimi bize

$$n^2(Ap^2 + Bq^2 + Cpr + Dqr) + mn(Cp + Dq) = 0$$

ikinci dereceden denklemini verir. P ve Q noktalarının S üzerinde oluşu kullanılarak (5.5.3)'nin $(i : j : z)$ çözümleri

$$\begin{aligned} i &= np = Cp^2 + Dpq, \\ j &= nq = Cpq + Dq^2, \\ z &= m + nr = -Ap^2 - Bq^2 \end{aligned}$$

formülleri ile elde edilir. Şimdi aşağıdaki sonucu elde ederiz.

Teorem 5.5.1 $\mathbb{F}$'de bir dizinin terimleri $u_0 = 0$, u_1, u_2 ve u_3 olsun ve $i \neq j$ iken $u_i \neq u_j$ ile verilsin. $0 \leq i \leq 3$ ve u_i, $G_{a,b}(\mathbb{F})$ kümesindeki rasyonel noktaların x-bileşenleri olmak üzere

$$G_{a,b} : x(ay^2 - 1) = y(bx^2 - 1), \qquad a, b \in \mathbb{F}, \quad ab(a - b) \neq 0$$

bağıntısıyla ifade edilen sonsuz sayıda genel Huff eğrisi vardır. Diğer bir deyişle $S = \{u_i : 0 \leq i \leq 3\}$ şeklindeki bir S-dizisine sahip sonsuz çoklukta genel Huff eğrisi vardır (Çelik ve ark. 2019).

İspat. $a = \dfrac{(bu_1^2 - 1)i + u_1 i^2}{u_1}$ ifadesinde i'nin değeri yerine yazıldığında

$$\begin{aligned} a =& u_2^2 \left(bu_1{}^2 - 1\right)^2 p^4 - 2\, u_1 u_2 \left(bu_2{}^2 - 1\right) \left(bu_1{}^2 - 1\right) p^3 q + u_1{}^2 \left(bu_2{}^2 - 1\right)^2 p^2 q^2 \\ & - \frac{u_2 \left(bu_1{}^2 - 1\right)^2}{u_1} p^2 + \left(bu_2{}^2 - 1\right) \left(bu_1{}^2 - 1\right) pq \end{aligned}$$

bulunur. Şimdi $(u_3, \ell) \in G_{a,b}(\mathbb{F})$ olduğunu varsayalım. Böylece

$$\begin{aligned} & pu_3 \left(bp^2 u_1{}^3 u_2 - bpq u_1{}^2 u_2{}^2 - p^2 u_1 u_2 + pq u_1{}^2 - bu_1{}^2 + 1\right) \\ & \left(bpu_1{}^2 u_2 - bqu_1 u_2{}^2 - pu_2 + qu_1\right) \ell^2 - u_1 \left(bu_3{}^2 - 1\right) \ell - u_1 u_3 = 0 \end{aligned}$$

bulunur. Burada $T = 1/\ell$ olarak seçilirse

$$\begin{aligned} & Z^2(b^2 p^4 u_1^5 u_2^2 u_3 - 2bp^4 u_1^3 u_2^2 u_3 - b^2 p^2 u_1^4 u_2 u_3 + p^4 u_1 u_2^2 u_3 + 2bp^2 u_1^2 u_2 u_3 \\ & - p^2 u_2 u_3) + qZ(-2b^2 p^3 u_1^4 u_2^3 u_3 + 2bp^3 u_1^4 u_2 u_3 + 2bp^3 u_1^2 u_2^3 u_3 + b^2 p u_1^3 u_2^2 u_3 \\ & - 2p^3 u_1^2 u_2 u_3 - bpu_1^3 u_3 - bpu_1 u_2^2 u_3 + pu_1 u_3) + q^2 p^2 u_1^3 u_3 (bu_2^2 - 1)^2 \\ & - TZu_1 \left(bu_3{}^2 - 1\right) - T^2 u_1 u_3 = 0 \end{aligned}$$

eğrisi elde edilir. $P = (q : T : Z) = (1 : 0 : u_1(-1+bu_2^2)/pu_2(-1+bu_1^2))$ noktası bu eğri üzerinde bulunur. Böylece yukarıdaki kuadratik yüzeyin tüm rasyonel çözümlerini parametrik olarak bulabiliriz. Varsayalım ki $Q = (q_1 : q_2 : q_3)$ kuadratik yüzey üzerinde bir nokta olsun. Kuadratik yüzey ile $dP + eQ$ doğrusunun kesişiminden bu rasyonel çözümler bulunabilir. Ayrıca buradan

$$\begin{aligned} d =& pu_2(bu_1{}^2 - 1)(q_3{}^2 b^2 p^4 u_1{}^5 u_2{}^2 u_3 - 2q_3{}^2 bp^4 u_1{}^3 u_2{}^2 u_3 \\ & - q_3{}^2 b^2 p^2 u_1{}^4 u_2 u_3 + q_3{}^2 p^4 u_1 u_2{}^2 u_3 + 2q_3{}^2 bp^2 u_1{}^2 u_2 u_3 \\ & - q_3{}^2 p^2 u_2 u_3 - u_1 q_2 q_3 b u_3{}^2 + u_1 q_2 q_3 + p^2 u_1{}^3 u_3 q_1{}^2 b^2 u_2{}^4 \\ & - 2p^2 u_1{}^3 u_3 q_1{}^2 b u_2{}^2 + p^2 u_1{}^3 u_3 q_1{}^2 - 2q_1 q_3 b^2 p^3 u_1{}^4 u_2{}^3 u_3 \\ & + 2q_1 q_3 bp^3 u_1{}^4 u_2 u_3 + 2q_1 q_3 bp^3 u_1{}^2 u_2{}^3 u_3 + q_1 q_3 b^2 p u_1{}^3 u_2{}^2 u_3 \end{aligned}$$

$$- 2q_1q_3p^3{u_1}^2u_2u_3 - q_1q_3bp{u_1}^3u_3 - q_1q_3bpu_1{u_2}^2u_3 + q_1q_3pu_1u_3$$
$$- u_1u_3{q_2}^2),$$

$$\begin{aligned} e =& u_1(b{u_2}^2 - 1)(-p{u_1}^3u_3q_1b^2{u_2}^2 + p^2u_3q_3u_2b^2{u_1}^4 + pu_1u_3q_1b{u_2}^2 \\ & - 2p^2u_3q_3u_2b{u_1}^2 + p{u_1}^3u_3q_1b + u_1q_2b{u_3}^2 + p^2u_3q_3u_2 - u_1q_2 \\ & - pu_1u_3q_1) \end{aligned}$$

bağıntıları elde edilir. Böylece ispat tamamlanır. ■

6. BİRİM ÇEMBER ÜZERİNDE GEOMETRİK DİZİ OLUŞTURAN RASYONEL NOKTALAR

6.1 Giriş

İlk olarak konikler ve birim çember hakkında bilinen bazı gerçekleri hatırlatalım. xy-düzlemindeki bir noktanın koordinatları rasyonel sayı ise bu nokta *rasyonel nokta* olarak adlandırılır. Eğer $a, b, c \in \mathbb{Q}$ olmak üzere

$$ax + by + c = 0$$

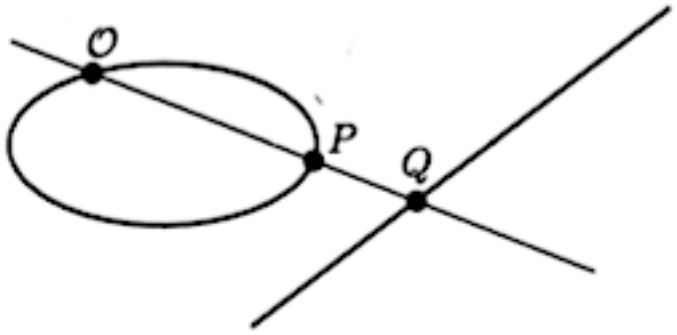
denklemi ise *rasyonel doğru* olarak adlandırılır. Şimdi iki rasyonel noktamız varsa bu noktalardan geçen doğrunun rasyonel bir doğru olduğu açıktır. $a, b, c, d, e, f \in \mathbb{Q}$ olmak üzere

$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$

polinom denklemi ile verilen düzlem eğri *rasyonel konik* olarak adlandırılır. Şimdi şu soruyu soralım: Rasyonel bir doğru ile rasyonel bir konik kesişirse kesişim noktaları rasyonel olur mu? Bazı örneklerde cevabın genelde "hayır"olduğu görülebilir. Eğer analitik geometri kullanırsak rasyonel konik ile rasyonel doğrunun kesişiminden x'e bağlı ikinci dereceden bir denklem elde ederiz. Bu denklemin katsayıları da rasyonel olacaktır. Böylece iki kesişim noktasının rasyonel olması için gerek ve yeter şart ikinci derece denklemin köklerinin rasyonel olmasıdır. Genelde kökler eşlenik ikinci dereceden irrasyoneller olabilir. Ancak bu noktalardan biri rasyonel ise diğeri de rasyoneldir. O halde şu doğrudur:

Rasyonel katsayılı ikinci dereceden bir denklemin bir rasyonel kökü varsa diğeri de rasyoneldir. Bu basit fikir bir konik üzerindeki rasyonel noktaları tamamen ifade etmeyi mümkün kılar. Bir rasyonel konik verilirse ilk soru bu konik üzerindeki noktaların rasyonel olup olmayacağıdır. Ancak varsayalım ki rasyonel konik üzerinde bir $\mathcal{O}$ noktası bilinsin. O zaman diğer noktaları da bulmak kolaydır. Konik üzerindeki $\mathcal{O}$ noktasından geçen bir

rasyonel doğru çizelim ve $\mathcal{O}$ noktasından geçen doğru üzerinde $\mathcal{O}$ noktasının koniğe göre izdüşümünü alalım. (Burada $\mathcal{O}$ noktasının doğru üzerinde izdüşümünü almak için $\mathcal{O}$'da koniğe teğet olan doğru kullanılır.)



Şekil 6.1.1. Bir doğru üzerinde koniğin izdüşümü

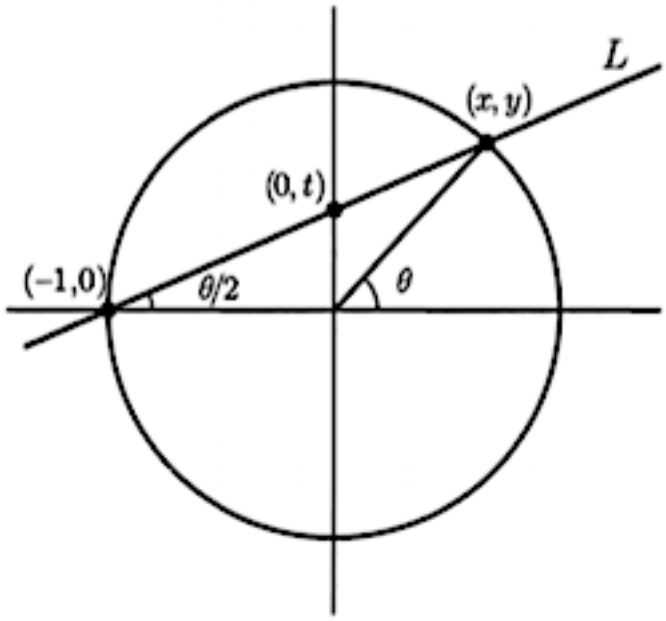
(Bu soruya cevap olarak; genel bir metot olan Hasse-Minkowski teoreminin ifadesi şöyledir: "Çeşitli sayıda değişkene sahip ikinci dereceden homojen bir polinomun tam sayılarda (hepsi birden sıfır olmayan) çözülebilir olması için gerek ve yeter şart bu denklemin reel sayılarda ve her bir p asalı için $p - sel$ sayılarda çözülebilir olmasıdır." Bu teoremin bazı uygulamaları için de Gouvêa'nın 3.5 bölümüne bakılabilir.)

Doğru koniği iki noktada keser ve konik üzerindeki her P noktası için doğru üzerinde bir Q noktası elde edilir. Tersine doğru üzerindeki her Q noktası için Q noktasını $\mathcal{O}$ noktasına birleştirerek konik üzerinde P noktası elde edilir. (Şekil 6.1.1.'e bakınız) Böylece konik ve doğru üzerindeki noktalar arasında bire-bir karşılık gelme durumu elde edilir. Bu durumda şunu görüyoruz ki konik üzerindeki P noktası rasyonel koordinatlara sahipse Q noktası da rasyonel koordinatlara sahiptir. Tersine Q rasyonel ise $\mathcal{O}$ rasyonel varsayılacağından P ve Q'dan geçen doğru koniği iki noktada keser ve bunlardan biri rasyoneldir. Böylece diğer nokta da rasyonel olur. Bu durumda konik üzerindeki rasyonel noktalar doğru üzerindeki rasyonel noktalara bire-bir karşılık gelir. Elbette doğru üzerindeki rasyonel noktalar bazı parametrelerin rasyonel değerleri olarak ifade edilebilir.

Şimdi bu prosedürü konik ailesinin bir üyesi olan

$$x^2 + y^2 = 1$$

birim çember üzerinde gerçekleştirelim. $(-1, 0)$ noktasının y ekseni üzerinde izdüşümünü alacağız. Bu nokta $(0, t)$ olsun.



Şekil 6.1.2. Çember denkleminin rasyonel parametrizasyonu

Eğer x ve y'yi biliyorsak, t'yi kolayca elde edebiliriz. $(-1, 0)$ ve $(0, t)$ noktalarından geçen L doğrusunun denklemi $y = t(1 + x)$'tir. (x, y) noktası L doğrusu ve çember üzerinde olsun. Böylece

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

bağıntısı elde edilir. t'nin sabit bir değeri için bu ikinci dereceden bir denklemdir. Bu denklemin kökleri çember ile L doğrusunun kesişim noktalarının apsisleridir. $x = -1$ bir köktür, çünkü $(-1, 0)$ noktası hem L hem de çember üzerindedir. Diğer kökü bulmak için denklemin her iki tarafını $1 + x$ çarpanı ile sadeleştirelim. Buradan $1 - x = t^2(1 + x)$ elde

edilir. $y = t(1 + x)$ eşitliğini kullanarak

$$x = \frac{1 - t^2}{1 + t^2} \quad y = \frac{2t}{1 + t^2} \tag{6.1.1}$$

formülleri elde edilir. Bu formüller çemberin rasyonel parametrizasyonudur. Ve şimdi yukarıdaki iddia bu formüllerden açıkça anlaşılmaktadır. Yani x ve y rasyonel sayılar ise t rasyonel sayı olacaktır. Tersine, eğer t bir rasyonel sayı ise o zaman bu formüllerden x ve y koordinatlarının rasyonel sayılar olacağı açıktır. Böylece (6.1.1)'de t yerine keyfi bir rasyonel sayı alarak çember üzerindeki rasyonel noktalar bulunur. Bu bize $(-1, 0)$ hariç tüm noktaları verecektir (eğer $(-1, 0)$ elde etmek istiyorsak, t'nin yerine ∞ koymak gerekir). Birim çember üzerinde $(-1, 0)$ hariç tüm noktalar bulunur.

Son zamanlarda bir çok yazar tarafından düzlem eğrilerinin çeşitli aileleri üzerinde geometrik dizilerin varlığı incelendi. İlk çalışma 2013'te Bremner ve Ulas tarafından yapıldı. Yazarlar ilk olarak, $n = 4$ uzunluklu S-geometrik dizilerini içeren (x-bileşeni açısından) sonsuz çoklukta ikili izomorf olmayan $C : y^2 = ax^n + b$ hipereliptik eğrilerinin var olduğunu gösterdiler. İkinci olarak da aynı yazarlar tarafından 5 noktanın üzerinde geometrik dizi oluşturduğu $y^2 = ax + b$ parabollerinin sonsuz çoklukta olduğu gösterildi (Bremner ve Ulas 2013). Bölüm 5.1'de geometrik dizileri bulunduran eliptik eğrilerin diğer modelleri ile ilgili sonuçlar ifade edildi. 2016'da Choudhry ve Juyal tarafından $n = 3$ uzunluklu S-aritmetik dizilerini içeren (x-bileşeni açısından) sonsuz çoklukta birim çember olduğu ve bu özellikteki üç noktanın birim çemberin birinci bölgesinde bulunduğu gösterildi (Choudhry ve Juyal 2016). Ancak yazarlar birim çember üzerinde dört rasyonel noktanın aritmetik dizi oluşturacak şekilde bulunup bulunmayacağını da açık problem olarak bıraktılar. Ertesi yıl Ciss ve Moody tarafından konikler üzerindeki aritmetik diziler göz önüne alındı (Ciss ve Moody 2017a). Bu yazarlar çalışmada ilk olarak $n = 3$ uzunluklu aritmetik dizileri (x-bileşenleri açısından) bulunduran sonsuz çoklukta $x^2 + y^2 = 1$ birim çemberi olduğunu Choudhry ve Juyal'in çalışmasından farklı bir yaklaşımla gösterdiler. Ayrıca bu yaklaşımı kullanarak $n = 3$ uzunluklu aritmetik dizileri bulunduran

(x-bileşenleri açısından) sonsuz çoklukta $x^2 - y^2 = 1$ birim hiperbolü olduğunu gösterdiler. İkinci olarak da aynı yazarlar tarafından $n = 8$ uzunluklu aritmetik dizileri bulunduran $ax^2 + ay^2 = 1$ koniklerinin sonsuz çoklukta olduğu ispatlandı.

Tezin bu bölümü orjinal sonuçlar içermektedir. Düzlem cebirsel eğri üzerindeki rasyonel noktaların x veya y-bileşenleri ortak çarpanı r olacak şekilde bir geometrik dizi oluşturursa düzlem cebirsel eğri üzerindeki rasyonel noktalarının dizisinin bir r-geometrik dizisi oluşturduğu söylenir.

Bu bölümde

$$C : x^2 + y^2 = 1 \tag{6.1.2}$$

birim çember denklemi üzerinde en az 3 uzunluklu r-geometrik dizilerini bulunduran sonsuz çoklukta r rasyonel sayısının varlığı ispatlanır.

6.2 Birim Çember Denklemi Üzerindeki 2 Uzunluklu Geometrik Diziler

$\mathbb{F}$ cisminde tanımlı C üzerindeki rasyonel noktaların kümesi

$$C(\mathbb{F}) = \{(x, y) : x^2 + y^2 = 1, x, y \in \mathbb{F}\} \tag{6.2.1}$$

şeklinde ifade edilir.

Tanım 6.2.1 Her $i = 2, \ldots, n$ için $\dfrac{x_i}{x_{i-1}} = r$ ise $C(\mathbb{Q})$'da $(x_1, y_1), \ldots, (x_n, y_n)$ rasyonel noktaların bir dizisi n uzunluklu bir r-geometrik dizisi oluşturur.

Yardımcı Teorem 6.2.2 $m \in \mathbb{Q}$ için $r = \dfrac{-4m}{m^2 + 2}$ olsun. $\dfrac{x_2}{x_1} = r$ olacak şekilde sonsuz çoklukta $(x_1, y_1), (x_2, y_2) \in C(\mathbb{Q})$ rasyonel nokta ikilisi vardır. Özellikle, uzunluğu 2 olan sonsuz sayıda r-geometrik dizisi vardır (Çelik ve ark. 2021).

İspat. $(x_1, y_1), (rx_1, y_2)$ noktaları $x_1^2 + y_1^2 = 1$ ve $(rx_1)^2 + y_2^2 = 1$ bağıntılarını sağlayacak şekilde olsun. $\mathbb{P}^3$'te

$$H_r : x_1^2 + y_1^2 = z^2, \qquad r^2 x_1^2 + y_2^2 = z^2$$

kuadratik yüzeylerinin kesişimini göz önüne alalım. Bölüm 2.3.4'te iki kuadratik yüzeyin kesişiminin bir eliptik eğriye karşılık gelişi ile ilgili prosedür ayrıntılı olarak ifade edilir. Bu prosedürün uygulaması MAGMA paket programının standart komutları ile kolayca yapılabilir (Bosma ve ark. 1997). Böylece MAGMA ile bu iki eğrinin kesişimine karşılık gelen Weierstrass formundaki eliptik eğri

$$E_r : y^2 = x(x-4)(x-4r^2)$$

şeklinde bulunur. Ayrıca E_r ve H_r eğrileri arasındaki $\phi_r : E_r \to H_r$ birasyonel izomorfizmi An ve ark. Teorem 3.1 (2001)'de tanımlanır.

$x = 2r^2$ seçildiğinde $y^2 = -8(r^2-2)r^4$ elde edilir. Burada $y/2r^2 = s$ alınırsa $Q : s^2 + 2r^2 = 4$ koniği elde edilir. Eğer (r_0, s_0), $Q : s^2 + 2r^2 = 4$ koniği üzerinde bir nokta ise o zaman $P_0 = (x(P_0), y(P_0)) = (2r_0^2, 2r_0^2 s_0) \in E_{r_0}(\mathbb{Q})$ sonsuz mertebeli bir noktadır.

Q koniği bir $(r, s) = (0, 2)$ rasyonel noktasına sahip olduğundan, bu koniğin tüm rasyonel parametrik çözümleri $(r, s) = (-4m/(m^2+2), 2(m^2-2)/(m^2+2))$ $(m \in \mathbb{Q})$ ile verilir. mP_0, P_0'ın m'inci katı olduğundan $C(\mathbb{Q})$'da bir r-geometrik dizisi oluşturan rasyonel noktaların x-bileşenleri x_1 ve $x_2 = rx_1$, olmak üzere $Q_m := \phi_r(mP_0) := (x_1, y_1, y_2, z) \in H_r(\mathbb{Q})$ eşitliği elde edilir. Bu da ispatı tamamlar. ■

Aslında yukarıdaki yardımcı teorem şu şekilde kuvvetlendirilebilir:

Önerme 6.2.3 Her bir r için, $\dfrac{x_2}{x_1} = r^2$ olmak üzere sonsuz çoklukta $(x_1, y_1), (x_2, y_2) \in C(\mathbb{Q})$ rasyonel nokta ikilisi vardır (Çelik ve ark. 2021).

İspat. $C : x^2 + y^2 = 1$ birim çember denkleminin rasyonel çözümleri $s \in \mathbb{Q}$ olmak üzere $(x_1, y_1), (x_2, y_2) \in C(\mathbb{Q})$ olup (6.1.1) eşitliklerinden

$$x_1 = \frac{2s}{1+s^2}, \qquad x_2 = \frac{2t}{1+t^2} = r^2\frac{2s}{1+s^2}$$

şeklinde alınabilir. Başka bir ifade ile böyle bir çiftin varlığı,

$$\mathcal{E}_r : t(s^2+1) = r^2 s(t^2+1)$$

düzlem eğrisi üzerinde bir rasyonel noktayı verir.

$\mathcal{E}_r$ eğrisi, bükülmüş Huff eğrisidir. Bölüm 3.8'e göre (3.8.2) ve (3.8.3) formüllerle $\mathcal{E}_r$ eğrisi

$$(x,y) = (-r^2(r^2t-s)/(-t+r^2s), -r^2(r^4-1)/(-t+r^2s)),$$
$$(s,t) = ((x-r^4)/y, r^2(x-1)/y)$$

dönüşümleri yardımıyla, Weierstrass formundaki

$$E'_r : y^2 = x(x-1)(x-r^4)$$

eliptik eğrisine izomorftur. Yani $\mathcal{E}_r$ ve E'_r eğrileri birbirine izomorftur.
Yukarıdaki Weierstrass denklemi Tanım 2.3.1'e göre bir Legendre formunda denklemdir ve eğrinin torsion grubu $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$'tür. $u \in \mathbb{Q}\backslash\{0,1\}$ olsun. $x = u^4$ olarak alındığında, $y^2 = u^4(u^4-1)(u^4-r^4)$ eğrisi elde edilir. $w = y/u^2$ olarak alındığında ise

$$H : w^2 = -(u^4-1)r^4 + (u^4-1)u^4 \tag{6.2.2}$$

dördüncü dereceden eliptik eğrisi elde edilir. $P = (r,w) = (1, u^4-1)$ noktası H eğrisi üzerinde sonsuz mertebeli bir noktadır. Çünkü özel olarak $u = 2$ seçildiğinde MAGMA prosedürleri yardımıyla (6.2.2) eğrisinin rankı 1 olan

$$y^2 = x^3 + 360x^2 + 57600x + 3456000 \tag{6.2.3}$$

üçüncü derece eliptik eğrisine izomorf olduğu ve $P = (1,15)$ noktasının sonsuz mertebeli

olduğu gösterilir. Sonuç olarak

$$(x, y) = (u^4, u^2(u^4 - 1)) \in E'_r(\mathbb{Q}) \qquad \text{sonsuz mertebeli bir nokta}$$

olacak şekilde sonsuz çoklukta r vardır. Daha doğrusu, $H(\mathbb{Q})$ eğrisinde $m \neq \pm 1$ olmak üzere mP'nin r-bileşeni olarak r'yi seçersek, o zaman $\mathcal{E}_r$ pozitif ranklı bir eğridir. $\mathcal{E}_r(\mathbb{Q})$'de $(u^4, u^2(u^4 - 1))$'in görüntüsünü bulmak için Joye ve ark. (2010) makalesindeki dönüşüm kullanılarak (6.2.2) eğrisi üzerinde sonsuz mertebeli bir nokta bulunabilir. ■

Örnek 6.2.4 $r = 5/4$ olsun. Burada r^2-geometrik dizilerini oluşturan birim çember üzerinde üç rasyonel nokta bulalım.
$(s, t) = (8, 1/5)$ için $(x_1, y_1) = (16/65, 63/65)$ ve $(x_2, y_2) = (5/13, 12/13)$,
$(s, t) = (64/273, 21/52)$ için $(34944/78625, 70433/78625)$ ve $(2184/3145, 2263/3145)$,
$(s, t) = (37523/119144, 67159/41605)$ olduğunda ise $(8941280624/15603268265,$
$12787317207/15603268265)$ ve $(2794150195/3120653653, 1389677628/3120653653)$
rasyonel noktaları bulunur (Çelik ve ark. 2021).

Yukarıdaki (s, t) noktaları, Önerme 6.2.3'ün ispatında $\varepsilon_{5/4}$ eğrisi üzerindeki rasyonel noktalardır. Ayrıca, $E'_{5/4}$ Weierstrass denklemi ile tanımlanan eğride bulunan bu üç rasyonel noktanın görüntüleri sırasıyla $(125/128, 375/2048)$, $(4225/256, 61425/1024)$ ve $(351125/114242, 876825375/436861408)$ şeklindedir.

Uyarı 6.2.5 r rasyonel değerleri ile Yardımcı Teorem 6.2.2'de bir konik üzerindeki rasyonel noktalar elde edilirken, Önerme 6.2.3'te pozitif ranklı bir eliptik eğri üzerindeki rasyonel noktalar elde edilir (Çelik ve ark. 2021).

6.3 Birim Çember Üzerindeki 3 Uzunluklu Geometrik Diziler

(6.1.2) birim çember denklemini göz önüne alalım. Varsayalım

$$(x_1, y_1) = (u/r, f),\ (x_2, y_2) = (u, g),\ (x_3, y_3) = (ur, h)$$

noktaları (6.1.2) denklemini sağlasın. Biliyoruz ki birim çember üzerindeki noktalar (6.1.1) deki gibi

$$(u/r, f) = \left(\frac{2t}{1+t^2}, \frac{1-t^2}{1+t^2}\right),\ (u, g) = \left(\frac{2s}{1+s^2}, \frac{1-s^2}{1+s^2}\right) \tag{6.3.1}$$

olup $r = \dfrac{2s}{1+s^2} \cdot \dfrac{1+t^2}{2t}$ bulunur. Şimdi, üçüncü nokta olan $(x_3, y_3) = (ur, h)$ noktasını (6.1.2)'de yerine yazdığımızda

$$h^2 = 1 - \left(\frac{2s}{1+s^2}\right)^4 \cdot \left(\frac{1+t^2}{2t}\right)^2$$

olup düzenlemeler yaptığımızda

$$t^2(s^2+1)^4 - 4s^4(t^2+1)^2 = \left(\frac{h(1+s^2)^2(2t)^2}{2}\right)^2 \tag{6.3.2}$$

elde edilir.

Sağ taraftaki eşitliğe değişken değiştirmesi yaparak, $H = h(s^2+1)^2 t$ olmak üzere

$$t^2(s^2+1)^4 - 4s^4(t^2+1)^2 = H^2 \tag{6.3.3}$$

dördüncü dereceden eğriyi elde ederiz.

$(t, H) = (s, s^5 - s)$ rasyonel noktası $\mathbb{Q}(s)$ cisminde tanımlı (6.3.3) dördüncü dereceden bir eliptik eğrisi üzerindedir. Bu eğri

$$E_s : y^2 = x(x + 16s^4)(x + (1+s^2)^4) \tag{6.3.4}$$

Weierstrass formundaki eliptik eğriye karşılık gelir ve bu eğrinin torsion grup yapısı $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$'dir.

Şimdi aşağıdaki ana sonucu verelim:

Teorem 6.3.1 Her bir r için $x^2 + y^2 = 1$ birim çember üzerinde en az 3 uzunluklu r-geometrik dizisini bulunduran sonsuz çoklukta r rasyonel sayısı vardır (Çelik ve ark. 2021).

İspat. Burada $\mathbb{Q}$ üzerinde tanımlı E_s eğrisinin pozitif ranka sahip olduğu sonsuz çoklukta s rasyonel değerinin bulunduğunun gösterilmesi gerekir. $x = 8s^3(1+s^2)$ noktası E_s üzerindeki rasyonel noktanın x-bileşeni ise $s^4 - 2s^3 + 6s^2 - 2s + 1$ rasyonel bir tam kare olmalıdır. Başka bir ifade ile $(s, w) = (0, \pm 1)$ rasyonel noktasının bir çözüm olduğu dördüncü dereceden

$$w^2 = s^4 - 2s^3 + 6s^2 - 2s + 1 \tag{6.3.5}$$

eliptik eğrisini elde ederiz. Teorem 2.3.5 kullanılarak bu dördüncü dereceden eliptik eğrinin Weierstrass denklemi

$$G : v^2 = u^3 - 972u \tag{6.3.6}$$

ile tanımlanan eliptik eğriye birasyonel denk olup $(u, v) = (-27, 81)$ noktası (6.3.6) eğrisi üzerinde sonsuz mertebeli bir noktadır. Ayrıca MAGMA paket programı kullanılarak $rank(G(\mathbb{Q})) = 1$ olduğu kontrol edilebilir. Böylece teoremin ispatı tamamlanır. ■

Aşağıdaki sonuç, yukarıdaki ispattan elde edilir.

Sonuç 6.3.2 $(\frac{2s}{1+s^2}, \frac{1-s^2}{1+s^2}) \in C(\mathbb{Q})$ noktasının C üzerinde en az 3 uzunluklu sonsuz sayıda geometrik dizide bulunduğu sonsuz çoklukta s rasyonel sayısı vardır (Çelik ve ark. 2021).

Aşağıdaki tabloda, $C(\mathbb{Q})$'da en az 3 uzunluktaki geometrik dizilerinin örnekleri gösterilmektedir.

Çizelge 6.3.1. Uzunluğu 3 olan Geometrik Diziler

(r, s, t)	(x_1, x_2, x_3)
(39/25, 3, 5)	(5/13, 3/5, 117/125)
(6409/3034, 4, 328/37)	(24272/108953, 8/17, 1508/1517)
(5987825/3616561, 5, 1537/181)	(278197/1197565, 5/13, 29939125 /47015293)
(55045/24531, 6, 234/17)	(7956/55045, 12/37, 220180/302549)
(7935762913/2225017375, 7, 125885/4949)	(623004865/7935762913, 7/25, 7935762913/7946490625)
(6548713889/6051759025, 8, 80392/9265)	(1489663760/6548713889, 16/65, 104779422224/393364336625)

Uyarı 6.3.3 Bu bölümdeki sonuçların niçin 4 uzunluklu geometrik dizilere genişletilemediği Tezin 7. bölümünde açıklanmıştır.

7. SONUÇLAR

Bu tez çalışmasında bazı düzlem cebirsel eğriler üzerindeki maksimum uzunluklu rasyonel dizilerin bulunması amaçlanmıştır. Bu amaca ulaşmak için eliptik eğriler, eliptik eğrilerin farklı modelleri ve birim çember üzerindeki rasyonel noktaların x-bileşenlerin oluşturduğu rasyonel diziler incelenmiş ve elde edilen sonuçlar SCI-Expanded indeksinde taranan uluslararası, sayılar teorisi profilli üç ayrı dergide yayınlanmıştır. Bu sonuçlar şöyle özetlenebilir:

$k, l, m \in \mathbb{Q}$ olmak üzere $\mathbb{Q}$ cismi üzerinde $E : y^2 = kx^3 + lx + m$ eliptik eğrisini göz önüne alalım. $i = 1, 2, \ldots, n$ iken $(x_i, y_i) \in E(\mathbb{Q})$ rasyonel noktalarının x_i-bileşenleri ardışık küpler olacak şekilde bir S-dizisinin $(S \subset \mathbb{Q})$ elemanları olsun. Tezin $4.$ bölümünde $n = 5$ uzunluklu bu özellikteki S-dizisini bulunduran E eliptik eğrilerinin sonsuz çoklukta olduğu gösterildi. Ayrıca bu özellikteki 5 rasyonel noktanın $E(\mathbb{Q})$'da lineer bağımsız olduğu ispatlanarak rankı en az 5 olan eliptik eğrilerinin sonsuz bir ailesi literatüre tanıtıldı.

$\mathbb{F}$ sayı cisminin keyfi bir S alt kümesi (bükülmüş) Edwards eğrileri ve (genel) Huff eğrileri üzerindeki rasyonel noktaların x-bileşenlerinden oluşan bir dizi olsun. Tezin $5.$ bölümünde üzerinde herhangi bir kısıtlama olmayan S-dizilerinin uzunluğu $|S| = 4, 5$ veya 6 iken bu S-dizilerini bulunduran yukarıdaki düzlem cebirsel eğrilerin sonsuz ailelerinin varlığı ispatlanır. Buradaki sonuçlar literatürde var olan bazı sonuçları geneller.

Düzlem cebirsel eğri üzerindeki rasyonel noktaların x veya y-bileşenleri ortak çarpanı r olacak şekilde bir geometrik dizi oluştururursa düzlem cebirsel eğri üzerindeki rasyonel noktaların dizisinin bir r-geometrik dizisi oluşturduğu söylenir. Tezin $6.$bölümünde $x^2 + y^2 = 1$ birim çember denklemi üzerinde en az 3-uzunluklu r-geometrik dizilerini bulunduran sonsuz çoklukta r-rasyonel sayısının varlığı ispatlanır. Eğer ur^2, Teorem 6.3.1'deki birim çember üzerindeki bir rasyonel noktanın x-bileşeni ise bu en az 4 uzun-

luklu bir r-geometrik dizisinin var olması demektir. Ancak bu da

$$\begin{aligned} t^2(s^2+1)^4 - 4s^4(t^2+1)^2 &= H_1^2, \\ t^4(s^2+1)^6 - 4s^6(t^2+1)^4 &= H_2^2 \end{aligned}$$

Diophant denklem sisteminin rasyonel çözümlerini incelemeyi gerektirir. Bu denklem sisteminin çalışılması ayrı bir araştırma sorusudur. Düzlemsel konikler üzerinde geometrik dizilerin varlığının araştırılması tez sonrası bir çalışma olarak ele alınacaktır.

KAYNAKLAR

Alvarado, A. 2009. An arithmetic progression on quintic curves. *J. Integer Seq.*, 12: Article 09.7.3.

An, S.Y., Kim, S.Y., Marshall, D.C., Marshall, S.H., McCallum, W.G., Perlis, A.R. 2001. Jacobians of genus one curves. *Journal of Number Theory*, 90: no.2, 304–315.

Asar, A. O., Arıkan, A., Arıkan, A. 2012. Cebir. Gazi Kitabevi, Ankara, 381 s.

Bernstein, A.J., Birkner, P., Joye, M., Lange, T., Peters, C., 2008. Twisted Edwards Curves. In: Vaudenay, S. (ed.) AFRICACRYPT. LNCS, vol 5023, 389–405. *Springer*, Heidelberg.

Bernstein, D., Lange, T., 2007. Faster Addition and Doubling on Elliptic Curves. *ASIACRYPT*, 29–50.

Bernstein, D. J., Lange, T., Farashahi, R., 2008. Binary Edwards curves In: Cryptographic Hardware and Embedded Systems CHES., 10th International Workshop, Washington, D.C., USA, August 10-13. *Proceedings, Lecture Notes in Computer Science.*, 244–265, Springer.

Bosma, W., Cannon, J., Playoust, C. 1997. The Magma algebra system I. The user language. *J. Symbolic Comput.*, 24: 235–265.

Bremner, A. 1999. On arithmetic progressions on elliptic curves. *Experiment Math.*, 8: 409–413.

Bremner, A. 2013. Arithmetic progressions on Edwards curves. *Journal of Integer Sequences*, 16: Article 13.8.5.

Bremner, A., Ulas, M. 2013. Rational points in geometric progressions on certain hyperelliptic curves. *Publ. Math. Deb.*, 82: 669–683.

Campbell, G. 2003. A note on arithmetic progressions on elliptic curves. *J. Integer Seq.*, 6: Article 03.1.3.

Cangül, İ.N. 2016. Soyut Cebir. *Dora Yayınları*, Bursa.

Cassels, J.W.S. 1991. Lectures on elliptic curves. volume 24 *of London Mathematical Society Student Texts.* Cambridge University Press, Cambridge.

Choudhry, A. 2015. Arithmetic progressions on Huff curves. 18: Article 15.5.2.

Choudhry, A., Juyal, J. 2016. Rational points in arithmetic progression on the unit circle. *J. Integer Seq.*, 19: Article 16.4.1.

Ciss, A. A., Moody, D. 2017. Arithmetic progressions on conics. 20: Article 17.2.6.

Ciss, A. A., Moody D. 2017. Geometric progressions on elliptic curves. *Glasnik Math.*,

52: 1–10.

Cremona, J. E. 1997. Algorithms for Modular Elliptic Curves. *Cambridge University Press.*, 2 nd edu,.

Çelik, G.S., Soydan, G. 2018. Elliptic curves containing sequences of consecutive cubes. *Rocky Mountain J. Math.*, 48: 2163–2174.

Çelik, G.S., Sadek, M., Soydan, G. 2019. Rational sequences on different models of elliptic curves. *Glasnik Math.*, 54: 53–64.

Çelik, G.S., Sadek, M., Soydan, G. 2021. Rational Points in Geometric Progression on the Unit Circle. *Publicationes Mathematicae Debrecen*, 98/3-4: 513–520.

Dam, M. R. 2012. Edwards Elliptic Curves. Rijksuniversiteit Groningen, Hollanda, Bitirme Tezi.

Edwards, H. 2007. A normal form for elliptic curves. *Bulletin of the American mathematical society*, 44: 393–422.

Faltings, G. 1983. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern,*Inventiones Mathematicae* 73: 349-366.

Fraleigh, J.B. 2003. A first course in abstract algebra. Pearson Education India.

Gouvêa, F.Q. 2003. p-adic numbers. An introduction, Springer,

Joye, M., Tibbouchi, M., Vergnaud, D. 2010. Huff's Model for Elliptic Curves. *Algorithmic Number Theory-ANTS-IX, Lecture Notes in Computer Science*, 6197: Springer, 234–250.

Huff, G. B. 1948. Diophantine problems in geometry and elliptic ternary forms. Duke Math. J. 15, 443–453 .

Kamel, M., Sadek, M. 2017. On sequences of consecutive squares on elliptic curves. *Glasnik Math.*, 52: 45–52.

Kato, K., N.Kurokawa, T.Saito. 2000. Number Theory 1 Fermat's Dream. *American Mathematical Society.* United States of America.

Lee, J. B., Vélez, W. Y. 1992. Integral solutions in arithmetic progression for $y^2 = x^3 + k$. *Per. Math. Hung.*, 25: 31–49.

Macleod, A. J. 2006. 14-term arithmetic progressions on quartic elliptic curves. *J. Integer Seq.*, 9: Article 06.1.2.

Mollin, R.A. 2001. An Introduction to Cryptography. Chapman and Hall/CRC. *United States of America*.

Montgomery, P.L. 1987. Speeding the Pollard and Elliptic Curve Methods of Factorizations, *Math. Comp. 48*.

Moody, D. 2011. Arithmetic progressions on Edwards curves. *J. Integer Seq.*, 14: Article 11.1.7.

Moody, D. 2011. Arithmetic progressions on Huff curves. *Ann. Math. Inform.*, 38: 111–

116.
Peeples Jr., W.D. 1954. Elliptic curves and rational distance sets. *Proc. Am. Math. Soc.* 5: 29–33.
Salami, S., Zargar, A.S. 2021 Families of Cubic Elliptic Curves a Containing Sequences of Consecutive Powers. *Rocky Mountain J. Math., basımda.*
Schmitt, S., Zimmer, H.G. 2003 Elliptic Curves A Computational Approach. *Walter de Gruyter.* Berlin. 367 p.
Silverman, J. H. 1994. Advanced Topics in the Arithmetic of Elliptic Curves. *Springer-Verlag*, New York.
Silverman, J. H. 2009. The Arithmetic of Elliptic Curves (2nd Edition), Graduate Texts in Mathematics, 106, Dordrecht, *Springer*.
Silverman, J. H., Tate, J. 1992. Rational Points on Elliptic Curves, Undergraduate Texts in Mathematics, *Springer*.
Taylor, R.L., Wiles, A. 1995. Ring Theoretic Properties of Certain Hecke Algebras, *Annals of Math.* 141: 553-572.
Ulas, M. 2005. A note on arithmetic progressions on quartic elliptic curves. *J. Integer Seq.*, 8: Article 05.3.1.
Ulas, M. 2009. On arithmetic progressions on genus two curves. *Rocky Mountain J. Math.*, 39: 971–980.
Washington, L.C. 2008. Elliptic curves: number theory and cryptography. *CRC press*.
Wu, H., Feng, R. 2010. Elliptic curves in Huff's model. Available at http://eprint.iacr.org /2010/390.pdf.

ÖZGEÇMİŞ

Adı Soyadı	:	Gamze SAVAŞ ÇELİK
Doğum Yeri ve Tarihi	:	BURSA 1990
Yabancı Dil	:	İNGİLİZCE
Eğitim Durumu (Kurum ve Yıl)	:	
Lise	:	YILDIRIM BEYAZIT LİSESİ, 2005-2009
Lisans	:	BURSA ULUDAĞ ÜNİVERSİTESİ, 2010-2013
Yüksek Lisans	:	BURSA ULUDAĞ ÜNİVERSİTESİ, 2014-2016
Doktora	:	BURSA ULUDAĞ ÜNİVERSİTESİ, 2017-2022
İletişim(e-posta)	:	gamzesavascelik@gmail.com
Akademik çalışmalar	:	

Bérczes, A. Pink, I., Savaş, G., Soydan, G. 2018. On the Diophantine equation $(x+1)^k + (x+2)^k + \cdots + (2x)^k = y^n$. *Journal of Number Theory*, 183: 326–351.

Çelik, G.S., Soydan, G. 2018. Elliptic curves containing sequences of consecutive cubes. *Rocky Mountain Journal of Mathematics*, 48: 2163–2174.

Çelik, G.S., Sadek, M., Soydan, G. 2019. Rational sequences on different models of elliptic curves. *Glasnik Matematicki*, 54: 53–64.

Çelik, G.S., Sadek, M., Soydan, G. 2021. Rational Points in Geometric Progression on the Unit Circle. *Publicationes Mathematicae Debrecen*, 98/3-4: 513–520.