T.C.
ULUDAĞ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SİNGÜLER EĞRİLER VE ELİPTİK BÖLÜNEBİLİR DİZİLER

Betül GEZER

DOKTORA TEZİ
MATEMATİK ANABİLİM DALI

BURSA-2009

T.C.
ULUDAĞ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SİNGÜLER EĞRİLER VE ELİPTİK BÖLÜNEBİLİR DİZİLER

Betül GEZER

Doç. Dr. Osman BİZİM
(Danışman)

DOKTORA TEZİ
MATEMATİK ANABİLİM DALI

BURSA-2009

T.C.
ULUDAĞ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SİNGÜLER EĞRİLER VE ELİPTİK BÖLÜNEBİLİR DİZİLER

Betül GEZER

DOKTORA TEZİ
MATEMATİK ANABİLİM DALI

Bu Tez 22 / 05 / 2009 tarihinde aşağıdaki jüri tarafından oybirliği/oy çokluğu ile kabul edilmiştir.

Doç. Dr. Osman BİZİM Prof. Dr. Gökay KAYNAK Prof. Dr. İ. Naci CANGÜL
Danışman

Doç. Dr. Yılmaz ŞİMŞEK Doç. Dr. Recep ŞAHİN

T.C.
ULUDAĞ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SİNGÜLER EĞRİLER VE ELİPTİK BÖLÜNEBİLİR DİZİLER

Betül GEZER

DOKTORA TEZİ
MATEMATİK ANABİLİM DALI

Bu Tez 22 / 05 / 2009 tarihinde aşağıdaki jüri tarafından oybirliği/~~oy çokluğu~~ ile kabul edilmiştir.

Doç. Dr. Osman BİZİM
Danışman

Prof. Dr. Gökay KAYNAK

Prof. Dr. İ. Naci CANGÜL

Doç. Dr. Yılmaz ŞİMŞEK

Doç. Dr. Recep ŞAHİN

ÖZET

Bu çalışmanın amacı "singüler eğriler" ve "eliptik bölünebilir diziler" gibi matematiğin iki önemli kavramını sonlu cisimler üzerinde çalışmak ve bu kavramlar arasındaki ilişkiyi ortaya koymaktır.

Çalışmanın birinci ana kısmında eliptik eğriler teorisi ele alınmış ve teorinin önemli özellikleri verilmiştir. Karakteristiği 2 ve 3 ten farklı olan bir $\mathbb{F}$ cismi üzerinde tanımlı

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

eşitliğini gerçekleyen sıralı ikililerin kümesi *eliptik eğri* olarak adlandırılır. Eğer $x^3 + Ax + B = 0$ kübik denkleminin katlı kökleri bulunması halinde bu noktaların kümesine *singüler eğri* adı verilir. Çalışmanın amaçlarından birisi de bu tip eğrilerin özelliklerini sonlu cisimler üzerinde ortaya koymaktır.

Çalışmanın üçüncü bölümünde, $p > 3$ bir asal sayı olmak üzere, $\mathbb{F}_p$ sonlu cismi üzerinde singüler eğriler ele alınmış bu eğrilerin üzerindeki nokta sayıları, ikinci ve üçüncü dereceden kalanlar yardımıyla belirlenmiştir. Daha sonra bu eğrilerin üzerindeki (x, y) noktalarının karakterleri, bu noktaların apsis ve ordinatları toplamı ile ilgili sonuçlar verilmiştir. Bu eğriler üzerindeki noktaların grup yapısı ve büküm noktaları belirlendikten sonra bu eğrilerin üzerindeki nokta sayıları ile ilgili işlemler $\mathbb{F}_p$ sonlu cisminden $\mathbb{F}_{p^n}$ ye genelleştirilmiştir.

Çalışmanın ikinci ana kısmında bir eliptik eğrinin bölüm polinomu kavramından ortaya çıkan eliptik bölünebilir diziler ele alınmıştır. Eliptik bölünebilir diziler ilk olarak 1948'de Morgan Ward' ın "*Memoir on elliptic divisibility sequences*" adlı makalesinde ele alınmıştır.

Çalışmanın beşinci bölümünde, Morgan Ward'ın yapmış olduğu çalışmalar geliştirilmiştir. İlk olarak sonlu cisimler üzerinde eliptik bölünebilir dizi kavramı tanımlandıktan sonra, belli ranklara sahip olan eliptik bölünebilir dizilerin genel terimleri ve periyotları belirlenmiştir. Daha sonra bu dizilerle eşleşen eliptik eğriler ve singüler eğriler belirlenmiştir, singüler eğrilerin ne zaman ortaya çıktığı ile ilgili sonuçlar verilmiştir.

Anahtar Kelimeler: Sonlu cisimler üzerinde singüler eğriler, rasyonel noktalar, büküm noktaları, sonlu cisimler üzerinde eliptik bölünebilir diziler, singüler eliptik bölünebilir diziler.

ABSTRACT

The aim of this work is to combine two topics of mathematics, "singular curves" and "elliptic divisibility sequences".

In the first part, the elliptic curve theory is discussed and some important properties of this theory are given. *An elliptic curve* is a curve E defined over $\mathbb{F}$ is given by an equation

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

where $\mathbb{F}$ is a field of characteristic not equal to 2 or 3. If the cubic $x^3 + Ax + B = 0$ has multiple roots, then the set of solution points form a *singular curve*.

In the third chapter, the rational points on singular curves over finite fields $\mathbb{F}_p$ (where $p > 3$ is a prime) are considered. Some results concerning the number of the points on the singular curves are given by means of quadratic residue character, and the cubic residue character. Also some results are given on the sum of x and y coordinates of the points (x, y) on these curves. Then the structure of the group of the rational points and torsion points on these curves are determined and finally the results concerning the number of points in $\mathbb{F}_p$ is generalize to $\mathbb{F}_{p^n}$.

In the second part, the theory of elliptic divisibility sequences which arise from elliptic curves and which contain a zero term is discussed. Elliptic divisibility sequences are described in detail in Morgan Ward's paper "*Memoir on elliptic divisibility sequences*" published in 1948.

In the fifth chapter, the techniques studied by Morgan Ward to characterize to sequences in certain ranks are developed. First of all, elliptic divisibility sequences over finite fields are defined. After that, general terms of these sequences over finite fields are given. Then elliptic curves and singular curves associated to this sequences are given and some results concerning of singular curves and singular elliptic divisibility sequences are given.

Key Words: Singular curves over finite fields, rational points on singular curves, torsion points on singular curves, elliptic divisibility sequences over finite fields, singular sequences.

İÇİNDEKİLER

SİMGELER DİZİNİ

R,	halka
$\mathbb{Z}$,	tam sayılar kümesi
$\mathbb{Q}$,	rasyonel sayılar kümesi
$\mathbb{F}$,	cisim
$\mathbb{F}^*$,	$\mathbb{F}$ cisminin sıfırdan farklı elemanlarının oluşturduğu çarpımsal grup
$\mathbb{F}_p$,	p elemanlı sonlu cisim
$\mathbb{F}_p^*$,	p elemanlı sonlu cismin çarpımsal grubu
$\overline{\mathbb{F}}$,	$\mathbb{F}$ cisminin cebirsel kapanışı,
$\mathbb{Z}[a, b]$,	katsayıları $\mathbb{Z}$ de olan polinomlar halkası
$\mathbb{Z}_n$,	modülo n de tamsayıların halkası
$\boldsymbol{U}_n$,	$\mathbb{Z}_n$ deki birimlerin kümesi
$\boldsymbol{Q}_p$,	modülo p de ikinci derece kalanların kümesi
$\boldsymbol{K}_p$,	modülo p de üçüncü derece kalanların kümesi
$\boldsymbol{K}_p^*$,	modülo p de sıfırdan farklı üçüncü derece kalanların kümesi
$\phi(m)$,	Euler Phi fonksiyonu
$\left(\frac{a}{p}\right)$,	a nın modülo p de Legendre sembolü ($p > 2$ asal)
$\left(\frac{a}{n}\right)$,	a nın modülo n de Jacobi sembolü
$\left(\frac{\Delta}{n}\right)$,	Δ nın modülo n de Kronecker sembolü
$E(\mathbb{F})$,	$\mathbb{F}$ cismi üzerinde tanımlı E eliptik eğrisi üzerindeki noktaların kümesi
$j(E)$,	E eliptik eğrisinin j-değişmezi
$\Delta(E)$,	E eliptik eğrisinin diskriminantı

$E[n]$,	E eliptik eğrisi üzerindeki n. mertebeden büküm (torsiyon) noktaların kümesi
$E_{ns}(\mathbb{F})$,	E eliptik eğrisi üzerindeki singüler olmayan noktaların oluşturduğu küme
$E(\mathbb{F}_p)$,	$\mathbb{F}_p$ sonlu cismi üzerinde tanımlı E eliptik eğrisi üzerindeki noktalar kümesi
$\#E(\mathbb{F}_p)$,	$\mathbb{F}_p$ cismi üzerinde tanımlı E üzerindeki noktalar kümesinin eleman sayısı
$E(\mathbb{F}_{q^n})$,	$\mathbb{F}_{q^n}$ cismi üzerinde tanımlı E eliptik eğrisi üzerindeki noktalar kümesi
$E(\mathbb{Q})$,	$\mathbb{Q}$ cismi üzerinde tanımlı E eliptik eğrisi üzerindeki noktalar kümesi
$E(\mathbb{F}_p)$,	$\mathbb{F}_p$ sonlu cismi üzerinde tanımlı E eliptik eğrisi üzerindeki noktaların kümesi
φ_q,	E eliptik eğrisinin q-Frobenius endomorfizmi
$\psi_n(x, y)$,	E eliptik eğrisinin n. bölüm polinomu
$[1\ h_2\ h_3\ h_4]$,	başlangıç terimleri 1, h_2, h_3, h_4 olan (h_n) dizisi
$\sigma(z, L)$,	L kafesi ile eşleşmiş olan Weierstrass σ fonksiyonu
$\wp(z, L)$,	L kafesi ile eşleşmiş olan Weierstrass $\wp$ fonksiyonu
ρ,	(h_n) eliptik bölünebilir dizisinin rankı
$\pi(h_n)$,	(h_n) eliptik bölünebilir dizisinin periyotu
$\Delta(h_2, h_3, h_4)$,	$[1\ h_2\ h_3\ h_4]$ dizisinin determinantı
$(h_n(p))$,	$\mathbb{F}_p$ cismi üzerinde tanımlı eliptik bölünebilir dizi
$(h_n(p))_s$,	$\mathbb{F}_p$ cismi üzerinde tanımlı singüler dizilerin temsilci dizileri
$\overline{[(h_n(p))]}$,	denk dizilerin sınıfı
$[E(h_n(p))]$,	E eliptik eğrisini veren dizilerin oluşturduğu denklik sınıfı
$\lfloor . \rfloor$,	tam değer (taban) fonksiyonu.

ŞEKİLLER DİZİNİ

Sayfa

GİRİŞ

Bu çalışma "Singüler Eğriler" ve "Eliptik Bölünebilir Diziler" gibi iki kavram ve bu iki kavram arasındaki ilişkileri ele almaktadır. Bu nedenle çalışma iki ana kısım olarak düşünülebilir; çalışmanın birinci kısmında, tamamen, eliptik eğriler teorisi ve özellikle de sonlu cisimler üzerinde tanımlı singüler eğriler ele alınmış, bu eğrilerin temel özellikleri verilmiştir. İkinci kısmında ise, sonlu cisimler üzerinde eliptik bölünebilir diziler ele alınmış, bu dizilerin temel özellikleri verilmiş ve eliptik eğriler ile bu diziler arasındaki ilişkiler incelenmiştir.

Eliptik eğriler, çok uzun zamandır çözülemeyen problemlerin bile çözülmesinde rol oynamış cebirin en modern kavramlarından birisidir. Son 20 – 30 yıl içinde eliptik eğrilerin sayılar teorisi ve diğer alanlarda önemli bir rol oynadığı görülmüştür. Eliptik eğriler, 1980 li yıllarda kriptoloji alanında kullanılmaya başlanmış ve çarpanlaştırma ve asallık testleri için eliptik eğri teknikleri geliştirilmiştir (Koblitz 1994) ve (Mollin 2001)). 1990 lı yıllarda ise bu eğriler, özellikle, Fermat'ın son teoreminin çözümündeki öneminden dolayı matematiğin oldukça popüler bir çalışma alanı haline gelmiştir. Bunun ile birlikte eliptik eğrilerin matematik dünyasına girişi ise oldukça eskidir. Eliptik eğriler ilk olarak, Diophant'ın Arithmetica'sının dördüncü kitabındaki yirmi dördüncü problemde görülmektedir.

Eliptik eğriler teorisi, çalışmanın ilk ana kısmında eliptik eğriler teorisi ile ilgili temel kavramlar ve gerekli teoremler verildikten sonra singüler eğri kavramı ele alınmıştır. Singüler eğri kavramı tanımı ve örnekleri verildikten sonra sonlu bir cisim üzerinde tanımlı singüler eğri aileleri oluşturulmuştur. Daha sonra bu ailelerdeki singüler eğrilerin üzerindeki rasyonel noktaların karakterleri ve bu noktaların sayıları belirlenmiş ve bu noktaların oluşturduğu kümelerin grup yapıları verilmiştir.

Çalışmanın ikinci ana kısmında ele alınan eliptik bölünebilir diziler ilk olarak 1948'de Morgan Ward'ın "*Memoir on elliptic divisibility sequences*" adlı makalesinde ortaya çıkmıştır. Ward, daha önce E. Lucas tarafından çalışılan Lucas dizilerinin özelliklerini eliptik bölünebilir dizilere taşımıştır. Dolayısıyla, eliptik bölünebilir diziler Lucas dizilerinin bir genelleştirilmesi olarak düşünülebilirler.

Bölünebilir dizilerden en iyi bilinenleri Fibonacci dizileri ve Mersenne dizileridir, bu diziler, sırasıyla,

$$F_n = F_{n-1} + F_{n-2}$$

ve

$$M_n = 2^{n-1} = 3M_{n-1} - 2M_{n-2}$$

lineer indirgeme bağıntılarını gerçeklerler. Eliptik bölünebilir diziler ise lineer olmayan

$$h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2$$

indirgeme bağıntısını gerçeklerler. Eliptik bölünebilir diziler bu özelliğe sahip olan ve çalışılan ilk bölünebilir dizilerdir ve bu özellikleri nedeniyle de oldukça ilginçtirler. Eliptik bölünebilir dizilerin gerçeklediği bu bağıntı aynı zamanda bir eliptik eğrinin bölüm polinomları tarafından da gerçeklenir. Ward (1948), her bir (h_n) eliptik bölünebilir dizisine karşılık bir E eliptik eğrisinin var olduğunu ve üstelik $P = (x_1, y_1)$ noktası E eliptik eğrisi üzerinde bir rasyonel nokta ise her $n \in \mathbb{N}$ için (h_n) eliptik bölünebilir dizisinin bölüm polinomları yardımıyla

$$h_n = \psi_n(x_1, y_1)$$

biçiminde ifade edildiğini göstermiştir, burada ψ_n, E eliptik eğrisinin n. bölüm polinomunu göstermektedir.

Özellikle eliptik eğriler teorisi ile olan yakın ilgisi nedeniyle eliptik bölünebilir diziler matematiğin birçok dalının inceleme konusu olmuşlardır. 2000 li yılların başında, kriptoloji ile olan ilişkilerinin de ortaya çıkmasından sonra bu dizilerin popülerlikleri daha da artmış ve bu dizileri temel alan birçok çalışma yapılmıştır. R.

Shipsey (2000), eliptik bölünebilir dizilerin eliptik eğrilerle olan ilişkisini kullanarak eliptik eğri kriptolojisi ile ilgili önemli sonuçlar elde etmiştir.

Bunların dışında eliptik bölünebilir diziler teorisi ile ilgili birçok çalışma yapılmıştır (Everest ve Ark. 2003, 2001, Ward 1948, Swart 2003, Shipsey 2000). Chudnovsky & Chudnovsky (1986), eliptik bölünebilir dizilerdeki asal sayıların ne zaman ortaya çıktıklarını ve bunların dağılımlarını araştırmışlardır. G. Everest (2001), bu çalışmaları geliştirmiştir.

Çalışmanın diziler ile ilgili kısmında, eliptik bölünebilir diziler hakkında genel bilgiler verildikten sonra eliptik bölünebilir diziler ve eliptik eğriler arasındaki ilişkiler yardımıyla singüler eliptik bölünebilir diziler ile singüler eğriler arasındaki ilişkiler üzerinde durulmuştur. Daha sonra sonlu bir cisim üzerinde tanımlı eliptik bölünebilir diziler ele alınmış ve bu halde, bu dizilerin temel özellikleri verilmiştir. Belli ranklara sahip olan eliptik bölünebilir dizilerin genel terimleri verilmiş, bu diziler içinde singüler diziler belirlenmiş ve bu dizilerle eşleşen eliptik eğriler ve singüler eğriler belirlenmiştir.

1. BÖLÜM
ÖNBİLGİLER

Bu bölümde çalışmada kullanılacak olan bazı temel kavramlar tanımlanacak ve bazı temel teoremler verilecektir, bu bölüm diğer bölümler için bir taban oluşturacaktır. Kısım 1.1 de grup teori ile ilgili bazı kavramlar ele alınacaktır. Kısım 1.2 de sonlu cisimlerin temel özellikleri üzerinde durulacaktır. Daha sonraki kısımlarda ise özellikle sayılar teorisi ile ilgili kavramlarla ilgilenilecektir. Kısım 1.3 de bir $\mathbb{Z}_n$ halkasındaki ikinci dereceden kalan kavramı verildikten sonra sonlu cisimler üzerinde ikinci dereceden kalanlarla ilgilenilecek ve bunlarla ilgili bazı sonuçlar verilecektir. Kısım 1.4 de ise sonlu cisimler üzerinde üçüncü dereceden kalan kavramı ve temel özellikleri verilecektir.

1.1 Temel Kavramlar

Bu kısımda çalışmada gerekli olacak grup teorisi ile ilgili bazı kavramların tanımları ve örnekleri verilecektir. Grup ve alt gruplarının mertebeleri arasındaki ilişkiyi belirten Lagrange teoremi grup teorinin en iyi bilinen ve en çok kullanılan teoremlerinden biridir.

1.1.1 Teorem (Lagrange). *G* bir grup ve *H*, *G* nin bir alt grubu olsun. Bu durumda *H* nin mertebesi *G* nin mertebesini böler (Fraleigh 1982).

Bu teoremin önemli sonuçları ise aşağıdaki teoremlerde verilmektedir.

1.1.2 Teorem. Mertebesi asal olan her grup bir devirli gruptur, yani bu grup bir tek eleman ile üretilebilir (Fraleigh 1982).

1.1.3 Teorem. Sonlu mertebeli bir grubun her hangi bir elemanın mertebesi grubun mertebesini böler (Fraleigh 1982).

1.1.4 Tanım. $\overline{u}$, R halkasının bir elemanı olmak üzere, $\overline{u}$ nin çarpmaya göre tersi,

$$\overline{u}\,\overline{v} = \overline{v}\,\overline{u} = \overline{1}$$

olacak şekilde bir $\overline{v} \in R$ elemanıdır. R halkasında çarpmaya göre tersi olan bir elemana *birim (unit)* denir ve R halkasındaki birimlerin kümesi $\boldsymbol{U}(R)$ veya kısaca $\boldsymbol{U}$ ile gösterilir.

Örneğin $\mathbb{Z}$ tamsayılar halkasındaki birimler 1 ve –1 dir. Aşağıdaki teorem, $\mathbb{Z}_n$ halkasındaki birimleri belirlemektedir.

1.1.5 Teorem. $\overline{u} \in \mathbb{Z}_n$ nin bir birim olması için gerek ve yeter şart $(u, n) = 1$ olmasıdır (Fraleigh 1982).

Örneğin, $\mathbb{Z}_6$ daki birimler $\boldsymbol{U}_6 = \{ \overline{1}, \overline{5} \}$ ve $\mathbb{Z}_8$ deki birimler $\boldsymbol{U}_8 = \{ \overline{1}, \overline{3}, \overline{5}, \overline{7} \}$ dir.

1.1.6 Tanım. $\overline{g} \in \mathbb{Z}_n$, $\boldsymbol{U}_n$ yi üretiyorsa g ye modülo n de bir *ilkel kök* denir.

Eğer $\overline{g}$ bir ilkel kök ise $\overline{g}$ nin 0 ile $n - 1$ arasındaki tüm kuvvetleri birbirinden farklıdır ve bunlar $\boldsymbol{U}_n$ yi oluştururlar. Örneğin, modülo 5 de $\overline{2}$ ve $\overline{3}$ birer ilkel köktür, bu iki elemanın kuvvetleri $\boldsymbol{U}_5$ i oluşturur.

İlkel kök teoremi, her bir asal sayının ilkel bir kökünün var olduğunu ve üstelik modülo p de bunların sayısının tam olarak $\phi(p - 1)$ tane olduğunu söyler, burada

$$\phi(m) = \#\{ a \mid 1 \le a \le m \text{ ve } (a, m) = 1 \}$$

Euler Phi fonksiyonudur. Örneğin, modulo 11 de $\phi(10) = 4$ olduğundan 4 tane ilkel kök vardır ve bunlar 2, 6, 7 ve 8 sayılarıdır.

Halkalar teorisinde, R bir halka olmak üzere her $a \in R$ için $n \cdot a = 0$ olacak biçimde bir $n \in \mathbb{N}$ sayısının varlığı oldukça önemlidir. Burada $n \cdot a$, n tane a nın toplamını belirtmektedir, yani $a + a + \ldots + a = n \cdot a$ dır.

1.1.7 Tanım. R bir halka olmak üzere her $a \in R$ için $n \cdot a = 0$ olacak biçimde bir $n \in \mathbb{N}$ sayısı varsa bu şekildeki sayıların en küçüğüne R halkasının *karakteristiği* denir. Eğer böyle bir sayı yok ise R halkasının karakteristiği 0 olarak alınır.

Örneğin, $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Q}$ ve $\mathbb{C}$ nin karakteristiği 0, $\mathbb{Z}_n$ nin karakteristiği ise n dir. Aşağıdaki teorem bir birimli halkanın karakteristiğinin nasıl belirleneceğini göstermektedir.

1.1.8 Teorem. R bir birimli (birimi 1) halka olsun. R nin karakteristiğinin $n > 0$ olabilmesi için gerek ve yeter şart n sayısının $n \cdot 1 = 0$ olacak biçimdeki en küçük pozitif tamsayı olmasıdır (Fraleigh 1982).

1.1.9 Tanım. $\mathbb{F}$ ve $\mathbb{L}$, $\mathbb{F} \subset \mathbb{L}$ özelliğinde iki cisim ve $\alpha \in \mathbb{L}$ olsun. $a_0, a_1, \ldots, a_{n-1} \in \mathbb{F}$ ve

$$f(X) = a_0 + a_1 X + \ldots + a_{n-1}X^{n-1} + X^n$$

olmak üzere $f(\alpha) = 0$ olacak biçimde bir f polinomu varsa α ya $\mathbb{F}$ cisminde bir *cebirsel sayı* denir. Eğer $\mathbb{L}$ nin her elemanı $\mathbb{F}$ de bir cebirsel sayı ise $\mathbb{L}$ cismine $\mathbb{F}$ nin bir *cisim genişlemesi* denir. $\mathbb{L}$, $\mathbb{F}$ nin bir cisim genişlemesi olmak üzere

$$\overline{\mathbb{F}} = \{ \alpha \in \mathbb{L} \mid \alpha, \mathbb{F} \text{ de cebirsel sayı} \} \subset \mathbb{L}$$

kümesine $\mathbb{F}$ nin bir *kapanışı* denir.

Örneğin, $\sqrt{1+\sqrt{3}}$ sayısı $\mathbb{Q}$ da bir cebirsel sayıdır ve $\mathbb{C}$, $\mathbb{Q}$ nun bir cisim genişlemesidir, $\mathbb{Q}$ ile $\mathbb{C}$ nin kapanışı ise $\mathbb{C}$ dir.

1.2 Sonlu Cisimler

p bir asal sayı olmak üzere modülo p deki tamsayılar mertebesi p olan $\mathbb{F}_p$ cismini oluştururlar. Her bir p asal sayısı ve $n \in \mathbb{N}$ için mertebesi p^n olan bir sonlu cisim vardır. Bu cisim literatürde mertebesi p^n olan Galois cismi olarak bilinir ve $GF(p^n)$ ile gösterilir.

$\mathbb{E}$, $\mathbb{F}$ cisminin n. dereceden bir cisim genişlemesi ve $\mathbb{F}$ cisminin eleman sayısı p ise $\mathbb{E}$ cisminin p^n tane elemanı vardır. Bunun sonucu olarak, $\mathbb{E}$, karakteristiği p olan bir sonlu cisim ise belli bir $n \in \mathbb{N}$ için $\mathbb{E}$ nin p^n tane elemanı vardır.

1.2.1 Tanım. $\mathbb{F}$ sonlu bir cisim ve $\alpha \in \mathbb{F}$ olmak üzere $\alpha^n = 1$ ise α ya $\mathbb{F}$ cisminin *n. kökü* denir, eğer n bu özellikteki en küçük pozitif tamsayı ise α ya *birimin n. ilkel kökü* denir.

Örneğin $x^3 = 1$ için $x^3 - 1 = (x - 1) \cdot (x^2 + x + 1) = 0$ olduğundan birimin üçüncü ilkel kökleri, $x_1 = 1$, $x_2 = \frac{-1-\sqrt{3}}{2}$ ve $x_3 = \frac{-1+\sqrt{3}}{2}$ dir.

Birimin ilkel kökü tanımından p^n elemanlı sonlu bir $\mathbb{F}$ cisminin sıfırdan farklı olan tüm elemanları birimin $p^n - 1$. kökleridir.

1.3 İkinci Dereceden Kalanlar

Bu kısımda ilk olarak bir $\mathbb{Z}_n$ halkasındaki ikinci dereceden kalanlar ele alınacak, daha sonra p bir asal sayı olmak üzere $\mathbb{F}_p$ sonlu cismi üzerinde ikinci dereceden kalanlarla ilgilenilecek ve bunlarla ilgili bazı sonuçlar verilecektir.

1.3.1 Tanım. $a \in \mathbb{Z}$, $n \in \mathbb{N}$ ve $(a, n) = 1$ olmak üzere

$$x^2 \equiv a \ (n) \tag{1.1}$$

olacak biçimde bir $x \in \mathbb{Z}$ varsa $a \in \mathbb{Z}$ ye modülo n de bir *ikinci dereceden kalan* denir. Modülo n de ikinci dereceden kalanların kümesi $\boldsymbol{Q}_n$ ile gösterilir.

Eğer (1.1) denkliğinin bir çözümü yoksa bu durumda $a \in \mathbb{Z}$ ye modülo n de bir *ikinci dereceden kalan değildir* denir.

Örneğin modülo 11 deki ve modülo 8 deki ikinci dereceden kalanların kümesi, sırasıyla, $\boldsymbol{Q}_{11} = \{ \overline{1}, \overline{3}, \overline{4}, \overline{5}, \overline{9} \}$ ve $\boldsymbol{Q}_8 = \{ \overline{1} \}$ dir.

Çalışmada $n = p$ asal sayı olması hali ile ilgileneceğinden aşağıda bu durumla ilgili bazı teoremler verilmiştir.

1.3.2 Teorem. $p > 2$ asal sayı olmak üzere modülo p de $\frac{p-1}{2}$ tane ikinci dereceden kalan ve $\frac{p-1}{2}$ tane ikinci dereceden kalan olmayan eleman vardır (Silverman 2006).

1.3.3 Teorem (Çarpım Teoremi). p bir tek asal sayı olmak üzere

i. Modulo p de iki tane ikinci dereceden kalan sayının çarpımı bir ikinci dereceden kalan sayıdır.

ii. Modulo p de bir ikinci dereceden kalan ve bir ikinci dereceden kalan olmayan sayının çarpımı bir ikinci dereceden kalan değildir.

iii. Modulo p de iki tane ikinci dereceden kalan olmayan sayının çarpımı bir ikinci dereceden kalan sayıdır (Silverman 2006).

Verilen bir $a \in \mathbb{Z}$ sayısının bir ikinci dereceden kalan olup olmadığını belirlemek için adına Legendre sembolü denilen bir sembol kullanılır ve bu sembol aşağıdaki gibi tanımlanır:

1.3.4 Tanım (Legendre Sembolü). $a \in \mathbb{Z}$ ve bir $p > 2$ asal sayısı için a tamsayısının *Legendre sembolü*

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & x^2 \equiv a\,(p) \text{ nin bir çözümü var} \\ 0 & p \mid a \\ -1 & x^2 \equiv a\,(p) \text{ nin çözümü yoktur} \end{cases} = \begin{cases} +1 & a \text{ bir ikinci dereceden kalan} \\ 0 & p \mid a \\ -1 & a \text{ bir ikinci dereceden kalan degil} \end{cases}$$

olarak tanımlanır.

Örneğin, $p = 11$ ise

$$\left(\frac{a}{11}\right) = \begin{cases} +1, & a \equiv 1,3,4,5,9\ (11) \\ 0, & 11 \mid a \\ -1, & a \equiv 2,6,7,8,10\ (11). \end{cases}$$

dir.

Aşağıdaki teorem, $x^2 \equiv -1\ (p)$ denkliğinin hangi asal sayılar için bir çözümü olduğunu göstermektedir.

1.3.5 Teorem. -1 sayısının modülo p de ikinci dereceden bir kalan olması için gerek ve yeter şart $p \equiv 1\ (4)$ olmasıdır (Silverman 2006 ve Mollin 2000).

1.3.6 Teorem. $p > 2$ asal sayı ve $p \nmid a$ olmak üzere a nın modülo p de bir ikinci dereceden kalan olması için gerekli ve yeter şart $a^{\frac{(p-1)}{2}} \equiv 1\ (p)$ olmasıdır (Silverman 2006).

Jacob Jacobi, Legendre sembolünü bileşik modlar için genelleştirmiş ve Jacobi sembolünü aşağıdaki gibi tanımlamıştır.

1.3.7 Tanım (Jacobi Sembolü). $n \in \mathbb{N}$ bir tek sayı, $a \in \mathbb{Z}$ ve $(a, n) = 1$ olsun. p_j ler asal sayılar olmak üzere $n = \prod_{j=1}^{k} p_j$ olsun. Bu durumda n sayısı için a tamsayısının *Jacobi sembolü*

$$\left(\frac{a}{n}\right) = \prod_{j=1}^{k}\left(\frac{a}{p_j}\right)$$

olarak tanımlanır, bu eşitliğin sağ tarafındaki sembol Legendre sembolünü belirtmektedir.

Örneğin, $n = 105 = 3 \cdot 5 \cdot 7$ ise $a = 2$ tamsayısı için,

$$\left(\frac{2}{105}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right)\left(\frac{2}{7}\right) = (-1)(-1)(1) = 1$$

dir.

Kronecker sembolü adı verilen sembol yukarıdaki sembollerin en genelidir. Dikkat edilirse, Jacobi sembolü n sayısının bir tek sayı olması halinde tanımlıdır, Kronecker sembolü ise herhangi bir n doğal sayısı için tanımlıdır.

1.3.8 Tanım (Kronecker Sembolü). $n \in \mathbb{N}$ ve $\Delta \in \mathbb{Z}$ sayısı $\Delta \equiv 0, 1\ (4)$ özelliğinde bir tam kare olmayan sayı olsun. Bu durumda m tek sayı ve $n = 2^{\alpha}m$ özelliğinde bir sayı olmak üzere,

$$\left(\frac{\Delta}{n}\right) = \begin{cases} 0 & (\Delta, n) > 1 \\ \left(\frac{\Delta}{2}\right)^{\alpha}\left(\frac{\Delta}{m}\right) & (\Delta, n) = 1 \end{cases}$$

olarak tanımlanır, burada

$$\left(\frac{\Delta}{2}\right) = \begin{cases} +1, & \Delta \equiv 1(8) \\ -1, & \Delta \equiv 5(8) \end{cases}$$

ve $\left(\frac{\Delta}{m}\right)$, Jacobi sembolünü belirtmektedir. Özel olarak, $\Delta = 2^k d$ ($d \in \mathbb{Z}$ tek) ve $(n, \Delta) = 1$ olmak üzere

$$\left(\frac{\Delta}{n}\right) = \left(\frac{2}{n}\right)^k \left(\frac{n}{|d|}\right)(-1)^{\frac{d-1}{2}\frac{n-1}{2}}$$

olur, burada $\left(\frac{n}{|d|}\right)$, Jacobi sembolünü belirtmektedir.

Örneğin, $n = 2831453 = 1033 \cdot 2741$ ve $\Delta = -21484 = -4 \cdot 41 \cdot 131 = -4 \cdot 5371$ için

$$\left(\frac{\Delta}{n}\right) = \left(\frac{2}{n}\right)^2 \left(\frac{2831453}{5371}\right)(-1)^{\frac{5371-1}{2}\frac{2831453-1}{2}} = \left(\frac{2831453}{5371}\right)$$

ve $2831453 \equiv 936\ (5371)$ olduğundan

$$\left(\frac{2831453}{5371}\right) = \left(\frac{936}{5371}\right) = \left(\frac{2}{5371}\right)^3 \left(\frac{3}{5371}\right)^2 \left(\frac{13}{5371}\right)$$

yazılabilir ve $5371 \equiv 3\ (8)$ olduğundan

$$-\left(\frac{13}{5371}\right) = -\left(\frac{5371}{13}\right) = -\left(\frac{2}{5371}\right) = 1$$

olarak bulunur.

Özellikle denkliklerin çözümlerinde kullanılan Fermat'ın küçük teoremi sayılar teorisinin en iyi bilinen teoremlerinden biridir.

1.3.8 Teorem (Fermat'ın Küçük Teoremi). p bir asal sayı ve a, modülo p de sıfırdan farklı bir sayı olsun. Bu durumda

$$a^{p-1} \equiv 1\ (p)$$

dir (Silverman 2006).

1.4 Üçüncü Dereceden Kalanlar

Bu kısımda $\mathbb{F}_p$ sonlu cismi üzerinde üçüncü dereceden kalanlarla ilgilenilecek ve bunlarla ilgili bazı sonuçlar verilecektir.

1.4.1 Tanım. p bir asal sayı olmak üzere

$$x^3 \equiv a \ (p) \tag{1.2}$$

olacak biçimde bir $x \in \mathbb{Z}$ varsa $a \in \mathbb{Z}$ ye modülo p de bir *üçüncü dereceden kalan* denir. Modülo p de üçüncü dereceden kalanların kümesi $\boldsymbol{K_p}$ ile gösterilir.

Eğer (1.2) denkliğinin bir çözümü yoksa bu durumda $a \in \mathbb{Z}$ ye modülo p de bir *üçüncü dereceden kalan değildir* denir.

$\boldsymbol{K_p^*} = \boldsymbol{K_p} - \{ 0 \}$, $\mathbb{Z}_p^*$ deki çarpma işlemine göre bir gruptur, aslında $\mathbb{Z}_p^*$ ın bir alt grubudur. Üstelik $p \equiv 1$ (3) bir asal sayı ve ω birimin 1 den farklı olan kübik kökü olmak üzere $\omega = \frac{-1+\sqrt{-3}}{2}$ ve ω^2 sayıları $\mathbb{Z}_p^*$ ın birer elemanıdır.

1.4.2 Tanım (Üçüncü Dereceden Kalan Karakteri). p tek asal sayı olmak üzere bir a tam sayısının *modülo p deki kübik karakteri* $\left(\frac{a}{p}\right)_3$ ile gösterilir ve

$$\left(\frac{a}{p}\right)_3 = \begin{cases} 0, & p \mid a \\ 1, & a \in K_p \\ \omega, \omega^2, & a \notin K_p \end{cases}$$

biçiminde tanımlanır.

1.4.3 Teorem. $p \equiv 1$ (3) bir asal sayı olmak üzere $x^3 \equiv a \ (p)$ denkliğinin çözülebilmesi için gerek ve yeter şart $a^{\frac{p-1}{3}} \equiv 1 \ (p)$ olmasıdır (Namlı 2001).

1.4.4 Teorem. Modülo p de farklı üçüncü dereceden kalanların sayısı,

$$p \equiv 1 \ (3) \ \text{ise} \ \frac{p+2}{3},$$

$$p \equiv 2 \ (3) \ \text{ise} \ p$$

dir (Namlı 2001).

2. BÖLÜM
ELİPTİK EĞRİLER

Bu bölümde eliptik eğriler hakkında bazı ön bilgiler verilecektir. Kısım 2. 1 de eliptik eğrilerin nasıl ortaya çıktığı üzerinde durulacak ve eliptik eğri kavramı tanımlanacaktır. Kısım 2. 2 de, bir cisim üzerinde tanımlanmış olan bir E eliptik eğrisinin noktalarının oluşturduğu küme üzerinde toplama işlemi tanımlanacak bu kümenin bir grup yapısına sahip olduğu gösterilecektir. Kısım 2. 3 de, eliptik eğriler üzerindeki sonlu mertebeli noktalarla ilgilenilecek ve bir E eliptik eğrisi üzerinde mertebesi iki ve üç olan noktaların grup yapısı verilecek ve n-mertebeli noktaların grup yapısı ile ilgili sonuçlar ele alınacaktır. Kısım 2. 4, de iki eliptik eğri arasındaki birasyonel denklik kavramı ele alınacaktır. Kısım 2. 5 de, singüler eğri kavramı ile ilgilenilecek ve singüler eğriler üzerinde bulunan singüler olmayan noktaların grup yapısı ile ilgilenilecektir. Kısım 2. 6 da, sonlu bir cisim üzerinde tanımlı eliptik eğriler ele alınacaktır. Kısım 2. 7 de, bir E eliptik eğrisinin Frobenius endomorfizmi tanımlanacak ve bu endomorfizmin izi yardımıyla da eliptik eğriler üzerindeki noktaların sayısının nasıl bulunabileceği ile ilgilenilecektir. Kısım 2. 8 de, bir E eliptik eğrisinin indirgemesi kavramı üzerinde durulacaktır. Kısım 2. 9 da, $\mathbb{F}_{q^n}$ üzerinde tanımlı E eliptik eğrisinin özellikleri belirtilecektir. Kısım 2.10 da ise bir eliptik eğrinin bölüm polinomların kavramı tanımlanacak ve bu polinomların bazı özellikleri incelenecektir.

2.1 Eliptik Eğriler

Eliptik eğriler teorisi, Fermat'ın son teoreminin çözümündeki rolünün öneminden dolayı matematiğin oldukça popüler bir çalışma alanı haline gelmiştir. Eliptik eğriler, çok uzun zamandır çözülemeyen problemlerin bile çözülmesinde rol oynamış cebirin en modern kavramlarından birisidir. Eliptik eğrilerin, matematik dünyasına girişi, ilk olarak Diophant'ın Arithmetica'sının dördüncü kitabındaki yirmi

dördüncü problemde görülür. Burada ki, problem şu şekildedir; verilen bir a sayısını, öyle iki parçaya ayrılısın ki, bu iki parçanın çarpımı başka bir sayının küpü ile kendisinin farkına eşit olsun, yani

$$y\,(a-y) = x^3 - x \qquad (2.1)$$

özelliğinde x ve y sayıları bulunabilir mi? Diophant bu problemi, $a = 6$ için $k = 3$ olmak üzere, $x = ky - 1$ alarak çözmüştür. Böylece (2.1) denklemi,

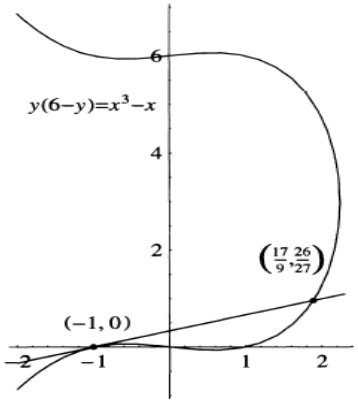
$$y\,(6-y) = (3y-1)^3 - 3y + 1$$

haline gelir ki, bu denklemin çözümleri $y = 0$ katlı kökü ve $y = \frac{26}{27}$ biçimindedir. $y = 0$ katlı kökü göz önüne alınmazsa, $y = \frac{26}{27}$ için $x = \frac{17}{9}$ olarak bulunur.

Diophant'ın probleminin çözümüne modern bir yaklaşım şu şekildedir: (2.1) eşitliğinin katlı kökü olan 0 yardımıyla eğri üzerindeki (–1, 0) noktası elde edilir. (–1, 0) noktasından bir teğet doğru çizilirse bu doğru (2.1) eşitliğinin belirttiği eğriyi $(\frac{17}{9}, \frac{26}{27})$ noktasında keser. Dolayısıyla, problemin çözümü $\frac{26}{27}$, $\frac{136}{27}$ $(6 = \frac{26}{27} + \frac{136}{27})$ olup bu sayıların çarpımı da

$$(\frac{17}{9})^3 - (\frac{17}{9})$$

sayısına eşittir. Aşağıdaki grafikte, (2.1) eşitliğinin belirttiği eğri ve ele alınan eşitliği gerçekleyen nokta görülmektedir.

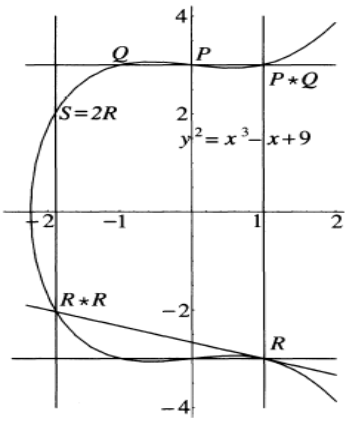


Şekil 2.1.1

Eğer (2.1) denkleminde $a = 6$ alınır, her iki taraftan 9 çıkarılır ve $x \to -x$ ve $y \to y + 3$ değişken değişimi uygulanırsa,

$$E : y^2 = x^3 - x + 9$$

eğrisi elde edilir. Dikkat edilirse, $x^3 - x + 9$ denkleminin farklı kökleri vardır. $(-1, 0)$ ve $(\frac{17}{9}, \frac{26}{27})$ noktaları ise $E : y^2 = x^3 - x + 9$ eğrisi üzerinde sırasıyla, $R = (1, -3)$ ve $R * R = (-\frac{17}{9}, -\frac{55}{27})$ noktalarına karşılık gelir. $R * R$ noktasının x eksenine göre simetriği alınarak E üzerinde, $2R = (-\frac{17}{9}, \frac{55}{27})$ noktası elde edilir. Aşağıdaki şekilde ise yeni eğri ve R, $R * R$ noktaları görülmektedir. Diophant bu işlemleri yaparken ileride adına eliptik eğriler teorisi denilecek olan bir teorinin temellerini atmıştır. Yaptığı bu işlemler ile eğri üzerindeki noktaların oluşturduğu kümenin toplamsal bir grup olduğu daha sonra görülmüştür.



Şekil 2.1.2

2.1.1 Tanım. $\mathbb{F}$ karakteristiği 2 ve 3 ten farklı bir cisim olsun. $A, B \in \mathbb{F}$ olmak üzere

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

biçimindeki denklemin tüm çözümlerinin oluşturduğu sıralı ikililerin kümesine bir *eliptik eğri* denir. Bu denkleme E eliptik eğrisinin *Weierstrass normal formu* veya sadece *Weierstrass formu* denir.

Eğer E, $\mathbb{F}$ cismi üzerinde tanımlı bir eliptik eğri ise E üzerindeki rasyonel noktaların kümesi $E(\mathbb{F})$ ile belirtilir, yani

$$E(\mathbb{F}) = \{ \boldsymbol{O} \} \cup \{ (x, y) \in \mathbb{F} \times \mathbb{F} \mid y^2 = x^3 + Ax + B \}$$

dir.

Buradaki $\boldsymbol{O} = (\infty, \infty)$ noktası sonsuzdaki nokta olarak adlandırılır ve bu noktanın daha sonra oluşturulacak grubun birim elemanı olduğu görülecektir.

Üstelik $x^3 + Ax + B$ kübik polinomu katlı köke sahip olmamalıdır, yani E bir eliptik eğri ise

$$4A^3 + 27B^2 \neq 0$$

dir. Örneğin; $y^2 = x^3 + 1$ ve $y^2 = x^3 - x$ birer eliptik eğri belirttiği halde $y^2 = x^3$ ve $y^2 = x^3 + x^2$ eşitlikleri (x^3 ve $x^3 + x^2$ katlı köke sahip olduğundan) birer eliptik eğri belirtmez.

Bununla birlikte $x^3 + Ax + B$ kübik polinomunun katlı kök bulunması hali de oldukça ilginç bir durumdur. Eğer kübik polinomun katlı kökleri var ise $y^2 = x^3 + Ax + B$ eşitliği adına singüler eğriler denilen eğrileri belirtir, çalışmanın önemli kısmında bu tip eğriler ele alınacak ve bu eğrilerin özellikleri ile ilgili sonuçlar verilecektir.

Bir eliptik eğrinin Weierstrass uzun formu aşağıdaki gibi verilir.

2.1.2 Tanım. $a_1, a_2, a_3, a_4, a_5, a_6 \in \mathbb{F}$ olmak üzere

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

biçimindeki denkleme E eliptik eğrisinin *Weierstrass uzun formu* denir.

Bu denklem için *Tate değerleri*

$$b_2 = a_1^2 + 4a_2$$

$$b_4 = a_1 a_3 + 2a_4$$

$$b_6 = a_3^2 + 4a_6$$

$$b_8 = a_1^2 a_6 - a_1 a_3 a_4 + 4a_2 a_6 + a_2 a_3^2 - a_4^2$$

olarak tanımlanır. Bundan başka E eliptik eğrisinin *diskriminantı* ve *j değişmezi*

$$\Delta(E) = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6$$

ve

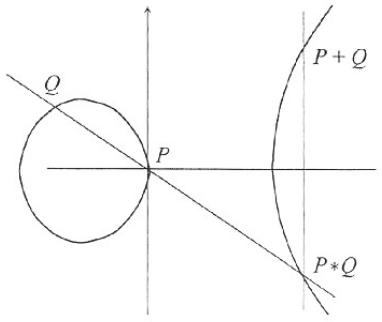
$$j = \frac{c_4^3}{\Delta}$$

olarak tanımlanır.

2.2 Eliptik Eğriler Üzerinde Toplama İşlemi

Bu kısımda, bir cisim üzerinde tanımlanmış olan bir E eliptik eğrisinin noktalarının oluşturduğu küme üzerinde toplama işlemi tanımlanarak bu kümenin bir grup yapısına sahip olduğu gösterilecektir. Bu nokta kümesi üzerindeki toplama işlemi aşağıdaki şekilde tanımlanır.

P ve Q, E eliptik eğrisi üzerinde farklı iki nokta olsun. Bu durumda P ve Q noktalarından geçen l doğrusu E eliptik eğrisini üçüncü bir noktada keser, eğer bu nokta $P * Q$ ile gösterilirse, P ve Q noktalarının toplamı olan $P + Q$, az önce elde edilen $P * Q$ noktasının x eksenine göre simetriği olarak tanımlanır.



Şekil 2.2.1

Bu toplama işlemi analitik olarak şöyle ifade edilebilir: $P = (x_1, y_1)$ ve $Q = (x_2, y_2)$, E eliptik eğrisi üzerinde farklı iki nokta ve bu iki noktadan geçen l doğrusunun denklemi $y = mx + b$ ise

$$y^2 = x^3 + Ax + B \text{ ve } y = mx + b$$

denklemlerinden

$$x^3 - m^2 x^2 + (A - 2mb)x + B - b^2 = 0 \qquad (2.2)$$

eşitliği elde edilir. Bu kübik polinomun kökleri x_1, x_2 ve $P * Q = (x_3, y_3)$ noktasının x koordinatı x_3 olmak üzere, $P * Q$ noktasının x eksenine göre simetriği olan nokta

$$P + Q = (x_3, -y_3)$$

noktasıdır.

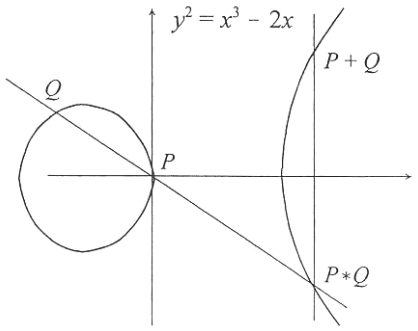
Yukarıda tanımlanan toplama işlemi örnekler yardımıyla aşağıdaki şekilde açıklanabilir; ilk olarak

$$E_1 : y^2 = x^3 - 2x$$

eğrisi ve bu eğri üzerindeki $P = (0, 0)$ ve $Q = (-1, 1)$ noktaları dikkate alınırsa P ve Q noktalarından geçen l doğrusunun denklemi $y = -x$ olur. O halde, bu eğri ve l doğrusunun kesiştikleri noktalar

$$x^3 - x^2 - 2x = 0$$

denklemi yardımıyla (0, 0), (–1, 1) ve (2, –2) olarak bulunur. Dolayısıyla, $P * Q = (2, -2)$ ve bu noktanın x eksenine göre simetriği olan nokta, yani $P + Q = (2, 2)$ dır. Aşağıdaki şekilde E_1 eğrisi üzerindeki P, Q, $P * Q$ ve $P + Q$ noktaları görülmektedir.

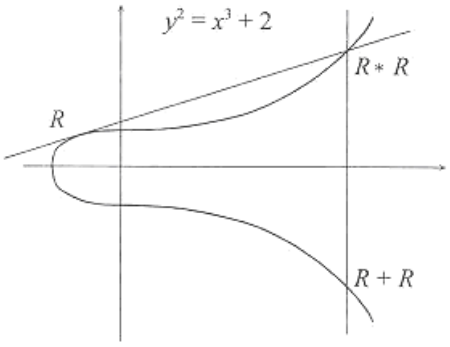


Şekil 2.2.2

Yukarıda farklı iki noktanın toplamı ile ilgili bir örnek ele alınmıştır, şimdi

$$E_2 : y^2 = x^3 + 2$$

eğrisi üzerindeki R = (–1, 1) noktasının kendisi ile toplamı dikkate alınacaktır. Bu durumda E_2 eğrisinin R noktasındaki teğeti olan l doğrusunun denklemi $y = \frac{3x+5}{2}$ dir. E_2 eğrisi ile l teğet doğrusunun kesiştikleri noktalar $(x + 1)^2 (x - \frac{17}{4}) = 0$ eşitliği yardımıyla, (–1, 1) ve $(\frac{17}{4}, \frac{71}{8})$ olarak bulunur. Dolayısıyla $R * R = (\frac{17}{4}, \frac{71}{8})$ ve böylece $R + R = (\frac{17}{4}, -\frac{71}{8})$ olarak elde edilir. Aşağıdaki şekilde E_2 eğrisi üzerindeki R, $R * R$ ve $R + R$ noktaları görülmektedir.



Şekil 2.2.3

2.2.1 Teorem. E, $\mathbb{F}$ cismi üzerinde tanımlı bir eliptik eğri olsun. Bu durumda E eliptik eğrisi üzerindeki noktalar aşağıdaki özellikleri gerçeklerler:

i. $P_1, P_2 \in E(\mathbb{F})$ olmak üzere $P_1 + P_2 = P_2 + P_1$ dir (değişme özelliği),

ii. $P \in E(\mathbb{F})$ olmak üzere $P + \boldsymbol{O} = P$ dir (birim eleman özelliği),

iii. $P \in E(\mathbb{F})$ ise $P + P' = \boldsymbol{O}$ olacak biçimde bir $P' \in E(\mathbb{F})$ vardır ve bu durumda $P' = -P$ dir (ters eleman özelliği),

iv. $P_1, P_2, P_3 \in E(\mathbb{F})$ olmak üzere $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$ dir (birleşme özelliği) (Washington 2003).

Yukarıda verilen teorem, E eliptik eğrisi üzerindeki noktaların oluşturduğu kümenin toplama işlemine göre bir değişmeli grup olduğunu belirtmektedir. Daha öncede belirtildiği gibi sonsuzdaki nokta "$\boldsymbol{O}$" bu grubun birim elemanıdır.

2.3 Eliptik Eğriler Üzerindeki Sonlu Mertebeli Noktalar

Bu kısımda, E eliptik eğriler üzerindeki sonlu mertebeli noktalar, yani büküm (torsiyon) noktaları ile ilgilenilecektir. İlk olarak sonlu mertebeli nokta kavramı açıklanacak daha sonra bir E eliptik eğrisi üzerinde mertebesi iki ve üç olan noktaların grup yapısı verilecek ve son olarak n-mertebeli noktaların grup yapısı ile ilgili sonuçlar ele alınacaktır.

2.3.1 Tanım. E, $\mathbb{F}$ cismi üzerinde tanımlı bir eliptik eğri ve $n \in \mathbb{N}$ olsun. Bu durumda

$$nP = \boldsymbol{O}$$

olacak biçimdeki $P \in E(\mathbb{F})$ noktasına *büküm* (*torsiyon*) *noktası* ya da *sonlu mertebeli nokta* denir. Bu şartı sağlayan en küçük n sayısına P noktasının *mertebesi* denir. Eğer P noktası bir büküm noktası değilse bu nokta *sonsuz mertebeli nokta* olarak adlandırılır.

2.3.2 Tanım. E, $\mathbb{F}$ cismi üzerinde tanımlı bir eliptik eğri ve $n \in \mathbb{N}$ olmak üzere

$$E[n] = \{ P \in E(\overline{\mathbb{F}}) \mid nP = \boldsymbol{O} \}$$

kümesine E eliptik eğrisinin *n. mertebeden noktalarının kümesi* ya da *n-büküm noktalarının kümesi* denir.

Dikkat edilirse $E[n]$ kümesi $E(\overline{\mathbb{F}})$ üzerinde tanımlanmıştır. Ayrıca $E[n]$ nin E nin bir alt grubu olduğu açıktır. Burada her $n \in \mathbb{N}$ için $\boldsymbol{O} \in E[n]$ dir.

Bir eliptik eğri üzerindeki iki mertebeli noktaların oluşturduğu grubun yapısı aşağıdaki önermede belirtilmiştir:

2.3.3 Önerme. E, $\mathbb{F}$ cismi üzerinde tanımlı bir eliptik eğri olsun. Eğer, $\mathbb{F}$ karakteristiği ikiden farklı bir cisim ise

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

eğer $\mathbb{F}$ karakteristiği iki olan bir cisim ise

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

dir (Washington 2003).

Aşağıdaki teorem ise bir eliptik eğri üzerindeki n mertebeli noktaların oluşturduğu grubun yapısı belirtilmektedir:

2.3.4 Teorem. E, $\mathbb{F}$ cismi üzerinde tanımlı bir eliptik eğri, $n \in \mathbb{N}$ olmak üzere $\mathbb{F}$ nin karakteristiği n yi bölmüyor veya sıfır ise

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

dır. Eğer $\mathbb{F}$ nin karakteristiği $p > 0$ ve $p \mid n$ ise $p \nmid n'$ olmak üzere $n = p^r n'$ için

$$E[n] \cong \mathbb{Z}_{n'} \otimes \mathbb{Z}_{n'} \text{ veya } E[n] \cong \mathbb{Z}_n \otimes \mathbb{Z}_{n'}$$

dir (Washington 2003).

2.3.5 Uyarı. Karakteristiği p olan bir cisim üzerinde tanımlı E eliptik eğrisi için $E[p] \cong \mathbb{Z}_p$ ise E eliptik eğrisine *sıradan* (*ordinary*) eğri ve $E[p] \cong \boldsymbol{O}$ ise *süpersingüler* eğri denir.

2.4 Birasyonel Denk Eliptik Eğriler

Bu kısımda iki eliptik eğri arasındaki birasyonel denklik kavramı ele alınacaktır. Buna göre verilen bir E eliptik eğrisi uygun birasyonel dönüşümlerle E den daha basit bir yapıya sahip bir E' eliptik eğrisine dönüştürülebilir.

2.4.1 Tanım. $\mathbb{F}$ cismi üzerinde tanımlı

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

ve

$$E' : y'^2 + a'_1x'y' + a'_3y' = x'^3 + a'_2x'^2 + a'_4x' + a'_6$$

E ve E' eliptik eğrileri verilsin. Bu durumda E eğrisini E' eğrisine dönüştüren

$$x = u^2\ x' + r, \qquad y = u^3\ y' + u^2\ s\,x' + t \qquad (u, r, s, t \in \mathbb{F}, u \neq 0) \tag{2.3}$$

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

Bu dönüşümlerin tersleri vardır ve tersleri

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

biçimindedir. Bu dönüşümlere *kendisi ve tersi rasyonel dönüşümler* denir. Bu durumda (2.3) de verilen dönüşümler E ve E' eliptik eğrileri arasında birebir-örten bir dönüşüm belirtir ve böylece $\mathbb{F}$ cismi üzerindeki birasyonel denklik ilişkisi bir denklik bağıntısı olur. Bu eğriler arasındaki bu birebir-örten dönüşüm $E(\mathbb{F})$ ve $E'(\mathbb{F})$ arasında bir izomorfizm oluşturur. Bu durumun tersi doğru değildir. Yani, E ve E'eğrileri $\mathbb{F}$ cismi üzerinde birasyonel denk olmasalar bile $E(\mathbb{F})$ ve $E'(\mathbb{F})$ izomorf olabilir.

2.4.2 Teorem. E, $\mathbb{F}$ cismi üzerinde tanımlı bir eliptik eğri (Kar($\mathbb{F}$) ≠ 2, 3) olsun. Bu durumda

$$E' : y^2 = x^3 + Ax + B \qquad (A, B \in \mathbb{F})$$

biçimindeki $E'(\mathbb{F})$ eğrisi için $\phi : E \to E'$ birasyonel dönüşümü vardır. (Schmitt ve Zimmer 2003).

Bu teorem, karakteristiği 2 ve 3 den farklı olan herhangi bir cisim üzerinde tanımlı bir E eliptik eğrisinin Weierstrass formunda ifade edilebileceğini belirtmektedir.

2.5 Singüler Eğriler

$x^3 + Ax + B = 0$ kübik denkleminin birbirinden farklı kökleri ya da katlı kökleri bulunabilir. Eğer bu kübik denklemin katlı kökü var ise $y^2 = x^3 + Ax + B$ eşitliğinin belirttiği eğrini bir eliptik eğri olmadığı daha önce belirtilmişti. Acaba $x^3 + Ax + B = 0$ kübik denklemi katlı kök bulunduruyorsa ne olur? Toplama kuralı bu durumda da geçerli olur mu? Bu kısımda bu sorulara yanıtlar aranacak, bu durumda eliptik eğrinin noktalarının oluşturduğu küme üzerindeki toplama işleminin, $\mathbb{F}$ nin elemanlarının toplamı, $\mathbb{F}^* = \mathbb{F} \setminus \{\bar{0}\}$ ın elemanlarının çarpımı veya $\mathbb{F}$ nin bir genişlemesindeki elemanlarının çarpımına dönüştüğü görülecektir. İlk olarak bu katlı kökler yardımıyla elde edilen eğri üzerindeki noktalar adlandırılacak ve bu noktaların karakteri belirlenecektir.

2.5.1 Tanım. C cebirsel eğrisi $f(x, y) = 0$ denklemiyle tanımlansın. Bu durumda $P = (x_o, y_o) \in C$ noktasının C eğrisinin bir *singüler noktası* olması için gerek ve yeter şart

$$\frac{\partial f}{\partial x}(x_o, y_o) = 0 \text{ ve } \frac{\partial f}{\partial y}(x_o, y_o) = 0$$

olmasıdır.

Eğer $P = (x_o, y_o)$ noktasında birinci kısmi türevler sıfırsa singüler nokta katlı bir noktadır. Bu katlı nokta, iki farklı teğetinin olması halinde *düğüm (node) noktası*, iki teğetinin çakışması halinde *çıkıntı (cusp) noktası* olarak adlandırılır. Singüler noktaları olan eğriye *singüler eğri*, singüler noktaları olmayan bir eğriye de *singüler olmayan eğri* denir.

2.5.2 Önerme. Weierstrass uzun formunda verilen eliptik eğriler aşağıdaki gibi sınıflandırılabilir:

i. Eğri singüler değildir $\Leftrightarrow \Delta \neq 0$. Diğer durumda eğri tek bir singüler noktaya sahiptir,

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

iii. Eğrinin bir *çıkıntısı* vardır $\Leftrightarrow \Delta = 0$ ve $c_4 = 0$ dır (Silverman 1986).

Bu çalışmada $E_1 : y^2 = x^3$, $E_2 : y^2 = x^3 + ax^2$ ($a \in \mathbb{F}^*$) denklemleriyle verilen singüler eğrilerle ilgilenilecektir. $P = (0, 0)$ ve $\boldsymbol{O}$ noktasının bu eğriler üzerinde olduğu açıktır. Ayrıca $\Delta_{E_1} = \Delta_{E_2} = 0$ olduğundan bu eğrilerin j değişmezleri tanımlı değildir. Üstelik $c_{4,E_1} = 0$ ve $c_{4,E_2} = 16a^2$ olduğundan E_1 eğrisinin çıkıntısı ve E_2 eğrisinin düğümü vardır. Her iki halde de singüler nokta $P = (0, 0)$ noktasıdır. Bu noktanın singüler nokta olduğu kısmi türevler yardımıyla görülebilir. Örneğin E_1 eğrisi için,

$$f(x, y) = y^2 - x^3 = 0$$

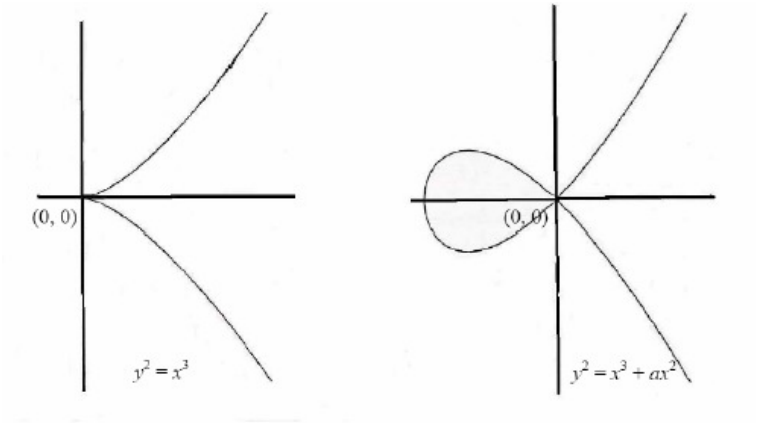
fonksiyonun kısmi türevleri

$$\frac{\partial f}{\partial x} = -3x^2, \qquad \frac{\partial f}{\partial y} = 2y$$

dir. O halde

$$y^2 - x^3 = 0, \qquad -3x^2 = 0, \qquad 2y = 0$$

denklemleri birlikte düşünülürse karakteristik ne olursa olsun bu üç denklemin bir tek çözümünün $x = y = 0$ olduğu görülür.



$P = (0, 0)$ noktası bir çıkıntıdır. $P = (0, 0)$ noktası bir düğümdür.

Şekil 2.5.1

İlk olarak $E_1 : y^2 = x^3$ denklemi ile verilen singüler eğri ele alınacak ve bu singüler eğrinin özellikleri üzerinde durulacaktır. Dikkat edilirse, $P = (0, 0)$ noktası E_1 üzerindeki tek singüler noktadır. Bu noktadan geçen herhangi bir doğru E_1 eğrisini bu noktadan başka en çok bir noktada kesebileceğinden $P = (0, 0)$ noktası ile eğrinin herhangi bir noktasının toplanması mümkün değildir, yani bu singüler nokta ile eğrinin singüler olmayan noktaları toplanamaz. Bu nedenle eğri üzerindeki singüler olmayan noktalar ve sonsuzdaki nokta olan $\boldsymbol{O}$ noktasının oluşturduğu noktaların kümesi dikkate alınır, bu noktaların kümesi $E_{ns}(\mathbb{F})$ ile gösterilir. Bu kümenin noktaları ile toplama işlemi yapılır ve bu noktalar için toplama işlemi daha önceki gibi tanımlıdır. Bu durumda eğrinin singüler olmayan herhangi iki noktasından geçen doğru hiçbir zaman $P = (0, 0)$ noktasından geçmez.

Aşağıdaki teorem bu singüler eğrinin üzerindeki singüler olmayan noktaların oluşturduğu $E_{ns}(\mathbb{F})$ kümesinin bir toplamsal grup olduğunu göstermektedir:

2.5.3 Teorem. $\mathbb{F}$ cismi üzerinde tanımlı $E_1 : y^2 = x^3$ eğrisi verilsin. $E_{ns}(\mathbb{F})$, $\boldsymbol{O}$ noktası ile birlikte E üzerindeki singüler olamayan noktaların kümesi olsun. Bu durumda

$$E_{ns}(\mathbb{F}) \to \mathbb{F}, \quad (x, y) \to \frac{x}{y}, \quad \boldsymbol{O} \to 0$$

dönüşümü bir izomorfizmidir ve $E_{ns}(\mathbb{F})$ bir toplamsal gruptur (Washington 2003, Silverman ve Tate 1992).

Benzer şekilde, $E_2 : y^2 = x^3 + ax^2$ denklemi ile verilen singüler eğri için de $P = (0, 0)$ noktası tek singüler noktadır. $\alpha^2 = a$ olmak üzere E_2 eğrisinin denklemi

$$\left(\frac{y}{x}\right)^2 = a + x$$

olarak da yazılabilir. x, 0 noktasına yaklaştıkça bu eşitliğin sağ tarafı a ya yaklaşır. O halde $x = 0$ olduğunda eğri

$$\left(\frac{y}{x}\right)^2 = a \text{ veya } \frac{y}{x} = \pm\alpha$$

olur. Bu ise (0, 0) noktasından geçen teğetlerin

$$y = \alpha x \text{ ve } y = -\alpha x$$

olduğunu gösterir. Böylece, bu durumda $E_{ns}(\mathbb{F})$ kümesinin grup yapısı aşağıdaki teorem ile verilebilir.

2.5.4 Teorem. $a \in \mathbb{F}^*$ olmak üzere $E_2 : y^2 = x^3 + ax^2$ eğrisi verilsin. Bu durumda $\alpha^2 = a$ olmak üzere ϕ dönüşümü

$$\phi : (x, y) \to \frac{y + \alpha x}{y - \alpha x} \ , \ \boldsymbol{O} \to 1$$

olarak tanımlı olsun. Bu durumda,

i. $\alpha \in \mathbb{F}$ ise ϕ dönüşümü $E_{ns}(\mathbb{F})$ ve $\mathbb{F}^*$ arasında bir izomorfizmdir,

ii. $\alpha \notin \mathbb{F}$ ise ϕ dönüşümü $E_{ns}(\mathbb{F})$ ve $\{ u + \alpha v \mid u, v \in \mathbb{F}, u^2 - av^2 = 1\}$ arasında bir izomorfizmdir, bu küme çarpma işlemi altında bir gruptur (Washington 2003, Silverman ve Tate 1992).

2.6 Sonlu Cisimler Üzerinde Tanımlı Eliptik Eğriler

Bu kısımda sonlu bir cisim üzerinde tanımlı eliptik eğriler ele alınacaktır. $\mathbb{F}_p$, p bir asal sayı olmak üzere p elemanlı sonlu bir cisim ve E eliptik eğrisi $\mathbb{F}_p$ cismi üzerinde tanımlı olsun. Bu durumda $x, y \in \mathbb{F}_p$ olacak biçimdeki E üzerindeki (x, y) ikilileri sonlu çoklukta olduğundan $E(\mathbb{F}_p)$ mutlaka sonlu bir grup oluşturur.

Sonlu cisimler üzerinde tanımlı eliptik eğrilerle ilgili çalışmaların büyük bir kısmı bu eğriler üzerindeki noktaların sayısının belirlenmesi ile ilgilidir. Sonlu bir cisim üzerinde tanımlı bir eliptik eğri üzerindeki noktaların sayısı için şöyle bir

tahminde bulunulabilir; her bir x değeri için, eliptik eğrinin denklemini gerçekleyen en çok iki y değeri bulunacağından $E(\mathbb{F}_p)$ üzerindeki noktaların sayısı için bir üst sınır $2p + 1$ olarak düşünülebilir, bu toplama sonsuzdaki $\boldsymbol{O}$ noktası da dahildir. Diğer yandan eğrinin bu denklemini gerçekleyen sonlu bir cisimdeki elemanların ikinci dereceden bir kalan olma olasılığı yüzde elli olduğundan bu noktaların sayısı p tane olacaktır. Böylece $E(\mathbb{F}_p)$ üzerindeki noktaların sayısı için bir üst sınır, $\boldsymbol{O}$ noktası ile birlikte $p + 1$ olur.

Aşağıda verilecek olan Hasse teoremi $E(\mathbb{F}_p)$ eğrisi üzerindeki noktaların sayısının yaklaşık olarak $p + 1$ olduğunu belirtmektedir.

2.6.1 Hasse Teoremi. E, $\mathbb{F}_p$ sonlu cismi üzerinde tanımlı bir eliptik eğri olsun. Bu durumda

$$|\#\, E(\mathbb{F}_p) - (p + 1)| \leq 2\sqrt{p}$$

dır (Silverman 1986).

Aşağıdaki teorem ise ikinci dereceden kalanlar yardımıyla bir eliptik eğri üzerindeki noktaların sayısının tam olarak ne olduğunu belirtmektedir.

2.6.2 Teorem. $E : y^2 = x^3 + Ax + B$ eliptik eğrisi $\mathbb{F}_p$ sonlu cismi üzerinde tanımlı bir eliptik eğri olmak üzere

$$\#\, E(\mathbb{F}_p) = p + 1 + \sum_{x \in F_p} \left(\frac{x^3 + Ax + B}{p} \right)$$

dir (Washington 2003).

2.7 Frobenius Endomorfizmi

Bu kısımda (x, y), E eliptik eğrisi üzerinde bir nokta olmak üzere (x^p, y^p) noktasını veren bir endomorfizm tanımlanacak ve bu endomorfizmin izi yardımıyla da eliptik eğriler üzerindeki noktaların sayısının nasıl bulunabileceği belirtilecektir.

2.7.1 Tanım. E, $\mathbb{F}_p$ sonlu cismi üzerinde tanımlı bir eliptik eğri olsun. E eliptik eğrisinin *p-Frobenius endomorfizmi*

$$\varphi_p : E \to E$$

$$\varphi_p(x, y) = (x^p, y^p), \quad \varphi_p(\boldsymbol{O}) = \boldsymbol{O}$$

olarak tanımlanır.

2.7.2 Teorem. E, $\mathbb{F}_p$ sonlu cismi üzerinde tanımlı bir eliptik eğri olsun. Bu durumda φ_p Frobenius endomorfizmi olmak üzere

$$\varphi_p^2 - a\varphi_p + p = 0$$

eşitliğini gerçekleyen bir tek a tamsayısı vardır. Diğer bir ifade ile $(x, y) \in E(\mathbb{F}_p)$ ise

$$\varphi_p^2(x, y) - a\varphi_p(x, y) + p(x, y) = 0$$

eşitliğini gerçekleyen bir tek a tamsayısı vardır. Bu a tamsayısına *p-Frobenius endomorfizminin izi* denir. Üstelik bu a tamsayısı $(m, p) = 1$ olmak üzere her m için

$$a \equiv \mathrm{iz}((\varphi_p)_m) \pmod{m}$$

denkliğini gerçekleyen tek tamsayıdır (Washington 2003, Schmitt ve Zimmer 2003).

Aşağıdaki teorem endomorfizmin izi yardımıyla eliptik eğri üzerindeki noktaların sayısını vermektedir.

2.7.3 Teorem. E, $\mathbb{F}_p$ sonlu cismi üzerinde tanımlı bir eliptik eğri olsun. p-Frobenius endomorfizminin izi a olmak üzere

$$\#\, E(\mathbb{F}_p) = p + 1 - a$$

dir (Schmitt ve Zimmer 2003).

2.7.4 Uyarı. $X^2 - aX + p$ biçimindeki polinoma Frobenius endomorfizminin *karakteristik polinomu* denir.

2.8 Bir Eliptik Eğrinin İndirgemesi

$E : y^2 = x^3 + Ax + B$ eliptik eğrisi $\mathbb{Q}$ cismi üzerinde tanımlı bir eğri ve p bir asal sayı olsun. Bu durumda modülo p de bir indirgeme dönüşümü vardır. İndirgeme dönüşümü kullanılarak E eğrisinden

$$\tilde{E} : y^2 = x^3 + \tilde{A}\, x + \tilde{B}$$

eliptik eğrisi elde edilir, burada $\tilde{A}, \tilde{B} \in \mathbb{F}_p$ dir. Bu eğri için aşağıdaki üç halden biri söz konusudur ve dolayısıyla E eliptik eğrisi aşağıdaki biçimde sınıflandırılabilir:

i. $\tilde{E}$ singüler olmayan bir eğri ise E *iyi indirgemeye* sahiptir,

ii. $\tilde{E}$ eğrisinin düğümü (node) varsa E *çarpımsal indirgemeye* sahiptir,

iii. $\tilde{E}$ eğrisinin çıkıntısı (cusp) varsa E *toplamsal indirgemeye* sahiptir.

Son iki haldeki gibi bir indirgeme söz konusu ise E eliptik eğrisi *kötü indirgemeye* sahiptir denir. Eğer E çarpımsal indirgemeye sahip ve düğümden geçen teğetlerin eğimleri $\mathbb{F}_p$ (ya da $\mathbb{F}_p$ de değilse) de ise bu indirgemeye *dağılan çarpımsal indirgeme* (ya da *dağılmayan çarpımsal indirgeme*) denir.

2.8.1 Örnek. $\mathbb{Q}$ cismi üzerinde tanımlı

$$E : y^2 = x(x + 35)(x - 55)$$

eliptik eğrisi dikkate alınırsa, bu durumda

$\mathbb{F}_5$ de $\qquad\qquad \tilde{E} : y^2 = x^3$

$\mathbb{F}_7$ de $\quad \tilde{E} : y^2 = x^2(x+1)$

$\mathbb{F}_{11}$ de $\quad \tilde{E} : y^2 = x^2(x+2)$

indirgenmiş eğrileri elde edilir. Birinci durumda $\tilde{E}$ eğrisinin çıkıntısı vardır ve dolayısıyla E, $\mathbb{F}_5$ de toplamsal indirgemeye sahiptir. İkinci durumda E, $\mathbb{F}_7$ de dağılan çarpımsal indirgemeye sahiptir ve son durumda ise teğetin eğimi $\alpha \notin \mathbb{F}_{11}$ olduğundan E, $\mathbb{F}_{11}$ de dağılmayan çarpımsal indirgemeye sahiptir. Eğer p asal sayısı 13 ten büyükse bu durumda kübik polinomun $\mathbb{F}_p$ de farklı kökleri olur ve dolayısıyla E eğrisi $\mathbb{F}_p$ üzerinde singüler olmayan bir eğri olur, yani E eğrisi $p > 13$ için iyi indirgemeye sahiptir. Dikkat edilirse, E eğrisi singüler bir eğri olamadığı halde bu eğrinin $\mathbb{F}_p$ üzerindeki indirgemeleri singüler olabilir.

2.9 $\mathbb{F}_{p^n}$ Üzerinde Tanımlı Eliptik Eğriler

Bu kısımda, aşağıda verilecek olan teorem ile $\mathbb{F}_p$ sonlu cismi üzerinde tanımlı eliptik eğrilerin nokta sayıları yardımıyla $\mathbb{F}_{p^n}$ üzerinde tanımlı olan eliptik eğrilerin üzerindeki noktaların sayısı belirlenecektir.

2.9.1 Teorem. p-Frobenius endomorfizminin izi a olmak üzere

$$\#E(\mathbb{F}_p) = p + 1 - a$$

olsun. Eğer

$$X^2 - aX + p = (X - \alpha)(X - \beta)$$

ise her $n \geq 1$ için

$$\# E(\mathbb{F}_{p^n}) = p^n + 1 - (\alpha^n + \beta^n)$$

dir (Washington 2003).

2.9.2 Örnek. $E : y^2 + xy = x^3 + 1$ denklemi ile verilen E eliptik eğrisi için $\# E(\mathbb{F}_2) = 4$ dir.

Bu durumda $a = 2 + 1 - 4 = -1$ olduğundan karakteristik polinom

$$X^2 + X + 2 = \left(X - \frac{-1+\sqrt{-7}}{2}\right)\left(X - \frac{-1-\sqrt{-7}}{2}\right)$$

biçimindedir. O halde Teorem 2.9.1 gereği

$$\# E(\mathbb{F}_4) = 4 + 1 - \left(\frac{-1+\sqrt{-7}}{2}\right)^2 - \left(\frac{-1-\sqrt{-7}}{2}\right)^2 = 8$$

olarak bulunur. Benzer biçimde

$$\left(\frac{-1+\sqrt{-7}}{2}\right)^{101} + \left(\frac{-1-\sqrt{-7}}{2}\right)^{101} = 2969292210605269$$

dir ve dolayısıyla

$$\# E(\mathbb{F}_{2^{101}}) = 2^{101} + 1 - 2969292210605269 = 2535301200456455833701195805484$$

olarak bulunur (Washington 2003).

2.10 Bölüm Polinomları

Bu kısımda bir eliptik eğrinin bölüm polinomları kavramı tanımlanacak ve bu polinomların bazı özellikleri incelenecektir. Daha sonra bir eliptik eğrinin bölüm polinomları yardımıyla eliptik bölünebilir diziler tanımlanacaktır.

2.10.1 Teorem. E, $\mathbb{F}$ cismi üzerinde tanımlı

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

denklemi ile verilmiş bir eliptik eğri olsun. Bu durumda E eliptik eğrisinin

$$\psi_n \in \mathbb{Z}[x, y, A, B]$$

bölüm polinomları

$$\psi_0 = 0,$$

$$\psi_1 = 1,$$

$$\psi_2 = 2y,$$

$$\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2,$$

$$\psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3),$$

$$\vdots$$

her $n \geq 2$ için,

$$\psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3$$

her $n \geq 3$ için,

$$\psi_{2n} = \left(\frac{\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2}{\psi_2} \right)$$

ve $n < 0$ için

$$\psi_{-n} = -\psi_n$$

biçimindedir (Washington 2003).

Aşağıdaki teoremde bir eliptik eğrinin bölüm polinomlarının gerçeklediği ve eliptik bölünebilir dizilerin tanımında da kullanılacak bir bilineer bağıntı verilmiştir.

2.10.2 Teorem. Bir eliptik eğrinin bölüm polinomları her $n, m \in \mathbb{Z}$ için

$$\psi_{m+n}\psi_{m-n} = \psi_{m+1}\psi_{m-1}\psi_n^2 - \psi_{n+1}\psi_{n-1}\psi_m^2$$

eşitliğini gerçeklerler (Charlap ve Robbins 1988).

2.10.3 Teorem. E, $\mathbb{F}$ cismi üzerinde tanımlı

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

denklemi ile verilmiş bir eliptik eğri olsun. Bu durumda her $n \in \mathbb{Z}$ için ψ_n bölüm polinomlarının katsayıları $R = \mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$ halkasındadır (Swart 2003).

2.10.4 Teorem. Bir eliptik eğrinin bölüm polinomları bölünebilirlik özelliğine sahiptir, yani $n \mid m$ ise $\psi_n \mid \psi_m$ dir (Ian Connel).

3. BÖLÜM

$\mathbb{F}_p$ ÜZERİNDE TANIMLI SİNGÜLER EĞRİLER

Çalışmanın bu bölümünde $p > 3$ bir asal sayı olmak üzere, $\mathbb{F}_p$ sonlu cismi üzerinde tanımlı $E_1 : y^2 = x^3$ ve $E_2 : y^2 = x^3 + ax^2$ singüler eğrileri ele alınacaktır. Kısım 3.1 de $E_1 : y^2 = x^3$ eğrisi ele alınacak bu eğri üzerindeki noktaların sayısı literatürdeki yöntemlerden farklı yöntemlerle verilecek, E_1 eğrisi üzerindeki singüler olmayan noktaların karakterleri belirlenecektir. Daha sonra bu eğriler üzerindeki noktaların apsis ve ordinatlarının toplamlarıyla ilgili bazı sonuçlar elde edilecek ve E_1 singüler eğrisi üzerindeki singüler olmayan noktaların grup yapısı belirlenecektir. Son olarak E_1 singüler eğrisi üzerindeki sonlu mertebeli noktaların neler olduğu belirlenecektir. Kısım 3.2 de E_1 singüler eğrisi için yapılan bu işlemler $E_2 : y^2 = x^3 + ax^2$ singüler eğrileri için yapılacaktır. Kısım 3.3 de ise $\mathbb{F}_{p^n}$ üzerinde tanımlı E_1 ve E_2 singüler eğrilerinin mertebeleri belirlenecektir.

3.1 $\mathbb{F}_p$ Üzerinde Tanımlı $E_1 : y^2 = x^3$ Eğrisi Üzerindeki Rasyonel Noktalar

Bu kısımda ilk olarak $E_1 : y^2 = x^3$ eğrisi üzerindeki rasyonel noktaların sayısı belirlenecektir. Daha sonra bu noktalarla ilgili bazı özellikler verilecek, bu eğri üzerindeki büküm noktaları belirlendikten sonra bu eğri üzerindeki singüler olmayan noktalar kümesinin grup yapısı belirlenecektir.

Aşağıdaki teorem E_1 eğrisi üzerindeki noktaların sayısını belirtmektedir:

3.1.1 Teorem. $\mathbb{F}_p$ sonlu cismi üzerinde tanımlı $E_1 : y^2 = x^3$ singüler eğrisi üzerindeki noktaların sayısı

$$\#E_1(\mathbb{F}_p) = p + 1$$

dir.

İspat. (x, y) noktası E_1 eğrisi üzerinde $P = (0, 0)$ ve $\boldsymbol{O}$ noktasından farklı bir nokta olsun. Bu durumda $y^2 = x^3$ eşitliğinden $t = x^3 \in \boldsymbol{Q}_p$ olacak biçimde bir t sayısı vardır. O halde bu biçimdeki t sayılarının sayısı $\boldsymbol{Q}_p$ nin eleman sayısı olan $\frac{p-1}{2}$ tanedir. Üstelik $y^2 = t$ olduğundan her bir t sayısı için iki tane y değeri vardır. Dolayısıyla bu biçimdeki (x, y) noktalarının sayısı $2 \cdot \frac{p-1}{2} = p - 1$ tanedir. Son olarak $P = (0, 0)$ singüler noktası ve $\boldsymbol{O}$ noktası dikkate alınarak E_1 singüler eğrisi üzerindeki noktaların sayısının $p + 1$ tane olduğu görülür.

3.1.2 Uyarı. $E_1 : y^2 = x^3$ singüler eğrisi üzerinde $P = (0, 0)$ singüler noktası ve $\boldsymbol{O}$ noktası ile birlikte $p + 1$ tane nokta vardır. Dikkat edilirse bu eğri bir süpersingüler eğri değildir.

Bu teorem ikinci dereceden kalanlar yardımıyla aşağıdaki şekilde ifade edebilir:

3.1.3 Teorem. $\mathbb{F}_p$ sonlu cismi üzerinde tanımlı $E_1 : y^2 = x^3$ singüler eğrisi üzerindeki noktaların sayısı

$$\#E_1(\mathbb{F}_p) = 2 + \sum_{x \in F_p} \rho(x)$$

dir, burada

$$\rho(x) = \begin{cases} 2, & \left(\frac{x^3}{F_p}\right) = 1 \\ 0, & \left(\frac{x^3}{F_p}\right) \neq 1 \end{cases}$$

dir.

İspat. Eğer $x^3 = y^2 = t \in \boldsymbol{Q}_p$ ise $\boldsymbol{U}_p$, $\mathbb{F}_p$ deki birimlerin kümesi olmak üzere $y \in \boldsymbol{U}_p$ nin iki değeri vardır. Eğer $x^3 = y^2 = t \notin \boldsymbol{Q}_p$ ise bu durumda t bir ikinci dereceden kalan

olmadığından böyle bir y değeri yoktur. Son olarak $P = (0, 0)$ singüler noktası ve $\boldsymbol{O}$ noktası ile birlikte $E_1 : y^2 = x^3$ singüler eğrisi üzerindeki noktaların sayısı $2 + \sum_{x \in F_p} \rho(x)$ dır.

3.1.4 Örnek. $\mathbb{F}_{11}$ üzerinde tanımlı $y^2 = x^3$ singüler eğrisi verilsin. Bu durumda bu eğri üzerindeki noktaların sayısı $\boldsymbol{Q}_{11} = \{ 1, 3, 4, 5, 9 \}$ olduğundan

$$\#E_1(\mathbb{F}_p) = 2 + \sum_{x \in F_p} \rho(x)$$

$$= 2 + \rho(0) + \rho(1) + \rho(2) + \rho(3) + \rho(4) + \rho(5) + \rho(6) + \rho(7) + \rho(8) + \rho(9) + \rho(10)$$

$$= 2 + 0 + 2 + 0 + 2 + 2 + 2 + 0 + 0 + 0 + 2 + 0 \; = \; 12$$

olarak bulunur.

Bu sonuç, ikinci dereceden kalanlar yerine üçüncü dereceden kalanlar yardımıyla yeniden ifade edebilir:

3.1.5 Teorem. $y^2 = x^3 = t$ olsun. Bu durumda $\mathbb{F}_p$ üzerinde tanımlı $E_1 : y^2 = x^3$ eğrisi üzerindeki noktaların sayısı

$$\#E_1(\mathbb{F}_p) = \begin{cases} 1 + \sum_{y \in F_p} f(t) & p \equiv 1(6) \\ 1 + \sum_{y \in F_p} g(t) & p \equiv 5(6) \end{cases}$$

dir, burada

$$f(t) = \begin{cases} 0, & t \notin K_p \\ 1, & p \mid t \\ 3, & t \in K_p^* \end{cases}$$

ve $g(t) = 1$ dir.

İspat. ***i.*** $p \equiv 1$ (6) olsun. Eğer $p \mid t$ ise $x^3 \equiv t$ (p) denkliği $x^3 \equiv 0$ (p) haline gelir ve bu halde tek çözüm $x \equiv 0$ (p) dir ve bu çözümden $P = (0, 0)$ noktası elde edilir. $t \notin \boldsymbol{K}_p^* = \boldsymbol{K}_p$ ise t üçüncü dereceden kalan değildir ve $x^3 \equiv t$ (p) denkliğinin çözümü yoktur. Eğer $t \in \boldsymbol{K}_p^*$ ise $p \equiv 1$ (6) ve $(p - 1 , 3) = 3$ olduğundan $x^3 \equiv t$ (p) denkliği üç tane çözüme sahiptir.

ii. $p \equiv 5\ (6)$ olsun. Eğer $p \mid t$ ise $x^3 \equiv t\ (p)$ denkliği $x^3 \equiv 0\ (p)$ haline gelir ve bu halde tek çözüm $x \equiv 0\ (p)$ dir ve yukarıdakine benzer biçimde bu çözümden $P = (0, 0)$ noktası elde edilir. $p \equiv 5\ (6)$ olduğundan her bir t sayısı bir üçüncü dereceden kalandır. Dolayısıyla her bir $t \in \boldsymbol{K}_p^*$ için $p \equiv 5\ (6)$ ve $(p - 1, 3) = 1$ olduğundan $x^3 \equiv t\ (p)$ denkliğinin bir tane çözümü vardır.

3.1.6 Örnek. $\mathbb{F}_{13}$ üzerinde tanımlı $y^2 = x^3$ singüler eğrisi verilsin. Bu durumda bu eğri üzerindeki noktaların sayısı $y^2 = x^3 = t$ ve $\boldsymbol{K}_{13} = \{ 0, 1, 5, 8, 12 \}$ olduğundan

$$\#E_1(\mathbb{F}_p) = 1 + \sum_{y \in F_p} f(t)$$

$$= 1 + f(0) + f(1) + f(4) + f(9) + f(3) + f(12) + f(10) + f(10) + f(12) + f(3) + f(9) + f(4) + f(1)$$

$$= 1 + 1 + 3 + 0 + 0 + 0 + 3 + 0 + 0 + 3 + 0 + 0 + 0 + 0 + 3 = 14$$

olarak bulunur.

Aşağıdaki teoremde $E_1 : y^2 = x^3$ singüler eğrisi üzerindeki singüler olmayan noktaların karakterleri belirlenmiştir:

3.1.7 Teorem. $\mathbb{F}_p$ sonlu cismi üzerinde tanımlı $E_1 : y^2 = x^3$ singüler eğrisi verilsin. Bu durumda (x, y) noktasının E_1 singüler eğrisi üzerinde singüler olmayan bir nokta olması için gerek ve yeter şart $x \in \boldsymbol{Q}_p$ ve $y \in \boldsymbol{K}_p$ olmasıdır.

İspat. (x, y) noktası E_1 singüler eğrisi üzerinde singüler olmayan bir nokta olsun. Bu durumda (x, y) noktası $y^2 = x^3$ eşitliğini gerçeklediğinden bu eşitlik $y^2 = x^2\ x$ olarak yeniden yazılırsa $x^2, y^2 \in \boldsymbol{Q}_p$ (x, y) olduğundan $x \in \boldsymbol{Q}_p$ dir. Tersine $x \in \boldsymbol{Q}_p$ ise $x^3 \in \boldsymbol{Q}_p$ olacağından $x^3 = y^2$ olacak biçimde bir $y \in \mathbb{F}_p$ noktası vardır. Üstelik $x = t^2$ ise $y = t^3$ tür.

Benzer biçimde $y^2 = x^3$ eşitliğinden $y^2 \in \boldsymbol{K}_p$ ve dolayısıyla $y \in \boldsymbol{K}_p$ dir. Tersine $y \in \boldsymbol{K}_p$ ise $y^2 \in \boldsymbol{K}_p$ olacağından $x^3 = y^2$ olacak biçimde bir $x \in \mathbb{F}_p$ noktası vardır. Üstelik $y = t^3$ ise $x = t^2$ dir.

3.1.8 Örnek. $\mathbb{F}_{17}$ üzerinde tanımlı $y^2 = x^3$ singüler eğrisi verilsin. Bu durumda

$\boldsymbol{Q}_{17}$ = { 1, 2, 4, 8, 9, 13, 15, 16 } ve $\boldsymbol{K}_{17}$ = { 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16 } olduğu dikkate alınırsa

$E_1(\mathbb{F}_{17})$ = { (0, 0), (1, 1), (1, 16), (2, 5), (2, 12), (4, 8), (4, 9), (8, 6), (8, 11), (9, 7), (9, 10),

(13, 2), (13, 15), (15, 3), (15, 3), (15, 14), (16, 4), (16, 3), $\boldsymbol{O}$ }

biçimindedir ve eğri üzerindeki bu noktalar için $x \in \boldsymbol{Q}_p$ ve $y \in \boldsymbol{K}_p$ dir.

"(x, y) noktası singüler olmayan bir noktadır $\Leftrightarrow x \in \boldsymbol{Q}_p$ ve $y \in \boldsymbol{K}_p$ " olduğu göz önüne alınarak $E_1 : y^2 = x^3$ singüler eğrisi üzerindeki noktaların apsisleri ve ordinatları ile ilgili sonuçlar verilebilir:

3.1.9 Teorem. $\mathbb{F}_p$ sonlu cismi üzerinde tanımlı $E_1 : y^2 = x^3$ singüler eğrisi verilsin. Bu eğri üzerindeki noktaların apsislerinin toplamı

$$\sum_{(x,y)\in E_1} x \equiv 0 \ (p)$$

ve bu eğri üzerindeki noktaların ordinatlarının toplamı

$$\sum_{(x,y)\in E_1} y \equiv 0 \ (p)$$

dır.

İspat. (x, y) noktası E_1 üzerinde singüler olmayan bir nokta ise $x \in \boldsymbol{Q}_p$ olduğundan E_1 üzerindeki tüm singüler olmayan (x, y) noktalarının x- koordinatlarının toplamı $\boldsymbol{Q}_p$ nin elemanlarının toplamına eşittir, yani,

$$\sum_{(x,y)\in E_{ns}} x \equiv \sum_{t\in Q_p} t \tag{3.1}$$

dir. $\boldsymbol{Q}_p$ nin elemanları { 1, 4, … , $(\frac{p-1}{2})^2$ } dir, dolayısıyla, $\boldsymbol{Q}_p$ nin elemanlarının toplamı

$$\frac{\left(\frac{p-1}{2}\right)\left(\frac{p-1}{2}+1\right)\left(2\frac{p-1}{2}+1\right)}{6} = \frac{p(p-1)(p+1)}{24} \tag{3.2}$$

olarak bulunur. Böylece (3.1) ve (3.2) eşitliklerinden

$$\sum_{(x,y)\in E_{ns}} x \equiv 0 \ (p)$$

olduğu görülür.

Benzer biçimde (x, y) noktası E_1 üzerinde singüler olmayan bir nokta ise $y \in \boldsymbol{K}_p$ olduğundan E_1 üzerindeki tüm singüler olmayan (x, y) noktalarının y-koordinatlarının toplamı $\boldsymbol{K}_p$ nin elemanlarının toplamına eşittir. Bu durumda iki hal söz konusudur.

i. $p \equiv 1\ (6)$ olsun. Bu durumda $c \neq 0$ olmak üzere bir $c \in \boldsymbol{K}_p$ vardır. Diğer bir ifade ile $c \equiv x^3\ (p)$ olacak biçimde bir $c \in \mathbb{F}_p$ vardır. $p - x \neq x$ olduğundan $(p - x)^3 \equiv -x^3 \equiv -c\ (p)$ ve dolayısıyla $-c \in \boldsymbol{K}_p$ dir. Dolayısıyla "$c \in \boldsymbol{K}_p \Leftrightarrow -c \in \boldsymbol{K}_p$" dir. $\boldsymbol{K}_p^*$ ın eleman sayısı $\frac{p-1}{3}$ olduğundan $\frac{p-1}{6}$ tane c ve $p - c$ çifti vardır. Bu biçimdeki her bir çiftin toplamı p tane olduğundan

$$\sum_{k \in K_p^*} k = \frac{p(p-1)}{6}$$

dir.

ii. $p \equiv 5\ (6)$ olsun. Bu durumda $\boldsymbol{K}_p = \mathbb{F}_p$ olduğundan

$$\sum_{k \in K_p} k = \frac{p(p+1)}{2}$$

olur. Dolayısıyla her iki halde de

$$\sum_{(x,y) \in E_{ns}} y \equiv 0\ (p)$$

dir. Son olarak $P = (0, 0)$ noktası ile birlikte

$$\sum_{(x,y) \in E_1} x \equiv \sum_{(x,y) \in E_1} y \equiv 0\ (p)$$

olarak bulunur.

Şimdi E_1 eğrisi üzerindeki singüler olmayan (x, y) noktalarının ordinatları ile ilgilenecektir. Aşağıdaki teoremde farklı ordinatlara sahip noktaların sayısının ne olduğu belirlenmiştir:

3.1.10 Teorem. $\mathbb{F}_p$ sonlu cismi üzerinde tanımlı $E_1 : y^2 = x^3$ singüler eğrisi verilsin. Bu durumda E_1 singüler eğrisi üzerindeki farklı ordinatlara sahip singüler olmayan (x, y) noktalarının sayısı

$$\begin{cases} \dfrac{p-1}{3} & p \equiv 1(6) \\ p-1 & p \equiv 5(6) \end{cases}$$

dir.

İspat. $y^2 \equiv x^3 \ (p)$ denkliğinde $y^2 = t$ olarak alınırsa $x^3 \equiv t \ (p)$ olur. Bu denkliğin çözümü ise iki farklı y değeri verir. Dolayısıyla iki hal söz konusudur.

İlk olarak $p \equiv 1 \ (6)$ olsun. Bu durumda, bu denkliğin farklı çözümlerinin sayısı $\frac{p+2}{3}$ tanedir. Bu çözümlerden bir tanesi 0 olduğundan $\frac{p+2}{3} - 1 = \frac{p-1}{3}$ çözümün iki farklı x değeri vardır.

Eğer $p \equiv 5 \ (6)$ ise bu durumda bu denkliğin farklı çözümlerinin sayısı p dir, bu çözümlerden bir tanesi 0 olduğundan, bu halde de $p - 1$ çözümün iki farklı x değeri vardır.

3.1.11 Örnek. $\mathbb{F}_7$ ve $\mathbb{F}_{23}$ üzerinde tanımlı $y^2 = x^3$ singüler eğrisi üzerindeki noktalar

$$E_1(\mathbb{F}_7) = \{ (0, 0), (1, 1), (1, 6), (2, 5), (2, 1), (2, 6), (4, 1), (4, 6), \boldsymbol{O} \},$$

$$E_1(\mathbb{F}_{23}) = \{ (0, 0), (1, 1), (1, 22), (2, 10), (2, 13), (3, 2), (3, 21), (4, 8), (4, 15),$$
$$(6, 3), (6, 20), (8, 11), (8, 12), (9, 4), (9, 19), (12, 7), (12, 16), (13, 9),$$
$$(13, 14), (16, 5), (16, 18), (18, 6), (18, 17), \boldsymbol{O} \}$$

biçimindedir. Burada farklı ordinatlar sırasıyla

$1, 6 \in \boldsymbol{K}_7^*$ ve $1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22 \in \boldsymbol{K}_{23}^*$

dir.

Aşağıdaki teorem ile E_1 singüler eğrisi üzerindeki singüler olmayan noktaların grup yapısı belirlenmiştir:

3.1.12 Teorem. $\mathbb{F}_p$ sonlu cismi üzerinde tanımlı $E_1 : y^2 = x^3$ singüler eğrisi verilsin. Bu durumda,

$$E_{ns}(\mathbb{F}_p) \cong \mathbb{Z}_p$$

dir.

İspat. Lagrange teoremi gereği, $E_{ns}(\mathbb{F}_p)$ nin mertebesi p ve p bir asal sayı olduğundan $E_1 : y^2 = x^3$ singüler eğrisi üzerindeki $\boldsymbol{O}$ dan farklı her bir singüler olmayan (x, y) noktasının mertebesi p dir. Dolayısıyla $E_{ns}(\mathbb{F}_p)$ kümesi $\mathbb{Z}_p$ ye izomorftur.

Eliptik eğri teorisinde büküm noktalar, yani sonlu mertebeli noktalar önemli bir yer tutar. Bu çalışma da $\mathbb{F}_p$ sonlu cismi ile ilgilenildiğinden $\mathbb{F}_p$ de tanımlı eliptik eğriler üzerindeki tüm noktalar birer büküm noktasıdır. Aşağıdaki teoremde $E_1 : y^2 = x^3$ singüler eğrisi üzerindeki sonlu mertebeli noktaların mertebelerinin sadece p olabileceği görülecektir.

3.1.13 Teorem. $\mathbb{F}_p$ sonlu cismi üzerinde tanımlı $E_1 : y^2 = x^3$ singüler eğrisi verilsin. Bu durumda,

$$E[p] \cong \mathbb{Z}_p$$

ve $m \neq p$ için

$$E[m] \cong \{ \boldsymbol{O} \}$$

dir.

İspat. m pozitif bir tamsayı olmak üzere mertebesi m olan bir büküm noktasının

$$E[m] = \{ P \in E_{ns}(\overline{\mathbb{F}}_p) \mid mP = \boldsymbol{O} \}$$

olduğu hatırlanırsa her bir $P = (x, y) \in E_n(\overline{\mathbb{F}}_p)$ noktasının mertebesi p olduğundan

$$E[p] \cong \mathbb{Z}_p$$

olarak bulunur.

3.2 $\mathbb{F}_p$ Üzerinde Tanımlı $E_2: y^2 = x^3 + ax^2$ Eğrisi Üzerindeki Rasyonel Noktalar

Bu kısımda ilk olarak $a \in \mathbb{F}_p^*$ olmak üzere $E_2 : y^2 = x^3 + ax^2$ eğrileri üzerindeki noktaların sayısı belirlenecektir. Daha sonra bu noktalarla ilgili bazı özellikler verilecek, bu eğriler üzerindeki büküm noktaları belirlenecek ve bu eğriler üzerindeki singüler olmayan noktalar kümesinin grup yapısı belirlenecektir.

E_2 eğrileri üzerindeki noktaların sayısını belirlemek için aşağıdaki teoreme ihtiyaç duyulacaktır.

3.2.1 Teorem. p bir tek asal sayı ve $f \in \mathbb{Z}[x]$ derecesi birden büyük bir polinom olsun. Bu durumda $y^2 \equiv f(x)$ denkliğinin $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$ çözümlerinin sayısı

$$N_p(f) = p + S_p(f)$$

dir, burada

$$S_p(f) = \sum_{x=0}^{p-1} \left(\frac{f(x)}{p} \right)$$

dir (Lemmermeyer 2000).

3.2.2 Teorem. $\mathbb{F}_p$ sonlu cismi üzerinde tanımlı $E_2 : y^2 = x^3 + ax^2$ ($a \in \mathbb{F}_p^*$) singüler eğrileri üzerindeki noktaların sayısı

$$\#E_2(\mathbb{F}_p) = \begin{cases} p & a \in Q_p \\ p+2 & a \notin Q_p \end{cases}$$

dir.

İspat. $y^2 \equiv f(x) = x^3 + ax^2$ olduğundan

$$S_p(f) = \sum_{x=0}^{p-1} \left(\frac{x^3 + ax^2}{p} \right) = \sum_{x=0}^{p-1} \left(\frac{x^2}{p} \right) \sum_{x=0}^{p-1} \left(\frac{x+a}{p} \right)$$

$$= \left(\left(\frac{0}{p} \right) + \sum_{x=1}^{p-1} \left(\frac{x^2}{p} \right) \right) \left(\left(\frac{a}{p} \right) + \sum_{x=1}^{p-1} \left(\frac{x+a}{p} \right) \right)$$

$$= (p-1)\left(\frac{a}{p}\right) = -\left(\frac{a}{p}\right)$$

dir. Dolayısıyla $y^2 \equiv f(x)$ denkliğinin çözümlerinin sayısı

$$N_p(f) = p + S_p(f) = p - \left(\frac{a}{p}\right)$$

olur. O halde $E_2 : y^2 = x^3 + ax^2$ singüler eğrileri üzerindeki noktaların sayısı $\left(\frac{a}{p}\right) = 1$ ise $\boldsymbol{O}$ noktası ile birlikte

$$\#E_2(\mathbb{F}_p) = p - 1 + 1 = p$$

ve $\left(\frac{a}{p}\right) = -1$ ise $\boldsymbol{O}$ noktası ile birlikte

$$\#E_2(\mathbb{F}_p) = p + 1 + 1 = p + 2$$

dir.

Bu teorem ikinci dereceden kalanlar yardımıyla aşağıdaki şekilde yeniden ifade edilebilir:

3.2.3 Teorem. $\mathbb{F}_p$ sonlu cismi üzerinde tanımlı $E_2 : y^2 = x^3 + ax^2$ ($a \in \mathbb{F}_p^*$) singüler eğrileri üzerindeki noktaların sayısı

$$\#\, E_2(\mathbb{F}_p) = 3 + \sum_{x \in F_p} \rho(x)$$

dir, burada

$$\rho(x) = \begin{cases} 2 & \left(\frac{x^3 + ax^2}{F_p}\right) = 1 \\ 0 & \left(\frac{x^3 + ax^2}{F_p}\right) \neq 1 \end{cases}$$

dir .

İspat. Eğer $x^3 + ax^2 = t \in \boldsymbol{Q}_p$ ise $y \in \boldsymbol{U}_p$ nin iki değeri vardır. Eğer $x^3 + ax^2 = t \notin \boldsymbol{Q}_p$ ise bu durumda t bir ikinci dereceden kalan olmadığından böyle bir y değeri yoktur. $y = 0$ ise x_1, $x_2 = 0$ ve $x_3 = p - a$ olmak üzere üç nokta daha vardır. Dolayısıyla $P = (0, 0)$ singüler

noktası ve $(p - a, 0)$ noktası da E_2 singüler eğrisi üzerindedir. Son olarak sonsuzdaki nokta $\boldsymbol{O}$ noktası ile birlikte noktaların sayısı $3 + \sum_{x \in F_p} \rho(x)$ dır.

3.2.4 Örnek. $\mathbb{F}_{13}$ üzerinde tanımlı $y^2 = x^3 + 12x^2$ singüler eğrisi verilsin. Bu durumda $\boldsymbol{Q}_{13} = \{ 1, 3, 4, 9, 10, 12 \}$ olduğundan bu eğri üzerindeki noktaların sayısı

$$\#E_1(\mathbb{F}_p) = 3 + \sum_{x \in F_p} \rho(x)$$

$$= \rho(0) + \rho(2) + \rho(3) + \rho(4) + \rho(5) + \rho(6) + \rho(7) + \rho(8) + \rho(9) + \rho(10) + \rho(11) + \rho(12)$$

$$= 3 + 0 + 2 + 0 + 2 + 2 + 0 + 0 + 0 + 0 + 2 + 2 = 13$$

olarak bulunur.

Aşağıdaki teoremde $E_2 : y^2 = x^3 + ax^2$ $(a \in \mathbb{F}_p^*)$ singüler eğrileri üzerindeki $(p - a, 0)$ biçimindeki noktaların karakterleri ile ilgili bir sonuç verilmiştir.

3.2.5 Teorem. $\mathbb{F}_p$ sonlu cismi üzerinde tanımlı $E_2 : y^2 = x^3 + ax^2$ $(a \in \mathbb{F}_p^*)$ singüler eğrileri verilsin. Bu durumda E_2 eğrileri üzerindeki $(p - a, 0)$ noktasının apsisi $a \in \boldsymbol{Q}_p$ ise

$$\begin{cases} p - a \in Q_p & p \equiv 1(4) \\ p - a \notin Q_p & p \equiv 3(4) \end{cases}$$

ve $a \notin \boldsymbol{Q}_p$ ise

$$\begin{cases} p - a \notin Q_p & p \equiv 1(4) \\ p - a \in Q_p & p \equiv 3(4) \end{cases}$$

özelliğindedir.

İspat. İlk olarak $a \in \boldsymbol{Q}_p$ olsun. Bu durumda $p \equiv 1$ (4) ise $-1 \in \boldsymbol{Q}_p$ olacağından $p - a \in \boldsymbol{Q}_p$ dır, eğer $p \equiv 3$ (4) ise $-1 \notin \boldsymbol{Q}_p$ olacağından $p - a \notin \boldsymbol{Q}_p$ olur. Benzer biçimde, $a \notin \boldsymbol{Q}_p$ ise, $p \equiv 1$ (4) için $p - a \notin \boldsymbol{Q}_p$ ve $p \equiv 3$ (4) için $p - a \in \boldsymbol{Q}_p$ dir.

3.2.6 Örnek. $\mathbb{F}_{13}$ üzerinde tanımlı $y^2 = x^3 + x^2$ singüler eğrisi üzerindeki (12, 0) noktası için, $12 \in \boldsymbol{Q}_{13}$ dir. $y^2 = x^3 + 5x^2$ singüler eğrisi üzerindeki (8, 0) noktası için, $8 \notin \boldsymbol{Q}_{13}$ dir.

Benzer biçimde $\mathbb{F}_{11}$ üzerinde tanımlı $y^2 = x^3 + x^2$ singüler eğrisi üzerindeki (10, 0) noktası için, $10 \notin \boldsymbol{Q}_{11}$ ve $y^2 = x^3 + 8x^2$ singüler eğrisi üzerindeki (3, 0) noktası için, $3 \in \boldsymbol{Q}_{11}$ dir.

Aşağıda $E_2 : y^2 = x^3 + ax^2$ singüler eğrileri üzerindeki $(p - a, 0)$ biçimindeki noktaların apsisleri toplamı ile ilgili bir sonuç verilmiştir.

3.2.7 Teorem. $\mathbb{F}_p$ sonlu cismi üzerinde tanımlı $E_2 : y^2 = x^3 + ax^2$ singüler eğrileri üzerindeki $(p - a, 0)$ noktalarının apsisleri toplamı

$$\sum_{(p-a,0)\in E_2} x \equiv 0 \ (p)$$

dır.

İspat. $a \in \boldsymbol{Q}_p$ olsun. Bu durumda $(p - a, 0)$ noktası E_2 üzerinde bir nokta ise $p \equiv 1 \ (4)$ için $p - a \in \boldsymbol{Q}_p$ olduğundan E_2 eğrileri üzerindeki tüm $(p - a, 0)$ noktalarının x- koordinatlarının toplamı $\boldsymbol{Q}_p$ nin elemanlarının toplamına eşittir, yani

$$\sum_{(p-a,0)\in E_2} x \equiv \sum_{t\in Q_p} t = \frac{p(p-1)(p+1)}{24} \equiv 0 \ (p)$$

dir. $p \equiv 3 \ (4)$ ise $p - a \notin \boldsymbol{Q}_p$ olduğundan E_2 eğrileri üzerindeki tüm $(p - a, 0)$ noktalarının x- koordinatlarının toplamı $\mathbb{F}_p^* \setminus \boldsymbol{Q}_p$ nin elemanlarının toplamına eşittir, yani

$$\sum_{(p-a,0)\in E_2} x \equiv \sum_{t\in F_p^* \setminus Q_p} t$$

dir. Dolayısıyla E_2 eğrileri üzerindeki tüm $(p - a, 0)$ noktalarının toplamı

$$\frac{p(p-1)}{2} - \frac{p(p-1)(p+1)}{24} = \frac{p(p-1)(11-p)}{24}$$

olarak bulunur. $a \notin \boldsymbol{Q}_p$ olması hali ise benzer biçimde görülür.

Aşağıdaki teoremde $E_2 : y^2 = x^3 + ax^2$ singüler eğrileri üzerindeki rasyonel noktaların apsisleri toplamı ile ilgili bir sonuç verilmiştir.

3.2.8 Teorem. $\mathbb{F}_p$ sonlu cismi üzerinde tanımlı $E_2 : y^2 = x^3 + ax^2$ singüler eğrileri üzerindeki singüler noktaların apsisleri toplamı

$$\sum_{x\in F_p}\left(1+\left(\frac{x^3+ax^2}{F_p}\right)\right)x$$

biçimindedir.

İspat. İkinci dereceden kalan tanımı gereği

$$\left(\frac{t}{F_p}\right)=\begin{cases}+1 & x^2\equiv t\,(p)\text{nin bir çözümü var}\\ 0 & p\mid t\\ -1 & x^2\equiv t\,(p)\text{nin çözümü yoktur}\end{cases}$$

olduğundan $1+\left(\frac{t}{F_p}\right)=0$, 1 ya da 2 dir. $y\equiv 0\ (p)$ ise $x^3+ax^2\equiv 0\ (p)$ dır ve $p\mid 0$ olduğundan $\left(\frac{x^3+ax^2}{F_p}\right)=0$ dır. Dolayısıyla denklemin çözümü olan her bir $(p-a,\ 0)$ noktası için $(1+0)\,x=x$ toplama eklenir. $x^3+ax^2=t$ olsun. $\left(\frac{t}{F_p}\right)=+1$ ise çözüm olan her bir $(x,\ y)$ noktası için $(x,\ -y\ )$ noktası da bir çözümdür. Böylece her bir t için $(1+1)\,x=2x$ toplama eklenir. Son olarak $\left(\frac{t}{F_p}\right)=-1$ ise $x^2\equiv t\ (p)$ nin hiç çözümü yoktur ve böyle $(x,\ y)$ noktaları için $(1+(-1))\,x=0$ dır.

Aşağıdaki teoremde $E_2: y^2=x^3+ax^2$ singüler eğrileri üzerindeki rasyonel noktaların ordinatları toplamı ile ilgili bir sonuç verilmiştir:

3.2.9 Teorem. $\mathbb{F}_p$ sonlu cismi üzerinde tanımlı $E_2: y^2=x^3+ax^2$ singüler eğrileri üzerindeki singüler noktaların ordinatları toplamı

$$\begin{cases}\sum\limits_{(x,y)\in E_2} y=\dfrac{p(p-1)}{2}, & a\in Q_p\\ \sum\limits_{(x,y)\in E_2} y=\dfrac{p(p-3)}{2}, & a\notin Q_p\end{cases}$$

diğer bir ifade ile her $a\in\mathbb{F}_p^*$ için

$$\sum_{(x,y)\in E_2} y\equiv 0\ (p)$$

dir.

İspat. Eğer $y \equiv 0\ (p)$ ise $x^3 + ax^2 \equiv 0\ (p)$ denkliğinin x_1, $x_2 \equiv 0$ ve $x_3 \equiv p - a\ (p)$ olmak üzere üç çözümü vardır. $x^3 + ax^2$ ifadesini kare yapan diğer x değerleri için $\left(\frac{x^3 + ax^2}{F_p}\right) = 1$ olduğundan $E_2 : y^2 = x^3 + ax^2$ singüler eğrisi üzerinde iki nokta elde edilir. O halde $a \in \boldsymbol{Q}_p$ ise $\frac{p-3}{2}$ tane ve $a \notin \boldsymbol{Q}_p$ ise $\frac{p-1}{2}$ tane x noktası vardır. Herhangi bir $t \in \mathbb{F}_p^*$ için $x^3 + ax^2 = t^2$ olsun. Bu durumda $y^2 \equiv t^2\ (p) \Leftrightarrow \pm y$ dir. Dolayısıyla bu biçimdeki y değerleri toplamı $t + (p - t) = p$ olur.

Aşağıdaki teoremde $E_2 : y^2 = x^3 + ax^2$ singüler eğrileri üzerindeki singüler olmayan rasyonel noktaların oluşturduğu grup yapısı verilmiştir.

3.2.10 Teorem. $\mathbb{F}_p$ sonlu cismi üzerinde tanımlı $E_2 : y^2 = x^3 + ax^2$ singüler eğrileri verilsin. Bu durumda

$$E_{ns}(\mathbb{F}_p) \cong \begin{cases} Z_{p-1}, & a \in Q_p \\ Z_{p+1}, & a \notin Q_p \end{cases}.$$

İspat. $E_{ns}(\mathbb{F}_p)$ nin grup yapısını belirlemek için $a \in \boldsymbol{Q}_p$ ve $a \notin \boldsymbol{Q}_p$ olmak üzere iki hal söz konusudur. Buna göre Teorem 2.5.4 gereği $\alpha \in \mathbb{F}$ olmak üzere $\alpha^2 = a$ ise

$$E_{ns}(\mathbb{F}) \cong \mathbb{F}^*$$

olduğundan $\mathbb{F}$ cismi yerine $\mathbb{F}_p$ sonlu cismi alınırsa $a \in \boldsymbol{Q}_p$ olması halinde

$$E_{ns}(\mathbb{F}_p) \cong \mathbb{F}_p^*$$

ve dolayısıyla

$$E_{ns}(\mathbb{F}_p) \cong \mathbb{Z}_{p-1}$$

olarak bulunur. Yine Teorem 2.5.4 gereği $\alpha \notin \mathbb{F}$ ise

$$E_{ns}(\mathbb{F}) \cong \{\, u + \alpha v \mid u, v \in \mathbb{F},\ u^2 - av^2 = 1 \,\}$$

dir. Benzer biçimde $\mathbb{F}$ cismi yerine $\mathbb{F}_p$ sonlu cismi alınırsa $a \notin \boldsymbol{Q}_p$ olması halinde

$$K = \{ u + \alpha v \mid u, v \in \mathbb{F}, u^2 - av^2 = 1 \}$$

kuadratik cisim genişlemesi $\mathbb{Z}_{p+1}$ e izomorf olduğundan

$$E_{ns}(\mathbb{F}_p) \cong \mathbb{Z}_{p+1}$$

olarak bulunur.

Bu cisim genişlemesinde $u = \bar{1} \in \mathbb{F}_p$ için $u^2 - av^2 = 1$ eşitliğinden $v = 0$ yani $\bar{1} \in K$ etkisiz elemanı elde edilir. $u = 0$ için iki hal söz konusudur.

i. $p \equiv 1\ (4)$ ise $\bar{0} \in \mathbb{F}_p$ elemanına karşılık K da bir eleman yoktur. Bu halde $-1 \in \boldsymbol{Q}_p$ ve $a \notin \boldsymbol{Q}_p$ olduğundan $-\frac{1}{a} \notin \boldsymbol{Q}_p$ dir. Dolayısıyla da $v^2 \equiv -\frac{1}{a}\,(p)$ denkliğinin çözümü yoktur.

ii. $p \equiv 3\ (4)$ olsun. Bu durumda $-1, a \notin \boldsymbol{Q}_p$ olduğundan $-\frac{1}{a} \in \boldsymbol{Q}_p$ dir. Dolayısıyla da $v^2 \equiv -\frac{1}{a}\ (p)$ denkliğin iki çözümü vardır. Bu çözümlerden elde edilen $\alpha v_1, \alpha v_2 \in K$ elemanlarının mertebeleri ise 4 tür. Gerçektende

$$(\alpha v_1)^2 = \alpha^2 v_1^2 = -1$$

ve dolayısıyla

$$(\alpha v_1)^4 = 1$$

dir. Son olarak $\overline{p-1} \in \mathbb{F}_p$ için $u^2 - av^2 = 1$ eşitliğinden $v = 0$ yani $u = p - 1$ elde edilir. Bu elemanın mertebesinin 2 olduğu açıktır.

Aşağıdaki teoremde, bu grupta bu elemandan başka iki mertebeli bir eleman olamayacağından, $E[2] \cong \mathbb{Z}_2$ olduğu görülecektir.

3.2.11 Teorem. $\mathbb{F}_p$ sonlu cismi üzerinde tanımlı $E_2 : y^2 = x^3 + ax^2$ singüler eğrileri verilsin. Bu durumda,

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

dir.

İspat. $\mathbb{F}$ karakteristiği 2 ve 3 ten farklı bir cisim olsun. $E : y^2 = (x - e_1)(x - e_2)(x - e_3)$ eğrisi $\mathbb{F}$ cismi üzerinde tanımlı ise $e_1, e_2, e_3 \in \overline{\mathbb{F}}$ olmak üzere

$$E[2] \cong \{ \boldsymbol{O}, (e_1, 0), (e_2, 0), (e_3, 0) \}$$

ve dolayısıyla

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

dir. O halde $y^2 = x^3 + ax^2$ eğrisi için

$$y^2 = x\,(x^2 + ax)$$

oluğundan

$$E[2] \cong \{ \boldsymbol{O}, (p - a, 0) \}$$

ve dolayısıyla

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

dir.

Şimdi $\mathbb{F}$ karakteristiği 2 ve 3 ten farklı bir cisim olmak üzere $\mathbb{F}$ cismi üzerinde tanımlı $E_2 : y^2 = x^3 + ax^2$ singüler eğrileri üzerindeki $E[3]$ kümesi yani mertebesi 3 olan noktalar belirlenecektir. "$3P = \boldsymbol{O}$ olması için gerek ve yeter şart $2P = -P$ noktasından geçen teğetin x-eksenine dik olmasıdır". Bir başka ifade ile $2P$ noktasının apsisi ile P nin apsisi aynıdır. Buna göre $m = \dfrac{3x^2 + 2ax}{2y}$ olmak üzere $m^2 - ax - 2x = x$ ve $y^2 = x^3 + ax^2$ olduğundan

$$(3x^2 + 2ax)^2 = 4(3x + a)(x^3 + ax^2)$$

ve gerekli düzenlemeler yapılarak

$$3x^4 + 4ax^3 = x^3\,(3x + 4a)$$

olarak bulunur. Bu polinomun biri üç katlı olmak üzere dört kökü vardır. Singüler olmayan noktalarla ilgilenildiğinden $x = 0$ kökü dikkate alınmaz. Diğer kök olan

$x = -\frac{4a}{3}$ değeri için ise iki tane y değeri ve dolayısıyla mertebesi üç olan iki nokta vardır. $\boldsymbol{O}$ noktası da $E[3]$ de olduğundan

$$E[3] \cong \{ \boldsymbol{O}, (-\frac{4a}{3}, \frac{4}{3}\sqrt{\frac{-a^3}{3}}), (-\frac{4a}{3}, -\frac{4}{3}\sqrt{\frac{-a^3}{3}}) \}$$

olarak bulunur. Bu küme ise $\mathbb{Z}_3$ e izomorftur.

3.2.12 Uyarı. $E_2 : y^2 = x^3 + ax^2$ singüler eğrileri $\mathbb{F}_p$ cismi üzerinde tanımlı olsun, bu eğriler üzerinde mertebesi üç olan noktalar bulunmak zorunda değildir. Örneğin $\mathbb{F}_{13}$ üzerinde tanımlı $E_2 : y^2 = x^3 + 2x^2$ singüler eğrisi için $\#E_{ns}(\mathbb{F}_{13}) = p + 1 = 14$ dir ve 3, 14 ile bölünmediğinden Lagrange teoremi gereği eğri üzerinde üç mertebeli nokta yoktur.

Aşağıdaki teoremde $\mathbb{F}_p^*$ sonlu cismi üzerinde tanımlı $E_2 : y^2 = x^3 + ax^2$ singüler eğrilerinin ne zaman üç mertebeli noktalara sahip olduğu belirtilmiştir:

3.2.13 Teorem. $\mathbb{F}_p^*$ sonlu cismi üzerinde tanımlı $E_2 : y^2 = x^3 + ax^2$ singüler eğrileri verilsin. Bu durumda $p \equiv 1\ (3)$ ise

$$E[3] \cong \begin{cases} Z_3 & a \in Q_p \\ \{O\} & a \notin Q_p \end{cases}$$

ve $p \equiv 2\ (3)$ ise

$$E[3] \cong \begin{cases} Z_3 & a \notin Q_p \\ \{O\} & a \in Q_p \end{cases}$$

dir.

İspat. $p \equiv 1\ (3)$ olsun. Bu durumda $a \in \boldsymbol{Q_p}$ ise

$$\#E_{ns}(\mathbb{F}_p) = p - 1$$

olduğundan $p \equiv 1\ (3)$ için $k \in \mathbb{Z}$ olmak üzere

$$\#E_{ns}(\mathbb{F}_p) = p - 1 = 3k$$

dır. Dolayısıyla Lagrange teoremi gereği bu eğriler üzerinde mertebesi üç olan noktalar vardır. Eğer $a \notin Q_p$ ise $\#E_{ns}(\mathbb{F}_p) = p + 1$ ve $p + 1$, 3 ile bölünmediğinden mertebesi üç olan nokta yoktur.

Eğer $p \equiv 2\ (3)$ ise bu durumda $a \notin Q_p$ ise

$$\#E_{ns}(\mathbb{F}_p) = p + 1$$

ve $p \equiv 2\ (3)$ olduğundan $k \in \mathbb{Z}$ olmak üzere

$$\#E_{ns}(\mathbb{F}_p) = p + 1 = 3k + 3$$

dir. Dolayısıyla Lagrange teoremi gereği bu eğriler üzerinde mertebesi üç olan noktalar vardır. Eğer $a \in Q_p$ ise $p - 1$, 3 ile bölünmediğinden mertebesi üç olan nokta yoktur.

3.3 $\mathbb{F}_{p^n}$ Üzerinde Tanımlı Singüler Eğriler

Bu kısımda $\mathbb{F}_{p^n}$ üzerinde tanımlı $E_1 : y^2 = x^3$ ve $E_2 : y^2 = x^3 + ax^2$ singüler eğrilerinin mertebeleri belirlenecektir.

3.3.1 Teorem. $\mathbb{F}_{p^n}$ üzerinde tanımlı $E_1 : y^2 = x^3$ ve $E_2 : y^2 = x^3 + ax^2$ singüler eğrileri verilsin. Bu durumda

$$\#E_1(\mathbb{F}_{p^n}) = p^n + 1$$

ve $n \geq 1$ olmak üzere

$$\#E_2(\mathbb{F}_{p^n}) = \begin{cases} p^n & a \in Q_p \\ p^n + 2 & a \notin Q_p \end{cases}$$

dir.

İspat. $E_1 : y^2 = x^3$ singüler eğrisi için Frobenius endomorfizminin izi 0 dır. Bu durumda Frobenius dönüşümünün karakteristik polinomu

$$X^2 + p \equiv X^2\ (p)$$

ve dolayısıyla $\alpha = \beta = 0$ dır. O halde Teorem 2.9.1 gereği

$$\#E_1(\mathbb{F}_{p^n}) = p^n + 1$$

olarak bulunur.

$E_2 : y^2 = x^3 + ax^2$ singüler eğrileri için iki hal söz konudur:

i. $a \in \boldsymbol{Q}_p$ ise $\#E(\mathbb{F}_p) = p$ olduğundan Frobenius endomorfizminin izi 1 dir. O halde Frobenius dönüşümünün karakteristik polinomu

$$X^2 - X + p \equiv X^2 - X\ (p)$$

biçimindedir ve dolayısıyla $\alpha = 0$ ve $\beta = 1$ dir. O halde Teorem 2.9.1 gereği

$$\#E_1(\mathbb{F}_{p^n}) = p^n + 1 - 1 = p^n$$

olarak bulunur.

ii. $a \notin \boldsymbol{Q}_p$ ise $\#E(\mathbb{F}_p) = p + 2$ olduğundan Frobenius endomorfizminin izi –1 dir. Dolayısıyla Frobenius dönüşümünün karakteristik polinomu

$$X^2 + X + p \equiv X^2 + X\ (p)$$

ve dolayısıyla $\alpha = 0$ ve $\beta = -1$ dir. O halde Teorem 2.9.1 gereği

$$\#E_1(\mathbb{F}_{p^n}) = p^n + 1 + 1 = p^n + 2$$

olarak bulunur.

4. BÖLÜM
ELİPTİK BÖLÜNEBİLİR DİZİLER

Bu bölümde eliptik bölünebilir diziler hakkında bazı ön bilgiler verilecektir. Kısım 4.1 de, bölünebilir dizi kavramı tanımlanacak daha sonra eliptik bölünebilir dizi kavramı üzerinde durulacaktır. Kısım 4. 2 de, bu dizilerin bazı temel özellikleri ele alınacaktır. Buna göre, bir eliptik bölünebilir dizinin bir terimini bulmak için duplikasyon formülleri adı verilen formüller verilecek, bir eliptik bölünebilir dizinin rankı ve periyodu kavramı üzerinde durulacaktır. Kısım 4. 3 de, denk dizi kavramı üzerinde durulacaktır. Kısım 4. 4 de, özel bir eliptik dizi sınıfı olan Lucas dizileri ve singüler dizi kavramı ele alınacak bu dizilerin özellikleri üzerinde durulacaktır. Kısım 4. 5 de, eliptik bölünebilir diziler ve eliptik eğriler arasındaki ilişkiler ele alınacaktır. Kısım 4. 6 ise singüler eliptik bölünebilir diziler ve singüler eğriler arasındaki ilişkiler ele alınacaktır.

4.1 Eliptik Bölünebilir Diziler

4.1.1 Tanım. (h_n) tamsayıların bir dizisi olsun. $m, n \in \mathbb{N}$ olmak üzere, $m \mid n$ olduğunda $h_m \mid h_n$ ise (h_n) dizisine bir *bölünebilir dizi* adı verilir.

0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, ...

olarak verilen Fibonacci dizisi bu dizilerin en iyi bilinen örneğidir.

Bu dizilerin bazıları doğrusal olmayan bir indirgeme bağıntısını da gerçeklerler, bu bağıntıyı gerçekleyen diziler eliptik bölünebilir dizilerdir. Bu dizilerin gerçeklediği doğrusal olmayan indirgeme bağıntısı (aşağıda (4.1) de verilen), eliptik eğriler ile yakından ilişkisi olan, eliptik bölüm polinomlarının indirgeme bağıntılarından başka bir şey değildir.

4.1.2 Tanım. (h_n) bir bölünebilir dizi olsun. Eğer (h_n) dizisinin terimleri her $m \geq n \geq 1$ için doğrusal olmayan

$$h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2 \tag{4.1}$$

indirgeme bağıntısını gerçekliyor ise (h_n) dizisine bir *eliptik bölünebilir dizi* (EBD) denir.

4.1.3 Uyarı. (h_n) dizisinin terimleri her $m \geq n \geq 1$ için doğrusal olmayan (4.1) indirgeme bağıntısını gerçekliyor fakat (h_n) dizisi bir bölünebilir dizi değil ise (h_n) dizisine bir *eliptik dizi* (ED) denir.

Morgan Ward (1948), eliptik bölünebilir dizilerin bir eliptik eğrinin bölüm polinomlarından ortaya çıktığını göstermiştir. Buna göre, eğer $P = (x_1, y_1)$ noktası $\mathbb{Q}$ üzerinde tanımlı bir E eliptik eğri üzerindeki bir rasyonel nokta ise her $n \in \mathbb{N}$ için (h_n) eliptik bölünebilir dizisi bölüm polinomları yardımıyla

$$h_n = \psi_n(x_1, y_1)$$

olarak tanımlanır. Gerçektende, P koordinatları tamsayı olan bir nokta ve E eliptik eğrisinin katsayıları olan a_i ler birer tamsayı iseler Teorem 2.10.3 gereği (h_n) dizisinin terimleri birer tamsayıdır ve Teorem 2.10.4 gereği bölünebilirlik özelliği ($m|n$ olduğunda $h_m|h_n$) gerçeklenir, yani, (h_n) bir eliptik bölünebilir dizidir.

Morgan Ward (1948) eliptik bölünebilir dizileri incelemiş, çalışmasında eliptik bölünebilir dizileri, Lucas dizilerinin bir genelleştirilmesi olarak vermiş ve Lucas dizilerinin birçok özelliklerini eliptik bölünebilir dizilere taşımıştır.

4.1.4 Örnek 1. $(h_n) = n$ olmak üzere

$$1, 2, 3, 4, 5, \ldots, n, \ldots$$

bir eliptik bölünebilir dizidir, bu diziye *tamsayılar dizisi* denir.

2. (F_n), başlangıç terimleri $F_0 = 0$, $F_1 = 1$ olan ve $n \geq 2$ olmak üzere

$$F_n = F_{n-1} + F_{n-2}$$

eşitliğini gerçekleyen Fibonacci dizisi olsun. Bu durumda (F_n) bölünebilir bir dizidir. Bu dizi yardımıyla genel terimi, her $n \geq 0$ için

$$h_n = (-1)^{\frac{1}{2}(n-1)(n-2)} F_n \text{ ve } h_{-n} = -h_n$$

olarak tanımlanan (h_n) dizisinin terimleri

$$\ldots, 3, 2, -1, -1, 0, 1, 1, -2, -3, 5, 8, -13, -21, \ldots$$

biçimindedir ve bu durumda (h_n) dizisi bir eliptik bölünebilir dizidir.

Bu örnekte olduğu gibi, bir eliptik bölünebilir dizinin h_0 teriminden önceki terimleri de söz konusu olabilir, ancak çalışmada bu terimler dikkate alınmayacaktır.

3. Terimleri

$$\ldots, -2, -1, 0, 1, 0, 1, 2, 1, 1, 7, \frac{27}{2}, 5, -\frac{169}{4}, -\frac{659}{2}, -\frac{4963}{8}, -\frac{5963}{8}, \ldots$$

olarak verilen dizi bir eliptik dizidir, dikkat edilirse bu dizi eliptik bölünebilir dizi değildir.

4. $\left(\frac{\cdot}{p}\right)$ Legendre sembolü olmak üzere, genel terimi

$$h_n = \left(\frac{n}{3}\right)$$

olarak verilen

$$\ldots, 0, 1, -1, 0, 1, -1, \ldots$$

dizisi bir eliptik bölünebilir dizidir.

5. $\left(\frac{\cdot}{n}\right)$ Kronecker sembolünü belirtmek üzere, genel terimi

$$h_n = \left(-\frac{8}{n}\right) = \begin{cases} 0, & n \text{ çift} \\ (-1)^{\left\lfloor \frac{n}{4} \right\rfloor}, & n \text{ tek} \end{cases}$$

olarak tanımlanan (h_n) dizisi bir eliptik bölünebilir dizidir.

6. Başlangıç terimleri,

$$C_0 = 0,\ C_1 = 1,\ C_2 = 1,\ C_3 = -1,\ C_4 = 1$$

olan ve

$$C_{m+2}C_{m-2} = C_{m+1}C_{m-1} + C_m^2$$

bağıntısı ile elde edilen (C_n) dizisi de bir eliptik bölünebilir dizidir.

4.2 Eliptik Bölünebilir Dizilerin Temel Özellikleri

Bir eliptik bölünebilir dizinin verilen bir teriminin bulunması için duplikasyon ve toplama formülleri kullanılır, bu formüller aşağıda verilmiştir:

i. Eğer

$$h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2$$

eşitliğinde $n = 2$ olarak alınırsa, her $m \in \mathbb{N}$ için

$$h_{m+2}h_{m-2} = h_{m+1}h_{m-1}h_2^2 - h_3h_1h_m^2 \tag{4.2}$$

toplama formülü elde edilir.

ii. Eğer

$$h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2$$

eşitliğinde $m = n + 1$, $n = n$ ve daha sonra $m = n + 1$, $n = n - 1$ olarak alınırsa aşağıdaki duplikasyon formülleri elde edilir:

$$h_{2n+1} = h_{n+2}h_n^3 - h_{n-1}h_{n+1}^3$$

$$h_{2n}h_2 = h_n(h_{n+2}h_{n-1}^2 - h_{n-2}h_{n+1}^2) \tag{4.3}$$

4.2.1 Uyarı 1. Bu çalışmada dizilerin başlangıç terimleri $h_o = 0$ ve $h_1 = 1$ olarak alınacaktır. Bu seçim dizilerin sayısında bir azalmaya sebep değildir. (4.1) ile verilen

$$\ldots, h_{-n}, \ldots, h_{-2}, h_{-1}, h_o, h_1, h_2, \ldots, h_n, \ldots$$

eliptik bölünebilir dizileri ile başlangıç terimi $h_o = 0$, $h_1 = 1$, olan diziler arasında birebir bir eşleme söz konusudur.

2. Eğer (4.2) eşitliğinde $m = 1$ olarak alınırsa,

$$h_3 h_{-1} = h_2 h_o h_2^2 - h_3 h_1 h_1^2$$

ve dolayısıyla ($h_o = 0$, $h_1 = 1$ olduğundan)

$$h_{-1} = -1 = -h_1$$

olur. (4.1) denkleminde de $m = 0$ olarak alınır ve $h_{-1} = -1 = -h_1$ olduğu kullanılırsa

$$h_{-n} = -h_n$$

eşitliği elde edilir. Dolayısıyla, dizinin başlangıç terimlerini $h_o = 0$ ve $h_1 = 1$ olarak almak bir kısıtlama değildir.

3. Başlangıç terimleri 1, h_2, h_3, h_4 olan (h_n) dizisi kısaca [1 h_2 h_3 h_4] biçiminde gösterilir.

4. Eğer $h_o = 0$, $h_1 = 1$, $h_2 h_3 \neq 0$ ise (4.1) eşitliğinin bir çözümüne *has* (*proper*) *çözüm* denir. Bu şekildeki bir has (proper) çözümün eliptik bölünebilir dizi olması için gerekli ve yeterli şart $h_2 \mid h_4$ olmak üzere h_2, h_3, h_4 terimlerinin birer tamsayı olmasıdır. Bu şartlardan bir ya da birkaçını sağlamayan dizilere ise *has olmayan eliptik bölünebilir* diziler denir. Üstelik $h_2 = 0$ ve $h_3 = 0$ olarak alınırsa elde edilecek diziler birer eliptik bölünebilir dizi olamaz ve başlangıç terimleri ile ifade edilemez. Bu halde dizi

$$0, 1, 0, 0, 0, 0, 0, 0, 0, 0, \ldots$$

biçimindedir. O halde bir eliptik bölünebilir dizinin sadece aynı anda ikinci ve üçüncü terimleri sıfır olamadığı gibi bundan başka ardışık herhangi iki terimi de sıfır olamaz.

5. $h_o = 0$, $h_1 = 1$ olmak üzere üçüncü ve dördüncü terimleri sıfırdan farklı olan dizilere *genel dizi* denir.

6. (h_n) bir eliptik bölünebilir dizi ise bu dizinin terimleri h_2, h_3, h_4 başlangıç terimleri ile bir tek şekilde belirlenir. Buna göre (h_n) dizisi, her $n \in \mathbb{N}$ için $h_n \neq 0$ özelliğinde bir dizi ise (4.2) eşitliğinden (h_n) dizisinin başlangıç terimleri $h_o = 0$, $h_1 = 1$, h_2, h_3, h_4 olan bir tek dizi olduğu görülür.

7. Başlangıç terimleri $h_0 = 0$, $h_1 = 1$, $h_2 h_3 \neq 0$ olan eliptik bölünebilir dizilerinin terimleri eliptik fonksiyonlar yardımıyla parametrelendirilebilirler. Gerçektende, (h_n) bir eliptik bölünebilir dizi ise her $n \geq 1$ için

$$(h_n) = \frac{\sigma(nz, L)}{\sigma(nz, L)^{n^2}}$$

olacak biçimde bir $L \subset \mathbb{C}$ kafesi ve $z \in \mathbb{C}$ sayısı vardır, burada $\sigma(z, L)$, L kafesi ile eşleşmiş olan Weierstrass σ fonksiyonudur (Ward 1948 ve Silverman 2006).

Üstelik L kafesi ile eşleşmiş $g_2(L)$, $g_3(L)$ modüler değişmez fonksiyonları ve $E(\mathbb{Q})$ eğrisi üzerindeki z noktası ile eşleşmiş olan $\wp(z, L)$ ve $\wp'(z, L)$ Weierstrass değerleri $\mathbb{Q}$ cismindedir. Yani $g_2(L)$, $g_3(L)$, $\wp(z, L)$ ve $\wp'(z, L)$ değerleri bir (h_n) dizisinin terimleri olacak biçimde aynı cisimde bulunurlar (Ward 1948 ve Silverman 2006).

8. Her bir çifte periyodik eliptik fonksiyon, $\wp$ ve $\wp'$ fonksiyonlarının birer rasyonel fonksiyonu olduğundan her bir çifte periyodik fonksiyon da bir eliptik bölünebilir dizi yardımıyla elde edebilir (Ward 1948 ve Silverman 2006).

4.2.2 Tanım. (h_n) bir eliptik bölünebilir dizi ve $m \in \mathbb{Z}$ olsun. Eğer m tamsayısı dizinin belli bir terimini bölüyor ise m tamsayısına (h_n) dizisinin bir *böleni* denir. Eğer m, h_ρ terimini bölüyor fakat $r \mid \rho$ olduğu halde m, h_r yi bölmüyor ise ρ ya (h_n) dizisinde m nin bir *rankı* denir.

Bu tanım, (h_n) dizisinin terimlerinin modülo m ($m \in \mathbb{N}$) ye göre düzenli olarak sıralandığını belirtmektedir.

4.2.3 Örnek. Başlangıç terimleri 0, 1, 1, –1, 1 olan

0, 1, 1, –1, 1, 2, –1, –3, –5, –7, –4, –23, 29, ...

olarak verilen (h_n) dizisinin modülo 5 deki rankı $\rho = 8$ dir.

Aşağıdaki iki teorem dizinin terimleri ile dizinin terimlerinin indisleri arasındaki ilişkiyi belirtmektedir.

4.2.4 Teorem. p, (h_n) eliptik dizisinin bir asal böleni ve ρ bu dizinin rankı olsun. Eğer

$$h_{\rho+1} \not\equiv 0 \ (p)$$

ise

$$h_n \equiv 0 \Leftrightarrow n \equiv 0 \ (\rho)$$

dır (Ward 1948).

4.2.5 Teorem. p, (h_n) eliptik dizisinin bir asal böleni ve ρ bu dizinin rankı olsun. Eğer

$$h_{\rho+1} \equiv 0 \ (p)$$

ise $\rho \leq 3$ ve belli bir $n \geq \rho$ sayısı için

$$h_n \equiv 0 \ (p)$$

dir (Ward 1948).

4.2.6 Uyarı. Bu iki teorem birlikte düşünülürse, (h_n) eliptik bölünebilir dizisi ve p asal sayısı için aşağıdaki durumlar gerçeklenir:

i. p, h_3 ve h_4 terimlerinin bir ortak katı değilse (h_n) eliptik bölünebilir dizisinin modülo p de bir tek ρ rankı vardır. Aksi durumda dizi modülo p de tüm terimleri sıfır olan bir dizi haline gelir ($h_2 \mid h_4$ olduğundan h_2 ve h_3 ün ortak böleni h_3 ve h_4 ünde ortak böleni olur).

ii. $(h_3, h_4) = 1$ özelliğindeki bir (h_n) eliptik bölünebilir dizisi için $(h_n, h_m) = h_{(m, n)}$ dir.

Aşağıdaki teorem, bir eliptik bölünebilir dizinin rankı için bir üst sınır belirtmektedir.

4.2.7 Teorem. (h_n) bir eliptik bölünebilir dizi olsun. Bu durumda (h_n) dizisi modülo p de $2p + 1$ den daha küçük en az bir ranka sahiptir (Ward 1948).

4.2.8 Örnek. Aşağıda $\mathbb{F}_5$ de farklı ranklara sahip dizi örnekleri aşağıda verilmiştir.

h_0	h_1	h_2	h_3	h_4	h_5	h_6	h_7	h_8	h_9	h_{10}	h_{11}	h_{12}	h_{13}	h_{14}	h_{15}	h_{16}	h_{17}	h_{18}	h_{19}	h_{20}	h_{21}	h_{22}	h_{23}	h_{24}	h_{25}	h_{26}	h_{27}	h_{28}	h_{29}	h_{30}	h_{31}
0	**1**	0	4	0	1	0	4	0	1	0	4	0	1	0	4	0	1	0	4	0	1	0	4	0	1	0	4	0	1	0	4
0	**1**	**1**	0	1	1	0	4	4	0	4	4	0	1	1	0	1	1	0	4	4	0	4	4	0	1	1	0	1	1	0	4
0	**1**	**1**	**1**	0	4	4	4	0	1	1	1	0	4	4	4	0	1	1	1	0	4	4	4	0	1	1	1	0	4	4	4
0	**1**	**2**	**1**	**2**	0	3	4	3	4	0	1	2	1	2	0	3	4	3	4	0	1	2	1	2	0	3	4	3	4	0	1
0	**1**	**1**	**2**	**2**	**4**	0	4	3	2	4	1	0	4	1	3	2	1	0	1	3	3	4	4	0	1	1	2	2	4	0	4
0	**1**	**2**	**1**	**1**	**2**	**1**	0	4	3	4	4	3	4	0	1	2	1	1	2	1	0	4	3	4	4	3	4	0	1	2	1
0	**1**	**2**	**3**	**2**	**4**	**3**	**2**	0	2	2	4	3	3	3	1	0	4	2	2	2	1	3	3	0	3	2	1	3	2	3	4
0	**1**	**1**	**1**	**2**	**1**	**2**	**3**	**2**	0	3	2	3	4	3	4	4	4	0	1	1	1	2	1	2	3	2	0	3	2	3	4
0	**1**	**1**	**1**	**4**	**3**	**2**	**4**	**2**	**1**	0	1	3	4	3	3	1	1	4	1	0	4	1	4	4	2	2	1	2	4	0	4

Bu dizilerin rankları sırasıyla 2, 3, 4, 5, 6, 7, 8, 9 ve 10 dur. Bu örnekten de görüldüğü gibi $\mathbb{F}_5$ de rankı en fazla 10 olan dizi vardır.

R. Shipsey (2000), (h_n) dizisinin modülo p deki rankı için Ward tarafından verilen sınırdan daha iyi bir sınır elde etmiştir. Buna göre (h_3, h_4) = 1 olmak üzere $\rho \leq 2\sqrt{p} + p + 1$ dir.

4.2.9 Tanım. (s_n) rasyonel sayıların bir dizisi olsun. Eğer yeterince büyük n ler için

$$s_{n+\pi} \equiv s_n (m) \tag{4.4}$$

olacak biçimde pozitif bir π sayısı varsa (s_n) modülo m de *periyodiktir* denir. Eğer (4.4) eşitliği tüm n ler için gerçekleniyorsa bu durumda (s_n) modülo m de *tamamen* (purely) *periyodiktir* denir. (4.4) eşitliğini gerçekleyen bu şekildeki en küçük π sayısına (s_n) nin modülo m de bir *periyotu* denir.

Ward'ın aşağıdaki teoremi rank ile periyot kavramları arasındaki ilişkiyi ortaya koymaktadır:

4.2.10 Teorem. (h_n) rankı üçten büyük olan bir eliptik bölünebilir dizi ve

$$a_1 \equiv \frac{h_2}{h_{\rho-2}} \ (p)$$

$a_2 \equiv h_{\rho-1}$ (p) denkliklerinin modülo p deki çözümlerinin mertebeleri sırasıyla e ve k olsun. Bu durumda (h_n) dizisi modülo p de periyodiktir ve $\tau = 2^{\alpha}[e, k]$ olmak üzere (h_n) dizisinin periyodu

$$\pi(h_n) = \tau \cdot \rho$$

dur, burada $[e, k]$, e ve k nın en küçük ortak katı ve

$$\alpha = \begin{cases} 1, & e, k \text{ tek} \\ -1, & e, k \text{ çift ve ikisi de ikinin bir katı} \\ 0, & \text{diger hallerde} \end{cases}$$

dır (Ward 1948).

4.3 Denk Eliptik Bölünebilir Diziler

Bu kısımda ilk olarak Ward (1948) tarafından verilen denklik kavramı tanımlanacak ve daha sonra denk dizilerin özellikleri üzerinde durulacaktır.

4.3.1 Teorem. (h_n) bir eliptik bölünebilir dizi olsun. Bu durumda herhangi bir θ sayısı ve her $n \in \mathbb{N}$ için,

$$h'_n = \theta^{n^2-1} \ h_n$$

olarak tanımlanan (h'_n) dizisi de bir eliptik bölünebilir dizidir (Ward 1948).

Bu teoremin doğal bir sonucu olarak Ward denk dizi kavramını aşağıdaki gibi vermiştir:

4.3.2 Tanım. Her $n \in \mathbb{N}$ için, $h'_n = \theta^{n^2-1} h_n$ eşitliğini gerçekleyen bir θ sayısı varsa (h_n) ve (h'_n) dizilerine *denk diziler* denir.

İleride diziler için başka bir denklik kavramı da tanımlanacağından dizilerin bu biçimdeki denkliğine *Ward anlamında denklik* denilecektir.

4.3.3 Uyarı 1. Tanımda verilen dizilerin denkliğinin bir denklik bağıntısı olduğu açıktır.

2. Ward'ın denk dizi kavramına göre, (h_n) ve (h'_n) dizilerinin birbirine denk olması için gerek ve yeter şart $h'_n = \theta^{n^2-1} h_n$ eşitliğini gerçekleyen bir $\theta \neq 0$ sabitinin var olmasıdır. Bu sayı gerçekte bir rasyonel sayıdır, gerçektende, $h_2 h_3 \neq 0$ ise $\theta^3 = \frac{h'_2}{h_2}$ ve $\theta^8 = \frac{h'_3}{h_3}$ sayıları birer rasyonel sayı olacağından $\frac{(\theta^3)^3}{\theta^8} = \theta$ sayısı da bir rasyonel sayıdır.

3. $h_2 h_3 \neq 0$ olmak üzere her bir (h_n) eliptik dizisi belli bir (h'_n) eliptik bölünebilir dizisine denktir. Gerçektende, $h_2 \neq 0$ ve h_2, h_3, h_4 terimlerinin paydalarının en küçük ortak katı a ise her $n \in \mathbb{N}$ için,

$$h'_n = (h_2 a^2)^{n^2-1} h_n$$

olarak tanımlanan (h'_n) dizisinin h'_2, h'_3, h'_4 başlangıç terimleri tamsayıdır ve $h'_2 \mid h'_4$ olduğundan (h'_n) dizisi bir EBD dir. Benzer biçimde $h_2 = 0$ ve h_3 teriminin paydası a ise her $n \in \mathbb{N}$ için, $h'_n = a^{n^2-1} h_n$ olarak tanımlanan (h'_n) dizisi de bir EBD dir.

4.4 Lucas Dizileri ve Singüler Diziler

Daha önce de belirtildiği gibi eliptik bölünebilir diziler, Edouard Lucas tarafından çalışılmış olan bölünebilir tamsayı dizilerinin genelleştirilmesidir. Morgan Ward, Lucas dizileri için verilen sonuçları eliptik bölünebilir dizilere genişletmiştir. Bu

kısımda ilk olarak Lucas dizileri ile bölünebilir diziler arasındaki ilişki üzerinde durulacaktır.

4.4.1 Tanım. c bir rasyonel sayı ve a, b sayıları $x^2 - cx + 1$ polinomunun birer kökü olsun. Bu durumda her $n \in \mathbb{N}$ için $a \neq b$ ise,

$$l_n = \frac{a^n - b^n}{a - b},$$

$a = b$ ise,

$$l_n = na^{n-1}$$

olarak tanımlanan (l_n) dizisine bir *Lucas dizisi* denir.

4.4.2 Uyarı 1. Terimleri

$$0, 1, c, c^2 - 1, c^3 - 2c, \ldots$$

olan (l_n) dizisi bir Lucas dizisidir (bu dizi c parametresine bağlı bir Lucas dizisidir) ve bu dizinin terimleri, her $n \in \mathbb{N}$ için, 2. mertebeden

$$l_n = cl_{n-1} - l_{n-2}$$

doğrusal indirgeme formülü ile elde edilir. Üstelik her bir l_n terimi bir rasyonel sayı olduğundan (l_n) dizisi aynı zamanda bir eliptik bölünebilir dizidir.

2. E. Lucas, her bir (l_n) Lucas dizisinin (4.1) eşitliğini gerçeklediğini de göstermiştir, dolayısıyla her bir Lucas dizisi bir eliptik dizidir, fakat eliptik bölünebilir dizilerin hepsi birer Lucas dizisi olmak zorunda değildir. Bir Lucas dizisinin bir eliptik bölünebilir dizi olabilmesi için gerek ve yeter şart c sayısının bir tamsayı olmasıdır.

Çalışmanın bu kısmında, singüler dizi kavramı ele alınacaktır. Burada $h_2h_3 \neq 0$ ve $c \neq 0, 1$ olması halinde Lucas dizilerinin birer özel singüler eliptik bölünebilir dizi olduğu görülecektir.

4.4.3 Tanım. $h_2h_3 \neq 0$ olmak üzere (h_n) eliptik bölünebilir dizisinin diskiriminantı,

$$\Delta(h_2, h_3, h_4) = h_4h_2^{15} - h_3^3h_2^{12} + 3h_4^2h_2^{10} - 20h_4h_3^3h_2^7 + 3h_4^3h_2^5 + 16h_3^6h_2^4 + 8h_4^2h_3^3h_2^2 + h_4^4$$

olarak tanımlanır.

Eğer $\Delta(h_2, h_3, h_4) = 0$ ise (h_n) dizisine *singüler dizi*, aksi halde (h_n) dizisine *singüler olmayan dizi* denir. Özel olarak, p bir asal sayı olmak üzere $\Delta(h_2, h_3, h_4) \equiv 0\ (p)$ ise diziye *modülo p de singüler dizi* denir.

4.4.4 Uyarı 1. (h_n) ve (h'_n) dizileri denk iki dizi ise her $n \in \mathbb{N}$ için,

$$h'_n = \theta^{n^2-1}\ h_n$$

olduğundan

$$\Delta(h_2,\ h_3, h_4) = \theta^{12}\,\Delta(h'_2,\ h'_3,\ h'_4)$$

dır. Dolayısıyla (h'_n) dizisinin singüler olması için gerek ve yeter şart (h_n) dizisinin singüler bir dizi olmasıdır.

2. Ward (1948) herhangi bir singüler eliptik bölünebilir dizinin tamsayı dizisine ya da bir Lucas dizisine denk olduğunu göstermiştir.

Aşağıdaki teoremde bir singüler dizinin başlangıç terimlerinin neler olabileceği belirtilmektedir.

4.4.5 Teorem. $h_2h_3 \neq 0$ olmak üzere bir (h_n) eliptik bölünebilir dizisinin singüler bir dizi olması için gerek ve yeter şart

$$h_2 = r,\ h_3 = s(r^2 - s^3),\ h_4 = rs^3(r^2 - 2s^3)$$

olacak biçimde r ve s tamsayılarının bulunmasıdır (Ward 1948).

Aşağıdaki teorem $h_2h_3 \neq 0$ olmak üzere tüm Lucas dizilerinin birer singüler dizi olduğunu göstermektedir.

4.4.6 Teorem. $h_2h_3 \neq 0$ olmak üzere bir (h_n) singüler eliptik bölünebilir dizisinin c ile parametrelendirilen bir Lucas dizisi olması için gerek ve yeter şart $r = c$, $s = 1$ olmasıdır (Ward 1948).

$s \neq 1$ olması halinde de singüler eliptik bölünebilir diziler için aşağıdaki sonuç verilebilir.

4.4.7 Teorem. (h_n) bir singüler eliptik bölünebilir dizi ve r, s sayıları yukarı da verilen sayılar olmak üzere

$$c = \frac{r\sqrt{s}}{s^2} \text{ ve } \theta^2 = s$$

olsun. (l_n) bir Lucas dizisi ise her $n \in \mathbb{N}$ için,

$$h_n = \theta^{n^2-1}(l_n)$$

dir (Ward 1948).

Bu teorem gösteriyor ki, her bir singüler EBD bir Lucas dizisidir veya bir Lucas dizisine denktir.

4.5 Eliptik Bölünebilir Diziler ve Eliptik Eğriler

Bu kısımda eliptik eğriler ve eliptik bölünebilir diziler arasındaki ilişki incelenecektir. Teorem 2.10.2 gereği $\mathbb{Q}$ üzerinde tanımlı bir E eliptik eğrisinin bölüm polinomları her $m, n \in \mathbb{N}$ için

$$\psi_{m+n}\psi_{m-n} = \psi_{m+1}\psi_{m-1}\psi_n^2 - \psi_{n+1}\psi_{n-1}\psi_m^2$$

bağıntısını gerçeklediğinden E üzerindeki herhangi bir $P = (x_1, y_1)$ rasyonel noktası da bu bağıntıyı gerçekler. Dolayısıyla her $n \in \mathbb{N}$ için, $h_n = \psi_n(x_1, y_1)$ olarak alınırsa (h_n) bir eliptik bölünebilir dizi olur. Bu durumun terside doğrudur, yani, $h_2h_3 \neq 0$ olmak üzere her (h_n) eliptik bölünebilir dizisi için $\mathbb{Q}$ üzerinde tanımlı bir E eliptik eğrisi ve bu eğri

üzerinde herhangi bir $P = (x_1, y_1)$ rasyonel noktası vardır. Aşağıdaki teorem verilen bir EBD ye karşılık bir eliptik eğrinin nasıl bulunacağını belirtmektedir.

4.5.1 Teorem. $h_2h_3 \neq 0$ olmak üzere (h_n) bir eliptik bölünebilir dizi olsun. Bu durumda a, $b \in \mathbb{Q}$ olmak üzere

$$E : y^2 = x^3 + ax + b$$

eliptik eğrisi ve ψ_n, E nin n. bölüm polinomunu göstermek üzere her $n \in \mathbb{N}$ için

$$\psi_n (x_1, y_1) = h_n$$

olacak biçimde E üzerinde bir $P = (x_1, y_1)$ rasyonel noktası vardır. Üstelik $[1\ h_2\ h_3\ h_4]$ dizisi ile eşleşen E eliptik eğrisi için,

$$a = -\frac{1}{2^4 3 h_2^8 h_3^4}\,(h_2^{20} + 4h_2^{15}h_4 - 16h_2^{12}h_3^3 + 6h_2^{10}h_4^2 - 8h_2^7h_3^3h_4 + 4h_2^5h_4^3 + 16h_2^4h_3^6 + 8h_2^2h_3^3h_4^2 + h_4^4),$$

$$b = \frac{1}{2^5 3^3 h_2^{12} h_3^6}\,(h_2^{30} + 6h_2^{25}h_4 - 24h_2^{22}h_3^3 + 15h_2^{20}h_4^2 - 60h_2^{17}h_3^3h_4 + 20h_2^{15}h_4^3 + 120h_2^{14}h_3^6$$

$$- 36h_2^{12}h_3^3h_4^2 + 15h_2^{10}h_4^4 - 48h_2^9h_3^6h_4 + 12h_2^7h_3^3h_4^3 + 64h_2^6h_3^9 + 6h_2^5h_4^5 + 48h_2^4h_3^6h_4^2 + 12h_2^2h_3^3h_4^4 + h_4^6),$$

$$P = (x_1, y_1) = \left(\left(\frac{h_4 + h_2^5}{h_2^2 h_3}\right)^2 + \frac{h_3}{3h_2^2},\ \frac{1}{2}h_2\right),$$

dir (Ward 1948).

4.5.2 Uyarı. Yukarıdaki teorem h_2 veya h_3 ün sıfır olması halinde kullanılamaz. Dolayısıyla eliptik eğrinin a ve b katsayıları, daha genel olan, aşağıdaki eşitlikler yardımıyla da bulunabilir.

4.5.3 Teorem. $[1\ h_2\ h_3\ ch_2]$ eliptik bölünebilir dizisi ile eşleşen $E : y^2 = x^3 + ax + b$ eliptik eğrisinin katsayıları ve bu eğri üzerindeki P noktası

$$a = 3^3(-h_2^{16} - 4ch_2^{12} + (16h_3^3 - 6c^2)h_2^8 + (8ch_3^3 - 4c^3)h_2^4 - (16h_3^6 + 8c^2h_3^3 + c^4)), \tag{4.5}$$

$$b = 2\cdot 3^3(h_2^{24} + 6ch_2^{20} - (24h_3^3 - 15c^2)h_2^{16} - (60ch_3^3 - 20c^3)h_2^{12} + (120h_3^6 - 36c^2h_3^3 + 15c^4)h_2^8$$
$$+ (-48ch_3^6 + 12c^3h_3^3 + 6c^5)h_2^4 + (64h_3^9 + 48c^2h_3^6 + 12c^4h_3^3 + c^6)), \tag{4.6}$$

$$P = (x_1, y_1) = (3\cdot (h_2^8 + 2ch_2^4 + 4h_3^3 + c^2), -108\, h_3^3 h_2^4) \tag{4.7}$$

ve

$$\Delta = 2^8 3^{12} h_3^9 h_2^8 (ch_2^{12} + (-h_3^3 c^2) h_2^8 + (-20ch_3^3 + 3c^3) h_2^4 + (16h_3^6 + 8c^2 h_3^3 + c^4))$$

eşitlikleri ile verilir (Silverman 2006).

4.5.4 Uyarı 1. Ward, verilen (h_n) dizisine karşılık gelen eliptik eğriyi bulurken eğrinin

$$E : y^2 = 4x^3 - g_2 x - g_3 \quad (g_2, g_3 \in \mathbb{Q})$$

biçiminde olduğunu kabul ederek işlemlerini yapmıştır. Eğrinin bu gösterimi ile

$$E : y^2 = x^3 + ax + b$$

gösterimi arasında bir fark yoktur. Eğer $y^2 = 4x^3 - g_2 x - g_3$ eşitliğinin her iki yanı 4 ile bölünür ve y, a, b olarak, sırasıyla $-\frac{1}{2}y$, $-\frac{g_2}{4}$ ve $-\frac{g_3}{4}$ alınırsa eğrinin denklemi

$$y^2 = x^3 + ax + b$$

haline dönüşür.

2. (h_n), $h_3 = 0$ özelliğindeki bir eliptik bölünebilir dizi olsun. Ward (1948), (h_n) dizisinin

$$E : y^2 = 4x^3 - g_2 x - g_3 \ (g_2, g_3 \in \mathbb{Q})$$

eliptik eğrisinin belli bir P rasyonel noktasında hesaplanan bölüm polinomlarının dizisi olması için gerek ve yeter şartın $h_4 = -h_2^5$ olduğunu göstermiştir.

3. E bir singüler eğri olarak alınsa bile teoremde belirten P noktası singüler nokta olamaz. Çünkü E üzerindeki singüler bir noktanın y-koordinatı sıfır olmalıdır, ancak P noktasının y-koordinatı, yukarıda görüldüğü gibi, $\frac{1}{2}\, h_2 \neq 0$ dır.

4.5.5 Tanım. $P = (x_1, y_1)$ noktası E üzerinde singüler olmayan bir nokta olmak üzere $\mathbb{Q}$ üzerinde tanımlı E eliptik eğrisi verilsin ve her $n \in \mathbb{N}$ için

$$\psi_n(x_1, y_1) = h_n$$

olsun. Bu durumda E eliptik eğrisine (h_n) *eliptik dizisi ile eşleşmiş eliptik eğri* denir.

4.5.6 Örnek 1. [1 2 3 4] dizisi ile eşleşen eğri yukarıdaki teorem uygulanarak

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

olarak bulunur.

2. [1 1 –1 1] dizisi ile eşleşen eğri de yukarıdaki teorem uygulanarak

$$E : y^2 = x^3 - 1296x + 11664$$

olarak bulunur.

4.5.7 Uyarı. Shipsey (2000), (h_n) dizisinin terimleri yardımıyla, E eliptik eğrisinin daha kolay bir yoldan bulanabileceği alternatif bir formül vermiştir. Bu formülü elde ederken yukarıdaki tanımda herhangi bir P noktası yerine singüler olmayan $P = (0, 0)$ noktasında hesaplanan $(\psi_n(0, 0))$ bölüm polinomlarını kullanmıştır. Eğer singüler olmayan $P = (0, 0)$ noktası E eliptik eğrisi üzerinde değil ise herhangi bir singüler olmayan nokta (0, 0) noktasına kaydırılarak aynı yöntem ile E eliptik eğrisi bulunabilir.

Aşağıdaki teorem bir eliptik bölünebilir dizi verildiğinde bu diziye karşılık gelen Weierstrass uzun formunda verilmiş bir eliptik eğrinin katsayılarının dizinin başlangıç terimleri yardımıyla bulunabileceğini belirtmektedir.

4.5.8 Teorem. $h_2h_3 \neq 0$ olmak üzere (h_n) bir EBD olsun. Bu durumda, [1 h_2 h_3 h_4] eliptik bölünebilir dizisi ile eşleşen

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

eliptik eğrisinin katsayıları,

$$a_3 = h_2$$

$$a_1 = \frac{h_4 + h_2^5 - 2h_2h_3a_4}{h_2^2h_3}$$

$$a_2 = \frac{h_2h_3^2 + (h_4 + h_2^5)a_4 - h_2h_3a_4^2}{h_2^3h_3}$$

a_4 keyfi

dir (Swart 2003).

4.5.9 Örnek. [1 1 –5 –26] dizisi ile eşleşen eğri yukarıdaki teorem uygulanarak

$$E : y^2 + xy + y = x^3 + x^2 + 2x$$

olarak bulunur.

4.5.10 Uyarı. Daha önce $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x$ biçiminde verilen bir E eliptik eğrisinin Tate değerleri,

$$b_2 = a_1^2 + 4a_2$$

$$b_4 = 2a_4 + a_1a_3$$

$$b_6 = a_3^2 + 4a_6$$

$$b_8 = a_1^2 a_6 + 4a_2a_6 - a_1a_3a_4 + a_2 a_3^2 - a_4^2$$

kullanılarak

$$\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

biçiminde tanımlanmıştı. Dolayısıyla bu değerler (h_n) dizisinin terimleri yardımı ile de,

$$b_8 = h_3$$

$$b_6 = a_3^2 = h_2^2$$

$$b_4 = \frac{h_4 + h_2^5}{h_2 h_3}$$

$$b_2 = \frac{b_4^2 + 4h_3}{h_2^2}$$

biçiminde ifade edilirler.

Aşağıdaki teorem Weierstrass uzun formda bir eliptik eğri verildiğinde eliptik eğrinin katsayıları yardımıyla eliptik bölünebilir dizinin başlangıç terimlerinin bulunabileceğini göstermektedir.

4.5.11 Teorem. $h_2h_3 \neq 0$ olmak üzere (h_n) bir EBD olsun. Bu durumda, (h_n) dizisi ile eşleşmiş olan

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

eliptik eğrisinin a_1, a_2, a_3, a_4 katsayıları yardımıyla, (h_n) dizisinin ilk üç terimi

$$h_2 = a_3$$

$$h_3 = a_2 a_3^2 - a_4^2 - a_1 a_3 a_4$$

$$h_4 = 2a_3 a_4 h_3 + a_1 a_3^2 h_3 - a_3^5$$

dir (Shipshey 2000).

4.5.12 Örnek. $E : y^2 + xy + y = x^3 + x^2 + 2x$ eğrisi için $a_1 = 1$, $a_3 = 1$, $a_2 = 1$, $a_4 = 2$ olduğundan bu eğri ile eşleşen eliptik bölünebilir dizinin başlangıç terimleri

$$h_2 = a_3 = 1$$

$$h_3 = a_2 a_3^2 - a_4^2 - a_1 a_3 a_4 = 1 - 4 - 2 = -5$$

$$h_4 = 2a_3 a_4 h_3 + a_1 a_3^2 h_3 - a_3^5 = 2 \cdot 1 \cdot 2 \cdot (-5) - 5 = -26$$

dır. Dolayısıyla bu eğri ile eşleşen dizi [1 1 –5 –26] olarak bulunur.

4.5.13 Uyarı. Bu örnek ve yukarıdaki teorem gösteriyor ki, verilen bir EBD ile

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x$$

formunda bir tek eliptik eğri ve bu formda verilen bir eliptik eğri ile bir tek EBD eşleşir.

Ward bir eliptik bölünebilir dizinin diskriminantı ile bu diziyle eşleşen eliptik eğrinin diskriminantının aynı olduğunu göstermiştir.

4.5.14 Teorem. $h_2 h_3 \neq 0$ olmak üzere (h_n) bir eliptik bölünebilir dizi ve E bu dizi ile eşleşen eliptik eğri olsun. Bu durumda (h_n) eliptik bölünebilir dizisinin diskriminantı E eliptik eğrisinin diskriminantına eşittir (Ward 1948).

4.6 Singüler Diziler ve Singüler Eğriler

Ward eliptik bölünebilir dizilerle eliptik eğriler arasındaki ilişkiye benzer bir durumun singüler eliptik bölünebilir diziler ve singüler eğriler için de geçerli olduğunu göstermiştir. Aşağıdaki teorem, (h_n) singüler eliptik bölünebilir dizisi için, Teorem 4.4.5 deki r ve s tamsayıları kullanılarak, E singüler eğrisinin a ve b katsayılarının bulunabileceğini göstermektedir.

4.6.1 Teorem. r ve s tamsayıları Teorem 4.4.5 da belirtilen sayılar ve $h_2h_3 \neq 0$ olmak üzere (h_n) singüler eliptik bölünebilir dizisi ile eşleşen E singüler eğrisinin a ve b katsayıları

$$a = -\frac{3}{4}\left[\frac{(r^2-4s^3)}{6s^2}\right]^2, \quad b = \frac{1}{4}\left[\frac{(r^2-4s^3)}{6s^2}\right]^3$$

dir. $x^3 + ax + b = 0$ denkleminin kökleri e_1, e_2, e_3 olmak üzere $\Delta = 0$ ve $e_1 = e_2$ ise

$$e_3 = -2e_1$$

ve

$$a = -\frac{3}{4}e_3^2, \qquad b = \frac{1}{4}e_3^3$$

dir (Ward 1948).

4.6.2 Teorem. $h_2h_3 \neq 0$ olmak üzere (h_n) singüler eliptik bölünebilir dizi olsun. Bu durumda $x^3 + ax + b = 0$ denkleminin kökleri

$$-\frac{(r^2-4s^3)}{6s^2}, \qquad \frac{(r^2-4s^3)}{12s^2}, \qquad \frac{(r^2-4s^3)}{12s^2}$$

dir ve üstelik $a = b = 0$ olması için gerek ve yeter şart $r^2 = 4s^3$ olmasıdır (Ward 1948).

4.6.3 Uyarı. (h_n) eliptik bölünebilir dizisi E eliptik eğrisi ile eşlemiş bir dizi olsun. E nin singüler eğri olması için gerek ve yeter şart (h_n) nin bir singüler dizi olmasıdır. Bu durum, Teorem 4.5.14 ün bir sonucu olarak görülür.

4.6.4 Örnek. $(h_n) = n$ olmak üzere

$$1, 2, 3, 4, 5, \ldots, n, \ldots$$

eliptik bölünebilir dizisi bir singüler dizidir ve bu dizi ile eşleştirilmiş E eliptik eğrisinin Tate değerleri

$$b_8 = h_3 = 3$$

$$b_6 = a_3^2 = h_2^2 = 2^2$$

$$b_4 = \frac{h_4 + h_2^5}{h_2h_3} = \frac{4+2^5}{2\cdot 3} = 6$$

$$b_2 = \frac{b_4^2 + 4h_3}{h_2^2} = \frac{6^2 + 4 \cdot 3}{2^2} = 12$$

biçimindedir. Dolayısıyla bu eğrinin diskiriminantı

$$\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6 = -12^2 \cdot 3 - 8 \cdot 6^3 - 27 \cdot 4^2 + 9 \cdot 12 \cdot 6 \cdot 4 = 0$$

olduğundan E bir singüler eğridir. Daha önce bu dizinin eşleştiği eğrinin $E : y^2 = x^3$ olduğu görülmüştü.

4.6.5 Teorem. $h_2 h_3 \neq 0$ olmak üzere (h_n) bir eliptik dizi ve $E(\mathbb{Q})$ bu eliptik diziye karşılık gelen eliptik eğri olsun. Bu durumda

"E (modülo p) bir singüler eğridir $\Leftrightarrow$ (h_n) modülo p de bir singüler dizidir"

(Swart 2003).

5. BÖLÜM

$\mathbb{F}_p$ ÜZERİNDE TANIMLI ELİPTİK BÖLÜNEBİLİR DİZİLER

Bu kısımda eliptik bölünebilir diziler, $p > 3$ bir asal sayı olmak üzere $\mathbb{F}_p$ sonlu cismi üzerinde incelenecektir. Bunun için ilk olarak $\mathbb{F}_p$ sonlu cismi üzerinde eliptik diziler tanımlanacak daha sonra eliptik bölünebilir diziler tanımlanacaktır. Bu diziler herhangi bir tamsayı dizisinin modülo p de bir indirgemesi değil, başlangıç terimleri $\mathbb{F}_p$ sonlu cisminden alınarak elde edilen dizilerdir. Kısım 5. 1 de, ilk olarak eliptik bölünebilir diziler sonlu cisimler üzerinde tanımlanacak daha sonra has ve has olmayan eliptik bölünebilir dizilerin sayıları verilecektir. Kısım 5. 2 de, $\mathbb{F}_p$ sonlu cismi üzerinde tanımlı singüler eliptik bölünebilir dizilerin özellikleri üzerinde durulacak ve bu dizilerin neler olduğu belirlenecek, denk singüler eliptik bölünebilir dizilerin özellikler verilecektir. Kısım 5. 3 de, $\mathbb{F}_p$ sonlu cismi üzerinde tanımlı rankları bilinen dizilerin genel terimleri ve periyotları belirlenecektir ve daha sonra belli ranklara sahip singüler dizilerin karakteri belirlenecektir. Kısım 5. 4 de, $\mathbb{F}_p$ sonlu cismi üzerinde tanımlı rankları bilinen eliptik bölünebilir dizilerle eşleşen eliptik ve singüler eğriler belirlenecek ve bu eğrilerin özellikleri üzerinde durulacaktır.

5.1 $\mathbb{F}_p$ Üzerinde Eliptik Bölünebilir Diziler

Bu kısımda daha önce tanımlanmış olan eliptik bölünebilir dizi kavramı sonlu cisimler üzerinde tanımlanacak ve bu dizilerin genel özellikleri verilecektir.

5.1.1 Tanım. (h_n) dizisinin $\mathbb{F}_p$ sonlu cisminden alınan terimleri doğrusal olmayan

$$h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2 \tag{5.1}$$

indirgeme bağıntısını gerçekliyor ise (h_n) dizisine $\mathbb{F}_p$ *de bir eliptik dizi* denir.

$\mathbb{F}_p$ cisminin sıfırdan farklı her bir elemanı bir diğer elemanı böleceğinden (h_n), $\mathbb{F}_p$ cismi üzerinde bir eliptik dizi ise (h_n) dizisi $\mathbb{F}_p$ *cismi üzerinde bir eliptik bölünebilir dizidir* denir.

5.1.2 Uyarı 1. Dikkat edilirse $\mathbb{F}_p$ cismi üzerinde tanımlanan eliptik dizi ve eliptik bölünebilir dizi kavramları aynıdır.

2. $\mathbb{F}_p$ cismi üzerinde tanımlı EBD ler $(h_n(p))$ ile gösterilecektir.

3. Daha önce tanımlanan dizilerinde olduğu gibi bu diziler içinde $h_0 = 0$, $h_1 = 1$ dır ve ardışık iki terim sıfır olamaz.

Aşağıdaki önerme, eliptik bölünebilir dizilerin sonlu cisimler üzerinde tanımlı olması halinde Teorem 4.2.4 e karşılık gelen dizilerin rankı ile ilgili bir sonuç verilmiştir.

5.1.3 Önerme. (h_n), $\mathbb{F}_p$ cismi üzerinde bir eliptik bölünebilir dizi ve ρ bu dizinin rankı olsun. Bu durumda

$$h_{\rho n} \equiv 0 \ \ (p)$$

dır.

İspat. (h_n) eliptik bölünebilir dizisinin rankı ρ olmak üzere ρ, ρn sayısını böldüğünden h_ρ terimi $h_{\rho n}$ terimini böler, dolayısıyla istenilen elde edilir.

Çalışmanın bu kısmında, ilk olarak $\mathbb{F}_p$ üzerinde tanımlı eliptik bölünebilir dizilerin sayısı belirlenecek, daha sonra singüler eliptik bölünebilir diziler tanımlanarak bu dizilerin sayısı belirlenecektir.

5.1.4 Teorem. $\mathbb{F}_p$ üzerinde tanımlı tüm eliptik bölünebilir dizilerin sayısı $p^3 - p^2 + p$ tanedir.

İspat. $h_o = 0$, $h_1 = 1$ olmak üzere h_2, h_3, h_4 terimlerinin seçimi için $\mathbb{F}_p$ de p alternatif söz konusu olduğundan p^3 tane dizi olacağı düşünülebilir. Ancak h_4, h_2 nin bir katı olacağından ve $h_2 = 0$ olması halinde h_4 sadece 0 olabileceğinden düşünülen dizi sayısından $h_2 = 0$ olması halinde $h_4 \neq 0$ olan dizilerin sayısı çıkarılırsa bu dizilerin sayısı da $p(p-1)$ dir. Dolayısıyla bu dizilerin sayısı $p^3 - p\,(p-1) = p^3 - p^2 + p$ dir.

5.1.5 Örnek. $\mathbb{F}_5$ üzerinde tanımlı tüm eliptik bölünebilir dizilerin sayısı 105 tanedir. Bu diziler Ek-1 ve Ek-2 de verilmiştir.

5.1.6 Teorem. $\mathbb{F}_p$ üzerinde tanımlı has olmayan (improper) eliptik bölünebilir dizilerin sayısı p^2 tanedir.

İspat. $h_2 \neq 0$ olarak seçilmesi halinde h_2 nin seçimi için $p - 1$ alternatif vardır. Bu halde $h_3 = 0$ da olabileceğinden $h_2 \neq 0$ olmak üzere her bir h_2 için p tane h_3 seçimi söz konusudur. Dolayısıyla $h_2 \neq 0$, h_3 ikilileri için $p(p-1)$ alternatif söz konusudur. Diğer yandan $h_3 \neq 0$ ve $h_2 = 0$ olması hali için de $p - 1$ alternatif söz konusudur. Son olarak $h_2 = 0$ ve $h_3 = 0$ halini de dikkate alırsak, has olmayan dizilerin sayısı

$$(p-1)\,p + (p-1) + 1 = p^2$$

tanedir.

5.1.7 Örnek. $\mathbb{F}_5$ üzerinde has olmayan 25 tane dizi vardır ve bunlar Ek-1 de verilmiştir.

5.1.8 Teorem. $\mathbb{F}_p$ üzerinde tanımlı has (proper) dizilerin sayısı $(p-1)^2\,p$ tanedir.

İspat. Eğer $(h_n(p))$ bir has (proper) eliptik bölünebilir dizi ise $h_2 \neq 0$, $h_3 \neq 0$ dir. Dolayısıyla h_2 ve h_3 terimlerinin seçimi için $p - 1$ alternatif söz konusudur. Böylece, sadece h_2 ve h_3 dikkate alındığında $(p-1)^2$ tane dizi elde edilir. h_4 terimi h_2 teriminin bir

katı ve h_4 teriminin seçimi için de p tane alternatif olduğu dikkate alınırsa, proper dizilerin sayısı $(p-1)^2\,p$ tane olarak bulunur.

5.1.9 Örnek. $\mathbb{F}_5$ üzerinde has (proper) 80 tane dizi vardır ve bunlar Ek-2 de verilmiştir.

5.2 $\mathbb{F}_p$ Üzerinde Tanımlı Singüler Eliptik Bölünebilir Diziler

Çalışmanın bu kısmında $\mathbb{F}_p$ üzerinde tanımlı singüler eliptik bölünebilir diziler ve bu diziler arasındaki ilişkiler ele alınacaktır.

(h_n) eliptik bölünebilir dizisi verilsin. Bu durumda,

$$\Delta(h_n) = 0 \Rightarrow (h_n) \text{ bir singüler dizidir} \Rightarrow E((h_n)) \text{ bir singüler eğridir}$$

ve üstelik

(h_n) bir singüler dizi $\Rightarrow (h_n(p))$ bir singüler dizidir $\Rightarrow E((h_n(p))$ bir singüler eğridir.

Diğer yandan (h_n) dizisi bir singüler dizi olmasa da $(h_n(p))$ dizisi bir singüler dizi olabilir, dolayısıyla da $E((h_n(p))$ bir singüler eğri olur. Örneğin [1 2 6 4] dizisi $(\Delta(h_n) = -\frac{1323}{8} \neq 0)$ bir singüler dizi olmadığı halde $\mathbb{F}_7$ de $\Delta(h_n(p)) = 0$ dır ve dolayısıyla bu dizi $\mathbb{F}_7$ de bir singüler dizidir, üstelik bu dizi $\mathbb{F}_7$ de $E : y^2 = x^3$ singüler eğrisi ile eşleşir.

Singüler diziler, eşleştikleri $E_1 : y^2 = x^3$ ve $E_2 : y^2 = x^3 + ax + b$ singüler eğrileri dikkate alınarak iki gruba ayırabilir. Buna göre bir singüler dizi E_1 eğrisi ile eşleşiyorsa bu tip dizilere *birinci tip singüler dizi*, E_2 eğrisi ile eşleşiyorsa bu tip dizilere *ikinci tip singüler dizi* adı verilir. Bu dizilerin iki grupta incelenmesinin nedeni, daha önce belirtildiği gibi, bu dizilerle eşleşen eğrilerin bir çıkıntıya veya bir düğüme sahip olmasıdır.

5.2.1 Teorem. Her p asal sayısı için [1 2 3 4] tamsayılar dizisi $E_1 : y^2 = x^3$ eğrisi ile eşleşir ve bu diziye denk olan tüm singüler dizilerde bu singüler eğri ile eşleşir. Üstelik bu dizilerin sayısı $p - 1$ tanedir.

İspat. (h_n) dizisi başlangıç terimleri [1 h_2 h_3 h_4] olan bir dizi ise bu diziye karşılık gelen

$$E : y^2 = x^3 + ax + b$$

eliptik eğrisinin katsayıları

$$a = 3^3(-h_2^{16} - 4ch_2^{12} + (16h_3^3 - 6c^2)h_2^8 + (8ch_3^3 - 4c^3)h_2^4 - (16h_3^6 + 8c^2h_3^3 + c^4))$$

$$b = 2 \cdot 3^3(h_2^{24} + 6ch_2^{20} - (24h_3^3 - 15c^2)h_2^{16} - (60ch_3^3 - 20c^3)h_2^{12} + (120h_3^6 - 36c^2h_3^3 + 15c^4)h_2^8$$

olduğundan bu eşitliklerde $h_2 = 2$, $h_3 = 3$, $h_4 = 4$ olarak alınırsa $E_1 : y^2 = x^3$ singüler eğrisi elde edilir.

(h'_n) dizisi, [1 2 3 4] dizisine denk bir dizi olsun. Her $n \in \mathbb{N}$ için, $h'_n = \theta^{n^2-1} h_n$ eşitliği kullanılarak bu diziye karşılık gelen eğrinin de $E_1 : y^2 = x^3$ eğrisi olduğu görülür.

"$(h_n(p))$ singüler dizisi $y^2 = x^3$ eğrisi ile eşleşir $\Leftrightarrow r^2 = 4s^3$"

ve $4 \in Q_p$ olduğundan

"$4s^3 \in Q_p \Leftrightarrow s^3 \in Q_p$ ve $s \in Q_p$ "

dir. Dolayısıyla her s için iki tane r değeri elde edileceğinden bu dizilerin sayısı

$$2|Q_p| = 2 \cdot \frac{p-1}{2} = p - 1$$

tanedir.

Aşağıdaki teoremde $\mathbb{F}_p$ üzerinde tanımlı has singüler dizilerin sayısı verilmiştir.

5.2.2 Teorem. $\mathbb{F}_p$ üzerinde tanımlı tüm has singüler dizilerin sayısı $(p - 1)(p - 2)$ tanedir.

İspat. $(h_n(p))$ dizisi has singüler dizi ve $h_2h_3 \neq 0$ olduğundan $r, s \in \mathbb{F}_p^*$ dir. Dolayısıyla r ve s sayıları için $p - 1$ tane alternatif olduğundan $(p - 1)^2$ tane (r, s) ikilisi vardır. Diğer yandan $h_3 = s(r^2 - s^3) \neq 0$ olduğundan $r^2 \neq s^3$ dir. İlk olarak $r^2 = s^3$ özelliğindeki (r, s) ikilileri dikkate alınırsa $p \equiv 1$ (6) ve $p \equiv 5$ (6) olmasına göre iki hal söz konusudur.

i. $p \equiv 1\ (6)$ olsun. Bu durumda $r^2 = s^3 \in \boldsymbol{K}_p^*$ olduğundan r sayıları için $\frac{p-1}{3}$ tane alternatif söz konusudur. Diğer yandan her bir r için $r^2 = s^3$ eşitliğini gerçekleyen s sayıları

$$r^2,\quad r^2\omega,\quad r^2\omega^2$$

dır, burada ω birimin küp köküdür. Dolayısıyla $r^2 = s^3$ eşitliğini gerçekleyen (r, s) sayı çiftlerinin sayısı $3 \cdot \frac{p-1}{3} = p - 1$ tanedir.

ii. $p \equiv 5\ (6)$ olsun. Bu durumda $r^2 = s^3 \in \boldsymbol{K}_p^*$ olduğundan r sayıları için $p - 1$ tane alternatif söz konusudur. Diğer yandan her bir r için $r^2 = s^3$ eşitliğini gerçekleyen s sayıları bir tane olup bu sayı $s = r^2$ dır. Dolayısıyla $r^2 = s^3$ eşitliğini gerçekleyen (r, s) sayı çiftlerinin sayısı bu halde $p - 1$ tanedir.

O halde her iki durumda da singüler dizilerin sayısı aynı olup

$$(p-1)^2 - (p-1) = (p-1)(p-2)$$

tanedir.

5.2.3 Sonuç. Birinci tip singüler dizilerin sayısı $(p - 1)$, ikinci tip singüler dizilerin sayısı $(p - 1) \cdot (p - 3)$ tanedir. Gerçektende, tüm singüler dizilerin sayısı $(p - 1) \cdot (p - 2)$ olduğundan bu dizilerden birinci tip singüler dizilerin sayısını çıkarırsak ikinci tip singüler dizilerin sayısı $(p - 1) \cdot (p - 2) - (p - 1) = (p - 1) \cdot (p - 3)$ tane olarak bulunur.

Aşağıdaki teoremde singüler dizilerin $\mathbb{F}_p$ de Ward anlamında denk olma koşulları belirlenmiştir:

5.2.4 Teorem. $(h_n(p))$ ve $(h'_n(p))$ iki singüler dizi olsun. Bu iki dizinin Ward anlamında denk olması için gerekli ve yeterli koşul $s \in \boldsymbol{Q}_p$ olmasıdır.

İspat. $(h_n(p))$ ve $(h'_n(p))$ EBD leri denktirler $\Leftrightarrow$ her $n \in \mathbb{N}$ için,

$$h'_n = \theta^{n^2-1}\ h_n$$

olacak biçimde bir θ tamsayısı vardır. Eğer bu iki dizi singüler diziler ise Teorem 4.4.7 gereği,

"(h_n) ve (h'_n) singüler dizileri denktirler $\Leftrightarrow c = \frac{r\sqrt{s}}{s^2}$ ve $\theta^2 = s$ olmak üzere her $n \in \mathbb{N}$ için,

$$h_n = \theta^{n^2-1}\,(h'_n)$$

dir, yani $s \in Q_p$ dir".

5.2.5 Örnek 1. $\mathbb{F}_5$ de

[1 1 2 4], [1 2 2 3], [1 3 2 2] ve [1 4 2 1]

dizileri için s tamsayıları sırasıyla 3, 2, 2 ve 3 dir ve bu değerler Q_5 de olmadıklarından bu diziler birbirlerine Ward anlamında denk değillerdir. Ancak bu dört singüler dizi aynı $E : y^2 = x^3 + 2x + 3$ singüler eğrisi ile eşleşir, dikkat edilirse bu eğri ikinci tip singüler eğridir.

2. $\mathbb{F}_7$ de

[1 3 1 0], [1 3 2 0], [1 3 4 0], [1 4 1 0], [1 4 2 0], [1 4 4 0]

dizileri için s tamsayıları sırasıyla 1, 2, 4, 1, 2, 4 dir ve bu değerler Q_7 dirler. Dolayısıyla bu diziler Ward anlamında birbirlerine denktirler. Üstelik bu diziler ikinci tip singüler $E : y^2 = x^3 + 2x + 2$ eğrisi ile eşleşir.

5.2.6 Tanım. $h_2h_3 \neq 0$ olmak üzere bir $(h_n(p))$ singüler eliptik bölünebilir dizilerinin terimleri

$$h_2 = r,\ h_3 = s(r^2 - s^3),\ h_4 = rs^3(r^2 - 2s^3)$$

olmak üzere $s = 1$ için elde edilen ve başlangıç terimleri

$$h_2 = r,\ h_3 = r^2 - 1,\ h_4 = r(r^2 - 2)$$

olan $(h_n(p))_s$ singüler dizisine $(h_n(p))$ singüler eliptik bölünebilir dizilerinin *temsilci dizisi* denir.

5.2.7 Uyarı 1. Tanımda, $s = 1$ için elde edilen $(h_n(p))_s$ singüler temsilci dizileri ya bir tamsayı dizisi ya da bir Lucas dizisidir.

2. $s \in Q_p$ olması halinde singüler diziler mutlaka bir temsilci diziye denktirler ve dolayısıyla singüler diziler temsilcileri yardımıyla denk singüler dizi sınıflarına ayrılırlar. Bu denk singüler dizi sınıfları $\overline{[(h_n(p))]}$ ile gösterilecektir.

3. Başlangıç terimleri $h_2 = r$, $h_3 = r^2 - 1$, $h_4 = r(r^2 - 2)$ olan $(h_n(p))_s$ dizisi temsilci dizi ise başlangıç terimleri

$$h_2' = -r = -h_2,\ h_3' = r^2 - 1 = h_3,\ h_4' = -r(r^2 - 2) = -h_4$$

olan $(h_n'(p))_s$ dizisi de diğer temsilci dizidir.

5.2.8 Tanım. (h_n) bir EBD olsun. Bu durumda $((-1)^{n-1} h_n)$ dizisi de bir EBD dir ve bu diziye (h_n) *dizisinin tersi* denir.

(h_n) ve bu dizinin tersi olan $((-1)^{n-1} h_n)$ dizilerinin denk oldukları aşağıdaki teoremde belirtilmiştir, bu nedenle bunlardan herhangi birisi temsilci dizi olarak seçilebilir.

5.2.9 Teorem. Başlangıç terimleri

$$h_2 = r,\ h_3 = r^2 - 1,\ h_4 = r(r^2 - 2)$$

olan $(h_n(p))_s$ singüler EBDsi ile başlangıç terimleri

$$h_2' = -r = -h_2,\ h_3' = r^2 - 1 = h_3,\ h_4' = -r(r^2 - 2) = -h_4$$

olan $(h_n'(p))_s$ singüler EBDleri, yani (h_n) ve $((-1)^{n-1} h_n)$ dizileri denk dizilerdir.

İspat. Denklik tanımından

$$h_2 = \theta^3 (h_2'),\quad h_3 = \theta^8 (h_3'),\quad h_4 = \theta^{15} (h_4')$$

eşitliklerini gerçekleyen bir θ sayısının olduğu gösterilirse ispat tamamlamış olur. Buna göre

$$h_2 = \theta^3 (-h_2),\quad h_3 = \theta^8\ h_3,\quad h_4 = \theta^{15} (-h_4),$$

eşitliklerinden $\theta^3 = -1$, $\theta^8 = 1$ ve $\theta^{15} = -1$ olarak elde edilir. Dolayısıyla $\theta = -1$ veya $p - 1$ aranan sayıdır.

5.2.10 Örnek. $\mathbb{F}_7$ de [1 3 1 0] dizisi bir temsilci dizidir ve bu diziye denk olan diziler

[1 3 2 0], [1 3 4 0], [1 4 1 0], [1 4 2 0] ve [1 4 4 0]

dizileridir. Dolayısıyla,

$$\overline{[1\ 3\ 1\ 0]} = \{ [1\ 3\ 1\ 0], [1\ 3\ 2\ 0], [1\ 3\ 4\ 0], [1\ 4\ 1\ 0], [1\ 4\ 2\ 0], [1\ 4\ 4\ 0] \}$$

dir. Bu dizi sınıfı için temsilci dizi olarak [1 4 1 0] dizisi de alınabilirdi. Bu dizilerin her birisi

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

singüler eğrisi ile eşleşirler.

Aşağıdaki teorem singüler bir dizinin tersinin de singüler olduğunu göstermektedir.

5.2.11 Teorem. Eğer $(h_n(p))$ bir singüler dizi ise $((-1)^{n-1}\, h_n(p))$ dizisi de bir singüler dizidir.

İspat. (h_n) singüler bir dizi olduğundan

$$\Delta(h_2, h_3, h_4) = h_4 h_2^{15} - h_3^3 h_2^{12} + 3h_4^2 h_2^{10} - 20h_4 h_3^3 h_2^7 + 3h_4^3 h_2^5 + 16h_3^6 h_2^4 + 8h_4^2 h_3^3 h_2^2 + h_4^4 = 0$$

dir, bu eşitlikte h_2 yerine $-h_2$ ve h_4 yerine $-h_4$ dizisi yazılırsa

$$\Delta(-h_2, h_3, -h_4) = 0$$

olduğu görülür. Bu ise $((-1)^{n-1} h_n(p))$ dizisinin de singüler bir dizi olduğunu gösterir.

5.2.12 Uyarı. Eğer $(h_n(p))$ bir temsilci dizi ise $((-1)^{n-1} h_n(p))$ dizisi de diğer temsilci dizidir üstelik bu dizilerden biri tamsayı dizisi ise diğeri bir Lucas dizisidir.

5.2.13 Teorem. $h_2 h_3 \neq 0$ olmak üzere $\mathbb{F}_p$ üzerinde tanımlı singüler diziler için temsilci dizi sayısı ve dolayısıyla denk dizi sınıflarının sayısı $\frac{p-3}{2}$ tanedir. Her bir denklik sınıfında ise $p - 1$ tane dizi vardır.

İspat. $s = 1$ özelliğindeki diziler temsilci diziler olduğundan r sayısı için p tane alternatif vardır. $r = 0$ olamaz, çünkü bu durumda $h_2 = r = 0$ olur. Diğer yandan, $h_2 h_3 \neq 0$

olduğundan r sayısı 1 ve $p-1$ de olamaz, çünkü bu durumda $h_3 = r^2 - 1 = 0$ olur. Üstelik $(h_n(p))$ ve $((-1)^{n-1} h_n(p))$ dizileri denk diziler olduklarından singüler diziler için temsilci dizi sayısı ve dolayısıyla denk dizi sınıfı sayısının $\frac{p-3}{2}$ tane olduğu görülür. Eğer $(h_n(p))$ ve $(h'_n(p))$ denk diziler ise $\theta = \sqrt{s}$ olmak üzere $h_n(p) = \theta^{n^2-1}(h'_n(p))$ olduğundan her bir denklik sınıfında $\boldsymbol{Q}_p$ nin eleman sayısının 2 katı kadar dizi yani $p-1$ tane dizi vardır.

5.2.14 Örnek. $\mathbb{F}_7$ de [1 2 3 4] ve [1 3 1 0] dizileri birer temsilci dizidirler. Bu dizilerin denklik sınıfları ise, sırasıyla,

$$\overline{[1\ 2\ 3\ 4]} = \{ [1\,2\,3\,4], [1\,2\,5\,4], [1\,2\,6\,4], [1\,5\,3\,3], [1\,5\,5\,3], [1\,5\,6\,3] \}$$

ve

$$\overline{[1\ 3\ 1\ 0]} = \{ [1\,3\,1\,0], [1\,3\,2\,0], [1\,3\,4\,0], [1\,4\,1\,0], [1\,4\,2\,0], [1\,4\,4\,0] \}$$

dir.

5.2.15 Teorem. $(h_n(p))$ singüler dizisi ve bu dizinin tersi olan $((-1)^{n-1} h_n(p))$ singüler dizisi aynı singüler eğri ile eşleşirler.

İspat. (h_n) dizisi başlangıç terimleri $h_2 = r$, $h_3 = r^2 - 1$, $h_4 = r(r^2 - 2)$ olmak üzere bu diziye karşılık gelen $E : y^2 = x^3 + ax + b$ singüler eğrisinin katsayıları

$$a = 3^3(-h_2^{16} - 4ch_2^{12} + (16h_3^3 - 6c^2)h_2^8 + (8ch_3^3 - 4c^3)h_2^4 - (16h_3^6 + 8c^2h_3^3 + c^4))$$

$$b = 2 \cdot 3^3(h_2^{24} + 6ch_2^{20} - (24h_3^3 - 15c^2)h_2^{16} - (60ch_3^3 - 20c^3)h_2^{12} + (120h_3^6 - 36c^2h_3^3 + 15c^4)h_2^8$$
$$+ (-48ch_3^6 + 12c^3h_3^3 + 6c^5)h_2^4 + (64h_3^9 + 48c^2h_3^6 + 12c^4h_3^3 + c^6))$$

olduğundan bu eşitlikte, h_2 yerine $-h_2$ ve h_4 yerine $-h_4$ alınırsa a ve b katsayılarının değişmediği görülür.

Şimdi özel bir singüler dizi sınıfı olan, $y^2 = x^3$ singüler eğrisi ile eşleşen dizileri ele alınacaktır.

5.2.16 Teorem. $(h_n(p))$ singüler dizisi $y^2 = x^3$ singüler eğrisi ile eşleşsin. Bu durumda $(h_n(p))$ singüler dizisinin temsilci dizilerinden biri [1 2 3 4] tamsayı dizisi, diğeri [1 −2 3 −4] Lucas dizisidir.

İspat. $y^2 = x^3$ singüler eğrisine karşılık gelen diziler $r^2 = 4s^3$ eşitliğini gerçeklediğinden ve $s = 1$ özelliğindeki diziler temsilci diziler olduğundan, $s = 1$ için $r = \pm 2$ olur ve dolayısıyla istenilen temsilci diziler [1 2 3 4] ve [1 −2 3 −4] olarak elde edilir.

5.2.17 Uyarı. $(h_n(p))$ ve $(h'_n(p))$ dizileri Ward anlamında denk diziler oldukları halde bunların aynı eliptik eğri ile eşleşmeleri gerekmemektedir. Örneğin $\mathbb{F}_{11}$ de [1 6 5 10] ve [1 7 4 10] dizleri Ward anlamında denk dizilerdir, fakat bu diziler sırasıyla

$$E_1 : y^2 = x^3 + 7x + 7 \quad \text{ve} \quad E_2 : y^2 = x^3 + 10x + 6$$

eliptik eğrileri ile eşleşirler. Bu nedenle Ward anlamında denklik tanımına alternatif bir denklik tanımı yapılabilir. Bu tanım EBD lere karşılık gelen eliptik eğrilerden faydalanarak yapılacaktır.

5.2.18 Tanım. $(h_n(p))$ ve $(h'_n(p))$ iki EBD olsun. Eğer bu iki dizi aynı E eliptik eğrisi ile eşleşmiş ise bu dizilere *eğrisel denk diziler* denir. Aynı E eliptik eğrisini veren dizilerin oluşturduğu dizi ailesi eğrisel denk dizilerin denklik sınıfını oluştururlar ve bu sınıf $[E(h_n(p))]$ ile gösterilir.

Bu şekilde tanımlanan dizilerin eğrisel denkliğinin bir denklik bağıntısı olduğu açıktır.

5.2.19 Örnek. (h_n) ve (h'_n) dizileri sırasıyla $\mathbb{F}_7$ de [1 2 1 1] ve [1 3 3 1] olan diziler olsun. Bu diziler Ward anlamında denk değillerdir. Gerçektende $h_2 = 2$ ve $h'_2 = 3$ dir, dolayısıyla $2 = \theta^{2^2-1}3$ dir, eşitliğinden $\theta^3 = 3$ olarak bulunur. 3, $\mathbb{F}_7$ de bir üçüncü dereceden kalan olmadığından bu eşitliği gerçekleyen bir θ sayısı yoktur. Diğer yandan bu iki dizi aynı

$$E : y^2 = x^3 + 3x + 4,$$

eliptik eğrisi ile eşleştiğinden bu iki dizi eğrisel denktir.

Bu örneğin de gösterdiği gibi Ward anlamındaki denklik kavramı ile eğrisel denklik kavramları bir birlerinden farklı denklik kavramlarıdır. Eğrisel denklik kavramından faydalanarak elde edilen eğrisel denklik sınıfları kullanılarak, kuadratik formlar yardımıyla asal sayıların gösterimleri elde edilebilir.

5.3 $\mathbb{F}_p$ Üzerinde Rankları Bilinen Dizilerin Genel Terimleri

Bu kısımda ilk olarak $\mathbb{F}_p$ üzerinde tanımlı belli ranklara sahip dizilerin genel terimleri ve periyotları belirlenecek, daha sonra belli ranklara sahip singüler dizilerin karakteri belirlenecektir.

Rankı İki Olan Diziler

Rankı iki olan diziler, yani h_2 teriminin sıfır olması hali dikkate alındığında, Önerme 5.1.3 gereği her $n \in \mathbb{N}$ için $h_{2n} = 0$ olduğu açıktır. Bu dizilerin genel terimleri aşağıdaki şekilde verilmiştir. Buna göre, eğer (h_n) başlangıç terimleri $[1\ 0\ h_3\ 0]$ $(h_3 \in \mathbb{F}_p^*)$ olan bir eliptik bölünebilir dizi ise bu dizinin genel terimi,

$$h_n = \begin{cases} 0, & n \text{ çift} \\ -(1)^{\left\lfloor \frac{n}{4} \right\rfloor} h_3^{\frac{n^2-1}{8}}, & n \text{ tek} \end{cases}$$

biçimindedir (Ward 1948).

5.3.1 Uyarı. Dikkat edilirse rankı iki olan, yani ikinci terimi sıfır olan bütün dizilerin diskriminantı sıfırdır, dolayısıyla rankı iki olan tüm diziler singüler dizilerdir.

Rankı Üç Olan Diziler

Bu kısımda rankı üç olan diziler, yani h_3 teriminin sıfır olan diziler ele alınacaktır. Bu durumda da, Önerme 5.1.3 gereği her $n \in \mathbb{N}$ için $h_{3n} = 0$ olduğu açıktır. Aşağıdaki teoremde bu biçimdeki dizilerin genel terimleri verilmiştir.

5.3.2 Teorem. [1 h_2 0 h_4] (h_2, $h_4 \in \mathbb{F}_p^*$) bir eliptik bölünebilir dizi olsun. Bu durumda bu dizinin genel terimi,

$$h_n = h_{3k+a} = \varepsilon\, h_4^{\frac{k(k+1)}{2}}\, h_2^{\frac{(k+2a-2)(k+2a-3)}{2}} \tag{5.2}$$

biçimindedir ve burada

$$\varepsilon = \begin{cases} +1 & n \equiv 1,2,4,5\ (12) \\ -1 & n \equiv 7,8,10,11\ (12) \end{cases}$$

dir.

İspat. Bu sonucun $n = 4$ için doğru olduğu açıktır. O halde $n > 4$ olarak kabul edilir. Her $n, m \in \mathbb{N}$ için

$$h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2$$

olduğundan bu eşitlikte $m = 2$ olarak alınırsa,

$$h_{n+2}h_{n-2} = h_{n+1}h_{n-1}h_2^2 - h_3h_1h_n^2$$

ve $h_3 = 0$ olduğundan

$$h_{n+2}h_{n-2} = h_{n+1}h_{n-1}h_2^2 \tag{5.3}$$

eşitliği elde edilir.

(5.2) eşitliğine tümevarım uygulayarak teoremin ispatı tamamlanır. İspatı tamamlamak için n sayısının özel değerlerini dikkate almak gerekir.

İlk olarak $n + 1 \equiv 4\ (12)$ olsun. O halde (5.2) eşitliğinin $n + 1$ için doğru olduğu varsayılır ve $n + 2$ için bu eşitliğin doğru olduğu gösterilirse ispat bu hal için tamamlanmış olur. Bu durumda, $n + 1 = 3(4r + 1) + 1$ ($r \in \mathbb{N}$) olarak yazılabilir, dolayısıyla $n + 2 = 3(4r + 1) + 2$ olur. Böylece

$$h_{n+2} = h_4^{8r^2+6r+1}\, h_2^{8r^2+10r+3}$$

olarak bulunur. Benzer şekilde hareket edilerek

$$h_{n+1} = h_4^{8r^2+6r+1}\, h_2^{8r^2+2r}$$

$$h_n = 0$$

$$h_{n-1} = h_4^{8r^2+2r}\, h_2^{8r^2+6r+1}$$

ve

$$h_{n-2} = h_4^{8r^2+2r}\, h_2^{8r^2-2r}$$

olarak bulunur. Bu değerler (5.3) eşitliğinde yerine koyulursa

$$h_{n+2}\, h_4^{8r^2+2r}\, h_2^{8r^2-2r} = h_4^{8r^2+6r+1}\, h_2^{8r^2+2r}\, (h_4^{8r^2+2r}\, h_2^{8r^2+6r+1})\, h_2^2$$

eşitliğinden

$$h_{n+2} = h_4^{8r^2+6r+1}\, h_2^{8r^2+10r+3}$$

olarak elde edilir. Böylece $n + 1 \equiv 4\ (12)$ hali için teorem ispatlanmış olur. Diğer hallerde benzer şekilde elde edilir.

5.3.3 Uyarı. (h_n) has eliptik bölünebilir dizi olduğundan $h_2 \mid h_4$ dür, dolayısıyla $c \in \mathbb{F}_p^*$ olmak üzere $h_4 = ch_2$ olarak yazılabilir. O halde rankı üç olan dizilerin genel terimi c parametresine bağlı olarak aşağıdaki gibi de verilebilir.

5.3.4 Teorem. $[1\ h_2\ 0\ h_4 = ch_2]$ $(h_2, c \in \mathbb{F}_p^*)$ bir eliptik bölünebilir dizi olsun. Bu durumda bu dizinin genel terimi,

$$h_n = h_{3k+a} = \varepsilon\, c^{\frac{k(k+1)}{2}}\, h_2^{(k+a-1)^2}$$

biçimindedir ve burada

$$\varepsilon = \begin{cases} +1, & n \equiv 1,2,4,5\,(12) \\ -1, & n \equiv 7,8,10,11\,(12) \end{cases}$$

dir.

İspat. Teorem tümevarım yöntemiyle Teorem 5.3.2 deki gibi ispatlanır.

5.3.5 Uyarı. Rankı iki olan diziler de olduğu gibi rankı üç olan tüm dizilerin de diskriminantı sıfırdır, dolayısıyla rankı üç olan tüm diziler de singüler dizilerdir.

Rankı Dört Olan Diziler

Bu kısımda rankı dört olan diziler, yani h_4 teriminin sıfır olan diziler ele alınacaktır. Bu durumda da Önerme 5.1.3 gereği her $n \in \mathbb{N}$ için $h_{4n} = 0$ olduğu açıktır. Aşağıdaki teoremde bu biçimdeki dizilerin genel terimleri verilmiştir.

5.3.6 Teorem. [1 h_2 h_3 0] (h_2, $h_3 \in \mathbb{F}_p^*$) bir eliptik bölünebilir dizi olsun. Bu durumda bu dizinin genel terimi,

$$h_n = h_{4k+a} = \varepsilon h_2^{\beta} h_3^{2k^2+ak+\alpha} \tag{5.4}$$

biçimindedir ve burada

$$\varepsilon = \begin{cases} +1, & n \equiv 1,2,3\,(8) \\ -1, & n \equiv 5,6,7\,(8) \end{cases},\ \alpha = \frac{1}{2}a^2 - \frac{3}{2}a + 1,\ \beta = \begin{cases} 1, & n \text{ çift} \\ 0, & n \text{ tek} \end{cases}$$

dir.

İspat. Bu sonucun $n = 5$ için doğru olduğu açıktır. O halde $n > 5$ olduğunu kabul edelim. Her $n \in \mathbb{N}$ için

$$h_{n+2}h_{n-2} = h_{n+1}h_{n-1}h_2^2 - h_3h_1h_n^2 \tag{5.5}$$

olduğundan (5.4) eşitliğine tümevarım uygulayarak teoremin ispatı tamamlanır. İlk olarak $n + 1 \equiv 2\,(8)$ olsun. O halde (5.4) eşitliğinin $n + 1$ için doğru olduğu varsayalım ve $n + 2$ için bu eşitliğin doğru olduğunu gösterelim. Bu durumda $n + 1 = 4 \cdot 2r + 2$ ($r \in \mathbb{N}$) ve dolayısıyla $n + 2 = 4 \cdot 2r + 3$ olur. Böylece

$$h_{n+2} = h_3^{8r^2+6r+1}$$

olarak bulunur. Benzer şekilde hareket edilerek

$$h_{n-2} = -h_3^{8r^2-2r}$$

$$h_n = h_3^{8r^2+2r}$$

olarak bulunur. Bu değerler (5.5) eşitliğinde yerine koyulursa

$$h_{n+2}\,(-h_3^{8r^2-2r}) = h_3^{16r^2+4r+1}$$

eşitliğinden

$$h_{n+2} = h_3^{8r^2+6r+1}$$

olarak elde edilir. Böylece $n + 1 \equiv 2$ (8) hali için teorem ispatlanmış olur. Diğer hallerde benzer şekilde elde edilir.

Şimdi h_4 teriminin sıfır olması halinde dizinin periyotunun ne olduğunu belirten aşağıdaki teorem verilebilir.

5.3.7 Teorem. [1 h_2 h_3 0] (h_2, $h_3 \in \mathbb{F}_p^*$) bir eliptik bölünebilir dizi olsun. Bu durumda bu dizinin periyotu,

$$\pi(h_n) = \begin{cases} 4(p-1), & h_3, \bmod p \text{ de bir ilkel kök} \\ 8r, & \text{diger hallerde} \end{cases}$$

dir ve burada

$$r = \begin{cases} q & q \text{ tek} \\ \dfrac{q}{2} & q \text{ çift} \end{cases}$$

dir.

İspat. Dizinin rankı 4 olduğundan $\rho = 4$ dir. Bu durumda

$$a_1 = \frac{h_2}{h_{\rho-2}} = \frac{h_2}{h_2} = 1$$

olduğundan a_1 in mertebesi $e = 1$ dir, $a_2 = h_{\rho-1} = h_3$ olduğundan a_2 nin mertebesi, eğer h_3, $\mathbb{F}_p$ de bir ilkel kök ise $k = p - 1$ değilse $k = q$ dur, burada q, $p - 1$ in bir asal bölenidir. O halde h_3 bir ilkel kök ise $\alpha = 0$ ve $\tau = 2^\alpha$ [e, k] olduğundan $\tau = p - 1$ dir ve dolayısıyla $\pi(h_n) = \tau \cdot \rho = 4(p - 1)$ olarak bulunur. Eğer h_3, $\mathbb{F}_p$ de bir ilkel kök değilse, $a_2 = h_3$ ün mertebesi $k = q$ dur. O halde $\alpha = 0$ veya 1 olabilir. Dolayısıyla $\tau = 2^\alpha$ [e, k] = q veya $2q$ dur. $\pi(h_n) = \tau \cdot \rho = 4q$ veya $8q$ dur.

Aşağıdaki teorem rankı 4 olan singüler eliptik bölünebilir dizilerin ne zaman ortaya çıktığı verilmiştir.

5.3.8 Teorem. [1 h_2 h_3 0] (h_2, $h_3 \in \mathbb{F}_p^*$) bir eliptik bölünebilir dizi olsun. Bu durumda (h_n) nin bir singüler EBD olabilmesi için gerek ve yeter şart $h_3^3 = \frac{h_2^8}{16}$ olmasıdır.

İspat. $\Delta(h_2, h_3, h_4) = h_4 h_2^{15} - h_3^3 h_2^{12} + 3h_4^2 h_2^{10} - 20h_4 h_3^3 h_2^7 + 3h_4^3 h_2^5 + 16h_3^6 h_2^4 + 8h_4^2 h_3^3 h_2^2 + h_4^4$ eşitliğinde $h_4 = 0$ olarak alınırsa

$$\Delta(h_2, h_3, h_4) = h_3^3 h_2^4 (-h_2^8 + 16h_3^3)$$

olarak bulunur. O halde

$$\Delta(h_2, h_3, h_4) = 0 \Leftrightarrow h_3^3 = \frac{h_2^8}{16}$$

dır.

Rankı Beş Olan Diziler

Bu kısımda rankı beş olan diziler, yani beşinci terimi sıfır olan diziler ele alınacaktır. Bu durumda, Önerme 5.1.3 gereği her $n \in \mathbb{N}$ için $h_{5n} = 0$ dir.

5.3.9 Teorem. [1 h_2 h_3 h_4] (h_2, h_3, $h_4 \in \mathbb{F}_p^*$), rankı beş olan bir eliptik bölünebilir dizi olsun. Bu durumda bu dizinin genel terimi,

$$h_n = h_{5k+a} = \varepsilon\, h_2^{-(5k^2+2ak+\beta)}\, h_3^{5k^2+2ak+\alpha} \tag{5.6}$$

dir ve burada

$$\varepsilon = \begin{cases} +1, & n \equiv 1,2,3,4 (10) \\ -1, & n \equiv 6,7,8,9 (10) \end{cases},\ \alpha = \frac{1}{2}a^2 - \frac{3}{2}a + 1,\ \ \beta = a^2 - 4a + 3$$

dir.

İspat. (h_n) rankı beş olan bir dizi olduğundan $h_5 = h_4 h_2^3 - h_3^3 = 0$ ve dolayısıyla $h_4 = \left(\frac{h_3}{h_2}\right)^3$ dir. Diğer yandan bu sonucun $n = 6$ için doğru olduğu açıktır. O halde $n > 6$ olduğunu kabul edilir. Her $n \in \mathbb{N}$ için

$$h_{n+2}h_{n-2} = h_{n+1}h_{n-1}h_2^2 - h_3 h_1 h_n^2 \tag{5.7}$$

olduğundan bu eşitliğe tümevarım uygulayarak teoremin ispatı tamamlanır. İlk olarak $n + 1 \equiv 2$ (10) olsun. (5.6) eşitliğinin $n + 1$ için doğru olduğunu varsayılır ve $n + 2$ için bu eşitliğin doğru olduğu gösterilirse ispat tamamlanır. Bu durumda $n + 1 = 5 \cdot 2r + 2$ ($r \in \mathbb{N}$) ve dolayısıyla $n + 2 = 5 \cdot 2r + 3$ olur. O halde

$$h_{n+2} = h_3^{20r^2+12r+1} h_2^{-(20r^2+12r)}$$

olarak bulunur ve böylece eşitliğin doğru olduğunu görülmüş olur. Benzer şekilde hareket edilerek

$$h_{n-2} = -h_3^{20r^2-4r} h_2^{-(20r^2-4r)}$$

ve

$$h_n = h_3^{20r^2+4r} h_2^{-(20r^2+4r)}$$

olarak bulunur. Bu değerler (5.7) eşitliğinde yerine koyulursa

$$h_{n+2}(-h_3^{20r^2-4r} h_2^{-(20r^2-4r)}) = -h_3(h_3^{20r^2+4r} h_2^{-(20r^2+4r)})^2$$

eşitliğinden

$$h_{n+2} = h_3^{20r^2+12r+1} h_2^{-(20r^2+12r)}$$

olarak elde edilir. Böylece $n + 1 \equiv 2$ (10) hali için teorem ispatlanmış olur. Diğer hallerde benzer şekilde elde edilir.

Şimdi h_5 teriminin sıfır olması halinde dizinin periyotunun ne olduğunu belirten aşağıdaki teorem verilebilir.

5.3.10 Teorem. [1 h_2 h_3 h_4] (h_2, h_3, $h_4 \in \mathbb{F}_p^*$) rankı beş olan bir eliptik bölünebilir dizi olsun. Bu durumda q, $\frac{h_2}{h_3}$ ün mertebesi olmak üzere dizinin periyotu,

$$\pi(h_n) = \begin{cases} \frac{5}{2}(p-1), & \frac{h_2}{h_3}, \bmod p \text{ de bir ilkel kök} \\ 10r, & \text{diger hallerde} \end{cases}$$

dir ve burada

$$r = \begin{cases} q & q \text{ tek} \\ \frac{q}{4} & q \text{ çift} \end{cases}$$

dir.

İspat. Dizinin rankı 5 olduğundan $\rho = 5$ dir. Bu durumda

$$a_1 = \frac{h_2}{h_{\rho-2}} = \frac{h_2}{h_3}$$

ve

$$a_2 = h_{\rho-1} = h_4 = \left(\frac{h_3}{h_2}\right)^3$$

olduğundan eğer $\frac{h_2}{h_3}$, $\mathbb{F}_p$ de bir ilkel kök ise a_1 in mertebesi $e = p - 1$ ve a_2 nin mertebesi $k = \frac{p-1}{3}$, eğer $\frac{h_2}{h_3}$, $\mathbb{F}_p$ de bir ilkel kök değilse, $e = q$ ve $k = \frac{q}{3}$ dir. O halde $\frac{h_2}{h_3}$ bir ilkel kök ise $\alpha = -1$ ve $\tau = \frac{p-1}{2}$ dir ve dolayısıyla $\pi(h_n) = \tau \cdot \rho = \frac{5}{2}(p-1)$ olur. Eğer $\frac{h_2}{h_3}$, $\mathbb{F}_p$ de bir ilkel kök değilse, q tek ise $\alpha = 1$ ve q çift ise $\alpha = -1$ dir. Dolayısıyla $\tau = 2q$ veya $\frac{q}{4}$ olur. O halde $\pi(h_n) = \tau \cdot \rho = 10q$ veya $\frac{5}{2}q$ dur.

Aşağıdaki teoremde rankı 5 olan singüler eliptik bölünebilir dizilerin ne zaman ortaya çıktığı gösterilmektedir.

5.3.11 Teorem. $[1\ h_2\ h_3\ h_4]$ ($h_2, h_3, h_4 \in \mathbb{F}_p^*$) rankı beş olan bir eliptik bölünebilir dizi olsun. Bu durumda (h_n) nin bir singüler eliptik bölünebilir dizi olabilmesi için gerek ve yeter şart $h_2^5 = \frac{11 \pm 5\sqrt{5}}{2} h_4$ olmasıdır.

İspat. (h_n) rankı beş olan bir dizi olduğundan $h_4 = \left(\frac{h_3}{h_2}\right)^3$ dir. Eğer

$$\Delta(h_2, h_3, h_4) = h_4 h_2^{15} - h_3^3 h_2^{12} + 3h_4^2 h_2^{10} - 20h_4 h_3^3 h_2^7 + 3h_4^3 h_2^5 + 16h_3^6 h_2^4 + 8h_4^2 h_3^3 h_2^2 + h_4^4$$

eşitliğinde $h_4 = \left(\frac{h_3}{h_2}\right)^3$ yazılırsa

$$\Delta(h_2, h_3, h_4) = -h_2^{10} + 11h_2^5 h_4 + h_4^2$$

olarak bulunur. O halde $\Delta(h_2, h_3, h_4) = 0 \Leftrightarrow h_2^5 = \frac{11 \pm 5\sqrt{5}}{2} h_4$ dır.

5.3.12 Teorem. [1 h_2 h_3 h_4] ($h_2, h_3, h_4 \in \mathbb{F}_p^*$) olan bir dizi olsun. Bu dizinin rankı beş olan bir singüler eliptik bölünebilir dizi olabilmesi için gerek ve yeter şart

$$p = 5 \text{ veya } p \equiv 1, 9 \ (10)$$

olmasıdır.

İspat. (h_n) nin bir singüler EBD olabilmesi için gerek ve yeter şart $h_2^5 = \frac{11 \pm 5\sqrt{5}}{2} h_4$ olmasıdır. O halde, "(h_n) nin bir singüler dizidir $\Leftrightarrow$ 5 bir ikinci dereceden kalandır veya $p = 5$ dir" ve dolayısıyla "5 bir ikinci dereceden kalandır $\Leftrightarrow p \equiv 1, 9 \ (10)$" dur.

Rankı Altı Olan Diziler

Bu kısımda rankı altı olan diziler, yani altıncı terimin sıfır olan diziler dikkate alınacaktır. Bu durumda, Önerme 5.1.3 gereği her $n \in \mathbb{N}$ için $h_{6n} = 0$ dir.

5.3.13 Teorem. [1 h_2 h_3 h_4] ($h_2, h_3, h_4 = ch_2 \in \mathbb{F}_p^*$) rankı altı olan bir eliptik bölünebilir dizi olsun. Bu durumda bu dizinin genel terimi,

$$h_n = h_{6k+a} = \varepsilon h_2^{\alpha} h_3^{\beta} c^{3k^2 + ak + \gamma} \tag{5.8}$$

biçimindedir, burada

$$\varepsilon = \begin{cases} +1, & n \equiv 1, 2, 3, 4, 5 \ (12) \\ -1, & n \equiv 7, 8, 9, 10, 11 \ (12) \end{cases}$$

ve

$$\alpha = \begin{cases} 1, & n \text{ çift} \\ 0, & n \text{ tek} \end{cases}, \ \beta = \begin{cases} 1, & 3 \mid n \\ 0, & 3 \nmid n \end{cases}, \ \gamma = \begin{cases} 0, & a \le 3 \\ a-3, & a > 3 \end{cases}$$

dir.

İspat. (h_n) rankı altı olan bir dizi olduğundan $h_6 = \frac{h_3}{h_2}(h_5 h_2^2 - h_4^2) = 0$ ve dolayısıyla $h_5 = \left(\frac{h_4}{h_2}\right)^2$ dir. Diğer yandan bu sonucun $n = 7$ için doğru olduğu açıktır. O halde $n > 7$ olduğunu kabul edilir. Her $n \in \mathbb{N}$ için

$$h_{n+2}h_{n-2} = h_{n+1}h_{n-1}h_2^2 - h_3 h_1 h_n^2 \tag{5.9}$$

olduğundan bu eşitliğe tümevarım uygulayarak teoremin ispatı tamamlanır. İlk olarak $n + 1 \equiv 2$ (12) olsun. (5.8) eşitliğinin $n + 1$ için doğru olduğunu varsayalım ve $n + 2$ için bu eşitliğin doğru olduğunu gösterelim. Bu durumda $n + 1 = 6 \cdot 2r + 2$ ($r \in \mathbb{N}$) ve dolayısıyla $n + 2 = 6 \cdot 2r + 3$ olur. O halde

$$h_{n+2} = h_3 c^{12r^2+6r}$$

olarak bulunur. Şimdi bunun doğru olduğunu görelim. Benzer şekilde hareket edilerek

$$h_{n-2} = -c^{12r^2-2r}$$

ve

$$h_n = c^{12r^2+2r}$$

olarak bulunur. Bu değerler (5.9) eşitliğinde yerine koyulursa

$$h_{n+2}(-c^{12r^2-2r}) = -h_3(c^{12r^2+2r})^2$$

eşitliğinden

$$h_{n+2} = h_3 c^{12r^2+6r}$$

olarak elde edilir. Böylece $n + 1 \equiv 2$ (12) hali için teorem ispatlanmış olur. Diğer hallerde benzer şekilde elde edilir.

Şimdi h_6 teriminin sıfır olması halinde dizinin periyotunun ne olduğunu belirten aşağıdaki teorem verilebilir.

5.3.14 Teorem. [1 h_2 h_3 h_4] (h_2, h_3, $h_4 \in \mathbb{F}_p^*$) rankı altı olan bir eliptik bölünebilir dizi olsun. Bu durumda q, $\frac{h_2}{h_4}$ ün mertebesi olmak üzere dizinin periyotu,

$$\pi(h_n) = \begin{cases} 6(p-1), & \frac{h_2}{h_4}, \bmod p \text{ de bir ilkel kök} \\ 12r, & \text{diger hallerde} \end{cases}$$

dir ve burada

$$r = \begin{cases} q & q \text{ tek} \\ \frac{q}{2} & q \text{ çift} \end{cases}$$

dir.

İspat. Dizinin rankı 6 olduğundan $\rho = 6$ dır. Bu durumda

$$a_1 = \frac{h_2}{h_{\rho-2}} = \frac{h_2}{h_4}$$

ve

$$a_2 = h_{\rho-1} = h_5 = \left(\frac{h_4}{h_2}\right)^2$$

olduğundan $\frac{h_2}{h_4}$, $\mathbb{F}_p$ de bir ilkel kök ise a_1 in mertebesi $e = p - 1$ ve a_2 nin mertebesi $k = \frac{p-1}{2}$ dir, bu durumda $\alpha = 0$ ve $\tau = p - 1$ dir. O halde $\pi(h_n) = \tau \cdot \rho = 6(p - 1)$ olur. Eğer $\frac{h_2}{h_4}$, $\mathbb{F}_p$ de bir ilkel kök değilse bu durumda iki hal söz konusudur, buna göre eğer q tek ise $e = q$ ve $k = q$ dur. Dolayısıyla $\alpha = 1$ ve $\tau = q$ olur ve bu durumda $\pi(h_n) = \tau \cdot \rho = 6q$ olur. Eğer q çift ise $e = q$ ve $k = \frac{q}{2}$ dir. O halde $\alpha = 0$ ve $\tau = 2q$ dir ve dolayısıyla $\pi(h_n) = \tau \cdot \rho = 12q$ dur.

Aşağıdaki teoremde rankı 6 olan singüler eliptik bölünebilir dizilerin ne zaman ortaya çıktığı verilmiştir.

5.3.15 Teorem. [1 h_2 h_3 h_4] (h_2, h_3, $h_4 \in \mathbb{F}_p^*$) rankı altı olan bir eliptik bölünebilir dizi olsun. Bu durumda (h_n) nin bir singüler EBD olabilmesi için gerek ve yeter şart $h_4 = \frac{h_2^5}{9}$ olmasıdır.

İspat. (h_n) rankı altı olan bir dizi olduğundan $h_5 = \left(\frac{h_4}{h_2}\right)^2$ ve dolayısıyla $h_3^3 = \frac{h_4 h_2^5 - h_4^2}{h_2^2}$ dir. Eğer bu değer

$$\Delta(h_2, h_3, h_4) = h_4 h_2^{15} - h_3^3 h_2^{12} + 3h_4^2 h_2^{10} - 20h_4 h_3^3 h_2^7 + 3h_4^3 h_2^5 + 16h_3^6 h_2^4 + 8h_4^2 h_3^3 h_2^2 + h_4^4$$

eşitliğinde yazılırsa

$$\Delta(h_2, h_3, h_4) = -h_4^3 h_2^5 + 9h_4^4$$

olarak bulunur. O halde $\Delta(h_2, h_3, h_4) = 0 \Leftrightarrow h_4 = \frac{h_2^5}{9}$ dır.

Rankı Yedi Olan Diziler

Bu kısımda rankı yedi olan diziler, yani yedinci terimin sıfır olan diziler dikkate alınacaktır. Aşağıdaki teoremde yedinci terimi sıfır olan eliptik bölünebilir dizilerin başlangıç terimlerinin neler olduğu belirlenmiştir.

5.3.16 Teorem. (h_n) $\mathbb{F}_p$ üzerinde tanımlı bir eliptik bölünebilir dizi olsun. (h_n) dizisinin yedinci teriminin sıfır olması için gerek ve yeter şart (h_n) dizisinin başlangıç terimlerinin $t \equiv 1$ (3) olmak üzere

$$[1\ 2^t\ 2^{\frac{8t+1}{3}}\ -2^{5t+1}] \text{ veya } [1\ -2^t\ 2^{\frac{8t+1}{3}}\ 2^{5t+1}]$$

olmasıdır.

İspat. $h_7 = h_5 h_3^3 - h_2 h_4^3$ olduğundan bu eşitlikte $h_5 = h_4 h_2^3 - h_3^3$ ve $h_4 = ch_2$ yazılırsa

$$h_7 = ch_2^4 h_3^3 - h_2^4 c^3 - h_3^6$$

olarak bulunur. O halde $h_7 = 0$ ise $h_3^3 = -ch_2$ veya $h_3^3 = c^2 - h_3^3$ ve dolayısıyla $c = -2h_2^4$ dır. Böylece, $h_3^3 = 2h_2^8$ ve $h_4 = -2h_2^5$ olarak bulunur. Üstelik $h_3^3 = 2h_2^8$ in bir küp olması için

gerek ve yeter şart $t \equiv 1\ (3)$ olmak üzere $h_2 = \pm 2^t$ olmasıdır. Dolayısıyla rankı yedi olan bir dizinin başlangıç terimleri $[1\ 2^t\ 2^{\frac{8t+1}{3}}\ -2^{5t+1}]$ veya $[1\ -2^t\ 2^{\frac{8t+1}{3}}\ 2^{5t+1}]$ dır.

Diğer yandan (h_n) dizisinin başlangıç terimleri

$$[1\ 2^t\ 2^{\frac{8t+1}{3}}\ -2^{5t+1}] \text{ veya } [1\ -2^t\ 2^{\frac{8t+1}{3}}\ 2^{5t+1}]$$

ise $h_5 = \pm\ 2^{8t+2}$ ve dolayısıyla $h_7 = 0$ dır.

Aşağıdaki teoremde rankı yedi olan dizilerin genel terimleri verilmiştir. Bu durumda, Önerme 5.1.3 gereği her $n \in \mathbb{N}$ için $h_{7n} = 0$ dir.

5.3.17 Teorem. (h_n) başlangıç terimleri Teorem 5.3.16 da verilen $\mathbb{F}_p$ üzerinde tanımlı ve rankı yedi olan bir eliptik bölünebilir dizi olsun. Bu durumda bu dizinin genel terimi,

$$h_n = h_{7k+a} = \varepsilon 2^{\alpha} h_2^{\beta} h_3^{\gamma}$$

biçimindedir, burada

$$\varepsilon = \begin{cases} +1, & n \equiv 1,2,3\ (7) \\ -1, & n \equiv 4,5,6\ (7) \end{cases}$$

ve

$$\alpha = \begin{cases} (\frac{1}{4}a^2 - \frac{5}{4}a + 6)k^2 + (-\frac{5}{4}a^2 - \frac{29}{4}a - 6)k + (\frac{3}{2}a^2 - \frac{13}{2}a + 6), & a = 1,2,3 \\ (\frac{1}{4}a^2 - \frac{11}{4}a + 12)k^2 + (-\frac{5}{4}a^2 + \frac{59}{4}a - 35)k + (\frac{3}{2}a^2 - \frac{29}{2}a + 36), & a = 4,5,6 \end{cases}$$

$$\beta = \begin{cases} (2a^2 - 10a + 27)k^2 + (-10a^2 + 52a - 48)k + (11a^2 - 48a + 45), & a = 1,2,3 \\ (2a^2 - 22a + 75)k^2 + (-10a^2 - 112a + 616)k + (-2a^2 - 7a + 22), & a = 4,5,6 \end{cases}$$

$$\gamma = \begin{cases} 1, & 3 \mid n \\ 0, & 3 \nmid n. \end{cases}$$

dir.

İspat. Genel terim ile ilgili benzer teoremlerin ispatlarında olduğu gibi tümevarım ile görülür.

Şimdi h_7 teriminin sıfır olması halinde dizinin periyotunun ne olduğunu belirten aşağıdaki teorem verilebilir.

5.3.18 Teorem. [1 h_2 h_3 h_4] (h_2, h_3, $h_4 \in \mathbb{F}_p^*$) rankı yedi olan bir eliptik bölünebilir dizi olsun. Bu durumda e, $\frac{h_2}{h_5}$ in mertebesi olmak üzere dizinin periyotu,

i. $p \equiv 1\ (6)$ ise $\pi(h_n) = \begin{cases} 42e, & e \text{ tek} \\ \frac{21}{2}e, & e \text{ çift} \end{cases}$,

ii. $p \equiv 5\ (6)$ ise $\pi(h_n) = \begin{cases} 14e, & e \text{ tek} \\ \frac{7}{2}e, & e \text{ çift} \end{cases}$

dir.

İspat. Rankı yedi olan bir dizinin başlangıç terimlerinin $t \equiv 1\ (3)$ olmak üzere

$$[1\ 2^t\ 2^{\frac{8t+1}{3}}\ -2^{5t+1}] \text{ veya } [1\ -2^t\ 2^{\frac{8t+1}{3}}\ 2^{5t+1}]$$

biçiminde olduğu daha önce belirtilmişti. Bu nedenle ispat iki hal için verilecektir.

1. Hal. İlk olarak dizinin başlangıç terimleri $[1\ 2^t\ 2^{\frac{8t+1}{3}}\ -2^{5t+1}]$ olsun. Dizinin rankı 7 olduğundan $\rho = 7$ dır. Bu durumda

$$a_1 = \frac{h_2}{h_{\rho-2}} = \frac{h_2}{h_5} = -2^{-7t-2}$$

ve

$$a_2 = h_{\rho-1} = h_6 = -2^{\frac{35t+10}{3}}$$

olduğundan a_1 ve a_2 nin mertebelerini $p \equiv 1\ (6)$ ve $p \equiv 5\ (6)$ olmak üzere $\mathbb{F}_p$ de ayrı ayrı incelemek gerektiğinden aşağıdaki iki hal söz konusudur.

i. $p \equiv 1\ (6)$ olsun. Bu durumda a_1 in mertebesi e ise a_2 nin mertebesi $k = 3e$ dir. O halde e tek ise k tek, e çift ise k da çifttir ve üstelik bu durumda e ve k ikinin aynı kuvveti ile bölünürler. O halde, e tek ise $\alpha = 1$ ve $\tau = 6 \cdot e$ dir, böylece

$$\pi(h_n) = \tau \cdot \rho = 6 \cdot e \cdot 7 = 42e$$

olur. Eğer e çift ise $\alpha = -1$ ve $\tau = \frac{3}{2} \cdot e$ dir, böylece

$$\pi(h_n) = \tau \cdot \rho = \frac{3}{2} \cdot e \cdot 7 = \frac{21}{2}e$$

olur.

ii. $p \equiv 5\ (6)$ olsun. Bu durumda a_1 in mertebesi e ise a_2 nin mertebesi de $k = e$ dir. O halde e tek ise $\alpha = 1$ ve $\tau = 2 \cdot e$ dir, böylece

$$\pi(h_n) = \tau \cdot \rho = 2 \cdot e \cdot 7 = 14e$$

olur. Eğer e çift ise $\alpha = -1$ ve $\tau = \frac{1}{2} \cdot e$ dir, böylece

$$\pi(h_n) = \tau \cdot \rho = \frac{1}{2} \cdot e \cdot 7 = \frac{7}{2} e$$

olur.

2. Hal. Dizinin başlangıç terimleri $[1\ -2^t\ 2^{\frac{8t+1}{3}}\ \ 2^{5t+1}]$ olarak alındığında

$$a_1 = \frac{h_2}{h_{\rho-2}} = \frac{h_2}{h_5} = 2^{-7t-2}$$

ve

$$a_2 = h_{\rho-1} = h_6 = 2^{\frac{35t+10}{3}}$$

olur ve ispat 1. haldeki gibi görülür.

Aşağıdaki teoremde rankı 7 olan singüler eliptik bölünebilir dizilerin ne zaman ortaya çıktığı verilmiştir.

5.3.19 Teorem. $[1\ h_2\ h_3\ ch_2]$ $(h_2, h_3, h_4 \in \mathbb{F}_p^*)$ rankı yedi olan bir eliptik bölünebilir dizi olsun. Bu durumda (h_n) nin bir singüler EBD olabilmesi için gerek ve yeter şart $p = 13$ olmasıdır.

İspat. Rankı yedi olan bir dizinin başlangıç terimleri

$$[1\ 2^t\ 2^{\frac{8t+1}{3}}\ \ -2^{5t+1}] \text{ veya } [1\ -2^t\ \ 2^{\frac{8t+1}{3}}\ \ 2^{5t+1}]$$

olduğundan

$$\Delta(h_2, h_3, h_4) = h_4 h_2^{15} - h_3^3 h_2^{12} + 3h_4^2 h_2^{10} - 20h_4 h_3^3 h_2^7 + 3h_4^3 h_2^5 + 16h_3^6 h_2^4 + 8h_4^2 h_3^3 h_2^2 + h_4^4$$

eşitliğinde bu değerler yazılırsa $\Delta(h_2, h_3, h_4) = 2^{19}\, 3^{12}\, 13$ dir ve dolayısıyla

$$\Delta(h_2, h_3, h_4) = 0 \Leftrightarrow p = 13$$

dir.

5.4 $\mathbb{F}_p$ Üzerinde Rankları Bilinen Dizilerle Eşleşen Eğriler

Bu kısımda $\mathbb{F}_p$ üzerinde tanımlı başlangıç terimleri ve rankları bilinen diziler ile eşleşen eğriler belirlenecek ve bu eğrilerin özellikleri incelenecektir.

Rankı İki Olan Dizilerle Eşleşen Eğriler

Bu kısımda rankı iki olan dizilerle eşleşen eğriler ele alınacaktır. Rankı iki olan tüm diziler singüler olduğundan bu dizilerle eşleşen tüm eğriler de singülerdir.

5.4.1 Teorem. [1 0 h_3 $ch_2 = 0$] ($c \in \mathbb{F}_p$ ve $h_3 \in \mathbb{F}_p^*$) bir eliptik bölünebilir dizi olsun. Bu durumda bu dizilerle eşleşen eğriler birer singüler eğridir ve bu eğriler

$$E : y^2 = x^3 - 27(4h_3^3 + c^2)^2 x + 54(4h_3^3 + c^2)^3 \tag{5.10}$$

eşitliği ile belirtilir. Üstelik $P = (x_1, y_1)$ noktası E eğrisi üzerinde bir nokta olmak üzere bu dizi

$$P = (x_1, y_1) = (3(4h_3^3 + c^2), 0)$$

noktasından elde edilen bir dizidir.

İspat. [1 h_2 h_3 ch_2] eliptik bölünebilir dizisi ile eşleşen E: $y^2 = x^3 + ax + b$ eliptik eğrisi için

$$\Delta = 2^8 \cdot 3^{12} h_3^9 h_2^8 (ch_2^{12} + (-h_3^3 + 3c^2)h_2^8 + (-20ch_3^3 + 3c^3)h_2^4 + (16h_3^6 + 8c^2h_3^3 + c^4))$$

olduğundan $h_2 = 0$ olarak alınırsa $\Delta = 0$ olarak bulunur, bu ise rankı iki olan dizilerle eşleşen tüm eğrilerin bir singüler eğri olduğunu gösterir.

$$a = 3^3(-h_2^{16} - 4ch_2^{12} + (16h_3^3 - 6c^2)h_2^8 + (8ch_3^3 - 4c^3)h_2^4 - (16h_3^6 + 8c^2h_3^3 + c^4))$$

$$b = 2 \cdot 3^3(h_2^{24} + 6ch_2^{20} - (24h_3^3 - 15c^2)h_2^{16} - (60ch_3^3 - 20c^3)h_2^{12} + (120h_3^6 - 36c^2h_3^3 + 15c^4)h_2^8 + (-48ch_3^6 + 12c^3h_3^3 + 6c^5)h_2^4 + (64h_3^9 + 48c^2h_3^6 + 12c^4h_3^3 + c^6))$$

olduğundan bu eşitliklerde $h_2 = 0$ olarak alınırsa

$$a = -27(16h_3^6 + 8c^2h_3^3 + c^4) = -27(4h_3^3 + c^2)^2$$

ve

$$b = 54(64h_3^9 + 48c^2h_3^6 + 12c^4h_3^3 + c^6) = 54(4h_3^3 + c^2)^3$$

olarak bulunur. Üstelik $P = (x_1, y_1)$ E eğrisi üzerinde bir nokta olmak üzere

$$P = (x_1, y_1) = (3(h_2^8 + 2ch_2^4 + 4h_3^3 + c^2),\ -108h_3^3h_2^4)$$

olduğundan $h_2 = 0$ için bu diziler

$$P = (x_1, y_1) = (3(4h_3^3 + c^2), 0), (c \in \mathbb{F}_p)$$

noktasından elde edilir.

5.4.2 Uyarı. Bu singüler eğriler bir düğüme ya da çıkıntıya sahiptir. Bu eğrilerin hangi durumlarda bir düğüme ya da çıkıntıya sahip olduğu aşağıdaki teoremde belirlenecektir.

5.4.3 Teorem. [1 0 h_3 0] ($h_3 \in \mathbb{F}_p^*$) bir eliptik bölünebilir dizi olsun. Bu durumda,

i. [1 0 h_3 0] dizisi çıkıntıya sahip bir singüler eğri ile eşleşir $\Leftrightarrow \begin{cases} h_3 \in Q_p, & p \equiv 1(4) \\ h_3 \notin Q_p, & p \equiv 3(4), \end{cases}$

ii. [1 0 h_3 0] dizisi düğüme sahip bir singüler eğri ile eşleşir $\Leftrightarrow \begin{cases} h_3 \notin Q_p, & p \equiv 1(4) \\ h_3 \in Q_p, & p \equiv 3(4) \end{cases}$

dır.

İspat. (5.10) eşitliğinde $h_3^3 = -\frac{c^2}{4}$ yazılırsa sonuç elde edilir.

5.4.4 Uyarı 1. Teorem 5.4.1 de [1 0 h_3 ch_2] ($c \in \mathbb{F}_p$) dizisinin

$$E : y^2 = x^3 - 27(4h_3^3 + c^2)^2 x + 54(4h_3^3 + c^2)^3$$

eğrisi ile eşleştiği gösterilmiştir. Eğer $\alpha = 4h_3^3 + c^2$ ve $\beta = 3\alpha$ olarak alınırsa

$$a = -3\beta^2,\ b = 2\beta^3$$

olacağından

$$E : y^2 = x^3 - 3\beta^2 x + 2\beta^3$$

ve

$$P = (\beta, 0)$$

olur.

2. [1 0 h_3 ch_2] ($h_3 \in \mathbb{F}_p^*$ ve $c \in \mathbb{F}_p$) dizisi has olmayan bir dizidir, dolayısıyla dördüncü terimi belirlerken c sayısı olarak $\mathbb{F}_p$ nin tüm elemanları seçilebilir. Bu nedenle bu özellikteki her bir dizi birden fazla eğri ile eşleşebilir.

5.4.5 Örnek. $\mathbb{F}_5$ de [1 0 1 0] dizisi, c = 0, 1, 2, 3 ve 4 olarak seçildiğinde, sırasıyla,

$$y^2 = x^3 + 3x + 1, \qquad P = (2, 0)$$
$$y^2 = x^3, \qquad P = (0, 0)$$
$$y^2 = x^3 + 2x + 3, \qquad P = (4, 0)$$
$$y^2 = x^3 + 2x + 3, \qquad P = (2, 0)$$
$$y^2 = x^3, \qquad P = (2, 0)$$

eğrileri ile eşleşirler. Benzer şekilde başlangıç terimleri [1 0 2 0], [1 0 3 0], [1 0 4 0] olan dizilerle eşleşen eğriler, c = 0, 1, 2, 3 ve 4 olarak seçildiğinde, sırasıyla,

$y^2 = x^3 + 2x + 2$	$y^2 = x^3 + 2x + 3$	$y^2 = x^3 + 3x + 4$
$y^2 = x^3 + 2x + 3$	$y^2 = x^3 + 3x + 1$	$y^2 = x^3 + 2x + 2$
$y^2 = x^3 + 3x + 4$	$y^2 = x^3 + 2x + 2$	$y^2 = x^3$
$y^2 = x^3 + 3x + 4$	$y^2 = x^3 + 2x + 2$	$y^2 = x^3$
$y^2 = x^3 + 2x + 3$	$y^2 = x^3 + 3x + 1$	$y^2 = x^3 + 2x + 2$

olarak bulunur.

Rankı Üç Olan Dizilerle Eşleşen Eğriler

Bu kısımda rankı üç olan diziler, yani h_3 teriminin sıfır olan dizilerle eşleşen eğriler ele alınacaktır. Rankı üç olan tüm diziler singüler olduğundan bu dizilerle eşleşen tüm eğriler de singülerdir.

5.4.6 Teorem. [1 h_2 0 ch_2] (h_2, $c \in \mathbb{F}_p^*$) bir eliptik bölünebilir dizi olsun. Bu durumda bu dizilerle eşleşen eğriler birer singüler eğridir ve

$$E : y^2 = x^3 - 27(h_2^4 + c)^4 x + 54(h_2^4 + c)^6 \qquad (5.11)$$

denklemi ile belirtilir. Üstelik $P = (x_1, y_1)$, E eğrisi üzerinde bir nokta olmak üzere bu dizi

$$P = (x_1, y_1) = (3(h_2^4 + c)^2, 0)\ (c \in \mathbb{F}_p^*)$$

noktasında elde edilen bir dizidir.

İspat. [1 h_2 h_3 ch_2] eliptik bölünebilir dizisi ile eşleşen $E : y^2 = x^3 + ax + b$ eliptik eğrisi için

$$\Delta = 2^8 \cdot 3^{12} h_3^9 h_2^8 (ch_2^{12} + (-h_3^3 + 3c^2)h_2^8 + (-20ch_3^3 + 3c^3)h_2^4 + (16h_3^6 + 8c^2h_3^3 + c^4))$$

$$a = 3^3(-h_2^{16} - 4ch_2^{12} + (16h_3^3 - 6c^2)h_2^8 + (8ch_3^3 - 4c^3)h_2^4 - (16h_3^6 + 8c^2h_3^3 + c^4))$$

$$b = 2 \cdot 3^3(h_2^{24} + 6ch_2^{20} - (24h_3^3 - 15c^2)h_2^{16} - (60ch_3^3 - 20c^3)h_2^{12} + (120h_3^6 - 36c^2h_3^3 + 15c^4)h_2^8$$
$$+ (-48ch_3^6 + 12c^3h_3^3 + 6c^5)h_2^4 + (64h_3^9 + 48c^2h_3^6 + 12c^4h_3^3 + c^6))$$

$$P = (x_1, y_1) = (3 \cdot (h_2^8 + 2ch_2^4 + 4h_3^3 + c^2), -108\, h_3^3 h_2^4)$$

olduğundan birinci eşitlikte $h_3 = 0$ olarak alınırsa $\Delta = 0$ olarak bulunur, bu ise rankı üç olan dizilerle eşleşen tüm eğrilerin bir singüler eğri olduğunu gösterir. Eğer ikinci ve üçüncü eşitliklerde $h_3 = 0$ olarak alınırsa,

$$a = -3^3(h_2^{16} + 4ch_2^{12} + 6c^2h_2^8 + 4c^3h_2^4 + c^4) = -27(h_2^4 + c)^4$$

ve

$$b = 54(h_2^{24} + 6ch_2^{20} + 15c^2h_2^{16} + 20c^3h_2^{12} + 15c^4h_2^8 + 6c^5h_2^4 + c^6) = 54(h_2^4 + c)^6$$

olarak bulunur. O halde bu EBD lerle eşleşen singüler eğriler

$$E : y^2 = x^3 - 27\ (h_2^4 + c)^4\, x + 54(h_2^4 + c)^6$$

biçimindedirler. Üstelik $P = (x_1, y_1)$ E eğrisi üzerinde bir nokta olmak üzere

$$P = (x_1, y_1) = (3(h_2^8 + 2ch_2^4 + 4h_3^3 + c^2), -108\, h_3^3 h_2^4)$$

olduğundan $h_3 = 0$ için [1 h_2 0 ch_2] dizisi

$$P = (x_1, y_1) = (3(h_2^8 + 2ch_2^4 + c^2), 0) = (3(h_2^4 + c)^2, 0),\ (c \in \mathbb{F}_p^*)$$

noktasından elde edilir.

5.4.7 Sonuç. $P = (x_1, y_1) = (3(h_2^4 + c)^2, 0),\ (c \in \mathbb{F}_p^*)$ noktası için

$$\text{“}x_1 \in \boldsymbol{Q}_p \Leftrightarrow p \equiv \pm 1\ (12)\text{”}$$

ve

$$\text{“}x_1 \notin \boldsymbol{Q}_p \Leftrightarrow p \not\equiv \pm 1\ (12)\text{”}$$

dolayısıyla P noktası için her iki halde de $\frac{p-1}{2}$ tane alternatif söz konusudur.

İspat. "$(h_2^4+c)^2 \in Q_p$ ve $3 \in Q_p \Leftrightarrow p \equiv \pm 1\ (12)$" olduğundan

$$3(h_2^4+c)^2 = x_1 \in Q_p \Leftrightarrow p \equiv \pm 1\ (12) \in Q_p$$

olduğu görülür. $|Q_p| = \frac{p-1}{2}$ olduğundan da her iki halde x_1 için $\frac{p-1}{2}$ tane alternatif söz konusudur.

5.4.8 Uyarı. Teorem 5.4.6 da $[1\ h_2\ 0\ ch_2]$ $(c \in \mathbb{F}_p^*)$ dizisinin

$$E : y^2 = x^3 - 27(h_2^4+c)^4 x + 54(h_2^4+c)^6$$

eğrisi ile eşleştiği gösterilmiştir. Buna göre eğer $\alpha = h_2^4 + c$ ve $\beta = 3\alpha^2$ olarak alınırsa

$$a = -3\beta^2,\ b = 2\beta^3$$

olacağından

$$E : y^2 = x^3 - 3\beta^2 x + 2\beta^3$$

ve

$$P = (\beta, 0)$$

olur.

5.4.9 Örnek. $\mathbb{F}_5$ de bu özellikteki diziler ve bunların eşleştikleri eğriler ile bu eğrilerin elde edildikleri P noktaları aşağıda verilmiştir.

[1 1 0 1]	$y^2 = x^3 + 3x + 1$,	$P = (2, 0)$
[1 1 0 2]	$y^2 = x^3 + 3x + 1$,	$P = (2, 0)$
[1 1 0 3]	$y^2 = x^3 + 3x + 4$,	$P = (3, 0)$
[1 1 0 4]	$y^2 = x^3$,	$P = (0, 0)$
[1 2 0 1]	$y^2 = x^3 + 3x + 4$,	$P = (3, 0)$
[1 2 0 2]	$y^2 = x^3 + 3x + 1$,	$P = (2, 0)$
[1 2 0 3]	$y^2 = x^3$,	$P = (0, 0)$
[1 2 0 4]	$y^2 = x^3 + 3x + 1$,	$P = (2, 0)$
[1 3 0 1]	$y^2 = x^3 + 3x + 1$,	$P = (2, 0)$
[1 3 0 2]	$y^2 = x^3$,	$P = (0, 0)$

[1 3 0 3]	$y^2 = x^3 + 3x + 1,$	$P = (2, 0)$
[1 3 0 4]	$y^2 = x^3 + 3x + 4,$	$P = (3, 0)$
[1 4 0 1]	$y^2 = x^3,$	$P = (0, 0)$
[1 4 0 2]	$y^2 = x^3 + 3x + 4,$	$P = (3, 0)$
[1 4 0 3]	$y^2 = x^3 + 3x + 1,$	$P = (2, 0)$
[1 4 0 4]	$y^2 = x^3 + 3x + 1,$	$P = (2, 0)$

Şimdi bu eğrilerin hangi durumlarda bir çıkıntıya sahip olduğu belirlenecektir.

5.4.10 Teorem. [1 h_2 0 ch_2] ($h_2 \in \mathbb{F}_p^*$ ve $c \in \mathbb{F}_p^*$) bir eliptik bölünebilir dizi olsun. Bu durumda, (h_n) dizisinin $E : y^2 = x^3$ singüler eğrisi ile eşlemesi için gerek ve yeter şart $h_4 = -h_2^5$ olmasıdır.

İspat. Yukarıdaki (5.11) eşitliğinde $h_2^4 = -c$ yazılırsa teoremin ispatı tamamlanır.

Rankı Dört Olan Dizilerle Eşleşen Eğriler

Şimdi de rankı dört olan diziler, yani h_4 teriminin sıfır olan dizilerle eşleşen eliptik ve singüler eğriler ele belirlenecektir. Aşağıdaki teoremde bu dizilerle eşleşen eliptik eğriler belirlenmiştir.

5.4.11 Teorem. [1 h_2 h_3 0] (h_2, $h_3 \in \mathbb{F}_p^*$) bir eliptik bölünebilir dizi olsun. Bu durumda bu dizilerle eşleşen eliptik eğriler

$$E : y^2 = x^3 + 27(-h_2^{16} + 16ch_3^3h_2^8 - 16h_3^6)x + 54(h_2^{24} - 24h_3^3h_2^{16} + 120h_3^6h_2^8 + 64h_3^9)$$

biçimindedir. Üstelik bu dizi E eğrisi üzerindeki

$$P = (x_1, y_1) = (3(h_2^8 + 4h_3^3), -108\, h_3^3h_2^4)$$

noktasından elde edilen bir dizidir.

İspat. $a = 3^3(-h_2^{16} - 4ch_2^{12} + (16h_3^3 - 6c^2)h_2^8 + (8ch_3^3 - 4c^3)h_2^4 - (16h_3^6 + 8c^2h_3^3 + c^4))$

$$b = 2 \cdot 3^3(h_2^{24} + 6ch_2^{20} - (24h_3^3 - 15c^2)h_2^{16} - (60ch_3^3 - 20c^3)h_2^{12} + (120h_3^6 - 36c^2h_3^3 + 15c^4)h_2^8$$

$$+(-48ch_3^6+12c^3h_3^3+6c^5)h_2^4+(64h_3^9+48c^2h_3^6+12c^4h_3^3+c^6))$$

$$P=(x_1,\,y_1)=(3\cdot(h_2^8+2ch_2^4+4h_3^3+c^2)\,,\,-108\,h_3^3h_2^4)$$

eşitliklerinde $c=0$ olarak ($h_4=0$ ve $h_2h_3\neq 0$ olduğundan $c=0$ olmalıdır) alınırsa

$$a=27\,(-h_2^{16}+16h_3^3h_2^8-16h_3^6) \tag{5.12}$$

$$b=54\,(h_2^{24}-24h_3^3h_2^{16}+120h_3^6h_2^8+64h_3^9) \tag{5.13}$$

$$P=(x_1,\,y_1)=(3\,(h_2^8+4h_3^3),\,-108\,h_3^3h_2^4) \tag{5.14}$$

olarak bulunur.

Aşağıdaki teoremde bu dizilerle eşleşen singüler eğriler belirlenmiştir.

5.4.12 Teorem. [1 h_2 h_3 0] ($h_2,\,h_3\in\mathbb{F}_p^*$) bir eliptik bölünebilir dizi ise bu dizilerle eşleşen singüler eğriler

$$E:y^2=x^3-\frac{27}{16}\,h_2^{16}x\;-\frac{54}{64}\,h_2^{24}$$

biçimindedir. Üstelik bu dizi E eğrisi üzerindeki

$$P=(x_1,\,y_1)=\left(\frac{15h_2^8}{4},-\frac{27h_2^{12}}{4}\right)$$

noktasından elde edilen bir dizidir.

İspat. Rankı dört olan bir eliptik bölünebilir dizi ile eşleşen eğrinin diskriminantı

$$\Delta=\;2^8\,3^{12}\,h_3^9h_2^8\;(-h_3^3h_2^8+16h_3^6)$$

dır. Eğer E bir singüler eğri ise $\Delta=0$ ve $h_2h_3\neq 0$ olduğundan $-h_3^3h_2^8+16h_3^6=0$ olmalıdır. $h_3\neq 0$ olduğundan $h_3^3=\frac{h_2^8}{16}$ olarak bulunur. (5.12), (5.13) ve (5.14) eşitliklerinde $h_3^3=\frac{h_2^8}{16}$ yazılırsa

$$a=-\frac{27h_2^{16}}{16}$$

$$b=\;54\left(h_2^{24}-\frac{3h_2^{24}}{2}+\frac{15h_2^{24}}{32}+\frac{1h_2^{24}}{64}\right)=-\frac{54h_2^{24}}{64}$$

ve

$$P=(x_1,\,y_1)=(3\,(h_2^8+4h_3^3),\,-108\,h_3^3h_2^4)=\left(3\left(h_2^8+4\frac{h_2^8}{16}\right),-108\frac{h_2^8}{16}h_2^4\right)=\left(\frac{15h_2^8}{4},-\frac{27h_2^{12}}{4}\right)$$

olarak bulunur.

5.4.13 Uyarı 1. Teorem 5.4.12 gereği $[1\ h_2\ h_3\ 0]$ dizisi

$$E : y^2 = x^3 - \frac{27}{16} h_2^{16} x - \frac{54}{64} h_2^{24}$$

eğrisi ile eşleşir. Buna göre $\alpha = \frac{3}{4} h_2^8$ ve $\beta = 3\alpha^2$ olarak alınırsa

$$a = -\beta,\ b = -2\beta^3$$

olacağından

$$E: y^2 = x^3 + \beta x + 2\beta^3$$

olur.

2. Bu haldeki tüm singüler eğrilerin bir düğümü vardır. Gerçektende, sadece $h_2 = 0$ için $E : y^2 = x^3$ singüler eğrisi elde edilir. Bu halde $h_2 \neq 0$ olduğundan bu dizlere karşılık gelen singüler eliptik eğrilerin çıkıntıları olamaz, singüler noktalar düğümlerdir.

5.4.14 Örnek. $\mathbb{F}_5$ de bu özellikteki diziler ve bunların eşleştikleri eğriler ve elde edildikleri P noktaları aşağıda verilmiştir.

[1 1 1 0]	$y^2 = x^3 + 3x + 4,$	$P = (0, 2)$
[1 1 2 0]	$y^2 = x^3 + x + 3,$	$P = (0, 2)$
[1 1 3 0]	$y^2 = x^3 + 4x,$	$P = (0, 2)$
[1 1 4 0]	$y^2 = x^3 + 4x + 4,$	$P = (0, 2)$
[1 2 1 0]	$y^2 = x^3 + 3x + 4,$	$P = (0, 2)$
[1 2 2 0]	$y^2 = x^3 + x + 3,$	$P = (0, 2)$
[1 2 3 0]	$y^2 = x^3 + 4x,$	$P = (0, 2)$
[1 2 4 0]	$y^2 = x^3 + 4x + 4,$	$P = (0, 2)$
[1 3 1 0]	$y^2 = x^3 + 3x + 4,$	$P = (0, 2)$
[1 3 2 0]	$y^2 = x^3 + x + 3,$	$P = (0, 2)$
[1 3 3 0]	$y^2 = x^3 + 4x,$	$P = (0, 2)$
[1 3 4 0]	$y^2 = x^3 + 4x + 4,$	$P = (0, 2)$
[1 4 1 0]	$y^2 = x^3 + 3x + 4,$	$P = (0, 2)$

[1 4 2 0] $y^2 = x^3 + x + 3$, $P = (0, 2)$

[1 4 3 0] $y^2 = x^3 + 4x$, $P = (0, 2)$

[1 4 4 0] $y^2 = x^3 + 4x + 4$, $P = (0, 2)$

Rankı Beş Olan Dizilerle Eşleşen Eğriler

Bu kısımda rankı beş olan diziler, yani h_5 teriminin sıfır olan dizilerle eşleşen eliptik ve singüler eğriler ele alınacaktır. Aşağıdaki teoremde bu dizilerle eşleşen eliptik eğriler belirlenmiştir.

5.4.15 Teorem. [1 h_2 h_3 ch_2] (h_2, h_3, $h_4 = ch_2 \in \mathbb{F}_p^*$) ve rankı beş olan bir eliptik bölünebilir dizi olsun. Bu durumda bu dizilerle eşleşen eliptik eğriler

$$E : y^2 = x^3 + 27(-h_2^{16} + 12ch_2^{12} - 14h_2^4c^3 - c^4)x + 54(h_2^{24} - 18h_2^{20}c + 75h_2^{16}c^2 + 75h_2^8c^4 + 18h_2^4c^5 + c^6) \qquad (5.15)$$

biçimindedir. Üstelik bu dizi E eğrisi üzerindeki

$$P = (x_1, y_1) = (3(h_2^8 + 4h_3^3), -108h_3^3h_2^4)$$

noktasından elde edilen bir dizidir.

İspat. Dizinin beşinci terimi, yani $h_5 = 0$ olduğundan $h_3^3 = h_2^4c$ dir. (4.5), (4.6) ve (4.7) eşitliklerinde $h_3^3 = h_2^4c$ yazılırsa istenilen elde edilir.

5.4.16 Örnek. $\mathbb{F}_7$ de rankı 5 olan diziler ve bunların eşleştikleri eğriler aşağıda verilmiştir.

[1 1 1 1] $y^2 = x^3 + 2x + 4$,

[1 1 2 1] $y^2 = x^3 + 2x + 4$,

[1 1 3 6] $y^2 = x^3 + 2x + 4$,

[1 1 4 1] $y^2 = x^3 + 2x + 4$,

[1 1 5 6] $y^2 = x^3 + 2x + 4$,

[1 1 6 6] $y^2 = x^3 + 2x + 4$,

[1 2 1 1] $y^2 = x^3 + 3x + 4$,

[1 2 2 1] $y^2 = x^3 + 3x + 4,$

[1 2 3 6] $y^2 = x^3 + 2x + 1,$

[1 2 4 1] $y^2 = x^3 + 3x + 4,$

[1 2 5 6] $y^2 = x^3 + 2x + 1,$

[1 2 6 6] $y^2 = x^3 + 2x + 1,$

[1 3 1 6] $y^2 = x^3 + 2x + 1,$

[1 3 2 6] $y^2 = x^3 + 2x + 1,$

[1 3 3 1] $y^2 = x^3 + 3x + 4,$

[1 3 4 6] $y^2 = x^3 + 2x + 1,$

[1 3 5 1] $y^2 = x^3 + 3x + 4,$

[1 3 6 1] $y^2 = x^3 + 3x + 4,$

[1 4 1 1] $y^2 = x^3 + 2x + 1,$

[1 4 2 1] $y^2 = x^3 + 2x + 1,$

[1 4 3 6] $y^2 = x^3 + 3x + 4,$

[1 4 4 1] $y^2 = x^3 + 2x + 1,$

[1 4 5 6] $y^2 = x^3 + 3x + 4,$

[1 4 6 6] $y^2 = x^3 + 3x + 4,$

[1 5 1 6] $y^2 = x^3 + 3x + 4,$

[1 5 2 6] $y^2 = x^3 + 3x + 4,$

[1 5 3 1] $y^2 = x^3 + 2x + 1,$

[1 5 4 6] $y^2 = x^3 + 3x + 4,$

[1 5 5 1] $y^2 = x^3 + 2x + 1,$

[1 5 6 1] $y^2 = x^3 + 2x + 1,$

[1 6 1 6] $y^2 = x^3 + 2x + 4,$

[1 6 2 6] $y^2 = x^3 + 2x + 4,$

[1 6 3 1] $y^2 = x^3 + 2x + 4,$

[1 6 4 6] $y^2 = x^3 + 2x + 4,$

[1 6 5 1] $y^2 = x^3 + 2x + 4,$

[1 6 6 1] $y^2 = x^3 + 2x + 4,$

$\mathbb{F}_{17}$ de rankı 5 olan bazı diziler ve bunların eşleştikleri eğriler aşağıda verilmiştir.

[1 1 1 1]	$y^2 = x^3 + 10x + 14$,
[1 2 2 1]	$y^2 = x^3 + 5x + 15$,
[1 3 3 1]	$y^2 = x^3 + 13x + 1$,
[1 4 4 1]	$y^2 = x^3 + 10x$,
[1 5 5 1]	$y^2 = x^3 + 16x + 3$,
[1 6 6 1]	$y^2 = x^3 + 14x + 16$,
[1 7 7 1]	$y^2 = x^3 + x + 6$,
[1 8 8 1]	$y^2 = x^3 + 12x + 8$,
[1 9 9 1]	$y^2 = x^3 + 7x + 15$,
[1 10 10 1]	$y^2 = x^3 + 4x + 11$,
[1 11 11 1]	$y^2 = x^3 + 16x + 2$,
[1 12 12 1]	$y^2 = x^3 + 4x + 14$,
[1 13 13 1]	$y^2 = x^3 + 9x$,
[1 14 14 1]	$y^2 = x^3 + 5x + 8$,
[1 15 15 1]	$y^2 = x^3 + 10x + 9$,
[1 16 16 1]	$y^2 = x^3 + 10x + 14$,

Aşağıdaki teorem singüler eğrilerin ne zaman ortaya çıktığını göstermektedir.

5.4.17 Teorem. [1 h_2 h_3 h_4] (h_2, h_3, $h_4 = ch_2 \in \mathbb{F}_p^*$, $p > 5$) rankı beş olan bir singüler eliptik bölünebilir dizi olsun. Bu durumda (h_n) dizisinin bir singüler E eğrisi ile eşleşmesi için gerek ve yeter şart $p \equiv 1, 9\ (10)$ olmasıdır.

İspat. (h_n) rankı beş olan bir dizi olduğundan $h_4 = ch_2 = \left(\frac{h_3}{h_2}\right)^3$ dir. Bu değer

$$\Delta = h_4h_2^{15} - h_3^3h_2^{12} + 3h_4^2h_2^{10} - 20h_4h_3^3h_2^7 + 3h_4^3h_2^5 + 16h_3^6h_2^4 + 8h_4^2h_3^3h_2^2 + h_4^4$$

eşitliğinde yazılırsa

$$\Delta = -h_2^{16} + 11h_2^{12}c + h_2^8c^2 = 0$$

ve dolayısıyla $\Delta = 0 \Leftrightarrow h_2^4 = \frac{11 \pm 5\sqrt{5}}{2} c$ dır. O halde, "(h_n) nin bir singüler dizisi bir singüler E eğrisi ile eşleşir $\Leftrightarrow$ 5 bir ikinci dereceden kalandır veya $p = 5$ dir" ve dolayısıyla "5 bir ikinci dereceden kalandır $\Leftrightarrow p \equiv 1, 9\ (10)$" dur.

Aşağıdaki teoremde rankı 5 olan singüler EBD ler ile eşleşen singüler eğriler belirlenmiştir.

5.4.18 Teorem. [1 h_2 h_3 ch_2] (h_2, h_3, $h_4 = ch_2 \in \mathbb{F}_p^*$, $p > 5$) rankı beş olan bir eliptik bölünebilir dizi ve $h_2^4 = \frac{11 \pm 5\sqrt{5}}{2} c$ olsun. Bu durumda bu dizilerle eşleşen singüler eğriler

$$E : y^2 = x^3 - \left(\frac{16605 \pm 7425\sqrt{5}}{2} \right) c^4 x - (411750 \pm 184140\sqrt{5})c^6 \qquad (5.16)$$

biçimindedir. Üstelik bu dizi E eğrisi üzerindeki

$$P = (x_1, y_1) = \left(\left(\frac{573 \pm 255\sqrt{5}}{2} \right) c^2, (-6642 \pm 2970\sqrt{5})c^3 \right)$$

noktasından elde edilen bir dizidir.

İspat. (5.15) eşitliğinde $h_2^4 = \frac{11 \pm 5\sqrt{5}}{2} c$ olarak alınırsa istenilen görülür.

Aşağıdaki teorem rankı beş olan tüm dizilerin $p = 5$ olması halinde $y^2 = x^3$ eğrisi ile eşleştiğini göstermektedir.

5.4.19 Teorem. [1 h_2 h_3 ch_2] (h_2, h_3, $h_4 = ch_2 \in \mathbb{F}_5^*$) rankı beş olan $\mathbb{F}_5$ üzerinde tanımlı bir singüler eliptik bölünebilir dizi ise bu diziler $y^2 = x^3$ singüler eğrisi ile eşleşirler.

İspat. (5.16) eşitliği $\mathbb{F}_5$ üzerinde düşünülürse de bu dizilerin $y^2 = x^3$ singüler eğrisi ile eşleştiği görülür.

5.4.20 Örnek. $\mathbb{F}_{11}$ de rankı 5 olan ve singüler eğriler ile eşleşen diziler ve bunların eşleştikleri eğriler aşağıda verilmiştir.

[1 1 1 1]	$y^2 = x^3 + 8x + 2$,
[1 1 10 10]	$y^2 = x^3 + 8x + 2$,
[1 2 2 1]	$y^2 = x^3 + 6x + 10$,
[1 2 9 10]	$y^2 = x^3 + 6x + 10$,
[1 3 3 1]	$y^2 = x^3 + 2x + 8$,
[1 3 8 10]	$y^2 = x^3 + 2x + 8$,
[1 4 4 1]	$y^2 = x^3 + 10x + 6$,
[1 4 7 10]	$y^2 = x^3 + 10x + 6$,
[1 5 5 1]	$y^2 = x^3 + 7x + 7$,
[1 5 6 10]	$y^2 = x^3 + 7x + 7$,
[1 6 6 1]	$y^2 = x^3 + 7x + 7$,
[1 5 5 10]	$y^2 = x^3 + 7x + 7$,
[1 7 7 1]	$y^2 = x^3 + 10x + 6$,
[1 7 4 10]	$y^2 = x^3 + 10x + 6$,
[1 8 8 1]	$y^2 = x^3 + 2x + 8$,
[1 8 3 10]	$y^2 = x^3 + 2x + 8$,
[1 9 9 1]	$y^2 = x^3 + 6x + 10$,
[1 9 2 10]	$y^2 = x^3 + 6x + 10$,
[1 10 10 1]	$y^2 = x^3 + 8x + 2$,
[1 10 1 10]	$y^2 = x^3 + 8x + 2$,

$\mathbb{F}_{31}$ de rankı 5 olan ve singüler eğriler ile eşleşen diziler ve bunların eşleştikleri eğriler aşağıda verilmiştir.

[1 3 16 30]	$y^2 = x^3 + 10x + 15$,
[1 3 18 30]	$y^2 = x^3 + 10x + 15$,
[1 3 28 30]	$y^2 = x^3 + 10x + 15$,
[1 5 6 30]	$y^2 = x^3 + 20x + 23$,

[1 5 26 30] $y^2 = x^3 + 20x + 23$,

[1 5 30 30] $y^2 = x^3 + 20x + 23$,

[1 6 1 30] $y^2 = x^3 + 20x + 23$,

[1 6 5 30] $y^2 = x^3 + 20x + 23$,

[1 6 25 30] $y^2 = x^3 + 20x + 23$,

[1 7 7 1] $y^2 = x^3 + 18x + 29$,

[1 7 4 1] $y^2 = x^3 + 18x + 29$,

[1 7 20 1] $y^2 = x^3 + 18x + 29$,

[1 9 17 30] $y^2 = x^3 + 5x + 30$,

[1 9 22 30] $y^2 = x^3 + 5x + 30$,

[1 9 23 30] $y^2 = x^3 + 5x + 30$,

[1 10 12 30] $y^2 = x^3 + 9x + 27$,

[1 10 21 30] $y^2 = x^3 + 9x + 27$,

[1 10 29 30] $y^2 = x^3 + 9x + 27$,

[1 11 11 1] $y^2 = x^3 + 18x + 29$,

[1 11 24 1] $y^2 = x^3 + 18x + 29$,

[1 11 27 1] $y^2 = x^3 + 18x + 29$,

[1 12 2 30] $y^2 = x^3 + 9x + 27$,

[1 12 10 30] $y^2 = x^3 + 9x + 27$,

[1 12 19 30] $y^2 = x^3 + 9x + 27$,

[1 13 13 1] $y^2 = x^3 + 10x + 15$,

[1 13 3 1] $y^2 = x^3 + 10x + 15$,

[1 13 15 1] $y^2 = x^3 + 10x + 15$,

[1 14 14 1] $y^2 = x^3 + 5x + 30$,

[1 14 8 1] $y^2 = x^3 + 5x + 30$,

[1 14 9 1] $y^2 = x^3 + 5x + 30$,

[1 17 8 30] $y^2 = x^3 + 5x + 30$,

[1 17 9 30] $y^2 = x^3 + 5x + 30$,

[1 17 14 30] $y^2 = x^3 + 5x + 30$,

[1 18 3 30] $y^2 = x^3 + 10x + 15$,

[1 18 13 30] $y^2 = x^3 + 10x + 15$,

[1 18 15 30] $y^2 = x^3 + 10x + 15$,

[1 19 19 1] $y^2 = x^3 + 9x + 27$,

[1 19 2 1] $y^2 = x^3 + 9x + 27$,

[1 19 10 1] $y^2 = x^3 + 9x + 27$,

[1 20 11 30] $y^2 = x^3 + 18x + 29$,

[1 20 24 30] $y^2 = x^3 + 18x + 29$,

[1 20 27 30] $y^2 = x^3 + 18x + 29$,

[1 21 21 1] $y^2 = x^3 + 9x + 27$,

[1 21 12 1] $y^2 = x^3 + 9x + 27$,

[1 21 29 1] $y^2 = x^3 + 9x + 27$,

[1 22 22 1] $y^2 = x^3 + 5x + 30$,

[1 22 17 1] $y^2 = x^3 + 5x + 30$,

[1 22 23 1] $y^2 = x^3 + 5x + 30$,

[1 24 4 30] $y^2 = x^3 + 18x + 29$,

[1 24 7 30] $y^2 = x^3 + 18x + 29$,

[1 24 20 30] $y^2 = x^3 + 18x + 29$,

[1 25 25 1] $y^2 = x^3 + 20x + 23$,

[1 25 1 1] $y^2 = x^3 + 20x + 23$,

[1 25 5 1] $y^2 = x^3 + 20x + 23$,

[1 26 26 1] $y^2 = x^3 + 20x + 23$,

[1 26 6 1] $y^2 = x^3 + 20x + 23$,

[1 26 30 1] $y^2 = x^3 + 20x + 23$,

[1 28 28 1] $y^2 = x^3 + 10x + 5$,

[1 28 16 1] $y^2 = x^3 + 10x + 5$,

[1 28 18 1] $y^2 = x^3 + 10x + 5$,

Rankı Altı Olan Dizilerle Eşleşen Eğriler

Bu kısımda rankı altı olan diziler, yani altıncı terimi sıfır olan dizilerle eşleşen eliptik ve singüler eğriler belirlenecektir. Aşağıdaki teoremde bu dizilerle eşleşen eliptik eğriler belirlenmiştir.

5.4.21 Teorem. [1 h_2 h_3 ch_2] (h_2, h_3, $ch_2 = h_4 \in \mathbb{F}_p^*$) rankı altı olan bir EBD ise bu dizilerle eşleşen eliptik eğriler

$$E : y^2 = x^3 + 27(-h_2^{16} + 12ch_2^{12} - 30h_2^8c^2 + 12h_2^4c^3 - 9c^4)x + 54(h_2^{24} - 18h_2^{20}c + 99h_2^{16}c^2 - 180h_2^{12}c^3 + 135h_2^8c^4 + 54h_2^4c^5 - 27c^6) \quad (5.17)$$

biçimindedir. Üstelik bu dizi E eğrisi üzerindeki

$$P = (x_1, y_1) = (3(h_2^8 + 6ch_2^4 - 3c^2), -108ch_2^8 - c^2h_2^4)$$

noktasından elde edilen bir dizidir.

İspat. Dizinin altıncı terimi $h_6 = 0$ olduğundan $h_3^3 = ch_2^4 - c^2$ dir. (4.5), (4.6) ve (4.7) eşitliklerinde $h_3^3 = ch_2^4 - c^2$ yazılırsa istenilen elde edilir.

Aşağıdaki teorem singüler eğrilerin ne zaman ortaya çıktığını göstermektedir.

5.4.22 Teorem. [1 h_2 h_3 ch_2] (h_2, h_3, $h_4 \in \mathbb{F}_p^*$) rankı altı olan bir eliptik bölünebilir dizi olsun. Bu durumda (h_n) dizisinin bir singüler eğri ile eşleşebilmesi için gerek ve yeter şart $h_2^4 = 9c$ olmasıdır.

İspat. (h_n) rankı altı olan bir dizi olduğundan $h_5 = \left(\frac{h_4}{h_2}\right)^2$ ve dolayısıyla $h_3^3 = ch_2^4 - c^2$ dir.

Üstelik (h_n) dizisi bir singüler dizi ise bu dizinin eşleştiği eğri de singüler bir eğridir. O halde

$$\Delta(h_2, h_3, h_4) = h_2^{16}c - h_3^3h_2^{12} + 3h_2^{12}c^2 - 20h_2^8c^3 + 16h_3^6h_2^4 + 8h_2^4c^2h_3 + h_2^4c^4 = 0$$

dır. Bu eşitlikte $h_3^3 = ch_2^4 - c^2$ yazılırsa

$$\Delta(h_2, h_3, h_4) = 0 \Leftrightarrow 9c = h_2^4$$

olarak bulunur.

5.4.23 Örnek. $\mathbb{F}_7$ de rankı 6 olan diziler ve bunların eşleştikleri eğriler aşağıda verilmiştir.

[1 1 1 3]	$y^2 = x^3 + 3x + 3$,
[1 1 1 5]	$y^2 = x^3 + 1$,
[1 1 2 3]	$y^2 = x^3 + 3x + 3$,
[1 1 2 5]	$y^2 = x^3 + 1$,
[1 1 4 3]	$y^2 = x^3 + 3x + 3$,
[1 1 4 5]	$y^2 = x^3 + 1$,
[1 2 1 2]	$y^2 = x^3 + 4x + 5$,
[1 2 2 2]	$y^2 = x^3 + 4x + 5$,
[1 2 3 1]	$y^2 = x^3 + 3x + 1$,
[1 2 3 3]	$y^2 = x^3 + 2x + 3$,
[1 2 4 2]	$y^2 = x^3 + 4x + 5$,
[1 2 5 1]	$y^2 = x^3 + 3x + 1$,
[1 2 5 3]	$y^2 = x^3 + 2x + 3$,
[1 2 6 1]	$y^2 = x^3 + 3x + 1$,
[1 2 6 3]	$y^2 = x^3 + 2x + 3$,
[1 5 1 5]	$y^2 = x^3 + 4x + 5$,
[1 5 2 5]	$y^2 = x^3 + 4x + 5$,
[1 5 3 4]	$y^2 = x^3 + 2x + 3$,
[1 5 3 6]	$y^2 = x^3 + 3x + 1$,
[1 5 4 5]	$y^2 = x^3 + 4x + 5$,
[1 5 5 4]	$y^2 = x^3 + 2x + 3$,
[1 5 5 6]	$y^2 = x^3 + 3x + 1$,
[1 5 6 4]	$y^2 = x^3 + 2x + 3$,
[1 5 6 6]	$y^2 = x^3 + 3x + 1$,
[1 6 1 2]	$y^2 = x^3 + 1$,
[1 6 1 4]	$y^2 = x^3 + 3x + 3$,

[1 6 2 2] $y^2 = x^3 + 1$,

[1 6 2 4] $y^2 = x^3 + 3x + 3$,

[1 6 4 2] $y^2 = x^3 + 1$,

[1 6 4 4] $y^2 = x^3 + 3x + 3$,

Aşağıdaki teoremde rankı altı olan dizilerle eşleşen singüler eğriler belirlenmiştir.

5.4.24 Teorem. [1 h_2 h_3 ch_2] (h_2, h_3, $ch_2 = h_4 \in \mathbb{F}_p^*$) rankı altı ve $h_2^4 = 9c$ olan bir EBD ise bu dizilerle eşleşen eliptik eğriler

$$E : y^2 = x^3 - 3888c^4 x - 93312c^6 \tag{5.18}$$

biçimindedir. Üstelik bu dizi E eğrisi üzerindeki

$$P = (x_1, y_1) = (396c^2, -7776c^3)$$

noktasından elde edilen bir dizidir.

İspat. (5.17) eşitliğinde $h_2^4 = 9c$ yazılırsa istenilen elde edilir.

5.4.25 Örnek. $\mathbb{F}_{11}$ de rankı 6 olan ve singüler eğriler ile eşleşen diziler ve bunların eşleştikleri eğriler aşağıda verilmiştir.

[1 1 7 5] $y^2 = x^3 + 10x + 5$,
[1 2 8 6] $y^2 = x^3 + 2x + 3$,
[1 3 10 5] $y^2 = x^3 + 8x + 9$,
[1 4 6 5] $y^2 = x^3 + 7x + 4$,
[1 5 2 5] $y^2 = x^3 + 6x + 1$,
[1 6 2 6] $y^2 = x^3 + 6x + 1$,
[1 7 6 6] $y^2 = x^3 + 7x + 4$,
[1 8 10 6] $y^2 = x^3 + 8x + 9$,
[1 9 8 5] $y^2 = x^3 + 2x + 3$,
[1 10 7 6] $y^2 = x^3 + 10x + 5$,

Rankı Yedi Olan Dizilerle Eşleşen Eğriler

Bu kısımda rankı yedi olan diziler, yani yedinci terimi sıfır olan dizilerle eşleşen eliptik ve singüler eğriler belirlenecektir. Aşağıdaki teoremde bu dizilerle eşleşen eliptik eğriler belirlenmiştir.

5.4.26 Teorem. [1 h_2 h_3 ch_2] (h_2, h_3, $ch_2 = h_4 \in \mathbb{F}_p^*$) rankı yedi olan bir EBD ise bu dizilerle eşleşen eliptik eğriler

$$E : y^2 = x^3 - 3483 \cdot 2^{16t} x + 121014 \cdot 2^{24t} \tag{5.19}$$

biçimindedir. Üstelik bu diziler E eğrisi üzerindeki

$$P = (x_1, y_1) = (27 \cdot 2^{8t}, -216 \cdot 2^{12t})$$

noktasından elde edilen bir dizidir.

İspat. Rankı yedi olan bir dizinin başlangıç terimleri

$$[1\ 2^t\ 2^{\frac{8t+1}{3}}\ -2^{5t+1}] \text{ veya } [1\ -2^t\ 2^{\frac{8t+1}{3}}\ 2^{5t+1}]$$

olduğundan eşitliklerinde bu değerler yazılırsa istenilen elde edilir.

5.4.27 Örnek. $\mathbb{F}_7$ de rankı 7 olan diziler ve bunların eşleştikleri eğriler aşağıda verilmiştir.

[1 1 1 2]	$y^2 = x^3 + 6x + 5$,
[1 1 2 2]	$y^2 = x^3 + 6x + 5$,
[1 1 4 2]	$y^2 = x^3 + 6x + 5$,
[1 2 1 6]	$y^2 = x^3 + 6x + 5$,
[1 2 2 6]	$y^2 = x^3 + 6x + 5$,
[1 2 3 4]	$y^2 = x^3$,
[1 2 4 6]	$y^2 = x^3 + 6x + 5$,
[1 2 5 4]	$y^2 = x^3$,
[1 2 6 4]	$y^2 = x^3$,
[1 3 3 4]	$y^2 = x^3 + 5x + 5$,
[1 3 3 5]	$y^2 = x^3 + 5$,

[1 3 5 4] $y^2 = x^3 + 5x + 5$,

[1 3 6 4] $y^2 = x^3 + 5x + 5$,

[1 3 6 5] $y^2 = x^3 + 5$,

[1 4 3 2] $y^2 = x^3 + 5$,

[1 4 3 3] $y^2 = x^3 + 5x + 5$,

[1 4 5 2] $y^2 = x^3 + 5$,

[1 4 5 3] $y^2 = x^3 + 5x + 5$,

[1 4 6 2] $y^2 = x^3 + 5$,

[1 4 6 3] $y^2 = x^3 + 5x + 5$,

[1 5 1 1] $y^2 = x^3 + 6x + 5$,

[1 5 2 1] $y^2 = x^3 + 6x + 5$,

[1 5 3 3] $y^2 = x^3$,

[1 5 4 1] $y^2 = x^3 + 6x + 5$,

[1 5 5 3] $y^2 = x^3$,

[1 5 6 3] $y^2 = x^3$,

[1 6 1 5] $y^2 = x^3 + 6x + 5$,

[1 6 2 5] $y^2 = x^3 + 6x + 5$,

[1 6 4 5] $y^2 = x^3 + 6x + 5$,

Aşağıdaki teorem ile rankı yedi olan bir dizinin sadece $\mathbb{F}_{13}$ de singüler eğrilerle eşleştikleri gösterilmektedir.

5.4.28 Teorem. [1 h_2 h_3 ch_2] (h_2, h_3, $h_4 \in \mathbb{F}_p^*$) rankı yedi olan bir eliptik bölünebilir dizi olsun. Bu durumda (h_n) dizisinin bir singüler eğri ile eşleşebilmesi için gerek ve yeter şart $p = 13$ olmasıdır.

İspat. Rankı yedi olan bir dizinin başlangıç terimleri

$$[1\ 2^t\ \ 2^{\frac{8t+1}{3}}\ \ -2^{5t+1}] \text{ veya } [1\ -2^t\ \ 2^{\frac{8t+1}{3}}\ \ 2^{5t+1}]$$

olduğundan

$$\Delta(h_2, h_3, h_4) = h_2^{16}c - h_3^3h_2^{12} + 3h_2^{12}c^2 - 20h_2^8c^3 + 16h_3^6h_2^4 + 8h_2^4c^2h_3 + h_2^4c^4 = 0$$

eşitliğinde bu değerler yazılırsa her iki halde de

$$\Delta(h_2, h_3, h_4) = 2^{19}\, 3^{12}\, 13\, 2^t$$

dir ve dolayısıyla

$$\Delta(h_2, h_3, h_4) = 0 \Leftrightarrow p = 13$$

dir.

Aşağıdaki teoremde rankı yedi olan dizilerle eşleşen singüler eğriler belirlenmiştir.

5.4.29 Teorem. [1 h_2 h_3 ch_2] (h_2, h_3, $ch_2 = h_4 \in \mathbb{F}_p^*$) rankı yedi olan bir EBD ise bu dizilerle eşleşen eliptik eğriler

$$E : y^2 = x^3 + 3x + 10$$

biçimindedir. Üstelik bu diziler E eğrisi üzerindeki

$$P = (x_1, y_1) = (9, 5)$$

noktasından elde edilen bir dizidir.

İspat. (5.19) eşitliğinde $p = 13$ olarak alınırsa istenilen elde edilir.

5.4.30 Örnek. $\mathbb{F}_{13}$ de rankı 7 olan

[1 1 7 10], [1 1 8 10], [1 1 11 10], [1 2 7 1], [1 2 8 1],
[1 2 11 1], [1 3 7 8], [1 3 8 8], [1 3 11 8], [1 5 7 11],
[1 5 8 11], [1 5 11 11], [1 8 7 2], [1 8 8 2], [1 8 11 2],
[1 10 7 5], [1 10 8 5], [1 10 11 5], [1 11 7 12], [1 11 8 12],
[1 11 11 12], [1 12 7 3], [1 12 8 3], [1 12 11 3]

singüler dizileri

$$E : y^2 = x^3 + 3x + 10$$

singüler eğrisi ile eşleşirler.

KAYNAKLAR

CHARLAP, L. S., ROBBINS, D. P., 1988. An Elementary Introduction to Elliptic Curves. Technical Report 31, Institute for Defense Analysis, Princeton.

CHUDNOVSKY, D. V., CHUDNOVSKY, G. V. 1986. Sequences of Numbers Generated by Addition in Formal Groups and New Primality Factorization Tests. Adv. in Appl. Math., 7 : 385-434.

CONELL, I. Elliptic Curve Handbook. www. math.mcgill.ca / conell / public / ECH1/.

EINSIEDLER, M., EVEREST, G., WARD, T. 2001. Primes in Elliptic Divisibility Sequences. LMS J. Comput. Math. 4 : 1-13, electronic.

EVEREST, G., van der POORTEN, A., SHPARLINSKI, I., WARD, T. 2003. Recurrence Sequences, Mathematical Surveys and Monographs 104, AMS, Providence, RI, 320 p.

EVEREST, G., WARD, T. 2001. Primes in Divisibility Sequences, Cubo Mat. Educ. 3 : 245-259.

FRALEIGH, J. B. 1982. A First Course In Abstract Algebra. Addison Wesley P.C., 478 p.

GEZER, B. ve BİZİM, O., Elliptic Divisibility Sequences in Certain Ranks Over Finite Fields, Hacettepe Journal of Mathematics and Istatistics (Yayına kabul edildi).

KOBLITZ, N. 1994. A Course in Number Theory and Cryptography. Springer-Verlag New york Inc, 235 p.

LEMMERMEYER, F. 2000. Reciprocity Laws. From Euler to Eisenstein. Springer Monogr. in Math., Springer-Verlag, 487 p.

MOLLIN, R.A. 2000. Fundamental Number Theory with Applications, Chapman&Hall/CRC, United States of America, 439 p.

MOLLIN, R. A. 2001. An Introduction to Cryptography. Chapman&Hall/CRC, United States of America, 373 p.

NAMLI, D. 2001. Kübik Rezidüler, Doktora Tezi, Balıkesir Üniversitesi (yayımlanmamış), Balıkesir Üniversitesi.

SHIPSEY, R. 2000. Elliptic Divisibility Sequences, PhD Thesis, Goldsmith's (University of London).

SILVERMAN, J. H. 1986. The Arithmetic of Elliptic Curves, Springer-Verlag, 402 p.

SILVERMAN, J.H. 2006. A Friendly Introduction to Number Theory, PrenticeHall,434p.

SILVERMAN, J. H., STEPHENS. N. 2006. The Sign of an Elliptic Divisibility Sequences, Journal of Ramanujan Math. Soc. 21: 1-17.

SILVERMAN, J. H., TATE, J. 1992. Rational Points on Elliptic Curves, Undergraduate Texts in Mathematics, Springer, 283 p.

SWART, C. S. 2003. Elliptic Curves and Related Sequences, PhD Thesis, Royal Holloway (University of London).

SCHMITT, S., ZIMMER, H. G. 2003. Elliptic Curves, Graduate Texts in Mathematics, Walter de Gruyter, 367 p.

WARD, M. 1948. The Law of Repetition of Primes in an Elliptic Divisibility Sequences, Duke Math. J. 15: 941-946.

WARD, M. 1948. Memoir on Elliptic Divisibility Sequences, Amer. J. Math. 70 : 31-74.

WASHINGTON, L. C. 2003. Elliptic Curves, Number Theory and Cryptography. Chapman&Hall/CRC, 428p.

EK-1

$\mathbb{F}_5$ DE HAS (PROPER OLMAYAN) DİZİLER (h_2 veya $h_3 = 0$)

h_0	h_1	h_2	h_3	h_4	h_5	h_6	h_7	h_8	h_9	h_{10}	h_{11}	h_{12}	h_{13}	h_{14}	h_{15}	h_{16}	h_{17}	h_{18}	h_{19}	h_{20}	h_{21}	h_{22}	h_{23}	h_{24}	h_{25}	h_{26}	h_{27}	h_{28}	h_{29}	h_{30}	h_{31}	h_{32}	h_{33}	h_{34}	h_{35}	h_{36}	h_{37}	h_{38}	h_{39}	h_{40}
0	1	0	0	0	0	0	0	0	0	0	0	0	0																												
0	**1**	**1**	**0**	**1**	**1**	**0**	**4**	**4**	**0**	**4**	**4**	0	1	1	0	1	1	0	4	4	0	4	4	0	1	1	0	1	1	0	4	4	0	4	4	0	1	1	0	1
0	**1**	**1**	**0**	**2**	**2**	**0**	**2**	**2**	**0**	**1**	**1**	**0**	**4**	**4**	**0**	**3**	**3**	**0**	**3**	**3**	**0**	**4**	**4**	0	1	1	0	2	2	0	2	2	0	1	1	0	4	4	0	3
0	**1**	**1**	**0**	**3**	**3**	**0**	**3**	**3**	**0**	**1**	**1**	**0**	**4**	**4**	**0**	**2**	**2**	**0**	**2**	**2**	**0**	**4**	**4**	0	1	1	0	3	3	0	3	3	0	1	1	0	4	4	0	2
0	**1**	**1**	**0**	**4**	**4**	0	1	1	0	4	4	0	1	1	0	4	4	0	1	1	0	4	4	0	1	1	0	4	4	0	1	1	0	4	4	0	1	1	0	4
0	1	1	0	0	0	0	0	0	0	0	0	0	0																												
0	**1**	**2**	**0**	**1**	**3**	**0**	**3**	**1**	**0**	**2**	**1**	**0**	**4**	**3**	**0**	**4**	**2**	**0**	**2**	**4**	**0**	**3**	**4**	0	1	2	0	1	3	0	3	1	0	2	1	0	4	3	0	4
0	**1**	**2**	**0**	**2**	**1**	**0**	**4**	**3**	**0**	**3**	**4**	0	1	2	0	2	1	0	4	3	0	3	4	0	1	2	0	2	1	0	4	3	0	3	4	0	1	2	0	2
0	**1**	**2**	**0**	**3**	**4**	0	1	2	0	3	4	0	1	2	0	3	4	0	1	2	0	3	4	0	1	2	0	3	4	0	1	2	0	3	4	0	1	2	0	3
0	**1**	**2**	**0**	**4**	**2**	**0**	**2**	**4**	**0**	**2**	**1**	**0**	**4**	**3**	**0**	**1**	**3**	**0**	**3**	**1**	**0**	**3**	**4**	0	1	2	0	4	2	0	2	4	0	2	1	0	4	3	0	1
0	1	2	0	0	0	0	0	0	0	0	0	0	0																												
0	**1**	**3**	**0**	**1**	**2**	**0**	**2**	**1**	**0**	**3**	**1**	**0**	**4**	**2**	**0**	**4**	**3**	**0**	**3**	**4**	**0**	**2**	**4**	0	1	3	0	1	2	0	2	1	0	3	1	0	4	2	0	4
0	**1**	**3**	**0**	**2**	**4**	**0**	**1**	**3**	**0**	**2**	**4**	0	1	3	0	2	4	0	1	3	0	2	4	0	1	3	0	2	4	0	1	3	0	2	4	0	1	3	0	2
0	**1**	**3**	**0**	**3**	**1**	**0**	**4**	**2**	**0**	**2**	**4**	0	1	3	0	3	1	0	4	2	0	2	4	0	1	3	0	3	1	0	4	2	0	2	4	0	1	3	0	3
0	**1**	**3**	**0**	**4**	**3**	**0**	**3**	**4**	**0**	**3**	**1**	**0**	**4**	**2**	**0**	**1**	**2**	**0**	**2**	**1**	**0**	**2**	**4**	0	1	3	0	4	3	0	3	4	0	3	1	0	4	2	0	1
0	1	3	0	0	0	0	0	0	0	0	0	0	0																												
0	**1**	**4**	0	1	4	0	1	4	0	1	4	0	1	4	0	1	4	0	1	4	0	1	4	0	1	4	0	1	4	0	1	4	0	1	4	0	1	4	0	1
0	**1**	**4**	**0**	**2**	**3**	**0**	**3**	**2**	**0**	**4**	**1**	**0**	**4**	**1**	**0**	**3**	**2**	**0**	**2**	**3**	**0**	**1**	**4**	0	1	4	0	2	3	0	3	2	0	4	1	0	4	1	0	3
0	**1**	**4**	**0**	**3**	**2**	**0**	**2**	**3**	**0**	**4**	**1**	**0**	**2**	**1**	**0**	**2**	**3**	**0**	**3**	**2**	**0**	**4**	**1**	0	1	4	0	3	2	0	2	3	0	4	1	0	4	1	0	2
0	**1**	**4**	**0**	**4**	**1**	**0**	**4**	**1**	**0**	**1**	**4**	0	1	4	0	4	1	0	4	1	0	1	4	0	1	4	0	4	1	0	4	1	0	1	4	0	1	4	0	4
0	1	4	0	0	0	0	0	0	0	0	0	0	0																												
0	**1**	**0**	**1**	**0**	**4**	**0**	**4**	0	1	0	1	0	4	0	4	0	1	0	1	0	4	0	4	0	1	0	1	0	4	0	4	0	1	0	1	0	4	0	4	0
0	**1**	**0**	**2**	**0**	**2**	**0**	**1**	**0**	**4**	**0**	**3**	**0**	**3**	**0**	**4**	0	1	0	2	0	2	0	1	0	4	0	3	0	3	0	4	0	1	0	2	0	2	0	1	0
0	**1**	**0**	**3**	**0**	**3**	**0**	**1**	**0**	**4**	**0**	**2**	**0**	**2**	**0**	**4**	0	1	0	3	0	3	0	1	0	4	0	2	0	2	0	4	0	1	0	3	0	3	0	1	0
0	**1**	**0**	**4**	0	1	0	4	0	1	0	4	0	1	0	4	0	1	0	4	0	1	0	4	0	1	0	4	0	1	0	4	0	1	0	4	0	1	0	4	0

EK-2

$\mathbb{F}_5$ DE HAS (PROPER) DİZİLER ($h_2 \neq 0,\ h_3 \neq 0$)

$h_0 h_1 h_2 h_3\ h_4\ h_5\ h_6\ h_7\ h_8\ h_9\ h_{10}\ h_{11} h_{12} h_{13} h_{14}\ h_{15} h_{16} h_{17} h_{18} h_{19} h_{20} h_{21} h_{22} h_{23} h_{24}\ h_{25} h_{26} h_{27} h_{28} h_{29} h_{30}\ h_{31} h_{32} h_{33}\ h_{34} h_{35}\ h_{36}\ h_{37}\ h_{38}\ h_{39}\ h_{40}$

0 1 1 1 0 4 4 4 0 1 1 1 0 4 4 4 0 1 1 1 0 4 4 4 0 1 1 1 0 4 4 4 0 1 1 1 0 4 4 4 0
0 1 1 1 1 0 4 4 4 4 0 1 1 1 1 0 4 4 4 4 0 1 1 1 1 0 4 4 4 4 0 1 1 1 1 0 4 4 4 4 0
0 1 1 1 2 1 2 3 2 0 3 2 3 4 3 4 4 4 0 1 1 1 2 1 2 3 2 0 3 2 3 4 3 4 4 4 0 1 1 1 2
0 1 1 1 3 2 3 0 2 3 2 4 4 4 0 1 1 1 3 2 3 0 2 3 2 4 4 4 0 1 1 1 3 2 3 0 2 3 2 4 4
0 1 1 1 4 3 2 4 2 1 0 1 3 4 3 3 1 1 4 1 0 4 1 4 4 2 2 1 2 4 0 4 3 1 3 2 1 4 4 4 0
0 1 2 1 0 4 3 4 0 1 2 1 0 4 3 4 0 1 2 1 0 4 3 4 0 1 2 1 0 4 3 4 0 1 2 1 0 4 3 4 0
0 1 2 1 1 2 1 0 4 3 4 4 3 4 0 1 2 1 1 2 1 0 4 3 4 4 3 4 0 1 2 1 1 2 1 0 4 3 4 4 3
0 1 2 1 2 0 3 4 3 4 0 1 2 1 2 0 3 4 3 4 0 1 2 1 2 0 3 4 3 4 0 1 2 1 2 0 3 4 3 4 0
0 1 2 1 3 3 4 4 4 4 1 0 1 1 4 1 3 2 1 3 1 0 4 2 4 3 2 4 1 4 4 0 4 1 1 1 2 2 4 3 4 0
0 1 2 1 4 1 4 3 4 0 1 2 1 4 1 4 3 4 0 1 2 1 4 1 4 3 4 0 1 2 1 4 1 4 3 4 0 1 2 1 4
0 1 3 1 0 4 2 4 0 1 3 1 0 4 2 4 0 1 3 1 0 4 2 4 0 1 3 1 0 4 2 4 0 1 3 1 0 4 2 4 0
0 1 3 1 1 1 1 3 1 0 4 2 4 4 4 4 4 2 4 0 1 3 1 1 1 1 3 1 0 4 2 4 4 4 4 2 4 0 1 3 1 1
0 1 3 1 2 3 1 4 1 1 0 1 4 4 4 3 3 1 2 1 0 4 3 4 2 2 1 1 1 4 0 4 4 1 4 2 3 4 2 4 0
0 1 3 1 3 0 2 4 2 4 0 1 3 1 3 0 2 4 2 4 0 1 3 1 3 0 2 4 2 4 0 1 3 1 3 0 2 4 2 4 0
0 1 3 1 4 2 4 0 1 3 1 4 2 4 0 1 3 1 4 2 4 0 1 3 1 4 2 4 0 1 3 1 4 2 4 0 1 3 1 4 2
0 1 4 1 0 4 1 4 0 1 4 1 0 4 1 4 0 1 4 1 0 4 1 4 0 1 4 1 0 4 1 4 0 1 4 1 0 4 1 4 0
0 1 4 1 1 3 3 4 3 1 0 1 2 4 2 3 4 1 1 1 0 4 4 4 1 2 3 1 3 4 0 4 2 1 2 2 4 4 1 4 0
0 1 4 1 2 2 2 0 3 3 3 4 1 4 0 1 4 1 2 2 2 0 3 3 3 4 1 4 0 1 4 1 2 2 2 0 3 3 3 4 1
0 1 4 1 3 1 3 3 3 0 2 2 2 4 2 4 1 4 0 1 4 1 3 1 3 3 3 0 2 2 2 4 2 4 1 4 0 1 4 1 3
0 1 4 1 4 0 1 4 1 4 0 1 4 1 4 0 1 4 1 4 0 1 4 1 4 0 1 4 1 4 0 1 4 1 4 0 1 4 1 4 0

0 1 1 2 0 2 4 1 0 4 1 3 0 3 4 4 0 1 1 2 0 2 4 1 0 4 1 3 0 3 4 4 0 1 1 2 0 2 4 1 0
0 1 1 2 1 3 4 3 2 0 3 2 1 2 4 3 4 4 0 1 1 2 1 3 4 3 2 0 3 2 1 2 4 3 4 4 0 1 1 2 1
0 1 1 2 2 4 0 4 3 2 4 1 0 4 1 3 2 1 0 1 3 3 4 4 0 1 1 2 2 4 0 4 3 2 4 1 0 4 1 3 2
0 1 1 2 3 0 2 3 4 4 0 1 1 2 3 0 2 3 4 4 0 1 1 2 3 0 2 3 4 4 0 1 1 2 3 0 2 3 4 4 0
0 1 1 2 4 1 0 4 1 3 4 4 0 1 1 2 4 1 0 4 1 3 4 4 0 1 1 2 4 1 0 4 1 3 4 4 0 1 1 2 4
0 1 2 2 0 2 3 1 0 4 2 3 0 3 3 4 0 1 2 2 0 2 3 1 0 4 2 3 0 3 3 4 0 1 2 2 0 2 3 1 0
0 1 2 2 1 0 4 3 3 4 0 1 2 2 1 0 4 3 3 4 0 1 2 2 1 0 4 3 3 4 0 1 2 2 1 0 4 3 3 4 0
0 1 2 2 2 3 3 3 4 0 1 2 2 2 3 3 3 4 0 1 2 2 2 3 3 3 4 0 1 2 2 2 3 3 3 4 0 1 2 2 2
0 1 2 2 3 1 0 4 2 3 3 4 0 1 2 2 3 1 0 4 2 3 3 4 0 1 2 2 3 1 0 4 2 3 3 4 0 1 2 2 3
0 1 2 2 4 4 0 4 1 2 3 1 0 4 2 3 4 1 0 1 1 3 3 4 0 1 2 2 4 4 0 4 1 2 3 1 0 4 2 3 4
0 1 3 2 0 2 2 1 0 4 3 3 0 3 2 4 0 1 3 2 0 2 2 1 0 4 3 3 0 3 2 4 0 1 3 2 0 2 2 1 0
0 1 3 2 1 4 0 4 4 2 2 1 0 4 3 3 1 1 0 1 4 3 2 4 0 1 3 2 1 4 0 4 4 2 2 1 0 4 3 3 1
0 1 3 2 2 1 0 4 3 3 2 4 0 1 3 2 2 1 0 4 3 3 2 4 0 1 3 2 2 1 0 4 3 3 2 4 0 1 3 2 2
0 1 3 2 3 3 2 3 1 0 4 2 3 2 2 3 2 4 0 1 3 2 3 3 2 3 1 0 4 2 3 2 2 3 2 4 0 1 3 2 3
0 1 3 2 4 0 1 3 2 4 0 1 3 2 4 0 1 3 2 4 0 1 3 2 4 0 1 3 2 4 0 1 3 2 4 0 1 3 2 4 0
0 1 4 2 0 2 1 1 0 4 4 3 0 3 1 4 0 1 4 2 0 2 1 1 0 4 4 3 0 3 1 4 0 1 4 2 0 2 1 1 0
0 1 4 2 1 1 0 4 4 3 1 4 0 1 4 2 1 1 0 4 4 3 1 4 0 1 4 2 1 1 0 4 4 3 1 4 0 1 4 2 1
0 1 4 2 2 0 3 3 1 4 0 1 4 2 2 0 3 3 1 4 0 1 4 2 2 0 3 3 1 4 0 1 4 2 2 0 3 3 1 4 0
0 1 4 2 3 4 0 4 2 2 1 1 0 4 4 3 3 1 0 1 2 3 1 4 0 1 4 2 3 4 0 4 2 2 1 1 0 4 4 3 3
0 1 4 2 4 3 1 3 3 0 2 2 4 2 1 3 1 4 0 1 4 2 4 3 1 3 3 0 2 2 4 2 1 3 1 4 0 1 4 2 4

0 1 1 3 0 3 4 1 0 4 1 2 0 2 4 4 0 1 1 3 0 3 4 1 0 4 1 2 0 2 4 4 0 1 1 3 0 3 4 1 0
0 1 1 3 1 4 4 2 0 2 1 4 4 3 4 1 0 4 1 2 1 1 4 3 0 3 1 1 4 2 4 4 0 1 1 3 1 4 4 2 0
0 1 1 3 2 0 3 2 4 4 0 1 1 3 2 0 3 2 4 4 0 1 1 3 2 0 3 2 4 4 0 1 1 3 2 0 3 2 4 4 0

0 1 1 3 3 1 1 0 4 4 2 2 4 4 0 1 1 3 3 1 1 0 4 4 2 2 4 4 0 1 1 3 3 1 1 0 4 4 2 2 4
0 1 1 3 4 2 3 0 2 3 1 2 4 4 0 1 1 3 4 2 3 0 2 3 1 2 4 4 0 1 1 3 4 2 3 0 2 3 1 2 4
0 1 2 3 0 3 3 1 0 4 2 2 0 2 3 4 0 1 2 3 0 3 3 1 0 4 2 2 0 2 3 4 0 1 2 3 0 3 3 1 0
0 1 2 3 1 1 2 0 3 4 4 2 3 4 0 1 2 3 1 1 2 0 3 4 4 2 3 4 0 1 2 3 1 1 2 0 3 4 4 2 3
0 1 2 3 2 4 3 2 0 2 2 4 3 3 3 1 0 4 2 2 2 1 3 3 0 3 2 1 3 2 3 4 0 1 2 3 2 4 3 2 0
0 1 2 3 3 2 1 0 4 3 2 2 3 4 0 1 2 3 3 2 1 0 4 3 2 2 3 4 0 1 2 3 3 2 1 0 4 3 2 2 3
0 1 2 3 4 0 1 2 3 4 0 1 2 3 4 0 1 2 3 4 0 1 2 3 4 0 1 2 3 4 0 1 2 3 4 0 1 2 3 4 0
0 1 3 3 0 3 2 1 0 4 3 2 0 2 2 4 0 1 3 3 0 3 2 1 0 4 3 2 0 2 2 4 0 1 3 3 0 3 2 1 0
0 1 3 3 1 0 4 2 2 4 0 1 3 3 1 0 4 2 2 4 0 1 3 3 1 0 4 2 2 4 0 1 3 3 1 0 4 2 2 4 0
0 1 3 3 2 2 4 0 1 3 3 2 2 4 0 1 3 3 2 2 4 0 1 3 3 2 2 4 0 1 3 3 2 2 4 0 1 3 3 2 2
0 1 3 3 3 4 2 2 0 2 3 4 2 3 2 1 0 4 3 2 3 1 2 3 0 3 3 1 2 2 2 4 0 1 3 3 3 4 2 2 0
0 1 3 3 4 1 3 0 2 4 1 2 2 4 0 1 3 3 4 1 3 0 2 4 1 2 2 4 0 1 3 3 4 1 3 0 2 4 1 2 2
0 1 4 3 0 3 1 1 0 4 4 2 0 2 1 4 0 1 4 3 0 3 1 1 0 4 4 2 0 2 1 4 0 1 4 3 0 3 1 1 0
0 1 4 3 1 2 2 0 3 3 4 2 1 4 0 1 4 3 1 2 2 0 3 3 4 2 1 4 0 1 4 3 1 2 2 0 3 3 4 2 1
0 1 4 3 2 1 4 0 1 4 3 2 1 4 0 1 4 3 2 1 4 0 1 4 3 2 1 4 0 1 4 3 2 1 4 0 1 4 3 2 1
0 1 4 3 3 0 2 2 1 4 0 1 4 3 3 0 2 2 1 4 0 1 4 3 3 0 2 2 1 4 0 1 4 3 3 0 2 2 1 4 0
0 1 4 3 4 4 1 2 0 2 4 4 1 3 1 1 0 4 4 2 4 1 1 3 0 3 4 1 1 2 1 4 0 1 4 3 4 4 1 2 0

0 1 1 4 0 1 4 4 0 1 1 4 0 1 4 4 0 1 1 4 0 1 4 4 0 1 1 4 0 1 4 4 0 1 1 4 0 1 4 4 0 1 1 4 0 1 4 4 0
0 1 1 4 1 2 4 2 0 2 1 2 4 4 4 1 0 4 1 1 1 3 4 3 0 3 1 3 4 1 4 4 0 1 1 4 1 2 4 2 0
0 1 1 4 2 3 1 4 4 0 1 1 4 2 3 1 4 4 0 1 1 4 2 3 1 4 4 0 1 1 4 2 3 1 4 4 0 1 1 4 2
0 1 1 4 3 4 0 4 2 4 4 1 0 4 1 1 3 1 0 1 2 1 4 4 0 1 1 4 3 4 0 4 2 4 4 1 0 4 1 1 3
0 1 1 4 4 0 1 1 4 4 0 1 1 4 4 0 1 1 4 4 0 1 1 4 4 0 1 1 4 4 0 1 1 4 4 0 1 1 4 4 0
0 1 2 4 0 1 3 4 0 1 2 4 0 1 3 4 0 1 2 4 0 1 3 4 0 1 2 4 0 1 3 4 0 1 2 4 0 1 3 4 0
0 1 2 4 1 4 0 4 4 4 3 1 0 4 2 1 1 1 0 1 4 1 3 4 0 1 2 4 1 4 0 4 4 4 3 1 0 4 2 1 1
0 1 2 4 2 2 3 2 0 2 2 2 3 4 3 1 0 4 2 1 2 3 3 3 0 3 2 3 3 1 3 4 0 1 2 4 2 2 3 2 0
0 1 2 4 3 0 2 1 3 4 0 1 2 4 3 0 2 1 3 4 0 1 2 4 3 0 2 1 3 4 0 1 2 4 3 0 2 1 3 4 0
0 1 2 4 4 3 2 4 3 0 2 1 3 2 1 1 3 4 0 1 2 4 4 3 2 4 3 0 2 1 3 2 1 1 3 4 0 1 2 4 4
0 1 3 4 0 1 2 4 0 1 3 4 0 1 2 4 0 1 3 4 0 1 2 4 0 1 3 4 0 1 2 4 0 1 3 4 0 1 2 4 0
0 1 3 4 1 3 3 4 2 0 3 1 2 2 4 1 2 4 0 1 3 4 1 3 3 4 2 0 3 1 2 2 4 1 2 4 0 1 3 4 1
0 1 3 4 2 0 3 1 2 4 0 1 3 4 2 0 3 1 2 4 0 1 3 4 2 0 3 1 2 4 0 1 3 4 2 0 3 1 2 4 0
0 1 3 4 3 2 2 2 0 2 3 2 2 4 2 1 0 4 3 1 3 3 2 3 0 3 3 3 2 1 2 4 0 1 3 4 3 2 2 2 0
0 1 3 4 4 4 0 4 1 4 2 1 0 4 3 1 4 1 0 1 1 1 2 4 0 1 3 4 4 4 0 4 1 4 2 1 0 4 3 1 4
0 1 4 4 0 1 1 4 0 1 4 4 0 1 1 4 0 1 4 4 0 1 1 4 0 1 4 4 0 1 1 4 0 1 4 4 0 1 1 4 0
0 1 4 4 1 0 4 1 1 4 0 1 4 4 1 0 4 1 1 4 0 1 4 4 1 0 4 1 1 4 0 1 4 4 1 0 4 1 1 4 0
0 1 4 4 2 4 0 4 3 4 1 1 0 4 4 1 2 1 0 1 3 1 1 4 0 1 4 4 2 4 0 4 3 4 1 1 0 4 4 1 2
0 1 4 4 3 3 4 4 1 0 4 1 1 2 2 1 1 4 0 1 4 4 3 3 4 4 1 0 4 1 1 2 2 1 1 4 0 1 4 4 3
0 1 4 4 4 2 1 2 0 2 4 2 1 4 1 1 0 4 4 1 4 3 1 3 0 3 4 3 1 1 1 4 0 1 4 4 4 2 1 2 0

ÖZGEÇMİŞ

27.04.1980 tarihinde Gaziantep'te doğan Betül Gezer; ilk, orta ve lise öğrenimini Gaziantep'te tamamladıktan sonra 1999 yılında Uludağ Üniversitesi Fen Edebiyat Fakültesi Matematik Bölümü'nde lisans öğrenimine başladı. 2003 yılında lisans öğrenimini tamamlamasının ardından yine aynı yıl Uludağ Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim dalında yüksek lisans öğrenimine başladı ve 2005 yılında yüksek lisans öğrenimini tamamladı. Aynı yıl Uludağ Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim dalında doktora öğrenimine başladı. 2009 yılı Ocak ayında Fen Edebiyat Fakültesi Matematik bölümünde Öğretim Görevlisi olarak çalışmaya başladı ve halen bu görevine devam etmektedir.

TEŞEKKÜR

107 T 311 nolu Tübitak Bilimsel ve Teknolojik Araştırma Projesi kapsamında hazırlanan bu çalışmanın tamamlanması sürecinde, her türlü yardım ve desteği esirgemeyen değerli Hocam Sayın Doç. Dr. Osman BİZİM'e, en içten teşekkürlerimi sunarım.