

58170

T.C
AKDENİZ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

ELİPTİK EĞRİLERİN RASYONEL NOKTALARI

SEVDA SEZER

YÜKSEK LİSANS TEZİ

MATEMATİK ANABİLİM DALI

ANTALYA

ELİPTİK EĞRİLERİN RASYONEL NOKTALARI

Sevda SEZER

YÜKSEK LİSANS TEZİ

MATEMATİK ANABİLİM DALI

1997

YÜKSEKÖĞRETİM KURULU
DOKÜMANİZEASYON MERKEZİ

T.C.
AKDENİZ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

ELİPTİK EĞRİLERİN RASYONEL NOKTALARI

Sevda SEZER

YÜKSEK LİSANS TEZİ

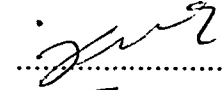
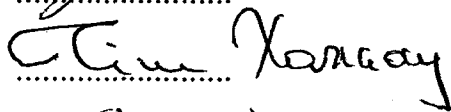
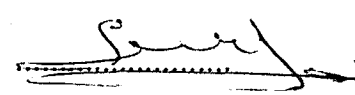
MATEMATİK ANABİLİM DALI

Bu tez 8/4/1997 tarihinde aşağıdaki jüri tarafından ...(90) not takdir edilerek
Oybirliği/Oyçokluğu ile kabul edilmiştir.

JÜRİ : Prof. Dr. Halil İ. KARAKAŞ
(Danışman)

Prof. Dr. Timur KARAÇAY

Doç. Dr. İlham ALİYEV

ÖZ

ELİPTİK EĞRİLERİN RASYONEL NOKTALARI

Sevda SEZER

Yüksek Lisans Tezi, Matematik Anabilim Dalı

Ocak 1997, 77 Sayfa

Bu çalışmada rasyonel sayılar cismi üzerinden eliptik eğrilerin rasyonel noktalarından oluşan grup incelenmiştir. Bu bağlamda, sonlu sayıda rasyonel nokta kullanılarak sözü edilen grubun tüm noktalarının üretilebileceğini ifade eden Mordell Teoremi'nin, ispatında ileri derecede cebirsel sayılar teorisi kullanıldığı için, ispatı özel bir durumda (grubun mertebesi iki olan bir rasyonel noktasının varlığı durumunda) yapılmıştır. Bunun sonucunda, Sonlu Üretilmiş Abel Gruplarının Temel Teoremi kullanılarak rasyonel noktalar grubunun mertebesi sonlu olan noktalarının Nagell-Lutz Teoremi ile belirlenebileceği ifade edilmiş ve Mazur Teoremi yardımıyla da mertebesi sonlu olan noktalardan oluşan altgrupların yapısının tam olarak belirlenebileceği açıklanmıştır. Ayrıca, rasyonel noktalar grubunun serbest Abel grubu kısmının rankının büyüklüğü hakkında kesin bir sonuç elde edilememiş olup, henüz rankı 16 veya 16 dan büyük olan eliptik eğri örnekleri bulunamamıştır.

ANAHTAR KELİMELER : Eliptik eğri, eliptik eğrilerin rasyonel noktaları, Mordell Teoremi, sonlu üretilmiş Abel grubu, serbest Abel grubu, Sonlu Üretilmiş Abel Gruplarının Temel Teoremi, Nagell-Lutz Teoremi, Mazur Teoremi, serbest Abel grubu, rank.

JÜRİ : Prof. Dr. Halil İ. KARAKAŞ
Prof. Dr. Timur KARAÇAY
Doç. Dr. İlham ALİYEV

ABSTRACT

RATIONAL POINTS OF ELLIPTIC CURVES

Sevda SEZER

M.S. in Mathematics

Advisor: Prof. Dr. Halil İ. KARAKAŞ

January, 1997, 77 pages

In this work, we investigate the group formed by the rational points of elliptic curves over the field of rational numbers. Mordell's Theorem, which states that this group can be generated by finitely many rational points, is proved here in a special case, in the case when the group has a rational point of order 2. The reason for this restriction is that the proof of Mordell's Theorem requires advanced techniques of algebraic number theory. As a result of Mordell's Theorem, the subgroup of elements of finite order of the group of rational points (of an elliptic curve) can be determined by using the Fundamental Theorem of Finitely Generated Abelian Groups and the theorem of Nagell-Lutz. Besides, it is pointed out that the subgroups formed by elements of finite order can be determined completely by using Mazur's Theorem. Moreover, not much is known about the rank of the free part of the group of rational points, and, yet, there is no example of elliptic curve with the rank of the group of rational points greater than 15.

KEY WORDS : Elliptic curves, rational points on elliptic curves, Mordell's Theorem, finitely generated Abelian group, Fundamental Theorem of Finitely Generated Abelian Groups, Nagel-Lutz Theorem, Mazur's Theorem, free Abelian group, rank.

COMMITTEE : Prof. Dr. Halil İ. KARAKAŞ
Prof. Dr. Timur KARAÇAY
Assoc. Dr. İlham ALİYEYEV

ÖNSÖZ

Eliptik eğriler, kübik eğriler içinde oldukça geniş bir yere sahiptir. Günümüzde çeşitli alanlarda uygulama imkanı olan eliptik eğrilerin önemi azımsanamayacak kadar çoktur. Çünkü, iki değişkenli ve tamsayı katsayılı bir kübik denklemin rasyonel çözümlerini belirlemek, uygun bir eliptik eğri üzerindeki rasyonel koordinatlı noktaları belirlemekle eşdeğerdir. Ayrıca, burada sözü edilen noktalar kümesinin, sonlu üretilmiş bir Abel grubu olması ve böylece tüm rasyonel noktaların (dolayısıyla, tüm rasyonel çözümlerin) belirlenebilme imkanının olması konu ile ilgilenen matematikçileri eliptik eğrilerle çalışmaya yönlendirmektedir. Bu da sayılar teorisi ile eğriler kuramı arasında bir bağlantı olduğunu göstermektedir.

Eliptik eğrilerin uygulama alanlarından biri de, her ülke için önemli bir yere sahip olan kriptografi (şifre biliminde) ki, kullanılabilirliğidir. Çünkü, çok büyük bir bileşik (asal olmayan) sayının çarpanlarına ayrılması işinin, sayı büyüdükçe güçleşmekte ve uzun zaman almakta olduğu herkes tarafından bilinmektedir. İşte bu fıkirden hareketle, ortaya çıkan şifreleme yöntemlerinde asal çarpanları belirlemek için eliptik eğriler kullanılarak şifrelerin çözülmesi sağlanmaktadır. Bu da, eliptik eğriler ile ilgili daha fazla çalışmaların yapılmasına ve bu konunun günümüzdeki öneminin her geçen gün artmasına yol açmaktadır.

Eliptik eğrilerin matematik camiasındaki bir diğer önemi de Fermat'ın son teoremi olarak bilinen meşhur teoremin, bu ünlü matematikçinin ölümünden ancak 350 yıl sonra, eliptik eğriler kullanılarak, ispatlanmış olmasından kaynaklanmaktadır.

Bu tezin birinci bölümünde, gerekli olan bazı ön bilgi, tanım ve teoremler verildikten sonra eliptik eğri kavramı açıklanarak, konuyla ilgili örnekler verilmiştir. İkinci bölümde ise konuyla ilgili önemli teoremlerden biri olan Mordell Teoremi ispatlanarak, bu teoremin bir kaç örnek üzerinde uygulamalarına yer verilmiştir. Tezin son bölümünde ise sonlu cisimler üzerinden eliptik eğri kavramı üzerinde durulmuş ve bunun bir uygulaması olarak Gauss Teoremi ispatlanmıştır.

Bugüne kadar yapmış olduğum tüm çalışmalarında bilgi ve desteğini benden hiç esirgemeyen danışmanım sayın Prof. Dr. Halil İ. KARAKAŞ'a sonsuz teşekkürlerimi sunarım.

İÇİNDEKİLER

ÖZ	i
ABSTRACT	ii
ÖNSÖZ	iii
İÇİNDEKİLER	iv
SİMGELER ve KISALTMALAR DİZİNİ	v
ŞEKİLLER DİZİNİ	vi
ÇİZELGELER DİZİNİ	vii
1. GİRİŞ	1
1.1. Projektif Düzlem ve Eliptik Eğri	4
1.2. Mertebesi Sonlu Olan Rasyonel Noktalar	21
2. MATERYAL ve METOD	23
2.1. Yükseklik Kavramı	23
2.2. $P + P'$ Noktasının Yüksekliği	23
2.3. $2P$ Noktasının Yüksekliği	26
2.4. Homomorfizm Dönüşümleri	30
2.5. Mordell Teoremi	35
2.6. Mordell Teoreminin Bazı Uygulamaları	44
2.7. Tekil Kübik Eğriler Grubu	55
2.8. Sonlu Cisimler Üzerinden Eliptik Eğriler	59
3. BULGULAR ve TARTIŞMA	70
4. SONUÇ	71
5. ÖZET	72
6. SUMMARY	74
7. KAYNAKLAR	76
ÖZGEÇMİŞ	77

SİMGELER DİZİNİ

Simgeler

$P * Q$	P ve Q dan geçen doğrunun kübik eğriyi kestiği üçüncü nokta
$P + Q$	cliptik eğri üzerinde P ve Q noktalarının toplamı
$\mathcal{O}$	kübik eğrinin sonsuzdaki noktası
$\mathcal{C}(\mathbf{Q})$	kübik eğri üzerindeki rasyonel noktalar
$\mathcal{C}(\mathbf{R})$	kübik eğri üzerindeki reel noktalar
$\mathcal{C}(\mathbf{C})$	kübik eğri üzerindeki kompleks noktalar
$\mathcal{D}_f$	$f(x)$ polinomunun diskriminantı
$\mathbf{Z}[x]$	katsayıları birer tamsayı olan polinomlar
$H(x)$	x rasyonel sayısının yüksekliği
$H(P)$	P rasyonel noktasının yüksekliği
$h(P)$	$H(P)$ nin logaritması
$2\mathcal{C}(\mathbf{Q})$	eğri üzerindeki rasyonel noktaların kendileriyle toplamı
Γ	$= \mathcal{C}(\mathbf{Q})$, eğri üzerindeki rasyonel noktalar grubu
T	$= (0, 0)$, mertebesi iki olan nokta
$\mathbf{Q}^*$	rasyonel sayıların çarpımsal grubu
$\mathbf{Q}^{*2}$	sıfırdan farklı rasyonel sayıların kareleri
$\Gamma[2]$	Γ içinde mertebesi iki olan noktalar
$\mathcal{C}_p$	$y^2 = x^3 + px$ in belirlediği eğri
$\mathcal{C}_{ns}$	kübik eğri üzerindeki non-singüler noktalar
$\mathcal{C}_{ns}(\mathbf{Q})$	kübik eğri üzerindeki non-singüler rasyonel noktalar
$\mathbf{F}_p$	$(mod\ p)$ ye göre tamsayılar cismi
$\mathbf{F}_q$	q elemanlı cisim
$\mathcal{C}(\mathbf{F}_p)$	$\mathbf{F}_p$ üzerinden $\mathcal{C}$ üzerindeki rasyonel noktalar
M_p	$\mathbf{F}_p$ üzerinden $\mathcal{C}$ üzerindeki rasyonel noktaların sayısı
$\mathbf{F}_p^*$	sonlu bir grubun çarpımsal grubu
$\mathcal{R}$	$\mathbf{F}_p^*$ içinde kübik residüler grubu
$\mathcal{S}, \mathcal{T}$	$\mathbf{F}_p^*$ içinde $\mathcal{R}$ nin eşkümeleri
$[\mathcal{X}, \mathcal{Y}, \mathcal{Z}], [\mathcal{X}\mathcal{Y}\mathcal{Z}]$	$\mathcal{P}_2(\mathbf{R})$ de toplamaları sıfır yapan üçlülerin kümesi
$\alpha_1, \alpha_2, \alpha_3$	kübik Gauss toplamaları
$\mathcal{P}_2(\mathbf{F})$	$\mathbf{F}$ cismi üzerinden izdüşümsel (projektif) düzlem
$\mathcal{P}_2(\mathbf{R})$	reel izdüşümsel düzlem
$F(X, Y, Z)$	izdüşümsel koordinatlarda homojen polinom
$[X, Y, Z], [X : Y : Z]$	izdüşümsel düzlemde bir noktanın koordinatları

ŞEKİLLER DİZİNİ

Şekil 1.1	$x^4 + y^4 = 1$ in belirlediği eğri,	2
Şekil 1.2	$x^5 + y^5 = 1$ in belirlediği eğri,	2
Şekil 1.1.1	Weierstrass Normal Formunda Eksenlerin Seçimi	12
Şekil 1.1.2.(a)	$\alpha_1, \alpha_2, \alpha_3 \in \mathbf{R}$ için $y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ ün belirlediği eliptik eğri	14
Şekil 1.1.2.(b)	$\alpha_1 \in \mathbf{R}, \alpha_2, \alpha_3 \in \mathbf{C} \setminus \mathbf{R}$ için $y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ ün belirlediği eliptik eğri	14
Şekil 1.1.3	Eliptik eğri üzerinde $+$ ikili işlemi	15
Şekil 1.1.4	Eliptik eğri üzerindeki noktalar grubunun birim elemanı	16
Şekil 1.1.5	Eliptik eğri üzerindeki noktalar grubunun değişme özelliği	16
Şekil 1.1.6	Eliptik eğri üzerindeki noktalar grubunda bir noktanın tersi ..	17
Şekil 1.1.7	Eliptik eğri üzerindeki noktalar grubunun birleşme özelliği ...	18
Şekil 1.1.8	Eliptik eğri üzerinde verilen iki noktanın toplamı	20
Şekil 2.7.1.(a)	$y^2 = x^3$ ün belirlediği tekil kübik eğri	56
Şekil 2.7.1.(b)	$y^2 = x^3 + x^2$ nin belirlediği tekil kübik eğri	56

ÇİZELGELER DİZİNİ

Çizelge 1.1.1	Verilen örnekler için $\mathcal{C}_f(\mathbf{Q})$ nun $y^2 = x^3 + Ax + B$ formu . . .	14
Çizelge 2.6.1	Verilen örnekler için $\mathcal{C}_f(\mathbf{Q})$ nun $tors \mathcal{C}_f(\mathbf{Q})$ altgrupları	55
Çizelge 2.8.1	Küçük p asal sayıları için A, B, M_p değerleri	69



1. GİRİŞ

17. yy hukukçusu ve çok yönlü matematikçi Pierre de Fermat, sayıların incelenmesinden ibaret olan, sayılar kuramının kurucusu sayılır. Fermat'ın ilham kaynaklarından birinin de, M.S. 3. yy da yunanlı bilge Diophantus tarafından yazılmış olan Aritmetica'nın bir çevirisi olduğu bilinmektedir.

Çözümleri tamsayılar veya rasyonel sayılar şeklinde ifade edilmesi gereken tam veya rasyonel katsayılı polinom denklemler *Diophantus denklemleri* olarak adlandırılır. Bundan dolayı, Diophantus denklemler teorisi sayılar teorisinin önemli bir dalını teşkil etmektedir.

Diophantus denklemlerine bir örnek olarak; matematikçileri yaklaşık 350 yıl boyunca uğraştıran ve Fermat'ın son teoremi olarak bilinen ünlü problem düşünülebilir. Çünkü; bu problem, $n \geq 3$ için $X^n + Y^n = Z^n$ denkleminin, hepsi birden sıfırdan farklı, X, Y, Z tamsayı çözümlerinin olmadığını veya buna denk olarak; $n \geq 3$ için

$$x^n + y^n = 1 \quad (1.1)$$

denkleminin rasyonel çözümlerinin sadece $x = 0$ veya $y = 0$ olması durumunda gerçekleştiğini ifade eder.

Başka bir örnek olarak da; $c \in \mathbb{Z}$ için

$$y^2 - x^3 = c \quad (1.2)$$

denkleminin tamsayı veya rasyonel çözümleri düşünülebilir. Bu denklemin rasyonel çözümleri ile ilgilenildiğinde, denklemin ilginç bir özelliğe sahip olduğu belirlenmiştir. Sözü edilen özellik; bu denklem için katlılık formülü olarak ta adlandırılan bir formülün var olmasıdır. Yani; $(x, y) \in \mathbb{Q}^2$ (1.2) denkleminin bir rasyonel çözümü ise

$$\left(\frac{x^4 - 8cx}{(2y)^2}, \frac{-x^6 - 20cx^3 + 8c^2}{(2y)^3} \right)$$

de aynı denklem için bir rasyonel çözüm oluşturur.

Bu özelliği 1621 de Bachet adlı bir matematikçi keşfettiği için, (1.2) denklemine *Bachet denklemi* de denir. Ayrıca, başlangıçtaki (x, y) çözümü için $x, y \neq 0$ ise, yukarıdaki işlem tekrarlanarak sonsuz tane farklı rasyonel çözüm elde edilebilir.

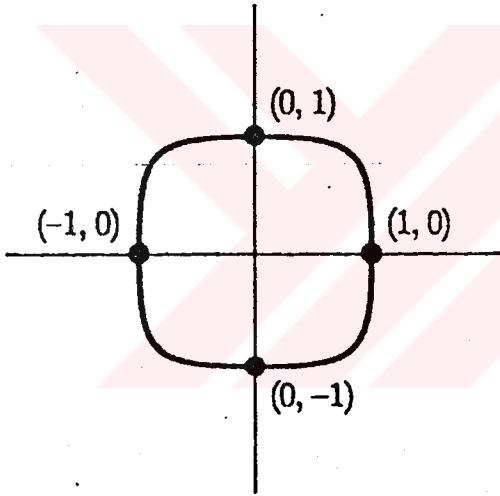
Örneğin, $y^2 - x^3 = -2$ denkleminde $(3, 5)$ çözümü ile başlanır ve Bachet katlılık formülü uygulanırsa;

$$(3, 5), \left(\frac{129}{10^2}, \frac{-383}{10^3} \right), \left(\frac{2340922881}{7660^2}, \frac{113259286337292}{7660^3} \right), \dots$$

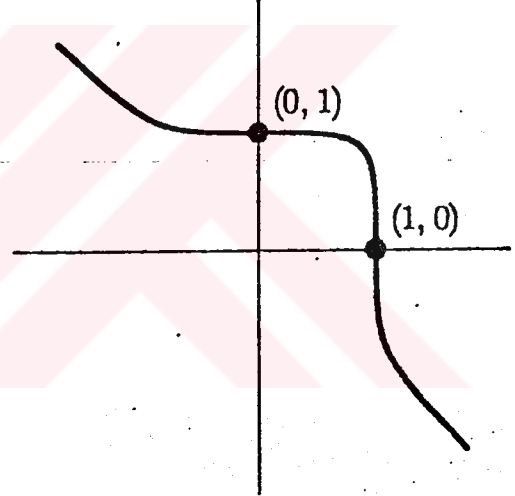
gibi, gittikçe büyüyen sayılarla, bir çözümler dizisi elde edilir.

1650 yılında Fermat, $y^2 - x^3 = -2$ denkleminin tamsayı çözümlerinin sadece iki tane, $(3, \mp 5)$, olduğunu iddia ederek, İngiliz matematik camiasına meydan okumuştur. Çünkü, sonsuz rasyonel çözüm arasından sadece iki tamsayı çözümün olması fikri, beklenen bir sonuç olmadığı için, bir tezat oluşturmıştır. Fermat'ın çağdaşlarından hiç biri bu problemi çözmemiş ve doğru ispat ancak 150 yıl sonra Axel Thue, tarafından verilebilmiştir. 1908 yılında Axel Thue $c \neq 0$ için (1.2) nin sadece sonlu sayıda tamsayı çözümlerinin olabileceğini ifade ve ispat ederek, Fermat'ın bu özel problemine genel bir cevap vermiştir.

n bir çift tamsayı olmak üzere, Fermat'ın (1.1) denklemi xy -düzleminde bir geometrik şekil olarak, düşünüldüğünde, karemsi bir çembere benzemektedir (Şekil 1.1). Fermat'ın son teoremindeki iddiaya denk olarak, bu karemsi çember üzerindeki rasyonel koordinatlar, sadece dört noktadan $(\mp 1, 0)$ ve $(0, \mp 1)$ den ibarettir. n sayısının tek tamsayı olması durumunda ise, Fermat denklemleri farklılıklar gösterdiği için, n nin çift olması durumunda olduğu gibi, grafiği aynı şekil üzerinde incelemek mümkün değildir. Sırasıyla; $n = 4$ ve $n = 5$ olması durumunda, aşağıdaki Şekil 1.1 ve Şekil 1.2, Fermat denklemlerinin belirlediği eğrileri göstermektedir:



Şekil 1.1 $x^4 + y^4 = 1$



Şekil 1.2 $x^5 + y^5 = 1$

Diophantus denklemlerinin en sade ve basit kısmı,

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = 0 \quad (1.3)$$

formundaki, bir değişkenli polinom denklemlerdir. Burada, $i = 1, 2, \dots, n$ olmak üzere, $a_i \in \mathbb{Z}$ için (1.3) ün tüm tamsayı ve rasyonel sayı çözümlerini belirlemek, Gauss Leması sayesinde, düşünüldüğü kadar zor değildir. Çünkü, p/q , sadeleştirilmiş biçimde verilen, (1.3) ün bir rasyonel çözümü ise, Gauss Leması, $q \mid a_n$ ve $p \mid a_0$ olması gerektiğini ifade eder. Dolayısıyla, bu lemadan yararlanılarak, mümkün olabilecek rasyonel çözümlerin bir listesi elde edilebilir. Bu mümkün çözümlerin hepsi sırayla (1.3) de denenerek, gerçek çözümler belirlenebilir. Böylece, bir değişkenli polinomlar için Diophantus denklemlerinin çözümleri kolayca belirlenmiş olur.

İki değişkenli Diophantus denklemleri için istenen çözümleri belirlemek, bir değişkenli durumdan biraz daha zordur. Bu tür denklemlere örnek olarak, daha önce sözü edilen, Fermat ve Bachet denklemleri verilebilir. Tamsayı katsayılı $f(x, y)$ polinomu için $f(x, y) = 0$ denklemine bakıldığında, doğal olarak şu sorular sorulabilir:

- (a) $f(x, y) = 0$ m hiç tamsayı çözümü var mı?
- (b) $f(x, y) = 0$ m hiç rasyonel sayı çözümü var mı?
- (c) $f(x, y) = 0$ m sonsuz çoklukta tamsayı çözümü var mı?
- (d) $f(x, y) = 0$ m sonsuz çoklukta rasyonel çözümü var mı?

Aşağıda, özel $f(x, y) = 0$ denklemleri için, bu soruların cevapları irdelenmektedir.

F bir cisim ve $f(x, y) \in F[x, y]$ olsun. Bu durumda, $f(x, y) = \sum_{i,j} a_{ij}x^i y^j$ olmak üzere sıfırdan farklı a_{ij} katsayıları arasından, $i + j$ nin en büyük değerine $f(x, y)$ polinomunun *derecesi* denir ve $\deg f$ ile gösterilir. Ayrıca, derecesi üç olan polinoma bir *kübik polinom*, bu polinomun belirlediği eğriye de bir *kübik eğri* adı verilir.

Yukarıdaki, (a) ve (d) sorularının cevaplandırılmasında işe basit polinomlarla, yani derecesi bir olan (iki değişkenli) polinomlarla başlanabilir. Bu tür polinomlara, belirledikleri eğriler doğru biçiminde olduğu için *doğrusal polinomlar* da denir. Katsayıları tamsayı olan, $ax + by = c$ doğrusal denklemi için verilen soruları cevaplamak oldukça kolaydır. Çünkü, sonsuz çoklukta rasyonel çözüm olduğu açıktır. Ayrıca, $\gcd(a, b) \mid c$ ise sonsuz çoklukta tamsayı çözümü var, aksi halde hiç tamsayı çözümü yoktur. Bundan dolayı, doğrusal denklemler için yukarıda verilen soruları cevaplamak, bir değişkenli denklemler için cevaplamaktan daha kolaydır.

Derecesi iki olan ve genelde kuadratik polinomlar olarak adlandırılan $f(x, y)$ polinomları düşünüldüğünde, bunların grafiklerinin koni kesitleri olduğu, analitik geometri bilgilerinden, bilinmektedir. $f(x, y) = 0$ denkleminin bir rasyonel çözüme sahip olması durumunda sonsuz rasyonel çözümü olduğu, geometri kullanılarak kolayca elde edilebilir. Bu nedenle, kuadratik eğrilerin çok basit olduğunu söylemek doğru olmasa bile, bu tür polinom denklemlerin çözümlerinin, genel olarak belirlendiği söylenebilir. Bu da; kuadratik polinomlar için yukarıdaki soruların cevaplandığı anlamına gelmektedir. Ayrıntılı bilgi için (Silverman ve Tate 1992) ye bakınız.

Derecesi üç olan $f(x, y)$ polinomları (yani, kübik polinomlar) için bu polinomların belirledikleri eğrilerin çoğunun (eliptik eğri adı verilen eğrilerin) üzerinde sonlu çoklukta tamsayı koordinatlı noktalar olduğu bilinmektedir (Siegel 1926). Böylece, genel olarak kübik denklemler için (a) ve (c) soruları cevaplandırılmış olur. Dolayısıyla, burada tamsayı katsayılı kübik denklemlerin rasyonel çözümlerinin olup

olmadığı önem taşır. Bunun için, bu tezin esas konusu Diophantus denklemlerinin özel bir kısmını oluşturan, bazı kübik denklemlerin rasyonel çözümlerini, yani, eliptik eğriler adı verilen eğriler üzerindeki rasyonel noktaları incelemekten ibarettir.

1.1. Projektif Düzlem ve Eliptik Eğriler

Bu tezin konusu; eliptik eğriler üzerindeki rasyonel noktaları incelemek olduğu için, bu bölümde konu ile ilgili temel kavramlar ve ön bilgiler tanıtılacaktır.

Tanım 1.1.1 : F bir cisim ve $f(x, y) \in F[x, y]$ olmak üzere

$$\mathcal{C}_f(\mathbf{F}) = \{ (a, b) : a, b \in F \text{ ve } f(a, b) = 0 \}$$

kümesine, F cismi üzerinden $f(x, y)$ polinomunun belirlediği eğri denir.

Özel olarak, F cismi yerine rasyonel sayılar cismi olan $\mathbf{Q}$ alındığında;

$$\mathcal{C}_f(\mathbf{Q}) = \{ (a, b) \in \mathbf{Q}^2 : f(a, b) = 0 \}$$

kümesine $f(x, y)$ nin belirlediği *rasyonel eğri* ve $(a, b) \in \mathcal{C}_f(\mathbf{Q})$ noktasına da bir *rasyonel nokta* adı verilir.

Tanım 1.1.2 : $f(x, y) \in F[x, y]$ ve $\deg f = n$ olsun. Bu takdirde, $f(x, y) = g(x, y).h(x, y)$ ve $1 \leq \min\{\deg g, \deg h\} < n$ olacak şekilde $g(x, y), h(x, y) \in F[x, y]$ varsa, $f(x, y)$ polinomuna F üzerinden *indirgenabilir* bir polinom, aksi halde F üzerinden *indirgenemez* bir polinomdur denir.

Örneğin; $f(x, y) = x^3 + 2x^2y + xy^2 + 3xy + 2x^2 + y^2 + x + y$ kübik polinomu $f(x, y) = (x^2 + xy + x + y)(x + y + 1)$ olarak ifade edilebildiği için $f(x, y)$ polinomu $\mathbf{Q}$ da (dolayısıyla, $\mathbf{R}$ ve $\mathbf{C}$ de) indirgenebilir bir polinomdur.

Eliptik eğrileri belirlemede önemli bir yere sahip olan izdüşümsel (projektif) düzlem aşağıdaki gibi tanımlanır.

Tanım 1.1.3 : $(x, y, z), (x', y', z') \in \mathbf{F}^3 \setminus \{(0, 0, 0)\}$ için “ $\sim$ ” bağıntısı;

$$(x, y, z) \sim (x', y', z') \iff \exists t \in \mathbf{F} \setminus \{0\} \ni x = tx', y = ty', z = tz'$$

olacak biçimde tanımlandığında. “ $\sim$ ” nın bir denklik bağıntısı olduğu (yansıma, simetri, geçişme özelliklerini sağladığı) açıktır. Bu durumda; “ $\sim$ ” bağıntısının $\mathbf{F}^3 \setminus \{(0, 0, 0)\}$ üzerinde oluşturduğu denklik sınıfları kümesi *izdüşümsel düzlem* veya *projektif düzlem* adı verilerek $\mathcal{P}_2(\mathbf{F})$ ile gösterilir. Yani,

$$\mathcal{P}_2(\mathbf{F}) \equiv (\mathbf{F}^3 \setminus \{(0, 0, 0)\}) / \sim$$

dır. Ayrıca: (x, y, z) yi içeren denklik sınıfı (X, Y, Z) ya da $X : Y : Z$ ile gösterilir. Burada, $\mathcal{P}_2(\mathbf{F})$ nin tanımından dolayı, $0 : 0 : 0$ noktasının $\mathcal{P}_2(\mathbf{F})$ nin bir elemanı olmadığı açıktır.

Reel düzlemdeki eğrilerle $\mathcal{P}_2(\mathbf{F})$ deki eğriler arasında bire-bir bir eşleme vardır. (Çünkü; $\deg f = n$ ve $a_{ij} \in \mathbf{F}$ olmak üzere $f(x, y) = \sum_{i,j} a_{ij} x^i y^j$ polinomunun belirlediği eğri $\mathcal{C}_f(\mathbf{F})$ ile gösterilecek olursa $\mathcal{P}_2(\mathbf{F})$ de bu eğriye karşılık gelecek eğri $\mathcal{C}_f^*(\mathbf{F})$ ile gösterilmek üzere $\mathcal{C}_f^*(\mathbf{F})$ eğrisi, $f(x, y)$ polinomunun homojenleştirilmesi dönüşümü adı verilen, bir dönüşüm ile elde edilen polinomun belirlediği eğridir. Kısacası;

$$F(X, Y, Z) = f\left(\frac{X}{Z}, \frac{Y}{Z}\right) \cdot Z^n = \sum_{i,j} a_{i,j} X^i Y^j Z^{n-i-j}$$

olmak üzere;

$$\mathcal{C}_f^*(\mathbf{F}) = \{ (X, Y, Z) : F(X, Y, Z) = 0 \}$$

eğrisi, projektif düzlemde $\mathcal{C}_f(\mathbf{F})$ ye karşılık gelen eğridir.

Yukarıdaki dönüşümün bu şekilde yani; $f(x, y)$ polinomunun homojenleştirilmesi ile tanımlanmasının esas nedeni, $(X, Y, Z) \in \mathcal{P}_2(\mathbf{F})$ için $F(X, Y, Z) = 0$ m temsilci seçiminden bağımsız olmasını sağlamaktır.

Benzer biçimde; $F(X, Y, Z) = 0$ m $\mathcal{P}_2(\mathbf{F})$ de oluşturduğu eğri olan $\mathcal{C}_f^*(\mathbf{R})$ ye karşılık, $F(X, Y, Z)$ nin dehomojenleştirilmesi dönüşümü adı verilen bir dönüşüm ile elde edilen $f(x, y)$ polinomunun oluşturduğu, $\mathcal{C}_f(\mathbf{F})$ eğrisi karşılık gelir. Yani;

$$f(x, y) = F(x, y, 1)$$

olmak üzere $\mathcal{C}_f^*(\mathbf{F})$ eğrisine, projektif düzlemde

$$\mathcal{C}_f(\mathbf{F}) = \{ (x, y) \in \mathbf{F}^2 : f(x, y) = 0 \}$$

eğrisi karşılık gelir.

Burada, $\mathcal{C}_f^*(\mathbf{F})$ nin üçüncü projektif koordinatı sıfır olan noktalarına sonsuzdaki noktalar adı verilir. $\mathcal{C}_f^*(\mathbf{F})$ nin sonsuzdaki noktaları dışındaki tüm noktaları; $X : Y : 1$ biçimindedir ve $\mathcal{C}_f(\mathbf{F})$ nin noktaları ile bu noktalar arasında bire-bir bir eşleme vardır. $\mathcal{C}_f^*(\mathbf{F})$ nin sonsuzdaki noktaları $\mathcal{C}_f(\mathbf{F})$ nin sonsuzdaki noktasına karşılık gelir. Diğer yandan; $\mathcal{C}_f(\mathbf{F})$ nin (x, y) noktası $\mathcal{C}_f^*(\mathbf{F})$ nin $X : Y : 1$ noktası ile özdeşlenerek $\mathcal{C}_f(\mathbf{F})$ eğrisi $\mathcal{C}_f^*(\mathbf{F})$ nin bir alt kümesi (veya parçası) olarak düşünülebilir. Bundan böyle, $\mathcal{C}_f(\mathbf{F})$ daima $\mathcal{C}_f^*(\mathbf{F})$ nin altkümesi olarak düşünülecektir.

Tanım 1.1.4 : $(x_0, y_0) \in \mathcal{C}_f(\mathbf{R})$ ve $i, j \in \mathbf{N} \cup \{0\}$ olmak üzere, $\forall i + j < k$ için

$$\left(\frac{\partial}{\partial x}\right)^i \left(\frac{\partial}{\partial y}\right)^j f(x, y) \Big|_{(x_0, y_0)} = 0$$

koşulunu sağlayan en büyük k tamsayısına (x_0, y_0) noktasının *katlılığı* denir. $k = 1$ ise, (x_0, y_0) noktasına *basit nokta*, aksi halde *tekil (singüler) nokta* veya *k katlı nokta* denir. Eğer, $\mathcal{C}_f(\mathbf{R})$ nin hiç tekil noktası yok ise, $\mathcal{C}_f(\mathbf{R})$ *tekil olmayan (nonsingüler) eğri* olarak adlandırılır.

Benzer biçimde, projektif eğri üzerindeki tekil nokta tanımı da aşağıdaki gibi verilebilir:

$(X_0, Y_0, Z_0) \in \mathcal{C}_f^*(\mathbf{R})$ ve $i, j, l \in \mathbf{N} \cup \{0\}$ olmak üzere, $\forall i + j + l < k$ için

$$\left(\frac{\partial}{\partial X}\right)^i \left(\frac{\partial}{\partial Y}\right)^j \left(\frac{\partial}{\partial Z}\right)^l F(X, Y, Z)|_{(X_0, Y_0, Z_0)} = 0$$

koşulunu sağlayan en büyük k tamsayısına (X_0, Y_0, Z_0) noktasının *katlılığı* denir. Eğer $k = 1$ ise, (X_0, Y_0, Z_0) noktasına $\mathcal{C}_f^*(\mathbf{R})$ nin bir *basit noktası*, aksi halde, söz konusu noktaya $\mathcal{C}_f^*(\mathbf{R})$ nin bir *tekil noktası* veya *k katlı noktası* denir. Ayrıca, $\mathcal{C}_f^*(\mathbf{R})$ nin hiç tekil noktası yok ise, $\mathcal{C}_f^*(\mathbf{R})$ ye *tekil (noktası) olmayan eğri* denir.

Bir $\mathcal{C}_f(\mathbf{R})$ eğrisi ile projektif düzlemde buna karşılık gelen $\mathcal{C}_f^*(\mathbf{R})$ eğrisinin tekil noktaları arasında aşağıdaki gibi bir ilişki vardır:

(X_0, Y_0, Z_0) noktası $\mathcal{C}_f^*(\mathbf{R})$ nin bir tekil noktası ise, iki durum söz konusudur:

i) $Z_0 \neq 0$ ise, $(\frac{X_0}{Z_0}, \frac{Y_0}{Z_0})$ noktası $\mathcal{C}_f(\mathbf{R})$ nin bir tekil noktasıdır.

ii) $Z_0 = 0$ ise, $\mathcal{C}_f(\mathbf{R})$ nin sonsuzdaki noktası bir tekil noktadır.

Örnek 1.1.1: $f(x, y) = y^2 - x^3 - x^2$ nin belirlediği eğrinin tekil noktaları belirlenmek istensin. Burada, $\mathcal{C}_f(\mathbf{R})$ nin sonsuzdaki noktası dışındaki noktaları arasında,

$$\frac{\partial f}{\partial x}(x, y) = -3x^2 - 2x = 0 \text{ için } x = 0 \text{ veya } x = -\frac{2}{3},$$

$$\frac{\partial f}{\partial y}(x, y) = 2y = 0 \text{ için } y = 0$$

ve $f(0, 0) = 0$ $f(-\frac{2}{3}, 0) \neq 0$ olduğundan dolayı, $(0, 0)$ noktası eğrinin bir tekil noktasıdır. Sonsuzdaki noktanın tekil nokta olup olmadığını incelemek için de reel izdüşümsel koordinatlara geçildiğinde

$$F(X, Y, Z) = Y^2 Z - X^3 - X^2 Z$$

ve böylece,

$$\frac{\partial F}{\partial X}(X, Y, Z) = -3X^2 - 2XZ,$$

$$\frac{\partial F}{\partial Y}(X, Y, Z) = 2YZ,$$

$$\frac{\partial F}{\partial Z}(X, Y, Z) = Y^2 - X^2$$

ifadeleri elde edilir. Son dört ifadenin sıfıra eşitlenmesiyle, $(0, 0, Z)$ nin $\mathcal{C}_f^*(\mathbf{R})$ nin tekil noktası olduğu görülür. $Z = 0$ için $(0, 0, 0) \notin \mathcal{P}_2(\mathbf{R})$ olduğundan dolayı, $Z \neq 0$ olmalıdır. Böylece, $\mathcal{C}_f^*(\mathbf{R})$ nin tekil noktasının $(0, 0, 1)$ olduğu görülür ve bu da $\mathcal{C}_f(\mathbf{R})$ nin tekil noktasının sadece $(0, 0)$ noktasından ibaret olduğunu gösterir.

Sonuç olarak, $\mathcal{C}_f(\mathbf{R})$ nin tekil noktalarını belirlemek yerine $\mathcal{C}_f^*(\mathbf{R})$ nin tekil noktalarını belirlemek yeterlidir. Tabii ki, burada $(0, 0, 0) \notin \mathcal{P}_2(\mathbf{R})$ olduğu gözönünde bulundurulmalıdır.

Tanım 1.1.5 : $f(x, y)$ reel katsayılı kübik bir polinom olmak üzere, eğer $f(x, y)$ polinomu $\mathbf{R}$ üzerinde indirgenemez ve $\mathcal{C}_f^*(\mathbf{R})$ nin $\mathcal{P}_2(\mathbf{R})$ de hiç tekil noktası yok ise, $\mathcal{C}_f(\mathbf{R})$ ye bir *eliptik eğri* denir.

Yukarıdaki tanımlarda reel sayılar cismi yerine herhangi bir F cismi alarak $f(x, y) \in F[x, y]$ için F üzerinden eliptik eğri tanımı da benzer şekilde verilebilir.

Bir çember yayının uzunluğu belirlenirken ortaya çıkan integral, ters trigonometrik fonksiyonlar yardımıyla hesaplanabilir. Elips üzerindeki bir yayın uzunluğu belirlenirken ortaya çıkan integral ise basit fonksiyonlar adı verilen fonksiyonlar yardımıyla hesaplanamaz. Bu integral üzerindeki çalışmalar, eliptik eğri kavramının doğmasına yol açmıştır. Geometrik olarak eliptik eğri ile elipsin pek az benzer özellikleri vardır. Eliptik eğri deyiminin kullanılması bu eğrinin elipse benzemesinden değil, elipsin yay uzunluğu ile ilgili integralden ortaya çıkmış olmasındandır. Elips ile eliptik eğri arasındaki diğer önemli bir fark ta, bir elipsi belirleyen $f(x, y)$ polinomunun derecesinin 2, eliptik eğriyi belirleyen polinomun derecesinin ise 3 olmasıdır.

Bu açıklamalardan sonra, $f(x, y) \in \mathbf{Q}[x, y]$ için $\mathcal{C}_f(\mathbf{R})$ bir eliptik eğri ise, $\mathcal{C}_f(\mathbf{Q})$ nun da bir eliptik eğri olduğu, tanımdan yararlanılarak, kolayca gösterilebilir. Benzer şekilde, $f(x, y) \in \mathbf{R}[x, y]$ ve $\mathcal{C}_f(\mathbf{C})$ bir eliptik eğri ise, $\mathcal{C}_f(\mathbf{R})$ nin de bir eliptik eğri olduğu görülebilir.

Teorem 1.1.1 : $f(x, y)$ kompleks katsayılı bir kübik polinom olmak üzere,

i) $\mathcal{C}_f(\mathbf{C})$ tekil değil ise, $f(x, y)$ $\mathbf{C}$ üzerinde indirgenemez,

ii) $g(x)$ kübik polinom ve $f(x, y) = y^2 - g(x)$ biçiminde ise, $\mathcal{C}_f(\mathbf{C})$ nin tekil noktası olmaması için gerek ve yeter şart, $g(x) = 0$ ın hiç katlı kökünün olmamasıdır.

İspat : i) Kabul edelim ki, $f(x, y)$ $\mathbf{C}$ üzerinde indirgenebilir olsun. Bu durumda, $f(x, y)$ polinomu; $a, b, c \in \mathbf{C}$ ve $q(x, y) \in \mathbf{C}[x, y]$ ikinci dereceden bir polinom olmak üzere

$$f(x, y) = (ax + by + c).q(x, y)$$

biçimindedir. Burada; a veya b den birinin sıfırdan farklı olduğu açıktır. Eğer $b \neq 0$ ise

$$f(x, y) = (y + \frac{a}{b}x + \frac{c}{b}).b.q(x, y)$$

şeklinde; $a \neq 0$ olması durumunda ise, uygun bir şekilde x ve y nin yerleri değiştirilerek,

$$f(x, y) = (y - mx - r).q(x, y), \quad m, r \in \mathbf{C}$$

yazılabilir. $\mathcal{C}_f(\mathbf{C})$ nin tekil noktasının olup olmadığını incelemek için, projektif ko-

ordinatlarda

$$\begin{aligned} F(X, Y, Z) &= f\left(\frac{X}{Z}, \frac{Y}{Z}\right) \cdot Z^3, \\ L(X, Y, Z) &= Y - m \cdot X - r \cdot Z, \\ Q(X, Y, Z) &= q\left(\frac{X}{Z}, \frac{Y}{Z}\right) \cdot Z^2, \end{aligned}$$

olmak üzere;

$$F(X, Y, Z) = L(X, Y, Z) \cdot Q(X, Y, Z)$$

olduğu kolayca görülebilir. Ayrıca,

$$P(X, Z) = Q(X, m \cdot X + r \cdot Z, Z)$$

olarak tanımlandığında, $P(X, Z)$ iki değişkene bağlı karesel formda ifade edilebilir. Bu tür her karesel form ya özdeş olarak sıfırdır ya da $\mathbb{C}$ üzerinde iki lineer formun çarpımı şeklinde yazılabilir. Her iki durumda da, her ikisi birden sıfır olmayan öyle X_0, Y_0 kompleks sayıları vardır ki; $P(X_0, Z_0) = 0$ dır. Şimdi,

$$Y_0 = m \cdot X_0 + r \cdot Z_0$$

olarak tanımlansın. Bu takdirde,

$$L(X_0, Y_0, Z_0) = Q(X_0, Y_0, Z_0) = 0$$

elde edilir. Diğer yandan, $F(X, Y, Z)$ nin kısmi türevleri hesaplandığında,

$$\begin{aligned} \frac{\partial F}{\partial X}(X, Y, Z) &= Q(X, Y, Z) \cdot \frac{\partial L(X, Y, Z)}{\partial X} + L(X, Y, Z) \cdot \frac{\partial Q(X, Y, Z)}{\partial X}, \\ \frac{\partial F}{\partial Y}(X, Y, Z) &= Q(X, Y, Z) \cdot \frac{\partial L(X, Y, Z)}{\partial Y} + L(X, Y, Z) \cdot \frac{\partial Q(X, Y, Z)}{\partial Y}, \\ \frac{\partial F}{\partial Z}(X, Y, Z) &= Q(X, Y, Z) \cdot \frac{\partial L(X, Y, Z)}{\partial Z} + L(X, Y, Z) \cdot \frac{\partial Q(X, Y, Z)}{\partial Z} \end{aligned}$$

olduğundan dolayı, (X_0, Y_0, Z_0) noktası için, $F(X_0, Y_0, Z_0) = 0$ ve

$$\begin{aligned} \frac{\partial F}{\partial X}(X_0, Y_0, Z_0) &= 0, \\ \frac{\partial F}{\partial Y}(X_0, Y_0, Z_0) &= 0, \\ \frac{\partial F}{\partial Z}(X_0, Y_0, Z_0) &= 0 \end{aligned}$$

olduğu kolayca görülebilir. Buradan, (X_0, Y_0, Z_0) ın $\mathcal{C}_f^*(\mathbb{R})$ nin tekil noktası olduğu sonucuna varılır. Eğer, $Z_0 \neq 0$ ise $(\frac{X_0}{Z_0}, \frac{Y_0}{Z_0})$ $\mathcal{C}_f(\mathbb{C})$ nin bir tekil noktası, aksi halde, X_0 ve Y_0 aynı anda sıfır olmadığı için, $\mathcal{C}_f(\mathbb{C})$ nin sonsuzdaki noktası bir tekil noktasıdır. Bu da; $\mathcal{C}_f(\mathbb{C})$ nin tekil noktaya sahip olduğunu gösterir. Böylece, çelişki elde edilir.

ii) $g(x)$ bir kübik polinom ve $f(x, y) = y^2 - g(x)$ biçiminde olmak üzere, eğer " $\mathcal{C}_f(\mathbb{C})$ nin tekil noktası olması için gerek ve yeter şart, $g(x)$ in katlı kökünün olmasıdır" önermesi ispatlanırsa, bu kısmın ispatı yapılmış olur.

($\implies$) : $a, b, c, d \in \mathbb{C}$ olmak üzere $f(x, y)$ polinomu;

$$f(x, y) = y^2 - (ax^3 + bx^2 + cx + d)$$

biçiminde yazılabilir. Buradan, izdüşümsel koordinatlarda

$$F(X, Y, Z) = Y^2 Z - aX^3 - bX^2 Z - cXZ^2 - dZ^3$$

olur. Bu ifadenin kısmi türevleri,

$$\frac{\partial F}{\partial X}(X, Y, Z) = -3aX^2 - 2bXZ - cZ^2 \quad (1.1.1)$$

$$\frac{\partial F}{\partial Y}(X, Y, Z) = 2YZ \quad (1.1.2)$$

$$\frac{\partial F}{\partial Z}(X, Y, Z) = Y^2 - bX^2 - 2cXZ - 3dZ^2 \quad (1.1.3)$$

dir. Kabul edelim ki, $\mathcal{C}_f(\mathbb{C})$ bir tekil noktaya sahiptir. $\mathcal{P}_2(\mathbb{C})$ nin (X_0, Y_0, Z_0) noktası yukarıdaki üç ifadeyi aynı anda sıfır yapan nokta olsun.

$Z_0 = 0$ durumunda (1.1.1) bağıntısından, $-3aX_0^2 = 0$ elde edilir. $g(x)$ kübik polinom olduğu için $a \neq 0$ dir. Dolayısıyla, $X_0 = 0$ olmalıdır. (1.1.3) bağıntısının sıfıra eşit olmasından da $Y_0 = 0$ elde edilir. Sonuç olarak, $(0, 0, 0) \notin \mathcal{P}_2(\mathbb{C})$ olduğundan dolayı, $F(X, Y, Z)$ nin $Z_0 = 0$ için hiç tekil noktasının olmadığı görülür. Dolayısıyla, $Z_0 \neq 0$ olmalıdır. $Z_0 \neq 0$ durumunda (1.1.2) bağıntısının sıfıra eşitlenmesiyle $Y_0 = 0$ elde edilir. Böylece,

$$F(X_0, 0, Z_0) = \frac{\partial F}{\partial X}(X_0, 0, Z_0) = 0$$

özdeşliği ile

$$g\left(\frac{X_0}{Z_0}\right) = g'\left(\frac{X_0}{Z_0}\right) = 0$$

özdeşliği denktir. Bu da, $g(x)$ in $\frac{X_0}{Z_0}$ noktasında katlı kökünün olması demektir.

($\Leftarrow$) : $g(x)$ in a gibi bir katlı kökü varsa, $(a, 0)$ noktasının $\mathcal{C}_f(\mathbb{C})$ nin tekil noktası olduğu kolayca görülebileceğinden dolayı ispat tamamlanmış olur.

Verilen bir $f(x, y)$ kübik polinomunun bir eliptik eğri tanımlayıp tanımlamadığını incelerken, $f(x, y)$ polinomunun indirgenemez olduğunu kanıtlamak zor olabilir. Teorem 1.1.1 in bir sonucu olarak, $f(x, y)$ nin bir eliptik eğri tanımlaması için $\mathcal{C}_f(\mathbb{C})$ nin $\mathcal{P}_2(\mathbb{C})$ de tekil noktası olmadığını göstermek yeterlidir. Ayrıca, buna denk olarak, ileride detaylı bir şekilde açıklanacağı gibi, $f(x, y)$ bir kübik polinom olmak üzere, çeşitli dönüşümlerle

$$f(x, y) = y^2 - (x^3 + ax^2 + bx + c)$$

biçimine indirgenebilir. Burada, Teorem 1.1.1 den yararlanarak, $\mathcal{C}_f(\mathbb{R})$ nin bir eliptik eğri tanımlaması için gerek ve yeter şartın $x^3 + ax^2 + bx + c = 0$ ın katlı kökünün olmaması gerektiği sonucuna varılır ki, bu da verilen eğrinin bir eliptik eğri olup olmadığını araştırırken çok büyük kolaylık sağlar.

Örnek 1.1.1 : $f(x, y) = x^3 - 3x^2 + 2x + y^2 + 2y + 1$ kübik polinomu için $\mathcal{C}_f(\mathbf{Q})$ nun bir eliptik eğri olduğunu iki yolla görelim.

Çözüm 1 : $\mathcal{C}_f(\mathbf{Q})$ nun eliptik eğri olduğunu göstermek için, tanım kullanılacak olursa, öncelikle $f(x, y)$ nin $\mathbf{Q}$ da indirgenemez olduğunu ve $\mathcal{C}_f^*(\mathbf{Q})$ nun $\mathcal{P}_2(\mathbf{Q})$ da tekil olmadığını göstermek gerekir. Bunları ayrı ayrı incelemeyen, Teorem 1.1.1. i) den $\mathcal{C}_f(\mathbf{C})$ nin $\mathbf{P}_2(\mathbf{C})$ de tekil noktaya sahip olmadığını göstermek yeterlidir. Çünkü; bu durumda, $f(x, y)$ nin $\mathbf{C}$ de (dolayısıyla $\mathbf{Q}$ da) indirgenemez olduğu ve $\mathcal{C}_f^*(\mathbf{Q})$ nun tekil noktaya sahip olmadığı gösterilmiş olur. Bu fikirden hareketle, verilen $f(x, y)$ polinomu homojenleştirilerek;

$$F(X, Y, Z) = X^3 - 3X^2Z + 2XZ^2 + Y^2Z + 2YZ^2 + Z^3 \quad (1.1.4)$$

$$\frac{\partial F}{\partial X}(X, Y, Z) = 3X^2 - 6XZ + 2Z^2 \quad (1.1.5)$$

$$\frac{\partial F}{\partial Y}(X, Y, Z) = 2YZ + 2Z^2 \quad (1.1.6)$$

$$\frac{\partial F}{\partial Z}(X, Y, Z) = -3X^2 + 4XZ + Y^2 + 4YZ + 3Z^2 \quad (1.1.7)$$

elde edilir. Kabul edelim ki, (X_0, Y_0, Z_0) noktası yukarıdaki (1.1.4)- (1.1.7) ifadelerini sıfır yapan nokta olsun. Bu durumda; (1.1.6) dan; $Z_0 = 0$ veya $Y_0 = Z_0$ olması gerektiği görülür.

i) $Z_0 = 0$ ise (1.1.5) den $X_0 = 0$ ve (1.1.7) den $Y_0 = 0$ olmalıdır. Bu durumda; $(0, 0, 0) \notin \mathcal{P}_2(\mathbf{C})$ olduğundan eğrinin sonsuzdaki noktasının tekil nokta olmadığı sonucuna varılır.

ii) $Z_0 = -Y_0$ ise ($Z_0 \neq 0$) kabul edebiliriz. Bu eşitlik, (1.1.4) , (1.1.5) ve (1.1.7) de yerleştirilip, sıfıra eşitlenirse sırasıyla

$$X_0^3 + 3X_0^2Y_0 + 2X_0Y_0^2 = 0 \quad (1.1.8)$$

$$3X_0^2 + 6X_0Y_0 + 2Y_0^2 = 0 \quad (1.1.9)$$

$$-3X_0^2 - 4X_0Y_0 = 0 \quad (1.1.10)$$

olduğu görülür. (1.1.9) ve (1.1.10) dan $2Y_0(X_0 - Y_0) = 0$ ve $Y_0 \neq 0$ olduğundan dolayı, $X_0 = Y_0$ olması gerekir. Bu da; (1.1.8) de yerine yerleştirilirse, $X_0 = 0$ ve dolayısıyla $Y_0 = 0, Z_0 = 0$ olmasını gerektirir. $(0, 0, 0) \notin \mathcal{P}_2(\mathbf{C})$ olduğundan, $\mathcal{C}_f(\mathbf{C})$ tekil değil ve dolayısıyla $f(x, y)$ $\mathbf{C}$ üzerinde indirgenemez (Teorem 1.1.1. i) den) olması nedeniyle $\mathcal{C}_f(\mathbf{C})$ bir eliptik eğridir. Diğer yandan, $f(x, y)$ rasyonel katsayılı olması nedeniyle, $\mathcal{C}_f(\mathbf{Q})$ nun da bir eliptik eğri olduğu sonucuna varılır.

Çözüm 2 : $f(x, y) = x^3 - 3x^2 + 2x + y^2 + 2y + 1$ yeniden düzenlenerek,

$$f(x, y) = (y + 1)^2 - (-x^3 + 3x^2 - 2x)$$

biçiminde yazılabilir. Burada, $y + 1$ yerine y ve $-x^3 + 3x^2 - 2x$ kübik polinomu yerine de $q(x)$ yazılırsa, $f(x, y) = y^2 - q(x)$ biçiminde olur. $q(x)$ polinomu,

$q(x) = -x(x-1)(x-2)$ biçiminde olduğundan, $q(x) = 0$ m çakışık kökü yoktur, Teorem 1.1.1 den $\mathcal{C}_f(\mathbf{Q})$ tekil değil ve $f(x, y)$, $\mathbf{Q}$ da indirgenemezdir. Bu da, $\mathcal{C}_f(\mathbf{Q})$ nun bir eliptik eğri olduğunu ve Teorem 1.1.1 in önemini gösterir.

$F(X, Y, Z) \in \mathbf{C}[X, Y, Z]$ olmak üzere, (X_0, Y_0, Z_0) noktası $F(X, Y, Z) = 0$ m belirlediği eğri üzerinde olsun. Bu eğriye (X_0, Y_0, Z_0) noktasında teğet olan doğrunun denklemi; $\frac{\partial F}{\partial X}(X_0, Y_0, Z_0)$, $\frac{\partial F}{\partial Y}(X_0, Y_0, Z_0)$ ve $\frac{\partial F}{\partial Z}(X_0, Y_0, Z_0)$ m hepsi birden sıfır olmamak koşuluyla,

$$\frac{\partial F}{\partial X}(X_0, Y_0, Z_0)(X - X_0) + \frac{\partial F}{\partial Y}(X_0, Y_0, Z_0)(Y - Y_0) + \frac{\partial F}{\partial Z}(X_0, Y_0, Z_0)(Z - Z_0) = 0$$

dır. Yukarıdaki şartlar (X_0, Y_0, Z_0) noktasının $F(X, Y, Z) = 0$ m belirlediği projektif eğrinin tekil bir noktası olmaması demektir. Yukarıda verilen teğet denklemi,

$$\frac{\partial F}{\partial X}(X_0, Y_0, Z_0).X + \frac{\partial F}{\partial Y}(X_0, Y_0, Z_0).Y + \frac{\partial F}{\partial Z}(X_0, Y_0, Z_0).Z = 0$$

biçiminde de ifade edilebilir. Bunun nedeni ise,

$$X.\frac{\partial F}{\partial X}(X, Y, Z) + Y.\frac{\partial F}{\partial Y}(X, Y, Z) + Z.\frac{\partial F}{\partial Z}(X, Y, Z) = (der F).F(X, Y, Z)$$

eşitliğine dayanır. Benzer şekilde, burada $f(x, y) = F(X, Y, 1)$ olmak üzere, (x_0, y_0) noktasında çizilen teğet denklemi ise

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

dır.

Aşağıdaki teorem iki farklı eğrinin farklı kesim noktalarının sayısı hakkında bilgi vermektedir (bu teoremin ispatı (Silverman ve Tate 1992) de bulunabilir):

Teorem 1.1.2 : (Bezout) Ortak çarpanları olmayan f ve g polinomlarının belirledikleri eğriler sırasıyla $\mathcal{C}_f$ ve $\mathcal{C}_g$ eğrileri olsun. Eğer, $\mathcal{C}_f \cap \mathcal{C}_g \neq \{\emptyset\}$ ise katlılık sayılmak üzere bu eğrilerin kesim noktalarının sayısı $der f \cdot der g$ tanedir

Bezout Teoreminden, bir eliptik eğri ile kesişen bir doğrunun (farklı olması gerekmeyen) tam üç tane ortak noktası olacağı sonucu çıkarılır. Bundan dolayı, $\mathcal{C}_f(\mathbf{R})$ bir eliptik eğri ve $P, Q \in \mathcal{C}_f(\mathbf{R})$ için P ve Q dan geçen doğru L olarak adlandırılırsa, L ve $\mathcal{C}_f(\mathbf{R})$ nin üçüncü bir ortak noktası olması gerektiği sonucuna varılır. Teoremden de anlaşıldığı gibi, bu üçüncü noktanın P ve Q dan farklı olması gerekmez. Bu şekilde elde edilen üçüncü nokta, $P * Q$ ile gösterilecek olursa, $*$ işleminin $\mathcal{C}_f(\mathbf{R})$ eliptik eğrisi üzerinde bir ikili işlem tanımladığı kolayca anlaşılabılır. $\mathcal{C}_f(\mathbf{R})$ eliptik eğrisi üzerinde P, Q ve bu şekilde elde edilen $P * Q$ noktaları çakışık olabilir. Bu durumda, L ile $\mathcal{C}_f(\mathbf{R})$ nin P de üç çakışık noktası (yani, kesim katlılığı 3) olur ve bu nokta eğrinin dönüm noktası olarak adlandırılır. Ayrıca, eğer P, Q veya $P * Q$ noktalarından herhangi ikisi (mesela, P ve Q) aynı nokta ise L doğrusu eğriye bu noktada teğettir.

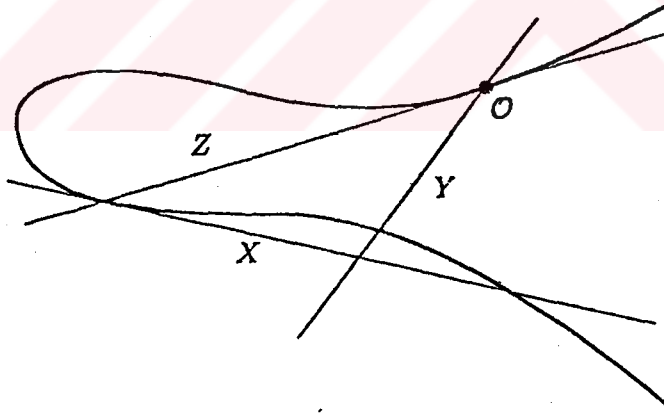
Doğal olarak $*$ ikili işlemiyle beraber, $C_f(\mathbf{R})$ üzerindeki noktaların bir grup oluşturup oluşturmadığı sorusu akla gelebilir. Ne yazık ki, bu sorunun cevabı, $\forall P \in C_f(\mathbf{R})$ için $P * P' = P$ olacak şekilde bir $P' \in C_f(\mathbf{R})$ noktasının olmamasından dolayı olumsuzdur. Buna rağmen, $*$ işleminden yararlanarak $+$ ile gösterilen yeni bir ikili işlemin tanımlanmasıyla $C_f(\mathbf{R})$ üzerindeki noktaların $+$ ikili işlemine göre bir grup oluşturduğunu gösterilebilir. Hatta, $+$ ikili işleminin uygun bir şekilde tanımlanmasıyla $C_f(\mathbf{R})$ nin tüm rasyonel noktalarından oluşan $C_f(\mathbf{Q})$ kümesi bazı şartlar sağlandığında $C_f(\mathbf{R})$ nin bir alt grubunu oluşturur. Böylece elde edilen bu grupların yapıları incelenerek, eliptik eğrilerin rasyonel noktaları hakkında daha fazla bilgi edinilebilir.

Bir rasyonel noktası olan herhangi bir kübik eğri için bu eğriyi oluşturan $f(x, y)$ polinomu, *Weierstrass normal formu* olarak adlandırılan

$$f(x, y) = y^2 - (x^3 + ax^2 + bx + c), \quad a, b, c \in \mathbf{Q} \quad (1.1.11)$$

formuna dönüştürülebilir. Dolayısıyla, eliptik eğrileri incelemek için sadece bu formdaki eliptik eğrilerin incelenmesi yeterli olacaktır. Sözü edilen dönüşümler aşağıda adım adım verilmektedir.

C bir kübik eğri, O da C üzerinde bir rasyonel nokta olsun. Eğriyi belirleyen $f(x, y)$ polinomunun normal formda olacak şekilde projektif düzlemde X, Y, Z koordinatları aşağıdaki gibi tanımlansın: O dan geçen teğet doğrusu Z eksenini, Z nin C yi kestiği diğer noktadan çizilen teğet de X eksenini olsun. Son olarak,



Şekil 1.1.1

O dan geçen ve Z ekseninden farklı herhangi bir doğru da, Y eksenini olarak seçilsin (Şekil 1.1.1 de görüldüğü gibi, burada O noktasının sonsuzdaki nokta olmadığı kabul edildi. Aksi durumda, X eksenini O dan geçmeyen herhangi bir doğru olarak seçilebilir. Eğer, eksenler bu şekilde belirlenip $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$ kabul edilirse, bazı doğrusal koşullar elde edilir. Bu, projektif dönüşüm olarak da adlandırılır. Elde edilen dönüşümler $f(x, y) = 0$ denkleminde yerleştirildiğinde,

$$xy^2 + (ax + b)y = cx^2 + dx + e$$

ve bu denklemin her iki yanının x ile çarpılmasıyla da,

$$(xy)^2 + (ax + b)xy = cx^3 + dx^2 + cx$$

elde edilir. xy yerine yeni bir adlandırma olarak y denirse

$$y^2 + (ax + b)y = cx^3 + dx^2 + cx$$

olur. Bu son eşitliğin sol tarafını bir tam kare yapmak için y yerine $y - \frac{1}{2}(ax + b)$ yazılırsa; $derf = 3$ olmak üzere $y^2 = f(x)$ biçimine dönüşür. Burada, $f(x)$ in başkatsayısı (x^3 ün katsayısı) λ ile işaret edilecek olursa, $\lambda = 1$ olmayabilir, fakat bu durumda x yerine λx , y yerine de $\lambda^2 y$ dönüşümleri uygulanırsa, $f(x)$ başkatsayısı 1 olan kübik bir polinom şekline dönüşür. Böylece, verilen $f(x, y) = 0$ denklemini (1.1.11) normal formuna indirgenmiş olur. Burada istenildiği takdirde, x yerine $x - \frac{a}{3}$ dönüşümü uygulanıp, denklem

$$y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Q}$$

biçiminde de ifade edilebilir.

Bundan sonra, $\mathbb{Q}$ cismi üzerinden bir rasyonel noktası olan kübik eğriler,

$$\mathcal{C} : y^2 = f(x) = (x^3 + ax^2 + bx + c), \quad a, b, c \in \mathbb{Q}$$

formunda düşünülecektir. Burada, $X = d^2x$ ve $Y = d^3y$ için verilen denklem $Y^2 = X^3 + d^2.a.X^2 + d^4.b.X + d^6.c$ olacağından, d sayısının yeteri kadar büyük seçilmesiyle a, b, c rasyonel sayıların paydaları yok edilebilir. Bu nedenle, (1.1.11) de a, b, c katsayılarının birer tamsayı olarak düşünülmesinde bir sakınca yoktur. Bu durumda, $f(x)$ kübik polinomunun diskriminantı $\mathcal{D}_f$ ile işaret edilecek olursa,

$$\mathcal{D}_f = -4a^3.c + a^2.b^2 + 18a.b.c - 4b^3 - 27c^2$$

dir. $A, B \in \mathbb{Z}$ olmak üzere $y^2 = x^3 + Ax + B$ için $\mathcal{D}_f$ nin, $\mathcal{D}_f = -4A^3 - 27B^2$ olacağı açıktır.

Aşağıdaki çizelgede diskriminantı küçük olan bazı eliptik eğriler için $f(x, y)$ nin $y^2 = x^3 + Ax + B$ biçiminde ifade edilebileceği A, B sayıları verilmiştir.

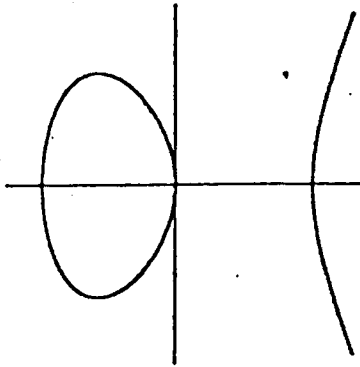
Çizelge 1.1.1 $\mathcal{C}_f(\mathbb{Q})$ nun $y^2 = x^3 + Ax + B$ Formunda İfadesi

$\mathcal{C}_f(\mathbb{Q})$	D_f	A	B
$y^2 + xy + y = x^3 - x^2$	-53	405	16038
$y^2 = x^3 + x^2 + x$	-48	864	-12096
$y^2 = x^3 - x^2 + x$	-48	864	12096
$y^2 + y = x^3 + x^2$	-43	-432	15120
$y^2 + xy = x^3 + x^2 + x$	-39	621	-12690
$y^2 + y = x^3 + x^2 - x$	-35	-1728	30672
$y^2 + y = x^3$	-28	-675	13662
$y^2 + xy - y = x^3$	-27	0	11664
$y^2 + xy + y = x^3$	-26	621	-9774
$y^2 + y = x^3 + x^2 + x$	-19	864	-432
$y^2 + xy = x^3 - 2x^2 + x$	-15	-27	8694
$y^2 + y = x^3 - x^2$	-11	-432	8208
$y^2 + 7xy + 2y = x^3 + 4x^2 + x$	15	-103707	8208
$y^2 + 3xy = x^3 + x$	17	-891	4374
$y^2 + y = x^3 - x$	37	-1296	11664
$y^2 + 2xy - 3y = x^3 - 1$	37	-4320	108432
$y^2 + xy = x^3 - 3x^2 + x$	57	-1977	-29106

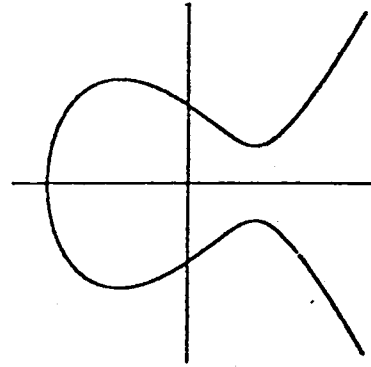
$f(x)$ $\mathbb{C}$ üzerinden çarpanlarına ayrılacak olursa, $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{C}$ olmak üzere $f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ tür. $f(x)$ in diskriminantının

$$D_f = (\alpha_1 - \alpha_2)^2 \cdot (\alpha_1 - \alpha_3)^2 \cdot (\alpha_2 - \alpha_3)^2$$

biçiminde de ifade edilebileceği ve ayrıca $D_f \neq 0$ olması için gerek ve yeter şartın $f(x) = 0$ ın katlı kökünün olmaması gerektiği kolayca görülebilir. Eğer, $\mathcal{C}_f(\mathbb{C})$ bir eliptik eğri ise, $f(x) = 0$ ın farklı kökleri olacağından dolayı, kökler için iki durum söz konusudur:



Şekil 1.1.2.a



Şekil 1.1.2.b

1. Durum : $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}$ (Şekil 1.1.2.a) .

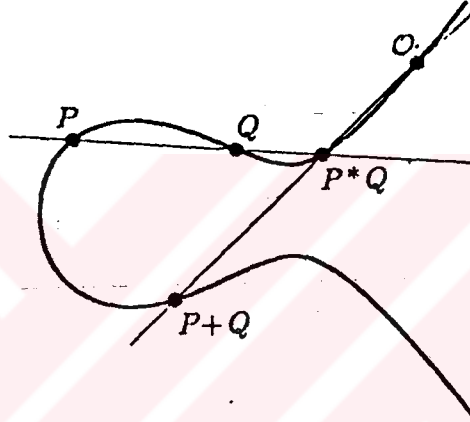
2. Durum : $\alpha_1 \in \mathbb{R}$ ve α_2 ve α_3 karmaşık eşlenik (Şekil 1.1.2.b)

Bu açıklamalardan sonra; $\mathcal{C}_f(\mathbf{R})$ bir eliptik eğri ve $\mathcal{O} \in \mathcal{C}_f(\mathbf{R})$ herhangi bir nokta olmak üzere, $\forall P, Q \in \mathcal{C}_f(\mathbf{R})$ için

$$P + Q = \mathcal{O} * (P * Q)$$

ile $\mathcal{C}_f(\mathbf{R})$ içinde bir $+$ ikili işlemi tanımlanabilir. Bu, geometrik olarak belirlenecek olursa; $P + Q$ noktası, P ve Q dan geçen doğrunun $\mathcal{C}_f(\mathbf{R})$ yi kestiği üçüncü nokta olan $P * Q$ ile $\mathcal{O}$ noktalarından geçen doğrunun $\mathcal{C}_f(\mathbf{R})$ yi kestiği üçüncü nokta olarak tanımlanır (Şekil 1.1.3).

$+$ ikili işleminin $\mathcal{C}_f(\mathbf{R})$ üzerinde iyi tanımlı olduğu kolayca görülebilir. Ayrıca, $\mathcal{O}$ noktasının keyfi seçiminden kaynaklanan herhangi bir sorunun olamayacağı, ilerki kısımlarda gösterilecektir.



Şekil 1.1.3

Aşağıdaki teorem, $\langle \mathcal{C}_f(\mathbf{R}), + \rangle$ nın bir Abel (değişmeli) grubu olduğunu ve $\mathcal{C}_f(\mathbf{Q}) \neq \emptyset$ olmak üzere; $\mathcal{C}_f(\mathbf{Q}) \leq \mathcal{C}_f(\mathbf{R})$ olduğunu ifade eder.

Teorem 1.1.3 : $\mathcal{C}_f(\mathbf{R})$ bir eliptik eğri ve $\mathcal{O}$ noktası bu eğrinin sonsuzdaki noktası da olabilen keyfi bir noktası olsun. Bu durumda, $\forall P, Q \in \mathcal{C}_f(\mathbf{R})$ için $P + Q = \mathcal{O} * (P * Q)$ olarak tanımlandığında;

a) $\mathcal{C}_f(\mathbf{R})$ üzerindeki noktalar $\mathcal{O}$ birim elemanlı bir değişmeli grup oluşturur.

b) $f(x, y)$ rasyonel katsayılı ise $\mathcal{C}_f(\mathbf{Q})$ nun $\mathcal{C}_f(\mathbf{R})$ nin bir altgrubu olması için gerek ve yeter koşul $\mathcal{O}$ noktasının bir rasyonel nokta olmasıdır.

İspat : a) $\langle \mathcal{C}_f(\mathbf{R}), + \rangle$ nın $\mathcal{O}$ birim elemanlı değişmeli bir grup olması için;

i) $\forall P \in \mathcal{C}_f(\mathbf{R})$ için $P + \mathcal{O} = P$,

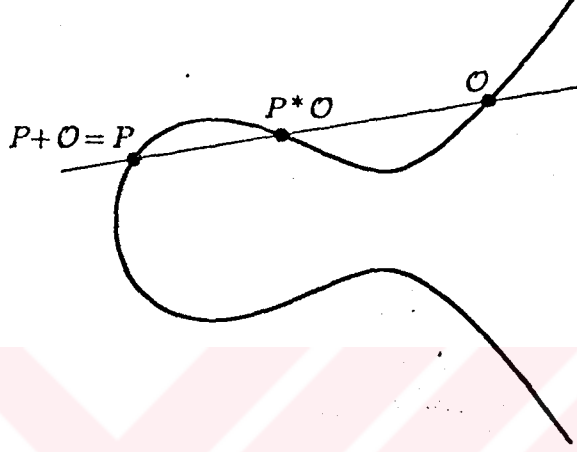
ii) $\forall P, Q \in \mathcal{C}_f(\mathbf{R})$ için $P + Q = Q + P$,

iii) $\forall P \in \mathcal{C}_f(\mathbf{R})$ için $\exists!(-Q) \in \mathcal{C}_f(\mathbf{R}) \ni Q + (-Q) = \mathcal{O}$,

iv) $\forall P, Q, R \in \mathcal{C}_f(\mathbf{R})$ için $(P + Q) + R = P + (Q + R)$

koşullarının sağlanması gerekir.

i) $\mathcal{O} \in \mathcal{C}_f(\mathbf{R})$ için P ve $\mathcal{O}$ dan geçen $\mathcal{D}$ doğrusu $\mathcal{C}_f(\mathbf{R})$ ile üçüncü bir $P * \mathcal{O}$ noktasında kesişir. $P + \mathcal{O} = \mathcal{O} * (P * \mathcal{O})$ olarak tanımlandığından dolayı; $\mathcal{O}$ ve $P * \mathcal{O}$ dan geçen doğru, yukarıda sözü edilen $\mathcal{D}$ doğrusuyla çakışır. Çünkü, iki doğrunun da $\mathcal{O}$ ve $P * \mathcal{O}$ noktaları ortaktır (Şekil 1.1.4). Dolayısıyla;



Şekil 1.1.4

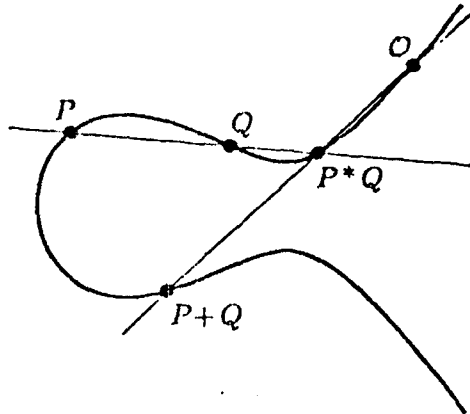
$$P + \mathcal{O} = \mathcal{O} * (P * \mathcal{O}) = P$$

dir.

ii) $\forall P, Q \in \mathcal{C}_f(\mathbf{R})$ için

$$P + Q = \mathcal{O} * (P * Q) = \mathcal{O} * (Q * P) = Q + P$$

olduğu açıktır (Şekil 1.1.5).

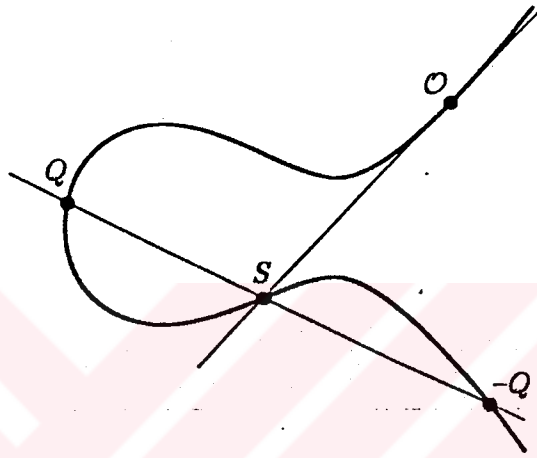


Şekil 1.1.5

iii) $\mathcal{C}_f(\mathbf{R})$ ye $\mathcal{O}$ noktasından çizilen teğet, eğriyi, bu noktada teğet ile $\mathcal{C}_f(\mathbf{R})$ nin çakışık iki ortak noktası olduğundan dolayı, $S = \mathcal{O} * \mathcal{O}$ noktasında keser. Bu durumda, $\forall Q \in \mathcal{C}_f(\mathbf{R})$ için $-Q = Q * S = Q * (\mathcal{O} * \mathcal{O})$ olarak seçilirse;

$$\begin{aligned} Q + (-Q) &= \mathcal{O} * (Q * (-Q)) \\ &= \mathcal{O} * (Q * (Q * (\mathcal{O} * \mathcal{O}))) \\ &= \mathcal{O} * (\mathcal{O} * \mathcal{O}) \\ &= \mathcal{O} \end{aligned}$$

elde edilir (Şekil 1.1.6).



Şekil 1.1.6

$-Q$ nun tektürlü belirli olduğu aşağıdaki gibi gösterilebilir. Kabul edelim ki, $Q + Q' = \mathcal{O}$ ve $-Q \neq Q'$ olacak şekilde bir $Q' \in \mathcal{C}_f(\mathbf{R})$ noktası olsun. Bu durumda;

$$\begin{aligned} Q + Q' = \mathcal{O} &\implies \mathcal{O} * (Q * Q') = \mathcal{O} \\ &\implies \mathcal{O} * (\mathcal{O} * (Q * Q')) = \mathcal{O} * \mathcal{O} \\ &\implies Q * Q' = \mathcal{O} * \mathcal{O} \end{aligned}$$

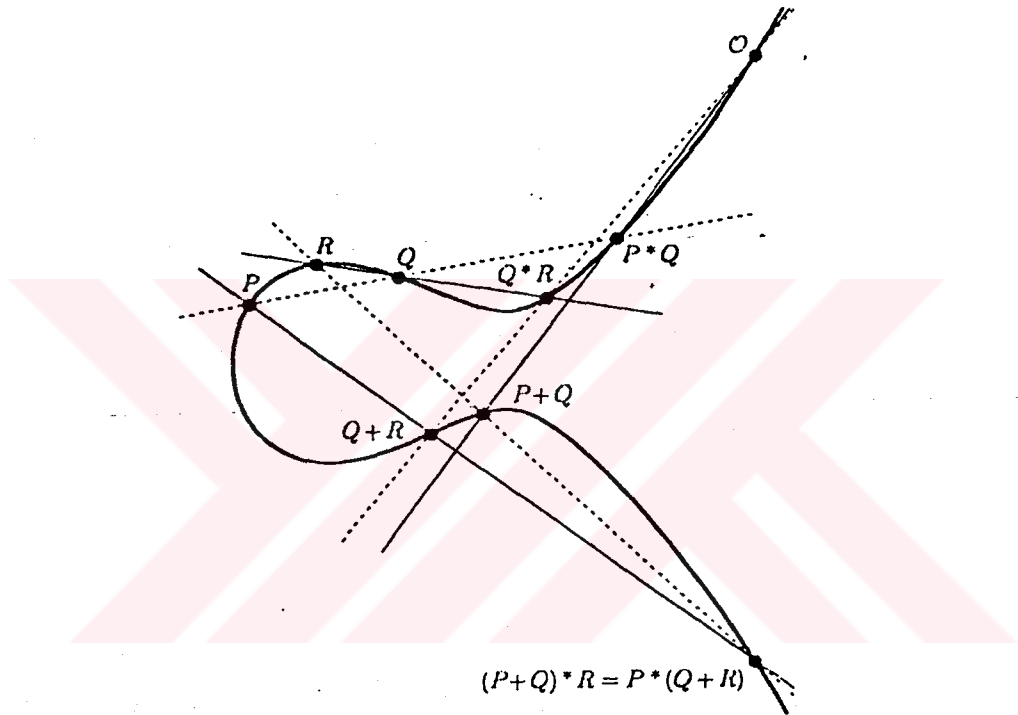
ve $Q' = Q * (Q * Q')$ yazılabileceğinden dolayı, $Q' = Q * (\mathcal{O} * \mathcal{O}) = -Q$ çelişkisi elde edilir. Dolayısıyla, $-Q$ noktası tek türlü belirli olmalıdır.

Birleşme özelliği ile ilgili olan ispata geçmeden önce, ispatta kullanılacak olan bir teoremin ifadesini vereceğiz. Aşağıdaki teoremin ispatı (Siegel ve Tate 1992) de bulunabilir.

Teorem 1.1.3 : (Cayley-Bacharach) C_1 ve C_2 projektif düzlemde ortak bileşenleri olmayan iki kübik eğri ve burada C_1 tekil olmayan bir eğri olsun. Bu eğrilerden farklı bir $\mathcal{D}$ eğrisi $C_1 \cap C_2$ nin, farklı olması gerekmeyen, sekiz noktasından geçerse, $C_1 \cap C_2$ nin dokuzuncu ortak noktasından da geçer.

iv) $P, Q, R \in \mathcal{C}_f(\mathbf{R})$ herhangi üç nokta olmak üzere, $(P+Q)+R = P+(Q+R)$ olduğunu göstermek için $(P+Q) * R = P * (Q+R)$ eşitliğini göstermek yeterlidir. Bunun için, burada kullanılacak teoremlerden biri de yukarıda ifade edilen Kübik

Cayley-Bacharach Teoremi'dir. Verilen $\mathcal{O}, P, Q, R$ noktaları için; $P*Q, P+Q, Q*R$ ve $Q+R$ noktaları geometrik olarak aşağıdaki (Şekil 1.1.7) deki gibi belirlenebilir. Şekil üzerinde de görüldüğü gibi $\mathcal{O}, P, Q, R, P*Q, P+Q, Q*R, Q+R$ noktalarının herbirisi; biri düz çizgili diğeri noktalarla çizilmiş olan iki doğru üzerindedir. $P+Q$ ve R den geçen doğru nokta nokta çizilmiş bir doğru ile $Q+R$ ve P den geçen doğru da düz çizgiyle çizilmiş olsun. Bu iki doğrunun kesim noktasına S denilmesi durumunda $S \in \mathcal{C}_f(\mathbf{R})$ olduğunu göstermek ispatı bitirir. Çünkü, bu durumda, $(P+Q)*R = P*(Q+R)$ eşitliği elde edilmiş olur. Bu fikirden hareketle; $\mathcal{O}, P, Q, R, P*Q, P+Q, Q*R, Q+R, S$ noktalarından dejenere olmuş iki kübik eğrinin geçtiği düşünülebilir.



Şekil 1.1.7

Çünkü, üç doğru denkleminin yanyana getirilip çarpılmasıyla elde edilen denklem bir kübik denklemdir. Bu yüzden; yukarıdaki şekildeki noktalar olarak çizilen üç doğrunun denklemleri çarpımı bir kübik denklem verir, benzer şekilde düz çizgiyle çizilen diğer üç doğru denklemlerinin çarpımı yine bir kübik denklem verir. Bu şekilde elde edilen kübik denklemlerden biri C_1 , diğeri C_2 olsun. $C_1 \cap C_2$ nin dokuz noktası olduğu açıktır. $\mathcal{C}_f(\mathbf{R})$ ile $C_1 \cap C_2$ nin sekiz ortak noktası olduğu bilindiğine göre Kübik Cayley- Bacharach Teoremi'ne göre, $S \in C_1 \cap C_2$ olduğundan dolayı, $S \in \mathcal{C}_f(\mathbf{R})$ olmalıdır. Bu da, $(P+Q)*R = P*(Q+R)$ olduğunu gösterir.

b) $f(x, y)$ nin rasyonel katsayılı bir polinom olması halinde; $\mathcal{C}_f(\mathbf{Q}) \leq \mathcal{C}_f(\mathbf{R}) \iff \mathcal{O} \in \mathcal{C}_f(\mathbf{Q})$ olduğu aşağıdaki gibi gösterilebilir:

($\implies$) : $\mathcal{C}_f(\mathbf{Q})$ nun $\mathcal{C}_f(\mathbf{R})$ nin bir alt grubu olması durumunda $\mathcal{O} \in \mathcal{C}_f(\mathbf{Q})$ olacağı açıktır.

($\Leftarrow$) : $\mathcal{O} \in \mathcal{C}_f(\mathbf{Q})$ olsun. Eğer P, Q rasyonel nokta ise, $P * Q$ da rasyonel nokta olduğundan dolayı, $\forall P, Q \in \mathcal{C}_f(\mathbf{Q})$ için $P + Q = \mathcal{O} * (P * Q) \in \mathcal{C}_f(\mathbf{Q})$ ve $\forall P \in \mathcal{C}_f(\mathbf{Q})$ için $-P = P * (\mathcal{O} * \mathcal{O}) \in \mathcal{C}_f(\mathbf{Q})$ dur. Dolayısıyla, $\mathcal{C}_f(\mathbf{Q}) \leq \mathcal{C}_f(\mathbf{R})$ dir.

Birim eleman olan $\mathcal{O}$ noktasının farklı seçilmesiyle, $\mathcal{C}_f(\mathbf{R})$ eliptik eğrisi üzerinde sonsuz çoklukta farklı toplama işlemi elde edilebilir. Bu, biraz umut kırıcı olabilir, ancak, aşağıdaki teoremin ifadesinden anlaşılacağı gibi, bu toplama işlemleri birbirleriyle yakından ilişkilidir.

Teorem 1.1.4 : $\mathcal{O}$ ve $\mathcal{O}'$ noktaları $\mathcal{C}_f(\mathbf{R})$ eliptik eğrisi üzerinde iki nokta olsun. Bu eğri üzerindeki P ve Q noktaları için $P + Q, \mathcal{O}$ noktasını birim eleman gibi kullanarak tanımlanan toplama işlemi ve $P \oplus Q$ da $\mathcal{O}'$ yü kullanarak tanımlanan toplama işlemi gösterebilir. Bu takdirde, $P \oplus Q = P + Q - \mathcal{O}'$ dir. $\mathcal{G}$, birimi $\mathcal{O}$ olan $\langle \mathcal{C}_f(\mathbf{R}), \oplus \rangle$ grubunu göstermek üzere, $\mathcal{G}$ ile $\mathcal{G}'$ grupları izomorftur, yani $\mathcal{G} \cong \mathcal{G}'$ dir.

İspat : $P \oplus Q = \mathcal{O}' * (P * Q)$ olduğu için

$$\begin{aligned} \mathcal{O}' + (P \oplus Q) &= \mathcal{O}' + \mathcal{O}' * (P * Q) \\ &= \mathcal{O} * (\mathcal{O}' * (\mathcal{O}' * (P * Q))) \\ &= P + Q \end{aligned}$$

olur. $-\mathcal{O}' = \mathcal{O}' * (\mathcal{O} * \mathcal{O})$ olduğu için;

$$P \oplus Q = P + Q + \mathcal{O}' * (\mathcal{O} * \mathcal{O}) = P + Q - \mathcal{O}'$$

olduğu görülür.

Diğer yandan, $\phi : \mathcal{G} \rightarrow \mathcal{G}'$ dönüşümü $\phi(P) = P + \mathcal{O}'$ olarak tanımlandığında,

$$\begin{aligned} \phi(P + Q) &= P + Q + \mathcal{O}' \\ &= (P + \mathcal{O}') + (Q + \mathcal{O}') - \mathcal{O}' \\ &= \phi(P) + \phi(Q) - \mathcal{O}' \\ &= \phi(P) \oplus \phi(Q) \end{aligned}$$

olduğundan dolayı, ϕ dönüşümü bir grup homomorfizmidir. ϕ nin bire-bir ve örten olduğu kolayca görülebilir. Bu nedenle, $\mathcal{G}$ ve $\mathcal{G}'$ izomorf gruplardır.

Teorem 1.1.4 ün bir sonucu olarak, eliptik eğri üzerinde $\mathcal{O}$ noktasının keyfi seçimiyle ilgili elde edilen grupların izomorf gruplar olması nedeniyle bu gruplara tek bir grup gözü ile bakılabilir. Bunun için, eliptik eğri üzerindeki izomorf gruplar $\mathcal{E}_f(\mathbf{R})$ veya $\mathcal{C}(\mathbf{R})$ ile temsil edilebilir. Ayrıca, $f(x, y)$ rasyonel katsayılı ve $\mathcal{C}_f(\mathbf{Q}) \neq \emptyset$ ise $\mathcal{O}$ noktası $\mathcal{O} \in \mathcal{C}_f(\mathbf{Q})$ olacak şekilde seçilebilir. Böylece, Teorem 1.1.4 den, $\mathcal{C}_f(\mathbf{Q})$ altgrupları $\mathcal{C}(\mathbf{Q})$ ile temsil edilecek olursa; $\mathcal{C}(\mathbf{Q}) \leq \mathcal{C}(\mathbf{R})$ olacağı açıktır.

Şimdi, $P, Q, R \in \mathcal{C}(\mathbf{R})$ farklı üç nokta olsun. Bu durumda; bu noktaların doğrudan olmaları için gerek ve yeter şart $P + Q + R = \mathcal{O} * \mathcal{O}$ olması gerektiği sonucu kolayca görülebilir (Niven, Zuckerman ve Montgomery, 1991).

Eliptik eğriyi tanımlayan denklem ve bu eğri üzerindeki P_1 ve P_2 noktalarının koordinatları kullanılarak, $P_1 + P_2$ noktasının koordinatlarını veren formül elde edilebilir.

Daha önce eliptik eğriyi veren denklemin (1.1.11) formunda olduğu ve bu denklemin diskriminantının sıfırdan farklı olması gerektiği vurgulanmıştı. Ayrıca; (1.1.11) ile tanımlanan her eliptik eğri, eğrinin dönüm noktası olan sonsuzdaki $0 : 1 : 0$ noktasını içerdiğinden dolayı, $\mathcal{O}$ noktası sonsuzdaki nokta olarak seçildiğinde, eğri üzerindeki üç noktanın toplamının $\mathcal{O}$ olması için gerek ve yeter şart, bu noktaların doğrudan olmasıdır.

$P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ eliptik eğri üzerinde iki nokta, $P_3 = P_1 + P_2 = (x_3, y_3)$ ve $x_1 \neq x_2$ kabul edelim. P_1 ve P_2 den geçen L doğrusunun eğimine m denilirse; $m = \frac{y_2 - y_1}{x_2 - x_1}$ dir. Eğrinin x - eksenine göre simetrik olmasından dolayı, L ile eğrinin üçüncü ortak noktası $P_1 * P_2 = -P_3 = (x_3, -y_3)$ tür ve L nin denklemi $y = y_1 + m(x - x_1)$ şeklindedir. Bu (1.1.11) de yerleştirilip, x_1 , x_2 , x_3 kökleri bulunabilir:

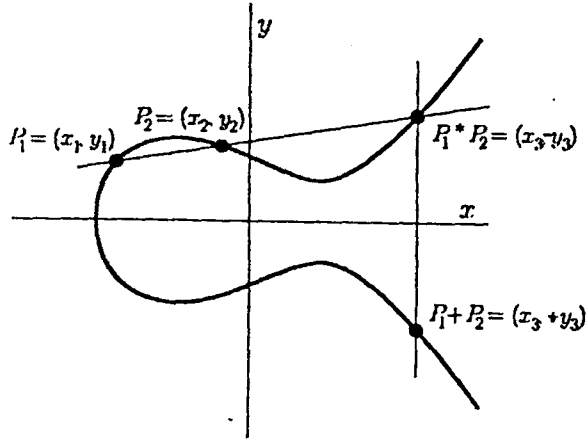
$$x^3 + (a - m^2)x^2 + (b + 2m^2x_1 - 2y_1m)x + (c - (mx_1 - y_1)^2) = 0$$

ve bu denklemin kökleri toplamı; $x_1 + x_2 + x_3 = -(a - m^2)$ olduğu için,

$$x_3 = m^2 - a - x_1 - x_2 \quad (1.1.12)$$

$$y_3 = -y_1 - m(x_3 - x_1) \quad (1.1.13)$$

formülleri elde edilir.



Şekil 1.1.8

Eğer $x_1 = x_2$ ise, ya $y_2 = -y_1$, bu durumda $P_2 = -P_1$ ve $P_1 + P_2 = \mathcal{O}$; ya da $y_2 = y_1$ olur. Bu durumda da, $P_1 = P_2$ olduğundan, $P_3 = 2P_1$ in koordinatlarını veren formül aşağıdaki gibi elde edilebilir:

Eğriye P_1 noktasında teğet olan doğrunun eğimi m olsun. Böylece, analiz

bilgilerinden,

$$m = \frac{3x_1^2 + 2ax_1 + b}{2y_1}$$

olmalıdır. Eğer $y_1 = 0$ ise, doğru dikeydir ve $2P_1 = \mathcal{O}$ dur. Dolayısıyla; $y_1 \neq 0$ için

$$x_3 = m^2 - a - 2x_1 \quad (1.1.14)$$

$$y_3 = -y_1 - m(x_3 - x_1) \quad (1.1.15)$$

formülleri elde edilmiş olur (Şekil 1.1.8).

Örnek 1.1.2 $f(x, y) = y^2 - x^3 + x + \frac{1}{4}$ ün belirlediği eliptik eğri üzerinde $P = (x_1, y_1) = (0, \frac{1}{2})$ olsun. P noktasının katları hesaplanmak istenirse, $2P = (x_3, y_3)$ için (1.1.14) ve (1.1.15) den,

$$m = \frac{3 \cdot 0^2 + 2 \cdot 0 \cdot 0 - 1}{2 \cdot \frac{1}{2}} = -1$$

olur. Böylece,

$$x_3 = (-1)^2 - 0 - 2 \cdot 0 = 1 \quad \text{ve} \quad y_3 = -\frac{1}{2} - (-1) \cdot (1 - 0) = \frac{1}{2}$$

elde edilir. $3P = P + 2P$ olduğundan dolayı, (1.1.12) ve (1.1.13) formüllerinde $(x_1, y_1) = (0, \frac{1}{2})$ ve $(x_2, y_2) = (1, \frac{1}{2})$ alınarak, $3P = (-1, -\frac{1}{2})$ olur. Benzer hesaplamalarla da.

$$4P = (2, -\frac{5}{2}), 5P = (\frac{1}{4}, -\frac{1}{5}), 6P = (6, -\frac{29}{2}), 7P = (-\frac{5}{9}, -\frac{43}{54}), \dots$$

olarak belirlenir.

1.2. Mertebesi Sonlu Olan Rasyonel Noktalar

Bir eliptik eğri üzerindeki mertebesi sonlu olan rasyonel noktaların belirlenmesinde aşağıdaki teorem önemli bir kriter görevini yapar (Silverman ve Tate 1992).

Teorem 1.2.1 : (Nagell-Lutz) $a, b, c \in \mathbf{Z}$ olmak üzere $\mathcal{C}_f(\mathbf{R})$, (1.1.11) in belirlediği eliptik eğri ve $(x_0, y_0) \in \mathcal{C}_f(\mathbf{R})$ sonlu mertebeli bir rasyonel nokta olsun. Bu takdirde, $x_0, y_0 \in \mathbf{Z}$ ve ayrıca ya $y_0 = 0$ ya da $\mathcal{D}_f, f(x)$ in diskriminantı olmak üzere, $y_0^2 | \mathcal{D}_f$ dir.

Nagell-Lutz Teoremi yardımıyla bir eliptik eğri üzerindeki mertebesi sonlu olan bütün rasyonel noktalar belirlenebilir. Bu noktalardan oluşan küme, $\mathcal{C}_f(\mathbf{Q})$ nun bir alt grubunu oluşturur ve bu gruba *burkulma (torsion) grubu* adı verilir. Çoğu zaman bu grup $\text{tors}\mathcal{C}(\mathbf{Q})$ veya $\mathcal{C}(\mathbf{Q})_{\text{sonlu}}$ ile sembolize edilir. Eğri. $y_0^2 \nmid \mathcal{D}_f$ iken başka tamsayı girdili noktaları da içerebilir ama, Siegel Teoremi (Siegel 1926) olarak bilinen bir teoreme göre, böyle noktaların sayısı en fazla sonlu sayıdadır. Bu tezin ikinci bölümünün sonunda, Nagell-Lutz Teoremi ile ilgili uygulamalara yer verilmiştir.

$tors\mathcal{C}(\mathbf{Q})$ grupları aşağıdaki teorem ile tam olarak belirlenmektedir.

Teorem 1.2.2 : (Mazur) $\mathcal{C}_f(\mathbf{Q})$ eliptik eğrisi üzerindeki sonlu mertebeli rasyonel noktalar grubu olan $tors\mathcal{C}(\mathbf{Q})$ aşağıdaki 15 gruptan birisine izomorftur:

$n = 1, 2, \dots, 9, 10, 12$ için $\mathbf{Z}_n$ veya $n = 1, 2, 3, 4$ için $\mathbf{Z}_{2n} \oplus \mathbf{Z}_2$ (Knapp 1992) .

Mazur Teoremi'nde sözü edilen 15 gruba örnek olarak (Bkz. Çizelge 2.6.1).



2. MATERİYAL VE METOD

Bu bölümde bir eliptik eğri üzerindeki rasyonel noktalardan oluşan grubun sonlu üretilmiş bir grup olduğunu; yani, sonlu rasyonel nokta kullanılarak eğri üzerindeki tüm rasyonel noktaların üretilebileceğini, ifade eden Mordell Teoremi ispatlanacaktır. Bunun için aşağıda; bu teoremin ispatında kullanılacak olan yükseklik kavramı açıklanarak, gerekli olan birkaç lemanın ispatına yer verilmiştir.

2.1. Yükseklik Kavramı

Tanım 2.1.1 : $x = \frac{m}{n} \in \mathbf{Q}$ ve $\text{obcb}(|m|, |n|) = 1$ için $H(x) = \max\{|m|, |n|\}$ ye x rasyonel sayısının yüksekliği denir.

Bu tanımdan yararlanarak eğri üzerindeki bir rasyonel noktanın yüksekliği de aşağıdaki gibi tanımlanır.

Tanım 2.1.2 : Bir eliptik eğri üzerindeki bir $P(x, y)$ rasyonel noktası için $H(P) = H(x)$ e bu rasyonel noktanın yüksekliği denir. Ayrıca, eğri üzerindeki $P_0 = (0, y_0)$ rasyonel noktasının yüksekliği 1 olarak tanımlanır, yani $H(P_0) = 1$ dir.

Eliptik eğri üzerindeki bir rasyonel noktanın yüksekliği ile ilgili olarak yapılan çalışmalarda, bu eğri üzerindeki herhangi iki P, R noktası için $H(P + R)$ nin $H(P).H(R)$ yardımı ile hesaplanabildiği sonucuna varılmıştır. Mordell Teoremi'nin ispatı için, burada olduğu gibi çarpımsal değil de, toplamsal özelliği olan bir fonksiyona ihtiyaç duyulacağından dolayı; gerekli olan bu fonksiyon $x \in \mathbf{Q}$ için $h(x) = \log H(x)$ biçiminde tanımlanabilir. Benzer şekilde burada, $P = (x, y) \in \mathcal{C}(\mathbf{Q})$ için $h(P) = \log H(x)$ olacağı açıktır.

2.2. $P + P'$ Noktasının Yüksekliği

Bundan sonraki gösterimlerimizde

$$\mathcal{C} : y^2 = x^3 + ax^2 + bx + c \quad (2.2.1)$$

ifadesi; $a, b, c \in \mathbf{Z}$ olmak üzere $f(x, y) = y^2 - x^3 - ax^2 - bx - c$ nin belirlediği $\mathcal{C}(\mathbf{R})$ eliptik eğrisini belirtecektir.

Lema 2.2.1 : $\forall M \in \mathbf{R}$ için $\{P \in \mathcal{C}(\mathbf{Q}) : h(P) \leq M\}$ kümesi sonludur.

İspat : $P = (x, y) \in \mathcal{C}(\mathbf{Q})$ için $h(P) = \log H(x)$ olarak tanımlandığından dolayı; eğer $\forall M \in \mathbf{R}$ için

$$S = \{P = (x, y) \in \mathcal{C}(\mathbf{Q}) : H(x) \leq e^M\}$$

kümesinin sonlu olduğu gösterilirse ispat yapılmış olur. Bu fikirden hareketle, $w = \lfloor e^M \rfloor$ olarak tanımlansın. Böylece,

$$S = \{P = (x, y) \in \mathcal{C}(\mathbf{Q}) : H(x) \leq e^M\}$$

$$= \{ P = (\frac{a}{b}, \frac{c}{d}) \in \mathcal{C}(\mathbf{Q}) : |a| \leq w, |b| \leq w, \text{obeb}(|a|, |b|) = 1 \}$$

olacağından ve istenen özellikleri sağlayan $(\frac{a}{b}, \frac{c}{d}) \in \mathcal{C}(\mathbf{Q})$ noktalarının sonlu sayıda olması gerektiğinden dolayı, $\forall M \in \mathbf{R}$ için $\{P \in \mathcal{C}(\mathbf{Q}) : h(P) \leq M\}$ nin sonlu olduğu sonucuna varılır.

Lema 2.2.2 : P' , $\mathcal{C}$ eliptik eğrisi üzerinde bir rasyonel nokta ise, a, b, c ve P' ye bağlı öyle bir k' sabiti vardır ki; $\forall P \in \mathcal{C}(\mathbf{Q})$ için

$$h(P + P') \leq 2h(P) + k'$$

eşitsizliği sağlanır.

İspat : Bu ispata başlamadan önce bazı hatırlatmalar yapmak gerekiyor. Bunlardan birincisi; her $P = (x, y) \in \mathcal{C}(\mathbf{Q})$ için $\text{obeb}(m, e) = \text{obeb}(n, e) = 1$ olacak şekilde öyle $m, n, e \in \mathbf{Z}$ ve $e > 0$ tamsayıları vardır ki; $x = \frac{m}{e^2}$, $y = \frac{n}{e^3}$ biçimindedir. Kısacası; $P = (x, y) \in \mathcal{C}(\mathbf{Q})$ nun koordinatlarının her birinin en sadeleştirilmiş biçimde yazılması durumunda; x in paydası bir tamsayının karesi, y nin paydası ise bu tamsayının küpü şeklindedir. Bunu görmek için; $M > 0$, $N > 0$ olmak üzere $x = \frac{m}{M}$ ve $y = \frac{n}{N}$ olsun. Bu ifadeler (2.2.1) denkleminde yerleştirildiğinde,

$$\frac{n^2}{N^2} = \frac{m^3}{M^3} + a \frac{m^2}{M^2} + b \frac{m}{M} + c$$

elde edilir. Burada paydaların eşitlenmesiyle de

$$M^3 n^2 = N^2 m^3 + a N^2 M m^2 + b N^2 M^2 m + c N^2 M^3 \quad (2.2.2)$$

olur. N^2 , (2.2.2) eşitliğinin sağ tarafındaki ifadeyi böldüğünden dolayı, $N^2 \mid M^3 n^2$ olmalı ve buradan, $\text{obeb}(n, N) = 1$ olması nedeniyle de $N^2 \mid M^3$ sağlanmalıdır. Diğer yandan, (2.2.2) den $M \mid N^2 m^3$ olması gerektiği ve $\text{obeb}(m, M) = 1$ olduğundan dolayı da $M \mid N^2$ olacağı açıktır. Buna dayanarak; (2.2.2) eşitliğinden $M^2 \mid N^2 m^3$ ve böylece $M \mid N$ olacağı görülür. Son olarak yine (2.2.2) den $M^3 \mid N^2 m^3$ olması gerektiğinden dolayı, $M^3 \mid N^2$ olmalıdır. Bu şekilde elde edilen $N^2 \mid M^3$ ve $M^3 \mid N^2$ özelliklerinden dolayı, $M^3 = N^2$ ve böylece $M \mid N$ olacağı açıktır. $e = \frac{N}{M}$ olmak üzere,

$$e^2 = \frac{N^2}{M^2} = \frac{M^3}{M^2} = M \quad \text{ve} \quad e^3 = \frac{N^3}{M^3} = \frac{N^3}{N^2} = N$$

eşitliklerinden, (x, y) koordinatlarının istenen biçimde, yani $x = \frac{m}{e^2}$, $y = \frac{n}{e^3}$ biçiminde yazılabileceği sonucuna varılır.

İkinci hatırlatma olarak; $P = (\frac{m}{e^2}, \frac{n}{e^3}) \in \mathcal{C}(\mathbf{Q})$ ve a, b, c (2.2.1) de ifade edilen katsayılar olmak üzere, bu katsayılarla bağlı öyle bir $K > 0$ sabiti vardır ki;

$$|n| \leq K.H(P)^{\frac{3}{2}}$$

eşitsizliği sağlanır.

Bu ifadenin kanıtı kısaca aşağıdaki gibi verilebilir:

$P = (\frac{m}{e^2}, \frac{n}{e^3})$ ün koordinatları, (2.2.1) de yerleştirilip, e^6 ile çarpıldığında

$$n^2 = m^3 + ac^2m^2 + bc^4m + ce^6$$

olduğu görülür. Bu eşitliğin her iki yanının mutlak değeri alınıp, üçgen eşitsizliği uygulanırsa;

$$\begin{aligned} |n^2| &\leq |m^3| + |ac^2m^2| + |bc^4m| + |ce^6| \\ &\leq H(P)^3 + |a|H(P)^3 + |b|H(P)^3 + |c|H(P)^3 \end{aligned}$$

olduğu görülür. Böylece; $K = \sqrt{1 + |a| + |b| + |c|}$ olmak üzere istenen eşitsizliğin sağlandığı sonucuna varılır.

Yukarıda yapılan bu hatırlatmalardan sonra, bu adımda, sadece eliptik eğri üzerindeki iki noktanın toplamı için kullanılan formülü yazıp, üçgen eşitsizliğini uygulamaktan ibaret olan Lema 2.2.2 nin ispatına geçilebilir: $P' \in \mathcal{C}(\mathbf{Q})$ ve $P' = \mathcal{O}$ ise, $\forall P \in \mathcal{C}(\mathbf{Q})$, $k' = 0$ için $h(P + P') \leq 2h(P) + k'$ olacağından dolayı istenenler sağlanır. Ayrıca; lemanın $P' \neq \mathcal{O}$ için, $\forall P \in \mathcal{C}(\mathbf{Q}) \setminus \{\mathcal{O}, P', -P'\}$ için ispatlanmasının yeterli olduğu açıktır. Bundan dolayı; $P' = (x', y') \neq \mathcal{O}$ eğri üzerinde bir sabit nokta, $P = (x, y) \in \mathcal{C}(\mathbf{Q})$ ve $P \notin \{\mathcal{O}, P', -P'\}$ için, $x \neq x'$ olacağından, iki noktanın toplamında belirlenen toplam formülü kullanılabilir; yani, $P + P' = (\xi, \eta)$ olmak üzere $h(P + P') = h(\xi)$ olacağından dolayı; ξ için (x', y') ve (x, y) den yararlanarak bir formül elde edilebilir. Birinci bölümde ifade edilen toplam formüllerinden;

$$\begin{aligned} \xi &= \frac{(y - y')^2}{(x - x')^2} - a - x - x' \\ &= \frac{(y - y')^2 - (x - x')^2(x + x' + a)}{(x - x')^2} \end{aligned}$$

olur. Paydadaki çarpma işlemleri yapıp $y^2 - x^3$ yerine $ax^2 + bx + c$, $y'^2 - x'^3$ yerine $ax'^2 + bx' + c$ yazılırsa; A, B, C, D, E, F, G sayıları (x', y') ve a, b, c nin terimlerine bağlı belli rasyonel sayılar olmak üzere,

$$\xi = \frac{Ay + Bx^2 + Cx + D}{Ex^2 + Fx + G} \quad (2.2.3)$$

biçiminde ifade edilebilir. Burada, ξ nin pay ve paydası $A, B, \dots, G$ nin paydalarının *okek* i ile çarpılırsa, $A, B, \dots, G$ ler tamsayı olarak da düşünülebilir. Burada önemli olan nokta, eğri ve P' noktasının belirli olması ve ayrıca (2.2.3) eşitliğinin $\{\mathcal{O}, P, P'\}$ dışındaki tüm P noktaları için sağlanıyor olmasıdır. Bu nedenle, ileride tanımlanacak olan k' sabiti $A, B, \dots, G$ ye bağlı, ama (x, y) ye bağlı olmayacak şekilde seçilebilir.

(2.2.3) de $x = \frac{m}{e^2}$, $y = \frac{n}{e^3}$ ifadeleri yerleştirilip, elde edilen ifadenin pay ve paydası e^4 ile çarpıldığında,

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

eşitliği elde edilebilir. Burada pay ve paydanın birer tamsayı olacağı açıktır, ama bu sayıların aralarında asal olup olmadıkları hakkında herhangi bir bilgi elimizde yoktur. Bunun için, ξ nin yüksekliğini hesaplamak için tanım kullanılamaz ama

$$H(\xi) \leq \max\{|Anc + Bm^2 + Cmc^2 + Dc^4|, |Em^2 + Fmc^2 + Gc^4|\}$$

yazılabilir. Burada, $c \leq H(P)^{\frac{1}{2}}$, $m \leq H(P)$ ve k sadece a, b, c katsayılarına bağlı olmak üzere $|n| \leq KH(P)^{\frac{3}{2}}$ olduğu için, üçgen eşitsizliğinden

$$\begin{aligned} |Anc + Bm^2 + Cmc^2 + Dc^4| &\leq |Anc| + |Bm^2| + |Cmc^2| + |Dc^4| \\ &\leq (|AK| + |B| + |C| + |D|)H(P)^2 \\ |Em^2 + Fmc^2 + Gc^4| &\leq |Em^2| + |Fmc^2| + |Gc^4| \\ &\leq (|E| + |F| + |G|)H(P)^2 \end{aligned}$$

eşitsizlikleri elde edilir. Böylece,

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

olur ve buradan her iki tarafın logaritması alınırsa; k' sabiti

$$k' = \log \max\{|AK| + |B| + |C| + |D|, |E| + |F| + |G|\}$$

biçiminde; (x', y') , a, b, c ye bağlı, fakat $P = (x, y)$ den bağımsız olarak seçildiğinde

$$h(P + P') \leq 2h(P) + k'$$

olur, bu da ispatı bitirir.

2.3. 2 P Noktasının Yüksekliği

Bir önceki kısımda $P + P'$ yüksekliğinin yaklaşık olarak P nin yüksekliğinin iki katından daha küçük olduğu Lema 2.2.2 nin ispatıyla verildi. Bu kısımda ise $2P$ nin yüksekliğinin P nin yüksekliğinin dört katından daha büyük olduğunu ifade eden lemanın ispatına yer verilecektir.

Lema 2.3.1 : (2.2.1) de ifade edilen a, b, c katsayılarına bağlı öyle bir k sabiti vardır ki; $\forall P \in \mathcal{C}(\mathbf{Q})$ için,

$$4h(P) \leq h(2P) + k$$

eşitsizliği sağlanır.

İspat : $\mathcal{C}(\mathbf{Q})$ kümesinin sonlu olması durumunda, k sabitinin $\forall P \in \mathcal{C}(\mathbf{Q})$ için $4h(P) \leq k$ olacak şekilde seçilmesiyle istenilenler sağlanır. $\mathcal{C}(\mathbf{Q})$ nun sonlu olup olmadığı hakkında herhangi bir bilgi verilmediğinden dolayı ispat yapılmış sayılamaz, ama eğri üzerinde mertebesi iki olan, yani $2P = \mathcal{O}$ özelliğindeki, noktaların sonlu sayıda olması nedeniyle, yukarıdaki açıklamaya dayanarak, bu tür noktaların ispat dışında bırakılmasında herhangi bir mahsur bulunmamaktadır. Bunun için, ispatı $2P \neq \mathcal{O}$ olan P noktaları için yapmak yeterli olacaktır. Bu kabulden hareketle;

$P = (x, y)$ ve $\mathcal{O} \neq 2P = (\xi, \eta)$ olsun. İki noktanın toplamının koordinatlarını veren, toplam formülleri kullanılarak,

$$\begin{aligned}\xi &= \frac{(3x^2 + 2ax + b)^2}{(2y)^2} - a - 2x \\ &= \frac{(f'(x))^2 - 4ay^2 - 8xy^2}{4y^2}\end{aligned}$$

ifadesinde, y^2 yerine $x^3 + ax^2 + bx + c$ yazılıp, payda yok edilirse;

$$\begin{aligned}\xi &= \frac{(f'(x))^2 - (8x + 4a) \cdot f(x)}{4 \cdot f(x)} \\ &= \frac{x^4 + \dots}{4 \cdot x^3 + \dots}\end{aligned}$$

biçiminde ifade edilebilir. Burada, $2P \neq \mathcal{O}$ olduğundan dolayı, $f(x) \neq 0$ ve $y^2 = f(x)$ in belirlediği eğri bir eliptik eğri olacağı için, $f(x)$ in hiç katlı kökü yoktur, yani, $f(x)$ ve $f'(x)$ in ortak kökü yoktur. Böylece, tamsayı katsayılı iki polinomun bölümü şeklinde ifade edilebilen ξ nin, pay ve paydasının hiç ortak kökünün olmadığı sonucuna varılır.

$h(P) = h(x)$ ve $h(2P) = h(\xi)$ olduğundan, eğer $4h(x) \leq h(\xi) + k$ olduğu gösterilebilirse, ispat bitmiş olur; bunun için de polinomların bölümü ve bunların yükseklikleri ile ilgili olan aşağıdaki lemaya ihtiyaç duyulur:

Lema 2.3.1* : $\phi(x)$ ve $\psi(x)$ ortak kökleri olmayan tamsayı katsayılı iki polinom ve ayrıca $d = \max\{ \text{der}\phi(x), \text{der}\psi(x) \}$ olsun. Bu durumda,

(a) ϕ ve ψ ye bağlı öyle bir $R \geq 1$ tamsayısı vardır ki, her $\frac{m}{n}$ rasyonel sayısı için

$$\text{obeb}(n^d \cdot \phi(\frac{m}{n}), n^d \cdot \psi(\frac{m}{n})) \mid R.$$

(b) ϕ ve ψ ye bağlı öyle bir k_1 sabiti vardır ki, ψ nin kökleri olmayan, her $\frac{m}{n}$ rasyonel sayısı için, aşağıdaki eşitsizlik sağlanır:

$$d \cdot h(\frac{m}{n}) - k_1 \leq h(\frac{\phi(\frac{m}{n})}{\psi(\frac{m}{n})}).$$

İspat(a) : Burada, $\phi(x)$ ve $\psi(x)$ in gerekirse yerleri değiştirilerek, $\text{der}(\phi) = d$ ve $\text{der}(\psi) = e \leq d$ kabul edilebilir. d nin bu şekilde belirlenmesiyle,

$$n^d \cdot \phi(\frac{m}{n}) = a_0 \cdot m^d + a_1 \cdot m^{d-1} \cdot n + \dots + a_d \cdot n^d$$

ve

$$n^d \cdot \psi(\frac{m}{n}) = b_0 \cdot m^e \cdot n^{d-e} + b_1 \cdot m^{e-1} \cdot n^{d-e+1} + \dots + b_e \cdot n^d$$

birer tamsayı olacağından dolayı, bunların obeb'inden sözedilebilir. Ayrıca, bundan sonra, notasyonlarda kolaylık sağlamaı nedeniyle; $\Phi(m, n) = n^d \cdot \phi(\frac{m}{n})$ ve $\Psi(m, n) = n^d \cdot \psi(\frac{m}{n})$ olarak kullanılacaktır.

Bu adımda amaç; m ve n tamsayılarından bağımsız olarak, $obeb(\Phi(m, n), \Psi(m, n))$ için bir ifade elde edebilmek olacaktır.

$\phi(x)$ ve $\psi(x)$ in ortak kökü olmadığından dolayı bunlar, $\mathbf{Q}[x]$ ile gösterilen, katsayıları rasyonel sayı olan polinomlar halkasında, aralarında asal polinomlardır ve bunlar, birim ideali üretir. Bu durumda; uygun $F(x), G(x) \in \mathbf{Q}[x]$ için

$$F(x) \cdot \phi(x) + G(x) \cdot \psi(x) = 1 \quad (2.3.1)$$

olur. A tamsayısı yeteri kadar büyük seçilerek; $A \cdot F(x)$ ve $A \cdot G(x)$ polinomları tamsayı katsayılı olacak biçimde ayarlanabilir. Ayrıca;

$$D = \max \{ \deg F(x), \deg G(x) \}$$

olsun. Burada, A ve D nin m ve n den bağımsız olarak seçildiğine dikkat edilmelidir. (2.3.1) de $x = \frac{m}{n}$ alınıp, eşitliğin her iki tarafı $A \cdot n^{D+d}$ ile çarpılırsa,

$$n^D \cdot A \cdot F(\frac{m}{n}) \cdot n^d \cdot \phi(\frac{m}{n}) + n^D \cdot A \cdot G(\frac{m}{n}) \cdot n^d \cdot \psi(\frac{m}{n}) = A \cdot n^{D+d}$$

ve buradan

$$\{n^D \cdot A \cdot F(\frac{m}{n})\} \cdot \Phi(m, n) + \{n^D \cdot A \cdot G(\frac{m}{n})\} \cdot \Psi(m, n) = A \cdot n^{D+d}$$

elde edilir.

$\gamma = \gamma(m, n) = obeb(\Phi(m, n), \Psi(m, n))$ için $\gamma \mid A \cdot n^{D+d}$ olur. Amacımız, γ nin m ve n den bağımsız belli bir sabiti böldüğünü göstermek olduğu için γ nin $A \cdot n^{D+d}$ çarpımını bölmesi, çarpımın n ye bağlı olmasından dolayı fazla bir önem taşımamaktadır. Ama bundan yararlanarak; a_0 sayısı $\phi(x)$ polinomunun başkatsayısı yani, $\phi(x)$ polinomunda x^d nin katsayısı olmak üzere $\gamma \mid A \cdot a_0^{D+d}$ olduğu gösterilebilir.

$\gamma \mid \Phi(m, n)$ olduğu için γ ,

$$A \cdot n^{D+d-1} \cdot \Phi(m, n) = A \cdot a_0 \cdot m^d \cdot n^{D+d-1} + A \cdot a_1 \cdot m^{d-1} \cdot n^{D+d} + \dots + A \cdot a_d \cdot n^{D+2d-1}$$

eşitliğinin sağ tarafındaki ifadeyi de böler. Bu ifadedeki birinci terim dışındaki tüm terimler $A \cdot n^{D+d}$ nin bir katı olduğundan dolayı, $\gamma \mid A \cdot a_0 \cdot m^d \cdot n^{D+d-1}$ olmalıdır. Böylece, $\gamma \mid obeb(A \cdot n^{D+d}, A \cdot a_0 \cdot m^d \cdot n^{D+d-1})$ elde edilir ve buradan, m ile n nin aralarında asal olmasından dolayı, $\gamma \mid A \cdot a_0 \cdot n^{D+d-1}$ olduğu sonucuna varılır. Dikkat edilirse, a_0 ile çarpıldığında n nin üssü bir aşağı indirgenmiş oldu.

Şimdi de $\gamma \mid A \cdot a_0 \cdot n^{D+d-2} \cdot \Phi(m, n)$ özelliğinden yararlanarak, yukarıdaki işlemin tekrarlanmasıyla, $\gamma \mid A \cdot a_0^2 \cdot n^{D+d-2}$ olacağı açıktır. Bu şekilde devam edilerek,

toplam $D + d$ tane işlem sonucunda, $\gamma \mid A.a_0^2$ olarak elde edilir. Burada, $R = A.a_0^{D+d}$ seçilmesiyle de, ispatın (a) şıkkı tamamlanmış olur.

(b) : Burada sonlu sayıdaki rasyonel sayı için, k_1 sabiti uygun bir şekilde seçilebileceğinden dolayı, ispatta bu sayıların gözardı edilmesi herhangi bir soruna neden olmaz. Bu bağlamda, $\frac{m}{n}$ rasyonel sayıları, $\phi(x)$ in kökleri olmayacak şekilde kabul edilebilir. Ayrıca, (a) şıkkındaki notasyonların kullanılmasına devam edilerek, yüksekliği hesaplanmak istenen ξ için,

$$\xi = \frac{\phi(\frac{m}{n})}{\psi(\frac{m}{n})} = \frac{n^d \cdot \phi(\frac{m}{n})}{n^d \cdot \psi(\frac{m}{n})} = \frac{\Phi(\frac{m}{n})}{\Psi(\frac{m}{n})}$$

olur. Böylece, ξ nin iki tamsayının bölümü şeklinde olduğu bilinmekte ama bu tamsayıların aralarında asal olup olmadıkları bilinmemektedir. Fakat, buna rağmen

$$H(\xi) \leq \max\{|\Phi(m,n)|, |\Psi(m,n)|\}$$

olacağı açıktır. (a) şıkında; m ve n den bağımsız bir $R \geq 1$ için, $\Phi(m,n)$ ve $\Psi(m,n)$ nin obeb 'inin R sayısını böldüğü ispatlanmıştır; bundan dolayı,

$$\begin{aligned} H(\xi) &\geq \frac{1}{R} \max\{|\Phi(m,n)|, |\Psi(m,n)|\} \\ &= \frac{1}{R} \max\{|n^d \cdot \phi(\frac{m}{n})|, |n^d \cdot \psi(\frac{m}{n})|\} \end{aligned}$$

olur ve burada $\max\{|a|, |b|\} \geq \frac{1}{2}(|a| + |b|)$ özelliğinden de yararlanarak

$$H(\xi) \geq \frac{1}{2R} \{|n^d \cdot \phi(\frac{m}{n})| + |n^d \cdot \psi(\frac{m}{n})|\}$$

olduğu görülebilir.

Diğer yandan, $(H(\frac{m}{n}))^d = \max\{|m|^d, |n|^d\}$ olacağından,

$$\frac{H(\xi)}{(H(\frac{m}{n}))^d} \geq \frac{1}{2R} \cdot \frac{\{|n^d \cdot \phi(\frac{m}{n})| + |n^d \cdot \psi(\frac{m}{n})|\}}{\max\{|m|^d, 1\}}$$

olur.

Reel değişkenli $p(t)$ fonksiyonu,

$$p(t) = \frac{|\phi(t)| + |\psi(t)|}{\max\{|t|^d, 1\}}$$

olacak biçimde tanımlandığında; ϕ nin derecesi d , ψ nin derecesi ise en fazla d olacağından dolayı, $|t|$ sonsuza yaklaşırken sıfırdan farklı bir limite sahip olur. Bu limit; $\deg \psi < d$ için $|a_0|$, $\deg \psi = d$ için de $|a_0| + |b_0|$ değerine eşit olur. Böylece, $p(t)$ fonksiyonu pozitif değerli olduğundan sıfırla sınırlanan bir kapalı aralık içinde yer alır. Dolayısıyla, kapalı ve sınırlı bir küme içinde $p(t)$ sürekli fonksiyonunun

maksimum ve minimum değerlere sahip olacağı açıktır. Ayrıca, kabulümüz gereği, $\phi(x)$ ve $\psi(x)$ in hiç ortak kökü olmaması nedeniyle, $\forall t \in \mathbf{R}$ için $p(t) > 0$ olur, bu da $p(t)$ 'nin minimumunun bir pozitif sayı olduğunu ifade eder, yani; $\exists c_1 \in \mathbf{R} \ni \forall t \in \mathbf{R}$ için $c_1 \leq p(t)$ olmalıdır. Bundan yararlanarak,

$$\frac{c_1}{2R} \left(H\left(\frac{m}{n}\right) \right)^d \leq H(\xi)$$

eşitsizliği elde edilir. Son olarak, burada her iki tarafın logaritmasını alınmasıyla, $k_1 = \log\left(\frac{2R}{c_1}\right)$ olmak üzere

$$d \cdot h\left(\frac{m}{n}\right) - k_1 \leq h(\xi)$$

olduğu sonucuna varılır ki, bu da Lema 2.3.1* ın ve dolayısıyla da Lema 2.3.1 in ispatını bitirir.

2.4. Homomorfizm Dönüşümleri

Bu kısımda Mordell Teoremi'nin ispatında son adımı oluşturan ve bir sonraki kısımda ispatı verilecek olan bir lemanın, ispatı için gerekli olan bilgilere yer verilecektir.

Mordell Teoremi'nin ispatını tamamlamak için $[\mathcal{C}(\mathbf{Q}) : 2\mathcal{C}(\mathbf{Q})]$ indeksinin yani, $\mathcal{C}(\mathbf{Q})/2\mathcal{C}(\mathbf{Q})$ bölüm grubunun sonlu olduğuna dair bir lemanın ispatına ihtiyaç duyulmaktadır; bu da Mordell Teoremi'nin ispatının en zor kısmını teşkil etmektedir. Maalesef; $\mathcal{C} : y^2 = f(x) = x^3 + a_1x^2 + b_1x + c_1$ biçimindeki her eliptik eğri için, bugüne kadar cebirsel sayılar teorisini kullanmadan, yukarıda sözü edilen lemanın ispatı yapılamadığından dolayı, burada en az bir rasyonel kökü olan $f(x) = 0$ için ispat yapılacaktır. Genel durumda, $f(x) = 0$ denkleminin herhangi bir s kökü alındığında aynı ispat metodu çalışır, fakat bunun için $\mathbf{Q}[s]$ cisim genişlemesi içinde çalışmak gerekeceğinden ve ayrıca bu cismin ideal sınıf grubu ve tersinir elemanlar grubu adı verilen gruplar hakkında temel kavramlara yer verilmesi gerektiğinden dolayı çalışmamızda bu yöntem tercih edilmemiştir. Bu nedenle, sözü edilen lema, $f(x) = 0$ ın bir x_0 rasyonel kökü olması durumunda ispatlanacaktır.

Bundan sonraki çalışmalarımızda, notasyonlarda kolaylık sağlaması açısından, $\mathcal{C}(\mathbf{Q})$ grubu yerine Γ sembolü kullanılacaktır.

$f(x_0) = 0$ ve $f(x)$ polinomunun başkatsayısı 1 olduğu için, koordinatlarda değişiklik yapılmasıyla $(x_0, 0)$ noktası yeni koordinatlarda orijin noktası olacak biçimde dönüştürülebilir. Tabii ki, bu dönüşüm γ grubunda herhangi bir soruna neden olmaz ve elde edilen yeni denklem, $a, b \in \mathbf{Z}$ olmak üzere

$$\mathcal{C} : y^2 = f(x) = x^3 + ax^2 + bx$$

biçimini alır. Bu durumda, $T = (0, 0) \in \Gamma$, $2T = \mathcal{O}$ ve $f(x)$ in diskriminantı, $D = b^2(a^2 - 4b)$ olur. Eliptik eğri için $f(x)$ in farklı kökleri olması $D \neq 0$ olmasını gerektirdiğinden dolayı; $b \neq 0$ ve $a^2 - 4b \neq 0$ olmalıdır. Şimdi, $a' = -2a$, $b' = a^2 - 4b$ olmak üzere

$$\mathcal{C}' : y^2 = f(x) = x^3 + a'x^2 + b'x$$

eğrisini ele alalım. $\mathcal{C}$ den $\mathcal{C}'$ ye, $\phi(T) = \mathcal{O}'$, $\phi(\mathcal{O}) = \mathcal{O}'$ ve $P = (x, y) \in \mathcal{C} \setminus \{T, \mathcal{O}\}$ için,

$$x' = x + a + \frac{b}{x} = \frac{y^2}{x^2} \quad \text{ve} \quad y' = y\left(\frac{x^2 - b}{x^2}\right).$$

olmak üzere $\phi(x, y) = (x', y')$ ile tanımlanan $\phi : \mathcal{C} \rightarrow \mathcal{C}'$ dönüşümünü düşünelim. ϕ nin iyi tanımlı olduğu yani; (x', y') nün $\mathcal{C}'$ eğrisi üzerinde olduğu, aşağıdaki gibi gösterilebilir:

$$\begin{aligned} (x')^3 + a'(x')^2 + b'x' &= x'((x')^2 + a'x' + b') \\ &= x'((x')^2 - 2ax' + (a^2 - 4b)) \\ &= \frac{y^2}{x^2} \left(\frac{y^4}{x^4} - 2a \frac{y^2}{x^2} + (a^2 - 4b) \right) \\ &= \frac{y^2}{x^2} \left(\frac{(y^2 - ax^2)^2 - 4bx^4}{x^4} \right) \\ &= \frac{y^2}{x^6} ((x^3 + bx)^2 - 4bx^4) \\ &= \left(\frac{y(x^2 - b)}{x^2} \right)^2 \\ &= (y')^2. \end{aligned}$$

Bu açıklamaların yanısıra, aşağıdaki teorem, ilerideki çalışmalarımızda büyük kolaylıklar sağlayacaktır:

Teorem 2.4.1 : $\mathcal{C}$ ve $\mathcal{C}'$ eliptik eğrileri; $a, b \in \mathbb{Z}$ ve $a' = -2a$, $b' = a^2 - 4b$ olmak üzere;

$$\mathcal{C} : y^2 = x^3 + ax^2 + bx$$

$$\mathcal{C}' : y^2 = x^3 + a'x^2 + b'x$$

denklemleri ile verilsin. $T = (0, 0) \in \mathcal{C}$ olmak üzere

(a) $\mathcal{C}$ den $\mathcal{C}'$ eğrisine

$$\phi(P) = \begin{cases} \left(\frac{y^2}{x^2}, \frac{y(x^2 - b)}{x^2} \right) & , \quad P = (x, y) \in \mathcal{C} \setminus \{T, \mathcal{O}\} \\ \mathcal{O}' & , \quad P = \mathcal{O} \quad \text{veya} \quad P = T \end{cases}$$

ile tanımlı bir $\phi : \mathcal{C} \rightarrow \mathcal{C}'$ homomorfizmi vardır ve $\phi = \{\mathcal{O}, T\}$ dir.

(b) : $\mathcal{C}$ için yapılan işlem $\mathcal{C}'$ ye uygulandığında; $\phi' : \mathcal{C}' \rightarrow \mathcal{C}''$ dönüşümü elde edilir. Burada; $\mathcal{C}''$ den $\mathcal{C}$ ye $(x, y) \rightarrow \left(\frac{x}{4}, \frac{y}{8}\right)$ dönüşümü ile $\mathcal{C}$ ile $\mathcal{C}''$ nün noktaları arasında bire-bir bir eşleme olduğu görülür, dolayısıyla bu eğriler izomorf olarak düşünülebilir. Bu nedenle,

$\psi : \mathcal{C}' \rightarrow \mathcal{C}$ dönüşümü

$$\psi(P') = \begin{cases} \left(\frac{(y')^2}{4(x')^2}, \frac{y'((x')^2 - b')}{8(x')^2} \right) & , \quad P' = (x', y') \neq \mathcal{O}', T' \\ \mathcal{O} & , \quad P' = \mathcal{O}' \quad \text{veya} \quad P' = T' \end{cases}$$

olacak şekilde tanımlandığında; $\psi \circ \phi(P) = 2P$, iki katlılık, özelliğini sağlar.

İspat (a) : Daha önce ϕ dönüşümünün $\mathcal{C}$ nin noktalarını $\mathcal{C}'$ nin noktalara dönüştürdüğü gösterilmişti. Bunun için burada sadece ϕ nin bir homomorfizm olduğu ve Çek $\phi = \{\mathcal{O}, T\}$ den olduğunu göstermek yeterlidir. $\forall P_1, P_2 \in \mathcal{C}$ için

$$\phi(P_1 + P_2) = \phi(P_1) + \phi(P_2) \quad (2.4.1)$$

olduğunu göstermek zordur. Çünkü, burada birçok durum söz konusudur. P_1 veya P_2 den birisinin $\mathcal{O}$ olması durumunda (2.4.1) eşitliğinin doğru olacağı açıktır. P_1 veya P_2 den birisinin T olması durumunda ise, kabul edelim ki $P_1 = T$ olsun; $\forall P \in \mathcal{C} \setminus \{T\}$ için $\phi(T + P) = \phi(P)$ olduğunu görmek için iki noktanın toplamının koordinatlarını veren formülleri kullanmak gereklidir. Bu durumda, $P = (x, y)$ için; $P + T = (\frac{b}{x}, \frac{-by}{x^2})$ olduğundan ve ayrıca bundan sonraki çalışmalarımızda, N eğri üzerinde bir nokta olmak üzere xN ve yN gösterimleri, N nin, sırasıyla, x ve y koordinatlarını işaret edecek şekilde tanımlanırsa,

$$P + T = (x(P + T), y(P + T))$$

ve

$$\phi(P + T) = (x'(P + T), y'(P + T))$$

olacağı açıktır. Burada,

$$\begin{aligned} x'(P + T) &= \left(\frac{y(P + T)}{x(P + T)} \right)^2 \\ &= \frac{\left(\frac{-by}{x^2} \right)^2}{\left(\frac{b}{x} \right)^2} \\ &= \frac{y^2}{x^2} \\ &= x'(P) \end{aligned}$$

ve benzer hesaplamalarla,

$$\begin{aligned} y'(P + T) &= \frac{y(P + T) \cdot (x(P + T)^2 - b)}{x(P + T)^2} \\ &= \frac{\frac{-by}{x^2} \left(\left(\frac{b}{x} \right)^2 - b \right)}{\left(\frac{b}{x} \right)^2} \\ &= y'(P) \end{aligned}$$

olduğundan dolayı; $P \neq T$ için $\phi(P + T) = \phi(P)$ eşitliği sağlanmış olur. $P = T$ için de $\phi(T + T) = \phi(T) + \phi(T)$ eşitliğinin iki tarafı da, $\mathcal{O}'$ olması nedeniyle, $\forall P \in \mathcal{C}$ için $\phi(P + T) = \phi(P)$ olur. Diğer yandan, ϕ fonksiyonu,

$$\begin{aligned} \phi(-P) &= \phi(x, -y) \\ &= \left(\left(\frac{-y}{x} \right)^2, \frac{-y(x^2 - b)}{x^2} \right) \\ &= -\phi(x, y) \\ &= -\phi(P) \end{aligned}$$

olduğundan dolayı, $\phi(-P) = -\phi(P)$ özelliğini sağlar. Böylece, ϕ nin bir homomorfizm olduğunu göstermek için, $P_1 + P_2 + P_3 = \mathcal{O}$ olmak üzere $\phi(P_1) + \phi(P_2) + \phi(P_3) = \mathcal{O}'$ olduğunu göstermek yeterlidir. Çünkü, böylece $\forall P_1, P_2 \in \mathcal{C}$ ve $P_1 + P_2 + P_3 = \mathcal{O}$ için

$$\phi(P_1 + P_2) = \phi(-P_3) = -\phi(P_3) = \phi(P_1) + \phi(P_2)$$

olduğu gösterilmiş olur. Ayrıca burada, yukarıdaki açıklamalara dayanarak; P_1, P_2, P_3 noktalarının hepsinin $\mathcal{O}$ veya T den farklı olduğu kabul edilebilir.

Eliptik eğri üzerinde, $P_1 + P_2 + P_3 = \mathcal{O}$ olması için gerekli ve yeterli koşulun bu noktaların doğrudan olması gerektiği konusu daha önce açıklanmıştı. Böylece, bu noktalardan geçen doğru, $y = \lambda x + \nu$ olmak üzere; ispatın tamamlanabilmesi için; $\phi(P_1), \phi(P_2)$ ve $\phi(P_3)$ noktalarının $\mathcal{C}'$ ile kesişen bir doğru üzerinde olduğu gösterilmelidir. Burada; $\nu \neq 0$ dır (çünkü; $\nu = 0$ olması durumunda, $y = \lambda x + \nu$ doğrusu $T = (0, 0)$ noktasından geçmiştir olur, bu da $\phi(P_1)$, $\phi(P_2)$ ve $\phi(P_3)$ noktalarının T den farklı kabul edilmesiyle çelişir). $\mathcal{C}'$ den geçen ve

$$\lambda' = \frac{\nu\lambda - b}{\nu}, \quad \nu' = \frac{\nu^2 - a\nu\lambda + b\lambda^2}{\nu}$$

olmak üzere, $y = \lambda'x + \nu'$ doğrusu tanımlansın. Bu durumda; $\phi(P_1) = \phi(x_1, y_1) = (x_1', y_1')$ noktası $y = \lambda'x + \nu'$ doğrusu üzerinde olur. Çünkü,

$$\begin{aligned} \lambda'x_1' + \nu' &= \frac{\nu\lambda - b}{\nu} \left(\frac{y_1}{x_1}\right)^2 + \frac{\nu^2 - a\nu\lambda + b\lambda^2}{\nu} \\ &= \frac{(\nu\lambda - b)y_1^2 + (\nu^2 - a\nu\lambda + b\lambda^2)x_1^2}{\nu x_1^2} \\ &= \frac{\nu\lambda(y_1^2 - ax_1^2) - b(y_1 - \lambda x_1)(y_1 + \lambda x_1) + \nu^2 x_1^2}{\nu x_1^2} \end{aligned}$$

ve ayrıca, $y_1^2 - ax_1^2 = x_1^3 + bx_1$, $y_1 - \lambda x_1 = \nu$ eşitlikleri kullanıldığında,

$$\begin{aligned} \lambda'x_1' + \nu' &= \frac{\lambda(x_1^3 + bx_1) - b(y_1 + \lambda x_1) + \nu x_1^2}{x_1^2} \\ &= \frac{x_1^2(\lambda x_1 + \nu) - by_1}{x_1^2} \\ &= \frac{(x_1^2 - b)y_1}{x_1^2} = y_1' \end{aligned}$$

eşitliği elde edilir. $\phi(P_2)$ ve $\phi(P_3)$ ün de $y = \lambda'x + \nu'$ doğrusu üzerinde olduğu, benzer işlemlerle gösterilebilir. $\phi(P_1)$, $\phi(P_2)$ ve $\phi(P_3)$ noktalarının hepsinin farklı olması durumunda; $\phi(P_1) + \phi(P_2) + \phi(P_3) = \mathcal{O}'$ özelliği sağlanacağından dolayı bu durumda ispat biter. Diğer yandan, sözü edilen noktalardan ikisinin veya üçünün çakışık olması durumunda da, $\phi(P_1) + \phi(P_2) + \phi(P_3) = \mathcal{O}'$ özelliği sağlanır (Silverman ve Tate, 1992).

ϕ nin tanımı gereği, Çek $\phi = \{\mathcal{O}', T'\}$ olduğu açıktır.

(b) : $C' : y^2 = x^3 + ax^2 + bx$ ve $C'' : y^2 = x^3 + 4ax^2 + 16bx$ olmak üzere;

$$\begin{aligned} f : C &\longrightarrow C'' \text{ için } f(x, y) = \left(\frac{x}{4}, \frac{y}{8}\right), \\ g : C'' &\longrightarrow C \text{ için } g(x, y) = (4x, 8y) \end{aligned}$$

dönüşümleri; $f \circ g(x', y') = (x', y')$ ve $g \circ f(x, y) = (x, y)$ yani; $f \circ g = 1 = g \circ f$ özelliğini sağladığından dolayı; C ve C'' arasında bire-bir bir eşleme vardır, bunun için gerektiğinde C'' eğrisi C eğrisi olarak düşünülebilir.

Burada, (a) şıkına dayanarak, ϕ homomorfizmine benzer şekilde bir

$$\phi' : C' \longrightarrow C''$$

homomorfizmi tanımlanabilir, bu da C yerine C' , a ve b yerine de a' ve b' , düşünülerek ϕ' nün tanımlanması demektir. f ve ϕ' iyi tanımlı homomorfizmler olacaklarından dolayı; $\psi = f \circ \phi'$ olmak üzere, $\psi : C' \longrightarrow C$ yine iyi tanımlı bir homomorfizm olur.

İspatın bitirilmesi için, son olarak $\psi \circ \phi$ nin iki katlılık özelliğine sahip yani; $\forall P \in C$ için $\psi \circ \phi(P) = 2P$ olduğunu göstermek gereklidir. Bu da; eğri üzerindeki iki noktanın toplamının koordinatlarını veren toplam formüllerinin kullanılmasıyla kolayca gösterilebilir:

$$2P = 2(x, y) = \left(\frac{(x^2 - b)^2}{4y^2}, \frac{(x^2 - b)(x^4 + 2ax^3 + 6bx^2 + 2abx + b^2)}{8y^3} \right)$$

olduğu, $\phi(x, y) = \left(\frac{y^2}{x^2}, \frac{y(x^2 - b)}{x^2} \right)$, ve $\psi(x', y') = \left(\frac{(y')^2}{4(x')^2}, \frac{y'((x')^2 - b')}{8(x')^2} \right)$ dönüşümleri kullanılarak,

$$\begin{aligned} \psi \circ \phi(x, y) &= \psi\left(\frac{y^2}{x^2}, \frac{y(x^2 - b)}{x^2}\right) = \left[\frac{\left(\frac{y(x^2 - b)}{x^2}\right)^2}{4\left(\frac{y^2}{x^2}\right)^2}, \frac{\frac{y(x^2 - b)}{x^2} \left(\left(\frac{y^2}{x^2}\right)^2 - (a^2 - 4b)\right)}{8\left(\frac{y^2}{x^2}\right)^2} \right] \\ &= \left(\frac{(x^2 - b)^2}{4y^2}, \frac{(x^2 - b)(y^4 - (a^2 - 4b)x^4)}{8y^3x^2} \right) \end{aligned}$$

elde edilir. Burada, $y^4 = x^2(x^2 + ax + b)^2$ eşitliğinden yararlanılarak

$$\begin{aligned} \psi \circ \phi(P) &= \psi \circ \phi(x, y) = \left(\frac{(x^2 - b)^2}{4y^2}, \frac{(x^2 - b)(x^2(x^2 + ax + b)^2 - (a^2 - 4b)x^4)}{8y^3x^2} \right) \\ &= \left(\frac{(x^2 - b)^2}{4y^2}, \frac{(x^2 - b)(x^4 + 2ax^3 + 6bx^2 + 2abx + b^2)}{8y^3} \right) \\ &= 2(x, y) = 2P \end{aligned}$$

olduğu sonucuna varılır. Kolayca görülebileceği gibi, toplam formülleri $x = 0$ veya $y = 0$ dışındaki $P = (x, y)$ noktaları için tanımlı olur. Dolayısıyla, ispatı tamamlamak için bu durumları ayrıca incelemek gerekir, bu da fazla zor değildir. Çünkü; $x = 0$ için $y = 0$ olacağından,

$$\psi \circ \phi(T) = \psi(O') = O = 2T$$

olur. $y = 0$ için de iki durum söz konusu olur:

i) $f(x) = 0$ in üç tane farklı $0, x_1, x_2$ gibi, reel kökü varsa; $(0, 0), (x_1, 0), (x_2, 0)$ noktalarının mertebeleri iki olduğundan dolayı,

$$\psi \circ \phi(x_1, 0) = \psi\left(\frac{0}{x_1^2}, \frac{0}{x_1^2}\right) = \mathcal{O} = 2(x_1, 0),$$

$$\psi \circ \phi(x_2, 0) = \psi(0, 0) = \mathcal{O} = 2(x_2, 0)$$

eşitlikleri sağlanır. Bu da; bu noktaların iki katlılık özelliğini sağladığını gösterir. Ayrıca, $\psi \circ \phi(\mathcal{O}) = \mathcal{O} = 2\mathcal{O}$ olduğu da açıktır.

ii) $f(x) = 0$ in yalnızca bir reel kökü varsa, bu kök sıfır olacağından ve bu durum yukarıda incelendiğinden dolayı; $\forall P \in \mathcal{C}$ için $\psi \circ \phi(P) = 2P$ olduğu sonucuna varılır. Bu da ispatı bitirir.

Benzer hesaplamalarla; $\phi \circ \psi(x', y') = 2(x', y')$ olduğu gösterilebilir ama aşağıdaki yöntem ile bunu görmek o kadar da zor değildir: ϕ homomorfizm olduğundan, öncelikle, $\phi(2P) = \phi(P) + \phi(P) = 2\phi(P)$ ve ayrıca, $\phi, \mathcal{C}$ den $\mathcal{C}'$ ye örten bir homomorfizmdir. Daha önce, $2P = \psi \circ \phi(P)$ olduğu ispatlanmıştı; bunun için

$$\phi \circ \psi(\phi(P)) = \phi(\psi \circ \phi(P)) = \phi(2P) = 2\phi(P)$$

ve $\forall P' \in \mathcal{C}'$ için $\exists P \in \mathcal{C} \ni \phi(P) = P'$ olur. Bu da; $\phi \circ \psi(P') = 2P'$ eşitliğinin sağlandığını gösterir.

2.5. Mordell Teoremi

Bu bölümde, aşağıda ifade edilen lema ve İniş Teoremi olarak adlandırılan teoremin ispatı verilecek ve böylece temel amaçlardan biri olan Mordell Teoremi'nin ispatı tamamlanacaktır.

Lema 2.5.1 : $[\Gamma : 2\Gamma]$ indeksi sonludur.

Bu lemanın ispatına geçmeden önce, ispatta gerekli olan bilgilere aşağıda yer verilmiştir. Bir önceki kısımdaki gösterimlerin kullanılmasıyla; $a, b \in \mathbb{Z}$ ve $a' = -2a$, $b' = a^2 - 4b$ olmak üzere,

$$\mathcal{C} : y^2 = x^3 + ax^2 + bx,$$

$$\mathcal{C}' : y^2 = x^3 + a'x^2 + b'x$$

eliptik eğrileri için

$$\phi : \mathcal{C} \longrightarrow \mathcal{C}' \quad \text{ve} \quad \psi : \mathcal{C}' \longrightarrow \mathcal{C}$$

dönüşümlerinin bileşkelerinin, iki katlılık özelliğini sağladığı bilinmektedir. Buna göre; $\Gamma = \mathcal{C}(\mathbb{Q})$ ve $\Gamma' = \mathcal{C}'(\mathbb{Q})$ olduğu hatırlanacak olursa; ϕ nin tanımından dolayı Γ dan Γ' ye bire-bir bir dönüşüm olduğu açıktır. Fakat, buna karşılık Γ' de bir nokta verildiğinde bu noktanın Γ daki bir noktanın görüntüsü olup olmadığı konusu

fazla açık değildir; yani ϕ nin örten olup olmadığı kolayca görülememektedir. Buna rağmen, Γ daki noktaların ϕ altındaki görüntülerinden oluşan $\phi(\Gamma)$ kümesinin Γ' nin bir alt grubu olduğu bilinmektedir.

$\phi(\Gamma)$ ile ilgili olarak aşağıdaki üç iddiayı ispatlayacağız.

İddia : i) $\mathcal{O}' \in \phi(\Gamma)$ dır.

ii) $T' = (0, 0) \in \phi(\Gamma) \iff b' = a^2 - 4b$ bir tamkaredir.

iii) $x' \neq 0$ olmak üzere, $P' = (x', y')$ olsun. Bu durumda; $P' \in \phi(\Gamma) \iff x'$ bir rasyonel sayının karesidir.

İspat : i) $\phi(\mathcal{O}) = \mathcal{O}'$ olduğundan $\mathcal{O}' \in \phi(\Gamma)$ dır.

ii) ϕ nin tanımından dolayı;

$$T' \in \phi(\Gamma) \iff \exists (x, y) \in \Gamma \ni \frac{y^2}{x^2} = 0$$

olduğu görülür. Burada, $x = 0$ olması durumunda, $(x, y) = (0, 0) = T$ ve $\phi(T) = \mathcal{O}'$, $\phi(T) \neq T'$ olduğundan dolayı; $x \neq 0$ dır. Dolayısıyla, $T' \in \phi(\Gamma)$ olması için gerek ve yeter şart, $\exists (x, y) \in \Gamma \ni x \neq 0, y = 0$ olmasıdır. Bu da

$$0 = x^3 + ax^2 + bx = x(x^2 + ax + b)$$

olmasını gerektirir. Denklemin sıfırdan farklı bir rasyonel kökü olması için gerek ve yeter şart, $x^2 + ax + b = 0$ kuadratik denkleminin rasyonel kökü olmasıdır. Bu da; denklemin diskriminantı olan $a^2 - 4b$ nin bir tamkare olmasıyla denktir.

iii) $x' \neq 0$ olmak üzere $(x', y') \in \phi(\Gamma)$ için ϕ nin tanımı gereği $x' = \frac{y'^2}{x'^2}$ olduğundan dolayı, x' bir rasyonel sayının karesidir. Tersine olarak, $w \in \mathbb{Q}$ olmak üzere, $x' = w^2$ olsun. Bu durumda amaç, $\mathcal{C}$ üzerinde görüntüsü (x', y') olan bir noktayı bulmak olduğu için, bu yönde çalışmalar yapılacaktır. Bununla beraber, ϕ homomorfizminin çekirdeği $\{\mathcal{O}, T\}$ den ibaret olduğu için, ilerideki çalışmalarımızda, $(x', y') \in \phi(\Gamma)$ olmak üzere Γ nin iki elemanının görüntüsünün (x', y') olduğu da gösterilecektir.

Buradan hareketle,

$$x_1 = \frac{1}{2}(w^2 - a + \frac{y'}{w}) \quad , \quad y_1 = x_1.w,$$

$$x_2 = \frac{1}{2}(w^2 - a - \frac{y'}{w}) \quad , \quad y_2 = -x_2.w$$

olmak üzere, $i = 1, 2$ için $P_i = (x_i, y_i) \in \mathcal{C}$ ve $\phi(P_i) = (x', y')$ olduğu aşağıda detaylıca açıklanacaktır. Burada, P_1 ve P_2 rasyonel noktalar oldukları için, $(x', y') \in$

$\phi(\Gamma)$ olacak ve bu da ispatı bitirecektir.

$$\begin{aligned} x_1.x_2 &= \frac{1}{4}((w^2 - a)^2 - \frac{(y')^2}{w^2}), \\ &= \frac{1}{4}((x' - a)^2 - \frac{(y')^2}{x'}), \\ &= \frac{1}{4}(\frac{(x')^3 - 2a(x')^2 + a^2x' - (y')^2}{x'}) \end{aligned}$$

ve $(y')^2 = (x')^3 - 2a(x')^2 + (a^2 - 4b)x'$ olduğundan dolayı, $x_1.x_2 = b$ olarak elde edilir. $i = 1, 2$ için $P_i = (x_i, y_i) \in \mathcal{C}$ olduğunu göstermek demek;

$$\frac{y_i^2}{x_i^2} = x_i + a + \frac{b}{x_i}$$

eşitliğinin sağlandığını göstermek demektir. Çünkü, bu durum

$$y_i^2 = x_i^3 + ax_i^2 + bx_i$$

eşitliğinin sağlanmasını ve dolayısıyla da $P_i \in \mathcal{C}$ olmasını gerektirir. y_1 ile y_2 nin tanımlarından, $\frac{y_i}{x_i} = \mp w$ ve

$$w^2 = \frac{1}{2}(2w^2 - 2a) + a = x_1 + x_2 + a$$

eşitlikleri elde edilir ki, bu da $x_1.x_2 = b$ olduğundan dolayı,

$$\frac{y_i^2}{x_i^2} = w^2 = x_1 + a + x_2 = x_i + a + \frac{b}{x_i}$$

demektir.

Şimdi de; $\phi(P_i) = (x', y')$ dönüşümünün gerçekleştiği gösterilecektir. Bunun için,

$$\frac{y_i^2}{x_i^2} = x' \quad \text{ve} \quad \frac{y_i(x_i^2 - b)}{x_i^2} = y'$$

olmalıdır. Burada birinci eşitlik, $y_i = \mp x_i.w$ olduğundan dolayı kolayca görülebilir, çünkü;

$$\frac{y_i^2}{x_i^2} = \frac{x_i^2.w^2}{x_i^2} = w^2 = x'$$

dür. İkinci eşitliğin sağlandığını göstermek için de, $b = x_1.x_2$ ve y_i nin tanımını kullanmak yeterlidir; çünkü,

$$\begin{aligned} \frac{y_1(x_1^2 - b)}{x_1^2} &= \frac{x_1.w.(x_1^2 - x_1.x_2)}{x_1^2} = w(x_1 - x_2) \\ \frac{y_2(x_2^2 - b)}{x_2^2} &= -\frac{x_2.w.(x_2^2 - x_1.x_2)}{x_2^2} = w(x_1 - x_2) \end{aligned}$$

olur. Burada, x_1 ve x_2 nin tanımından $x_1 - x_2 = \frac{y'}{w}$ olmalıdır. Bu da;

$$\frac{y_i(x_i^2 - b)}{x_i^2} = y'$$

eşitliğinin sağlandığını ispatlar.

Amacımız, $[\Gamma : 2\Gamma]$ indeksinin, yani; $\Gamma/2\Gamma$ bölüm grubunun sonlu olduğunu ifade eden lemayı ispat etmek olduğu için, daha sonra detaylıca açıklanacağı gibi, bu adımda $[\Gamma' : \phi(\Gamma)]$ ve $[\Gamma : \psi(\Gamma)]$ indekslerinin sonlu olduğunu göstermek yeterli olacaktır. Kısacası; s , $b' = a^2 - 4b$ nin farklı asal çarpanlarının sayısını, r de b nin farklı asal çarpanlarının sayısını göstermek üzere, aşağıdaki önerme yardımıyla

$$[\Gamma' : \phi(\Gamma)] \leq 2^{s+1} \quad (2.5.1)$$

ve

$$[\Gamma : \psi(\Gamma')] \leq 2^{r+1} \quad (2.5.2)$$

olduğu gösterilebilir.

Burada; (2.5.1) veya (2.5.2) önermelerinden birini kanıtlamak yeterli olacağından; bu çalışmada (2.5.2) nin kanıtına yer verilmiştir. (2.5.1) in kanıtı için de benzer yöntem izlenebilir.

Yukarıdaki iddiadaki (i), (ii) ve (iii) önermelerinden; $\psi(\Gamma')$ nün elemanlarının $\mathcal{O}$ ve x - koordinatı sıfırdan farklı bir rasyonel sayının karesi olan $(x, y) \in \Gamma$ noktalarından ve ayrıca, b bir tamkare olmak üzere, $T = (0, 0)$ dan ibaret olduğu anlaşılmaktadır.

İspat için temel fikir, $\Gamma/\psi(\Gamma')$ bölüm grubundan sonlu elemanlı bir gruba bire-bir bir homomorfizm bulunabilmesidir. Burada, $\mathbf{Q}^*$ sıfırdan farklı rasyonel sayılardan oluşan çarpımsal grubu ve $\mathbf{Q}^{*2}$ de; $\mathbf{Q}^*$ in elemanlarının karelerinden oluşan çarpımsal altgrubu gösterebilir; yani,

$$\mathbf{Q}^* = \{x \in \mathbf{Q} : x \neq 0\} \quad \text{ve} \quad \mathbf{Q}^{*2} = \{x^2 : x \in \mathbf{Q}^*\}$$

olsun. Bu durumda aşağıdaki önerme ile $[\Gamma : \psi(\Gamma')]$ indeksinin sonlu olduğu elde edilir.

Önerme 2.5.1 : $\eta : \Gamma \rightarrow \mathbf{Q}^*/\mathbf{Q}^{*2}$ dönüşümü aşağıdaki gibi tanımlansın:

$$\begin{aligned} \eta(\mathcal{O}) &= 1 \pmod{\mathbf{Q}^{*2}}, \\ \eta(T) &= b \pmod{\mathbf{Q}^{*2}} \quad \text{ve } x \neq 0 \text{ olmak üzere,} \\ \eta(x, y) &= x \pmod{\mathbf{Q}^{*2}} \end{aligned}$$

olsun. Bu durumda,

(a) η bir homomorfizmdir.

(b) Çek $\eta = \psi(\Gamma')$ dır ve bu nedenle, temel homomorfizmin teoreminden, $\Gamma/\psi(\Gamma')$ den $\mathbf{Q}^*/\mathbf{Q}^{*2}$ ne bire-bir bir homomorfizmi vardır.

(c) b sayısını bölen farklı asal sayılar $p_1, p_2, \dots, p_t$ olmak üzere; $\tilde{\eta}$ nin görüntüsü $\mathbf{Q}^*/\mathbf{Q}^{*2}$ nin bir altgrubu olan $\{ \mp p_1^{\varepsilon_1} p_2^{\varepsilon_2} \dots p_t^{\varepsilon_t} : \text{her } \varepsilon_i = 0 \text{ veya } 1 \} / \mathbf{Q}^{*2}$ içinde kapsanır.

(d) $[\Gamma : \psi(\Gamma')] \leq 2^{t+1}$ dir.

İspat : (a) $P = \mathcal{O}$ için $\mathcal{O} = -\mathcal{O}$ olduğundan,

$$\eta(-\mathcal{O}) = \eta(\mathcal{O}) = 1 = \eta(\mathcal{O})^{-1} \pmod{\mathbf{Q}^{*2}},$$

ve $P = T$ için de $T = -T$ olduğundan

$$\eta(-T) = \eta(T) = \eta(T)^{-1} = b \pmod{\mathbf{Q}^{*2}},$$

son olarak, $x \neq 0$ olmak üzere, $P = (x, y)$ için

$$\eta(-P) = \eta(x, -y) = x \equiv \frac{1}{x} = \eta(x, y)^{-1} = \eta(P)^{-1} \pmod{\mathbf{Q}^{*2}}$$

olduğundan, η dönüşümü Γ daki noktaların terslerini, o noktaların η altındaki görüntülerinin terslerine görüntülüyor demektir. Bu nedenle, η nin bir homomorfizm olduğunu ispatlamak için; $P_1 + P_2 + P_3 = \mathcal{O}$ olmak üzere, $\eta(P_1) \cdot \eta(P_2) \cdot \eta(P_3) \equiv 1 \pmod{\mathbf{Q}^{*2}}$ nin sağlandığını göstermek yeterlidir.

Birinci bölümde, bir eliptik eğri üzerindeki üç noktanın toplamının sıfır olması için gerek ve yeter şart olarak bu noktaların aynı doğru üzerinde, yani; doğrudan olmaları gerektiğinden söz edilmişti. Bu doğrunun denklemi; $y = \lambda x + \nu$ ve sözü edilen noktaların x koordinatları sırasıyla x_1, x_2, x_3 olmak üzere, daha önce x_1, x_2, x_3 ün,

$$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x + (c - \nu^2) = 0$$

denkleminin kökleri olduğu açıklanmıştı. Bu; $y^2 = x^3 + ax^2 + bx + c$ kübik denklemi için yapılmıştı ve burada,

$$\begin{aligned} x_1 + x_2 + x_3 &= \lambda^2 - a, \\ x_1 \cdot x_2 + x_2 \cdot x_3 + x_1 \cdot x_3 &= b - 2\lambda\nu, \\ x_1 \cdot x_2 \cdot x_3 &= \nu^2 - c \end{aligned}$$

olduğu bilinmektedir. Bizim incelediğimiz eğriler için $c = 0$ olduğundan dolayı,

$$x_1 \cdot x_2 \cdot x_3 = \nu^2 \in \mathbf{Q}^{*2}$$

elde edilir. Bu da; $\eta(P_1) \cdot \eta(P_2) \cdot \eta(P_3) \equiv 1 \pmod{\mathbf{Q}^{*2}}$ olması demektir.

Burada; P_1, P_2 ve P_3 noktalarının hepsinin $\mathcal{O}$ ve T den farklı olması durumunda ispat bitmiş olur. Aşağıda, bu noktaların $\mathcal{O}$ veya T olması durumları

incelenmiştir. $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, $P_3 = (x_3, y_3)$ ve $P_1 + P_2 = -P_3$ olmak üzere;

(i⁰) $P_1 = P_2 = \mathcal{O}$ ise $P_3 = \mathcal{O}$ olacağından,

$$\eta(P_1 + P_2) = \eta(\mathcal{O}) = \eta(-\mathcal{O}) = \eta(-P_3) \equiv \eta(P_3)^{-1} = \eta(P_1) \cdot \eta(P_2) \pmod{Q^{*2}}$$

dir.

(ii⁰) $P_1 = \mathcal{O}$, $P_2 \neq \mathcal{O}$ ise,

$$\eta(P_1 + P_2) \equiv 1 \cdot \eta(P_2) \equiv \eta(P_1) \cdot \eta(P_2) \pmod{Q^{*2}}$$

olur.

(iii⁰) $P_1 = P_2 = T$ ise,

$$\begin{aligned} \eta(P_1 + P_2) &\equiv \eta(\mathcal{O}) \equiv 1 \pmod{Q^{*2}}, \\ \eta(P_1) \cdot \eta(P_2) &\equiv b^2 \equiv 1 \pmod{Q^{*2}} \end{aligned}$$

olduğundan istenen özellik sağlanır.

(iv⁰) $P_1 = T$, $P_2 \neq T$ olması durumunda, daha önce,

$$T + P_2 = \left(\frac{b}{x_1}, \frac{-b \cdot y_1}{x_1^2} \right)$$

olarak elde edildiğinden,

$$\eta(T + P_2) = \frac{b}{x_1} \equiv b \cdot x_1 \pmod{Q^{*2}}$$

olur.

(v⁰) $P_3 = \mathcal{O}$ veya $P_3 = T$ durumları ayrı ayrı incelenecek olursa; $P_3 = \mathcal{O}$ için $P_1 = -P_2$ olacağından, $x_1 = x_2$ olmalıdır. Bu durumda,

$$\eta(P_1 + P_2) = \eta(\mathcal{O}) = 1 \pmod{Q^{*2}},$$

$$\eta(P_1) \cdot \eta(P_2) = x_1^2 \equiv 1 \pmod{Q^{*2}}$$

olduğundan dolayı, istenen özellik sağlanır. $P_3 = T$ ise de $P_1 + P_2 = T$ den $P_1 + (-T) = -P_2$ olur ve bu da $P_1 + T = -P_2$ durumuna dönüşür; bu durum, daha önce (iv⁰) de incelenmişti. Böylece, (a) şıkkının ispatı tamamlanmış olur.

(b) η nın tanımı ve $\psi(\Gamma')$ nün tanımından sonra verilen İddia i) , ii) , iii) den dolayı, Çek $\eta = \psi(\Gamma')$ olacağı açıktır.

(c) η nın görüntüsünün belirlenmesi için Γ eğrisi üzerindeki rasyonel noktaların x-koordinatlarının belirlenmesi yeterlidir. $(x, y) \in \Gamma$ için $obeb(m, e) = obeb(n, e) = 1$

olmak üzere $x = \frac{m}{c^2}$ ve $y = \frac{n}{c^3}$ biçiminde olduğu birinci bölümde ispatlanmıştı. Bu ifadeler $y^2 = x^3 + ax^2 + bx$ denkleminde yazılıp payda yok edilirse,

$$n^2 = m^3 + am^2c^2 + bmc^4 = m(m^2 + amc^2 + bc^4)$$

olduğu görülür. $d = obcb(m, m^2 + amc^2 + bc^4)$ olarak tanımlansın. Bu durumda, $d|m$ ve $obcb(m, c) = 1$ olması nedeniyle, $d|b$ olmalıdır.

Böylece, $obcb(q_i, r_i) = 1$ olmak üzere,

$$n^2 = m(m^2 + amc^2 + bc^4) = (\mp q_1^{h_1} \cdot q_2^{h_2} \cdots q_u^{h_u})(\mp r_1^{k_1} \cdot r_2^{k_2} \cdots r_v^{k_v})$$

biçiminde yazılabilir. Bu da, n^2 nin bir tamkare olması nedeniyle, $i = 1, 2, \dots, u$ için h_i nin çift sayı; dolayısıyla, $\mp q_1^{h_1} \cdot q_2^{h_2} \cdots q_u^{h_u}$ çarpımının bir tamkare olması gerektiğini ifade eder. Kısacası, $s \in \mathbb{Z}$, $\varepsilon_i \in \{0, 1\}$ ve b nin farklı asal çarpanları $p_1, \dots, p_t$ olmak üzere,

$$m = \mp s^2 \cdot p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_t^{\varepsilon_t}$$

biçimindedir. Bu nedenle,

$$\eta(P) = x = \frac{m}{c^2} \equiv \frac{s^2}{c^2} \cdot (\mp p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_t^{\varepsilon_t}) \equiv \mp p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_t^{\varepsilon_t} \pmod{\mathbb{Q}^{*2}}$$

dir ve böylece, η nın görüntüsünün yukarıda belirtilen küme içinde kapsandığı ispatlanmış olur. $x = 0$ için $m = 0$ olacağından, yukarıda elde edilen ifadelerin sağlanamayabileceği düşünülebilir. Fakat, $m = 0$ durumunda $n = 0$ olması nedeniyle, $(x, y) = (0, 0) = T$ ve η nın tanımı gereği, $\eta(T) = b \pmod{\mathbb{Q}^{*2}}$ olup, $m = 0$ durumu için herhangi bir sorun teşkil etmez.

(d) (b) şikkından, $\Gamma/\psi(\Gamma') = \Gamma/\psi(\Gamma') \cong \eta(\Gamma)$ idi. (c) şikkından da $\eta(\Gamma)$ nın $\{\mp p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_t^{\varepsilon_t} : \text{her } \varepsilon_i = 0 \text{ veya } 1\} / \mathbb{Q}^{*2}$ içinde içerildiğinden, ve bu grubun eleman sayısının 2^{t+1} olması nedeniyle; $\#|\Gamma/\psi(\Gamma')| \leq 2^{t+1}$ sonucuna varılır ki, bu da

$$[\Gamma : \psi(\Gamma')] \leq 2^{t+1}$$

olduğunu ispatlar.

Buraya kadar yapılanlar kısaca hatırlanacak olursa; $\phi : \Gamma \longrightarrow \Gamma'$, $\psi : \Gamma' \longrightarrow \Gamma$ homomorfizm dönüşümleri elde edildi ve $\phi \circ \psi$ ile $\psi \circ \phi$ nin iki katlılık özelliğini sağladıkları ispatlandı. Ayrıca, $[\Gamma : \psi(\Gamma')]$ ve $[\Gamma' : \phi(\Gamma)]$ indekslerinin sonlu olduğu gösterildi. Şimdi de, $[\Gamma : 2\Gamma]$ indeksinin sonlu olduğunu ifade eden Lema 2.5.1 in ispatını bitirmek için aşağıdaki lemanın ispatlanması yeterlidir.

Lema 2.5.2 : $\mathcal{A}$ ve $\mathcal{B}$ Abel grupları ve $\phi : \mathcal{A} \longrightarrow \mathcal{B}$, $\psi : \mathcal{B} \longrightarrow \mathcal{A}$ dönüşümleri

$$\forall a \in \mathcal{A} \quad \text{için} \quad \psi \circ \phi(a) = 2a,$$

$$\forall b \in \mathcal{B} \quad \text{için} \quad \phi \circ \psi(b) = 2b$$

koşullarını sağlayan homomorfizmler; ayrıca, $[\mathcal{B} : \phi(\mathcal{A})]$ ve $[\mathcal{A} : \psi(\mathcal{B})]$ indeksleri sonlu olsun. Bu durumda, $[\mathcal{A} : 2\mathcal{A}]$ sonlu ve daha da fazlası,

$$[\mathcal{A} : 2\mathcal{A}] \leq [\mathcal{A} : \psi(\mathcal{B})] \cdot [\mathcal{B} : \phi(\mathcal{A})]$$

eşitsizliği sağlanır.

İspat : $[\mathcal{A} : \psi(\mathcal{B})]$ sonlu olduğundan, $\psi(\mathcal{B})$ nin $\mathcal{A}$ içinde sonlu çokluktaki eşkümelerinin temsilcileri olan $a_1, a_2, \dots, a_n$ elemanları bulunabilir. Benzer biçimde, $[\mathcal{B} : \phi(\mathcal{A})]$ sonlu olduğundan istenen özelliği sağlayan $b_1, b_2, \dots, b_m$ elemanları seçilebilir. Bu durumda,

$$\mathcal{S} = \{a_i + \psi(b_j) : 1 \leq i \leq n, 1 \leq j \leq m\}$$

kümesi $\mathcal{A}/2\mathcal{A}$ eşkümelerinin tüm temsilcilerini içerir. Bunu görmek için, $a \in \mathcal{A}$ olsun. $a_1, a_2, \dots, a_n$ elemanları $\mathcal{A}/\psi(\mathcal{B})$ nin eşkümelerinin temsilcileri olduğundan; $a - a_i \in \psi(\mathcal{B})$ ve dolayısıyla, $\exists b \in \mathcal{B} \ni a - a_i = \psi(b)$ dir. Benzer şekilde; $\exists b_j \in \mathcal{B} \ni b - b_j \in \phi(\mathcal{A})$ ve $\exists \tilde{a} \in \mathcal{A} \ni b - b_j = \phi(\tilde{a})$ olur. Bu durumda;

$$\begin{aligned} a &= a_i + \psi(b) = a_i + \psi(b_j + \phi(\tilde{a})) \\ &= a_i + \psi(b_j) + \psi(\phi(\tilde{a})) \\ &= a_i + \psi(b_j) + 2\tilde{a} \end{aligned}$$

olur. Bu da; a nın $\mathcal{A}/2\mathcal{A}$ daki temsilcisinin $a_i + \psi(b_j) \in \mathcal{S}$ olduğunu gösterir. Buradan $[\mathcal{A} : 2\mathcal{A}]$ nin sonlu ve ayrıca

$$[\mathcal{A} : 2\mathcal{A}] \leq [\mathcal{A} : \psi(\mathcal{B})] \cdot [\mathcal{B} : \phi(\mathcal{A})]$$

olduğu sonucuna varılır.

Böylece, Lema 2.5.2 nin yardımıyla Lema 2.5.1 in ispatı tamamlanmış olup, aşağıda ispatı verilecek olan teorem yardımıyla da Mordell Teoremi'nin ispatı için gerekli olan tüm hazırlıklar tamamlanmış olacaktır.

Teorem 2.5.1 (İniş Teoremi) : Γ bir değişmeli grup ve $h : \Gamma \rightarrow [0, \infty)$ fonksiyonu aşağıdaki üç özelliği sağlasın:

(a) $\forall M \in \mathbb{R}$ için $\{P \in \Gamma : h(P) \leq M\}$ sonlu olsun,

(b) Γ nın her P' elemanı için, öyle bir k' sabiti bulunabilsin ki; $\forall P \in \Gamma$ için $h(P + P') \leq 2h(P) + k'$ eşitsizliği sağlansın,

(c) Öyle bir k sabiti bulunsun ki; $\forall P \in \Gamma$ için $4h(P) \leq h(2P) + k$ olsun.

Ve bunlara ek olarak;

(d) $[\Gamma : 2\Gamma]$ indeksi sonlu olsun.

Bu takdirde, Γ sonlu üretilmiş bir Abel grubu olur.

İspat : $[\Gamma : 2\Gamma] = n$ ve $R_1, R_2, \dots, R_n \in \Gamma$ olmak üzere;

$$\Gamma/2\Gamma = \{R_1 + 2\Gamma, R_2 + 2\Gamma, \dots, R_n + 2\Gamma\}$$

olsun. $P \in \Gamma$ verilmiş olsun. Bu takdirde, $1 \leq i_1 \leq n$ olmak üzere, $P + 2\Gamma = R_{i_1} + 2\Gamma$ olacak şekilde bir $R_{i_1} \in \Gamma$ vardır. Bu da;

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

eşitliği sağlanacak şekilde bir $P_1 \in \Gamma$ noktasının varlığını ifade eder. P için yapılan işlemler, P_1 için yapılsa;

$$\begin{array}{rclcl} P_1 & - & R_{i_2} & = & 2P_2, \quad P_2 \in \Gamma, \text{ ve benzer şekilde,} \\ P_2 & - & R_{i_3} & = & 2P_3, \quad P_3 \in \Gamma, \\ & & \cdot & & \cdot \\ & & \cdot & & \cdot \\ & & \cdot & & \cdot \\ P_{m-1} & - & R_{i_m} & = & 2P_m, \quad P_m \in \Gamma \end{array}$$

elde edilir.

Yukarıdaki eşitliklerden yararlanılarak;

$$P = R_{i_1} + 2R_{i_2} + 2^2R_{i_3} + \cdots + 2^{m-1}R_{i_m} + 2^mP_m$$

olduğu ve burada P nin R_i ler ve P_m noktasıyla üretildiği görülebilir. R_i ler sonlu sayıda olduğu için, bundan sonraki adımlardaki amacımız; m sayısını yaterince büyük bir şekilde seçerek, $h(P_m)$ yi belli bir sabit sayıdan küçük olacak şekilde belirlemek olacak.

Teoremin (b) özelliğinde P' yerine $-R_i$, $1 \leq i \leq n$, alındığında $\forall P \in \Gamma$ ve her $i = 1, \dots, n$ için $h(P - R_i) \leq 2h(P) + k_i$ olacak şekilde k_i sabitlerinin varlığı bilinmektedir. $k' = \max\{k_1, k_2, \dots, k_n\}$ olarak seçilirse; $\forall P \in \Gamma$ ve $i = 1, \dots, n$ için $h(P - R_i) \leq 2h(P) + k'$ olacağı açıktır.

Ayrıca, $P_j \in \{P, P_1, P_2, \dots\}$ için, (c) özelliğinden;

$$\begin{aligned} 4h(P_j) &= h(2P_j) + k \\ &= h(P_{j-1} - R_{i_j}) + k \\ &= 2h(P_{j-1} + k') + k, \\ h(P_j) &\leq \frac{3}{4}h(P_{j-1}) - \frac{1}{4}[h(P_{j-1}) - (k' + k)] \end{aligned}$$

elde edilir. Burada,

$$k + k' \leq h(P_{j-1}) \text{ için } h(P_j) \leq \frac{3}{4}h(P_{j-1})$$

olduğundan dolayı; $h(P_m) \leq k' + k$ olacak şekilde bir $m \in \mathbb{N}$ vardır. Böylece, verilen P elemanı, $a_1, a_2, \dots, a_n \in \mathbb{N}$ ve $h(S) \leq k' + k$ olmak üzere

$$P = a_1R_1 + a_2R_2 + \cdots + a_nR_n + 2^mS$$

biçiminde ifade edilebilir. (a) ve (d) özelliklerinden de

$$\{R_1, R_2, \dots, R_n\} \cup \{S \in \Gamma : h(S) \leq k' + k\}$$

sonlu kümesinin, Γ yı ürettiği sonucuna varılır, bu da Γ nın sonlu üretilmiş olduğunu ispatlar.

Bir rasyonel noktası olan her $\mathcal{C}$ eliptik eğrisi için $\mathcal{C}(\mathbb{Q})$ grubunun sonlu üretilmiş bir Abel grubu olduğunu ifade eden Mordell Teoreminin genel ispatına, gerek ispat yönteminin burada yapılan ispat yöntemine benzememesi, gerekse ispatta ileri derecede cebir kullanılması nedeniyle, yer verilmemiştir. Bunun için burada sözü edilen tüm eliptik eğriler için değil de, $f(x) = 0$ ın bir rasyonel kökü olması durumunda ki (mertebesi iki olan bir rasyonel noktaya sahip); eliptik eğriler için Mordell Teoremi'nin ispatına yer verilmiştir.

Teorem 2.5.2 (Mordell) : $\mathcal{C}$; $a, b \in \mathbb{Z}$ olmak üzere $y^2 = x^3 + ax^2 + bx$ denkleminin belirlediği bir eliptik eğri olsun. Bu durumda, $\mathcal{C}(\mathbb{Q})$ grubu sonlu üretilmiş bir Abel grubudur.

İspat : Lema 2.2.1 , Lema 2.2.2 , Lema 2.3.1 ve Lema 2.5.1 e göre $\mathcal{C}(\mathbb{Q}) = \Gamma$ iniş teoremindeki dört özelliği sağladığından dolayı, $\mathcal{C}(\mathbb{Q})$ nun sonlu üretilmiş bir Abel grubu olacağı açıktır.

Mordell Teoremi, $\mathcal{C}$ üzerinde sonlu rasyonel nokta kullanılarak diğer tüm rasyonel noktaların, geometriden yararlanılarak, üretilebileceğini ifade eder. İniş teoreminin ispat yönteminde ise, bir eliptik eğri verildiğinde, yukarıda sözü edilen üreteçler kümesinin nasıl belirleneceği konusunda yol gösterilmektedir. Buna rağmen, tüm eliptik eğriler için üreteçlerin belirlenmesi yönteminin o kadar da kolay olduğu söylenemez. Bir sonraki kısımda, Mordell Teoremi'nin uygulaması ile ilgili olarak bir kaç örnek incelenecektir.

2.6. Mordell Teoremi'nin Bazı Uygulamaları

Bu kısımda, Mordell Teoremi ile ilgili sayısal örneklere yer verilecektir.

Bir önceki kısımda, $\mathcal{C} : y^2 = x^3 + ax^2 + bx$ eliptik eğrisi üzerindeki rasyonel noktalar grubu olan Γ nın sonlu üretilmiş bir Abel grubu olduğu detaylıca açıklanmıştı. Buradan, Sonlu Üretilmiş Abel Gruplarının Temel Teoreminden yararlanarak, Γ nın

$$\Gamma \cong \underbrace{\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{r \text{ tane}} \oplus \mathbb{Z}_{p_1^{v_1}} \oplus \mathbb{Z}_{p_2^{v_2}} \oplus \cdots \oplus \mathbb{Z}_{p_s^{v_s}} \quad (2.6.1)$$

biçiminde olduğu sonucuna varılır ki; her $i = 1, \dots, s$ için p_i bir asal sayı ve $v_i \in \mathbb{N}$ olmak üzere; $\mathbb{Z}_{p_i^{v_i}}$, $p_i^{v_i}$ modülüne göre (toplamsal) $p_i^{v_i}$ elemanlı devirli grubu göstermektedir. Bu izomorfizmin bir sonucu olarak $\exists P_1, \dots, P_r, Q_1, \dots, Q_s \in \Gamma$ öyle ki, $\forall P \in \Gamma$ için

$$P = n_1 P_1 + \cdots + n_r P_r + m_1 Q_1 + \cdots + m_s Q_s$$

biçiminde olur. Burada; n_i katsayıları P tarafından tektürlü olarak ve ayrıca m_i katsayıları da; $(\text{mod } p_i^{v_i})$ ye göre belirlenir. r doğal sayısı da; Γ nın rank ı olarak adlandırılır. Γ nın sonlu olması için gerek ve yeter şartın $r = 0$ olduğu kolayca

görülebılır. Bu durumda,

$$\mathbf{Z}_{p_1^{v_1}} \oplus \mathbf{Z}_{p_2^{v_2}} \oplus \cdots \oplus \mathbf{Z}_{p_s^{v_s}}$$

altgrubu Γ nın sonlu mertebeli elemanlarından oluşur ve bu grubun mertebesi $p_1^{v_1} p_2^{v_2} \cdots p_s^{v_s}$ dir. Tabii ki burada, Γ nın üreticileri için birçok seçenek olması nedeniyle $P_1, P_2, \dots, P_r, Q_1, \dots, Q_s$ noktaları tektürlü belirli değildir.

Γ nın sonlu üretildiğini ispatlarken, $\Gamma/2\Gamma$ bölüm grubunun temsilcilerinden faydalanılmıştı. Bunun için $\Gamma/2\Gamma$ nın temsilcilerini tam olarak belirleyebilmek büyük önem kazanır ve bu elemanları belirlemede aşağıda elde edilecek sonuçların kullanılmasıyla büyük kolaylıklar sağlanacaktır.

(2.6.1) de ki izomorfizmden yararlanarak;

$$2\Gamma \cong 2\mathbf{Z} \oplus 2\mathbf{Z} \oplus \cdots \oplus 2\mathbf{Z} \oplus 2\mathbf{Z}_{p_1^{v_1}} \oplus 2\mathbf{Z}_{p_2^{v_2}} \oplus \cdots \oplus 2\mathbf{Z}_{p_s^{v_s}}$$

olacağından dolayı;

$$\Gamma/2\Gamma \cong \mathbf{Z}/2\mathbf{Z} \oplus \cdots \oplus \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}_{p_1^{v_1}}/2\mathbf{Z}_{p_1^{v_1}} \oplus \cdots \oplus \mathbf{Z}_{p_s^{v_s}}/2\mathbf{Z}_{p_s^{v_s}}$$

olur. Burada; $\mathbf{Z}/2\mathbf{Z} \cong \mathbf{Z}_2$ ve

$$\mathbf{Z}_{p_i^{v_i}}/2\mathbf{Z}_{p_i^{v_i}} \cong \begin{cases} \mathbf{Z}_2 & , \quad p_i = 2 \\ 0 & , \quad p_i \neq 2 \end{cases}$$

olması nedeniyle;

$$[\Gamma/2\Gamma] = 2^{r+(p_j=2 \text{ olan } j \text{ lerin sayısı})}$$

olacağı açıktır.

Diğer yandan mertebesi iki olan tüm elemanlardan oluşan altgrup $\Gamma[2]$ ile gösterilecek olursa; bu altgrubun eleman sayısı aşağıdaki gibi belirlenebilir.

Sözü edilen belirleme için, öncelikle “ acaba hangi durumlar için

$$2(n_1P_1 + \cdots + n_rP_r + m_1Q_1 + \cdots + m_sQ_s) = \mathcal{O}$$

olur? ” sorusu cevaplandırılmalıdır. İlk olarak, $n_i = 0$ ve $2m_j \equiv 0 \pmod{p_j^{v_j}}$ olması durumunda istenen özellik sağlanır. Ayrıca; eğer p bir tek asal sayı ve $2m \equiv 0 \pmod{p^v}$ ise, $m \equiv 0 \pmod{p^v}$ olduğu; $p = 2$ ve $2m \equiv 0 \pmod{p^v}$ için de $m \equiv 0 \pmod{p^{v-1}}$ kongruansının sağlandığı görülür. Bu nedenle, $\Gamma[2]$ altgrubunun eleman sayısı; $\#\Gamma[2]$ ile gösterilirse;

$$\#\Gamma[2] = 2^{(p_j=2 \text{ olan } j \text{ lerin sayısı})}$$

olarak elde edileceğinden dolayı

$$[\Gamma : 2\Gamma] = 2^r \cdot \#\Gamma[2]$$

sonucuna varılır ve bu formül rankı r olan tüm sonlu üretilmiş Abel grupları için sağlanır.

Aşağıdaki açıklamaların ışığı altında; $\# \Gamma[2]$ nin belirlenmesinin sanıldığı kadar zor olmadığı ortaya çıkar. Çünkü; bir $P = (x, y)$ noktasının mertebesinin iki olması için gerek ve yeter şartın $y = 0$ olması gerçeğinden hareketle;

$$\# \Gamma[2] = \begin{cases} 2 & , \quad a^2 - 4b \text{ bir tamkare değil} \\ 4 & , \quad a^2 - 4b \text{ bir tamkare} \end{cases}$$

olduğu görülür.

Bu sonuçtan ve Lema 2.5.1 in ispatından yararlanarak Γ nın rankı için bir formül geliştirilebilir.

Daha önce, $\phi : \Gamma \rightarrow \Gamma'$ ve $\psi : \Gamma' \rightarrow \Gamma$ dönüşümlerinin uygun bir şekilde tanımlanmasıyla, $\psi \circ \phi(P) = 2P$ özelliğinin sağlanacağı açıklanmıştı. Bu nedenle,

$$[\Gamma : 2\Gamma] = [\Gamma : \psi \circ \phi(\Gamma)]$$

olur. Ayrıca; $P_1 \in 2\Gamma$ için $\exists P_2 \in \Gamma$ öyle ki $P_1 = 2P_2$ ve

$$P_1 = 2P_2 = \psi \circ \phi(P_2) = \psi(\phi(P_2))$$

de $\phi(P_2) \in \Gamma'$ olduğundan dolayı; $P_1 \in \psi(\Gamma')$ olması gerektiğinden, aşağıdaki alt-gruplar zinciri oluşturulabilir:

$$2\Gamma \leq \psi(\Gamma') \leq \Gamma.$$

Buradan da indekslerin özelliklerinden

$$[\Gamma : 2\Gamma] = [\Gamma : \psi(\Gamma')] \cdot [\psi(\Gamma') : \psi \circ \phi(\Gamma)] \quad (2.6.2)$$

eşitliği sağlanır. Bundan sonraki amacımız; $[\psi(\Gamma') : \psi \circ \phi(\Gamma)]$ indeksini analiz etme olduğundan burada bir hatırlatma yapmak gerekir: $\mathcal{A}$ bir Abel grubu; $\mathcal{B}$, $\mathcal{A}$ içinde sonlu indekse sahip bir altgrup ve $\mathcal{A}'$ herhangi bir altgrup olmak üzere, $\psi : \mathcal{A} \rightarrow \mathcal{A}'$ bir homomorfizm olsun. Bu durumda, grup teorisinin temel izomorfizm teoreminden,

$$\frac{\psi(\mathcal{A})}{\psi(\mathcal{B})} \cong \frac{\mathcal{A}}{\mathcal{B} + \text{Çek}(\psi)} \cong \frac{\mathcal{A}/\mathcal{B}}{(\mathcal{B} + \text{Çek}(\psi))/\mathcal{B}} \cong \frac{\mathcal{A}/\mathcal{B}}{(\text{Çek}(\psi))/(\text{Çek}(\psi) \cap \mathcal{B})}$$

olacağından, $[\psi(\mathcal{A}) : \psi(\mathcal{B})]$ indeksi için

$$[\psi(\mathcal{A}) : \psi(\mathcal{B})] = \frac{[\mathcal{A} : \mathcal{B}]}{[\text{Çek}(\psi) : \text{Çek}(\psi) \cap \mathcal{B}]}$$

formülü elde edilir.

Burada $\mathcal{A} = \Gamma'$, $\mathcal{B} = \phi(\Gamma)$ olarak düşünüldüğünde;

$$[\Gamma : 2\Gamma] = \frac{[\Gamma : \psi(\Gamma')] \cdot [\Gamma' : \phi(\Gamma)]}{[\text{Çek}(\psi) : \text{Çek}(\psi) \cap \phi(\Gamma)]}$$

olur. Ayrıca; $T' \in \phi(\Gamma) \iff b' = a^2 - 4b$ bir tamkare ifadesi daha önce ispatlandığından ve $\zeta\epsilon k\psi = \{\mathcal{O}', T'\} \in \phi(\Gamma)$ olduğundan dolayı;

$$[\zeta\epsilon k\psi : \zeta\epsilon k(\psi) \cap \phi(\Gamma)] = \begin{cases} 2 & , \quad b' \text{ bir tamkare değil} \\ 1 & , \quad b' \text{ bir tamkare} \end{cases}$$

elde edilir. Böylece,

$$2^r = \frac{[\Gamma : 2\Gamma]}{\#\Gamma[2]} = \left[\frac{[\Gamma : \psi(\Gamma')] \cdot [\Gamma' : \phi(\Gamma)]}{4} \right]$$

sonucuna varılır ki, bu da yukarıdaki eşitlikteki, payların 2 nin kuvvetleri biçiminde olduğunu ifade eder.

Önerme 2.4.1 in (d) şıkından yararlanarak; $[\Gamma : \psi(\Gamma')]$ ve $[\Gamma' : \phi(\Gamma)]$ indekslerinin sonlu olduğu kabul edilebilir. Doğal olarak, bu indekslerin tam olarak belirlenip belirlenmeyeceği sorusu akla gelebilir. Bunun için aşağıdaki hatırlatmalara gerek duyulur. Daha önce, Lema 2.5.1 in ispatını yaparken,

$$\eta : \Gamma \longrightarrow \mathbb{Q}^*/\mathbb{Q}^{*2} \text{ dönüşümünün}$$

$$\begin{aligned} \eta(\mathcal{O}) &= 1 \pmod{\mathbb{Q}^{*2}}, \\ \eta(T) &= b \pmod{\mathbb{Q}^{*2}} \text{ ve } x \neq 0 \text{ için} \\ \eta(x, y) &= x \pmod{\mathbb{Q}^{*2}} \end{aligned}$$

olarak tanımlandığında; $\zeta\epsilon k(\eta) = \psi(\Gamma')$ olduğu görülmüştü. Böylece,

$$\Gamma/\psi(\Gamma') \cong \Gamma/\zeta\epsilon k(\eta) \cong \eta(\Gamma)$$

olur. Bu da

$$[\Gamma : \psi(\Gamma')] = \#\eta(\Gamma)$$

olduğunu ispatlar. Benzer biçimde,

$$\eta' : \Gamma' \longrightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$$

homomorfizmi tanımlanarak,

$$[\Gamma' : \phi(\Gamma)] = \#\eta'(\Gamma')$$

eşitliği görülebilir.

Sonuç olarak bu indekslerle ilgili eşitliklerden yararlanarak Γ nın rankının hesaplanmasında kullanılacak olan

$$2^r = \frac{\#\eta(\Gamma) \cdot \#\eta'(\Gamma')}{4}$$

formülü elde edilebilir. Burada, $\eta(\Gamma)$ nın elemanları, genel olarak, Γ üzerindeki noktaların x koordinatlarının $\pmod{\mathbb{Q}^{*2}}$ ne göre tanımlandığından dolayı; bazı durumlarda bu noktaları belirlemek ve böylece $\#\eta(\Gamma)$ yı belirlemek o kadar da zor değildir.

Daha önceki kısımlarda $P = (x, y) \in \Gamma$ için $m, n, c \in \mathbf{Z}$, $c > 0$ olmak üzere (x, y) noktasının

$$x = \frac{m}{c^2} \quad \vee \quad y = \frac{n}{c^3}$$

biçimde (en sadeleştirilmiş şekilde) ifade edilebileceği ispatlanmıştı.

Eğer $m = 0$ ise, $(x, y) = T$ ve $\eta(T) = b$ olur. Bu da; $T \in \Gamma$ olması nedeniyle her zaman için $b \in \eta(\Gamma)$ olması demektir. Eğer $a^2 - 4b$ bir tamkare, yani $a^2 - 4b = d^2$ biçiminde ise, Γ nın mertebesi 2 olan noktalarının y koordinatı sıfır (dolayısıyla $n = 0$) olacağından dolayı, O ve T den başka mertebesi iki olan diğer noktalar

$$\left(\frac{-a+d}{2}, 0 \right) \quad \vee \quad \left(\frac{-a-d}{2}, 0 \right)$$

dır. Böylece, $a^2 - 4b = d^2$ için $\frac{-a \mp d}{2} \in \eta(\Gamma)$ olduğu sonucuna varılır. Aksi durumda, yani $a^2 - 4b$ bir tamkare değil ise, mertebesi 2 olan noktalar O ve T den ibaret olduğundan, istenenler sağlanır. Bu şekilde; $m = 0$ veya $n = 0$ için olası durumlar incelendiğinden, bundan sonra $m, n \neq 0$ durumları incelenecektir. $x = \frac{m}{c^2}$ ve $y = \frac{n}{c^3}$ değerleri; $y^2 = x^3 + ax^2 + bx$ denkleminde yerleştirildiğinde,

$$\begin{aligned} n^2 &= m^3 + am^2e^2 + bme^4 \\ &= m(m^2 + ame^2 + be^4) \end{aligned} \quad (2.6.3)$$

eşitliği elde edilir. Burada; $b_1 = \text{obeb}(m, b)$ ve $m, b_1 > 0$ olmak üzere $m = b_1.m_1$, $b = b_1.b_2$, $\text{obeb}(m_1, b_2) = 1$ ve $m_1 > 0$ özelliklerini sağlayan $m_1, b_2 \in \mathbf{Z}$ vardır. Bu eşitlikler (2.6.3) te yerleştirildiğinde:

$$\begin{aligned} n^2 &= b_1.m_1(b_1^2m_1^2 + ab_1m_1e^2 + b_1b_2e^4) \\ &= b_1^2.m_1(b_1m_1^2 + am_1e^2 + b_2e^4) \end{aligned}$$

olur. Böylece, $b_1^2|n^2$ ve dolayısıyla $b_1|n$ elde edilir ki, bu da $n = b_1.n_1$ biçiminde ifade edilebileceğini gösterir. Bu nedenle,

$$n_1^2 = m_1(b_1m_1^2 + am_1e^2 + b_2e^4)$$

dür ve ayrıca, $\text{obeb}(b_2, m_1) = \text{obeb}(e, m_1) = 1$ olduğundan dolayı da m_1 ile $b_1m_1^2 + am_1e^2 + b_2e^4$ aralarında asal olmalıdır. Ayrıca, çarpımları bir tamkare ve $m_1 > 0$ olması; m_1 ve $b_1m_1^2 + am_1e^2 + b_2e^4$ ün her ikisinin de bir tamkare olmasını gerektirir. Bu da n_1 sayısının

$$M^2 = m_1 \quad \vee \quad N^2 = b_1m_1^2 + am_1e^2 + b_2e^4$$

olmak üzere, $n_1 = MN$ biçiminde çarpanlara ayrılabilirdiğini gösterir. m_1 in yok edilmesiyle de

$$N^2 = b_1M^4 + aM^2e^2 + b_2e^4$$

ve

$$x = \frac{m}{c^2} = \frac{b_1.m_1}{c^2} = \frac{b_1.M^2}{c^2}$$

$$y = \frac{n}{e^3} = \frac{b_1 \cdot n_1}{e^3} = \frac{b_1 \cdot MN}{e^3}$$

eşitlikleri elde edilir.

Böylece, eğri üzerindeki her P noktasının $x \neq 0$ koordinatı ($\text{mod } Q^{*2}$) düşünüldüğünde, $x = \frac{b_1 \cdot M^2}{e^2}$ olduğundan dolayı b_1 , b nin bir çarpanı olmak üzere, bir b_1 değerine eşit olur. Bu da, b_1 in alacağı değerler sonlu sayıda olacağından dolayı büyük kolaylıklar sağlayacaktır.

Buraya kadar yapılan açıklamaların ışığı altında, $\eta(\Gamma)$ nin eleman sayısını belirlemenin o kadar da zor olmadığı sonucuna varılır. Çünkü, b tamsayısını $b = b_1 \cdot b_2$ olacak şekilde olası tüm çarpanlarına ayırıp, her çarpım şekli için

$$N^2 = b_1 \cdot M^4 + a \cdot M^2 \cdot e^2 + b_2 \cdot e^4$$

denklemini yazılır. Burada; a , b_1 , b_2 nin sabitler M , e , N nin de bilinmeyenler olduğuna dikkat edilmelidir. Bu durumda; $\eta(\Gamma)$, b ($\text{mod } Q^{*2}$) ve yukarıda sözü edilen denklemde $M \neq 0$ olacak şekildeki çözümlere sahip denklemlerdeki b_1 ($\text{mod } Q^{*2}$) den oluşmaktadır. Ayrıca, $x = \frac{m}{e^2}$ ve $y = \frac{n}{e^3}$ ün sadeleştirilmiş biçim olması nedeniyle,

$$\begin{aligned} \text{obeb}(M, e) &= \text{obeb}(N, e) = \text{obeb}(b_1, e) = 1, \\ \text{obeb}(b_2, m_1) &= 1 \text{ olduğu için } \text{obeb}(b_2, M) = \text{obeb}(M, N) = 1 \end{aligned}$$

ve ayrıca, mümkün olabilecek tüm olası çözümlerin, bu yan koşulların hepsini birden sağlaması gerekmektedir.

Yukarıda genellemede sanki $\eta(\Gamma)$ nin $a^2 - 4b = d^2$ olması durumunda mertebesi 2 olan ve $\mathcal{O}$, T noktalarından farklı olan iki noktanın eksik kaldığı veya unutulduğu düşünülebilir. Fakat,

$$b = \left(\frac{-a + d}{2} \right) \left(\frac{-a - d}{2} \right)$$

olması nedeniyle,

$$N^2 = \left(\frac{-a \mp d}{2} \right) M^4 + a M^2 e^2 + \left(\frac{-a \mp d}{2} \right) e^4$$

denklemini için $(M, e, N) = (1, 1, 0)$ bir çözüm oluşturur ve böylece mertebesi 2 olan bu iki noktanın da, yukarıda sözü edilen genel inceleme içinde yer aldığı görülebilir.

Buraya kadar yapılan işlemler kısaca açıklanacak olursa, önce

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

denklemini için $b = b_1 \cdot b_2$ olacak şekilde tüm olası çarpanlara ayırma işlemi yapıp ve her durum için

$$N^2 = b_1 \cdot M^4 + a \cdot M^2 \cdot e^2 + b_2 \cdot e^4$$

denkleminin $M \neq 0$ olmak üzere (M, e, N) çözümünün olup olmadığı incelenir. Eğer çözüm varsa,

$$x = \frac{b_1 \cdot M^2}{e^2}, \quad y = \frac{b_1 \cdot M \cdot N}{e^3}$$

olduğundan dolayı, çözüme sahip b_1 ler için

$$\eta(\Gamma) = \{b \pmod{\mathbf{Q}^{*2}}, \quad b_1 \pmod{\mathbf{Q}^{*2}}\}$$

olarak belirlenir.

Bu yöntemin en kötü tarafı, sözü edilen denklemlerin çözümünün olup olmadığına karar vermek için elimizde bir metodun olmamasıdır. Bu küçük zorluğa rağmen; $\#\eta(\Gamma)$ yı, benzer biçimde $\#\eta'(\Gamma')$ nü ve dolayısıyla da rankı hesaplamak için bir yöntemle sahip bulunmaktayız.

Bu açıklamalardan sonra, Mordell Teoremi'nin uygulamalarına yer verilebilir, yani verilen $\mathcal{C}$ eliptik eğrileri için $\mathcal{C}(\mathbf{Q})$ nun hangi gruba izomorf olduğu, rankı hesaplamak için geliştirilen yukarıdaki yöntem yardımıyla belirlenebilir.

Örnek 2.6.1 : $\mathcal{C} : y^2 = x^3 - x$ olmak üzere, $\mathcal{C}(\mathbf{Q})$ nun ne tür bir gruba izomorf olduğunu belirlemek için öncelikle; $b = -1$ i mümkün olan tüm çarpanlarına ayırmak gerekir: $b = -1.1$ ve $b = 1.(-1)$ dışında b nin farklı bir çarpanlarına ayrılış şekli sözkonusu olmadığından dolayı, $b_1 = \mp 1$ olabilir. Tanım gereği

$$\eta(\mathcal{O}) = 1 \quad \text{ve} \quad \eta(T) = b = -1$$

olduğundan dolayı da; $\eta(\Gamma) = \{\mp 1 \pmod{\mathbf{Q}^{*2}}\}$ ve $\#\eta(\Gamma) = 2$ olduğu bu şekilde kolayca görülebilir.

Diğer yandan, $\mathcal{C}'$ nün yukarıdaki tanımından dolayı,

$$\mathcal{C}' : y^2 = x^3 + 4x$$

olacağı açıktır. Burada; $a' = 0$ ve $b' = 4$ olduğundan b_1 için mümkün olabilecek durumlar,

$$\mp 4 \equiv \mp 1 \pmod{\mathbf{Q}^{*2}}$$

kongruansı gözönüne alındığında; $b_1 = \mp 1, \mp 2$ olabilir. Bu durumda, aşağıdaki dört denklem

$$\begin{aligned} \text{(i)} \quad N^2 &= M^4 + 4e^4, \\ \text{(ii)} \quad N^2 &= -M^4 - 4e^4, \\ \text{(iii)} \quad N^2 &= 2M^4 + 2e^4, \\ \text{(iv)} \quad N^2 &= -2M^4 - 2e^4 \end{aligned}$$

için (M, e, N) çözümlerinin olup olmadığı sorusu cevaplandırılmalıdır. $N^2 > 0$ olacağından dolayı, (ii) ve (iv) denklemlerinin hiç bir tamsayı çözümünün olmadığı kolayca görülebilir. Tanım gereği $\eta'(\mathcal{O}') = 1 \pmod{\mathbf{Q}^{*2}}$ olması nedeniyle, $b_1 = 1$

için ifade edilen (i) denkleminin çözümü olup olmadığının ayrıca incelenmesine gerek yoktur; bu durumda çözüm olarak $(M, c, N) = (1, 0, 1)$ alınır. Dikkat edilirse, $c = 0$ olması durumu $P = \mathcal{O}'$ olmasına karşılık gelmektedir.

Diğer yandan,

$$2^r = \frac{\#\eta(\Gamma) \cdot \#\eta'(\Gamma')}{4}$$

olduğundan dolayı, $\#\eta(\Gamma) \cdot \#\eta'(\Gamma')$ çarpımı en azından 4 olmalıdır; bu da $\#\eta'(\Gamma') = 2$ olmasını; yani, (iii) denkleminin bir tamsayı çözüme sahip olduğunu ifade eder. Bu açıklama yapılmadan da $(M, c, N) = (1, 1, 2)$ nin (iii) denkleminin bir çözümü olduğu, deneme yanılma yöntemiyle de bulunabilir. Bu da Γ nın (dolayısıyla da Γ' nün) rankının sıfır olduğunu gösterir; böylece, $\mathcal{C}$ ve $\mathcal{C}'$ nün rasyonel noktalar grubu olan Γ ve Γ' nün tüm noktalarının mertebelerinin sonlu olduğu sonucuna varılır.

Burada, mertebesi sonlu olan noktaların belirlenmesinde, daha önce birinci bölümde ifade ve ispat edilen Nagell-Lutz Teoremi kullanılabilir. Buna göre, eğer $P = (x, y) \in \Gamma$ bir sonlu nokta ise, ya $y = 0$ ya da $y|b^2(a^2 - 4b) = 4$ olması gerekiyor. $y = 0$ olan noktalar $(0, 0)$, $(\mp 1, 0)$ olduğundan ve ayrıca 4 ü bölen sayılar için yani; $y = \mp 1, \mp 2, \mp 4$ olması durumunda, eğri üzerinde bu y değerlerine karşılık hiç bir x rasyonel sayısı bulunmadığından dolayı,

$$\mathcal{C}(\mathbb{Q}) = \{\mathcal{O}, (0, 0), (-1, 0), (1, 0)\}$$

olduğu elde edilir. Ayrıca, $y = 0$ olması nedeniyle bu noktaların her birinin mertebesi 2 dir ve böylece,

$$\mathcal{C}(\mathbb{Q}) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

sonucuna varılır.

Benzer biçimde, Γ' nün sonlu mertebeli noktaları, Nagell-Lutz Teoremi'nin kullanılmasıyla; ya $y = 0$ ya da $y|b'^2(a'^2 - 4b') = -256$ olacağından dolayı; gerek bilgisayar yardımıyla gerekse uzun hesaplamalar sonucunda;

$$\mathcal{C}'(\mathbb{Q}) = \{\mathcal{O}, (0, 0), (2, 4), (2, -4)\}$$

olduğu ortaya çıkar. Burada, mertebesi 2 olan yalnızca bir nokta $(0, 0)$, olduğundan veya $(2, 4) + (2, -4) = (0, 0)$ olması nedeniyle,

$$\mathcal{C}'(\mathbb{Q}) \cong \mathbb{Z}_4$$

olur.

Örnek 2.6.2 : $\mathcal{C} : y^2 = x^3 + x$ eğrisi için $\mathcal{C}(\mathbb{Q})$ nun hangi gruba izomorf olduğu araştırılırken $b = 1 = 1.1 = (-1).(-1)$ olması nedeniyle, sadece $b_1 = \mp 1$ durumu söz konusudur. Burada: $\eta(\mathcal{O}) = \eta(T) = 1 \pmod{\mathbb{Q}^{*2}}$ ve $b_1 = -1$ için $N^2 = -M^4 - e^4$ eşitliğinin hiç tamsayı çözümü olmadığından, $\eta(\mathcal{C}(\mathbb{Q})) = \{1 \pmod{\mathbb{Q}^{*2}}\}$ ve böylece $\#\eta(\Gamma) = 1$ olur.

Diğer yandan, $C' : y^2 = x^3 - 4x$ olacağından, burada $a = 0$, $b = -4$ ve $\mp 4 \equiv \mp 1 \pmod{Q^{*2}}$ sözkonusudur. Böylece; $b_1 = \mp 1, \mp 2$ olabilir. Yukarıdaki; Örnek 2.6.1 de olduğu gibi, rankın

$$2^r = \frac{\# \eta(C(Q)) \cdot \# \eta'(C'(Q))}{4}$$

ve $\# \eta(C(Q)) = 1$ olması nedeniyle $\# \eta'(C'(Q)) = 4$ olmalıdır; bu da

$$\# \eta'(C'(Q)) = \{\mp 1, \mp 2 \pmod{Q^{*2}}\}$$

olmasını gerektirir, böylece rankın sıfır olduğu elde edilir. Bir önceki örnekte olduğu gibi yine Nagell-Lutz Teoremi'nin uygulanmasıyla da

$$C(Q) = \{O, (0, 0)\} \cong Z_2$$

ve

$$C'(Q) = \{O', (0, 0), (2, 0), (-2, 0)\} \cong Z_2 \oplus Z_2$$

olması gerektiği sonucuna varılır.

Örnek 2.6.3 : $C : y^2 = x^3 - 5x$ eğrisi için $C(Q)$ nun hangi gruba izomorf olduğunu belirlemede, öncelikle, $b_1 = \mp 1, \mp 5$ durumları için,

$$\begin{aligned} \text{(i)} \quad N^2 &= M^4 - 5e^4, \\ \text{(ii)} \quad N^2 &= -M^4 + 5e^4, \\ \text{(iii)} \quad N^2 &= 5M^4 - e^4, \\ \text{(iv)} \quad N^2 &= -5M^4 + e^4 \end{aligned}$$

denklemlerinin tamsayı çözümlerinin olup olmadığı araştırılmalıdır. Dikkat edilirse, burada (i) ve (ii) denklemlerinde M ve e değişkenlerinin yer değiştirmesi durumunda, (iii) ve (iv) denklemlerinin elde edilebileceği açıktır. Bu da; (i) ve (ii) nin, istenen özelliklere sahip, tamsayı çözümünün olması için gerek ve yeter şartın (iii) ve (iv) ün tamsayı çözümünün olması demektir. Bunun için, sadece (i) ve (ii) nin çözümlerinin incelenmesi veya bunun yerine (iii) ve (iv) ün çözümlerinin incelenmesi yeterlidir. Ayrıca, burada $\eta(O) = 1 \pmod{Q^{*2}}$ ve $\eta(T) = -5 \pmod{Q^{*2}}$ olması nedeniyle de, sadece (ii) veya (iii) nin çözümünün incelenmesi, $\eta(C(Q))$ nun tam olarak belirlenmesinde yeterli olacaktır.

Deneme-yanılma yöntemiyle (ii) de,

$$2^2 = -(1^4) + 5.1^4$$

olması nedeniyle; $(M, e, N) = (1, 1, 2)$ nin istenen özelliklere sahip bir çözümü olduğu görülür ki; bu da (iii) de $(M, e, N) = (1, 1, 2)$ nin bir çözüm olması demektir. Buradan,

$$\eta(C(Q)) = \{\mp 1, \mp 5\} \pmod{Q^{*2}}$$

olduğu görülür.

Diğer yandan, tanımı gereği, $C' : y^2 = x^3 + 20x$ ve burada $b' = 20$ olması nedeniyle; b_1' için $b_1' = \mp 1, \mp 2, \mp 4, \mp 5, \mp 10$ ve ∓ 20 durumları sözkonusudur.

Fakat, $\mp 4 \equiv \mp 1 \pmod{Q^{*2}}$, $\mp 20 \equiv \mp 5 \pmod{Q^{*2}}$ ve $b_1 < 0$ için $b_2 < 0$ olacağı dikkate alındığında,

$$\eta'(C'(Q)) \subseteq \{1, 2, 5, 10\} \pmod{Q^{*2}}$$

olacağı görülür. Ayrıca, $\eta'(T') = 20 \equiv 5 \pmod{Q^{*2}}$ kongruansının sağlanması nedeniyle, burada sadece

$$N^2 = 2M^4 + 10e^4$$

denkleminin istenen özelliklere sahip tamsayı çözümünün olup olmadığının incelenmesi yeterlidir; çünkü, bu durumda, M ve e nin yer değiştirilmesiyle elde edilen

$$N^2 = 10M^4 + 2e^4$$

denkleminin tamsayı çözümünün olup olmadığı da belirlenmiş olur. Kabul edelim ki, $N^2 = 2M^4 + 10e^4$ ün yukarıda açıklanan ve asallıkla ilgili koşullardan birisi olan $obcb(M, b_2') = obeb(M, 10) = 1$ özelliğini sağlayacak şekilde bir tamsayı çözümü olsun. Bu durumda, $obeb(M, 5) = 1$ ve Fermat Teoremi'nden $M^4 \equiv 1 \pmod{5}$ olmalıdır, bu da yukarıdaki eşitliği

$$N^2 \equiv 2 \pmod{5},$$

kongruansına dönüştürür ve bu kongruansın da hiç bir çözümü olmadığı; $N = 1, 2, 3$ ve 4 ün son denklemde yerleştirilip, denenmesiyle görülebilir.

Bu açıklamalar doğrultusunda,

$$\eta'(C'(Q)) = \{1, 5\} \pmod{Q^{*2}}$$

ve böylece,

$$2^r = \frac{\# \eta(C(Q)) \cdot \# \eta'(C'(Q))}{4} = \frac{4 \cdot 2}{4} = 2$$

olduğundan dolayı, $C(Q)$ nun rankının 1 olduğu sonucuna varılır. Dolayısıyla, önceki örneklerdeki benzer hesaplamalarla da

$$C(Q) \cong \mathbb{Z} \oplus \mathbb{Z}_2$$

olacağı görülür.

Yukarıdaki açıklama ve örneklerden de anlaşılacağı üzere, söz konusu durumlar için, $N^2 = b_1 M^4 + b_2 e^4$ denkleminin istenen özelliklere sahip bir çözümünün olup olmadığının belirlenmesi o kadar kolay değildir. Buna rağmen, aşağıdaki örnek, bir tür özel eliptik eğriler için $C(Q)$ nun rankını hesaplamada büyük kolaylık sağlayacaktır:

Örnek 2.6.4 : $C_p : y^2 = x^3 + px$ eğrisi için $C_p' : y^2 = x^3 - 4px$ olacağından; $b_1 = \mp 1$, $\mp p$ ve $b_1' = \mp 1, \mp 2, \mp 2p, \mp p$ durumları söz konusudur.

$\eta(O) = 1$, $\eta(T) = p$ olması, $b_1 = -1$ ve $-p$ için istenen çözüm bulunamaması nedeniyle de;

$$\eta(C(Q)) = \{1, p\} \pmod{Q^{*2}}$$

olur. Diğer yandan: $\# \eta'(C_p'(\mathbf{Q})) = 2, 4$ veya en fazla 8 olabileceğinden dolayı, $C_p(\mathbf{Q})$ nun rankı sırasıyla, 0, 1 veya 2 olabilir.

Aşağıda ispatı verilmemekle beraber, $C_p(\mathbf{Q})$ nun rankını belirlemede kolaylık sağlayacak bir yöntem geliştirilmiştir. Buna göre, p bir asal sayı olmak üzere $C_p : y^2 = x^3 + px$ eliptik eğrisi için,

$p \equiv 1$ veya $9 \pmod{16}$ ise, $C_p(\mathbf{Q})$ nun rankı 0 veya 2,

$p \equiv 3, 5, 13$ veya $15 \pmod{16}$, ise $C_p(\mathbf{Q})$ nun rankı genel olarak 1

dir ve bu henüz kanıtlanmamış bir iddia olmakla beraber, $p = 877$ ye kadar olan asal sayılar için bu iddianın sağlandığı Bremner ve Cassals (Bremner ve Cassels, 1984) adlı matematikçiler tarafından kanıtlanmıştır.

$p \equiv 7$ veya $11 \pmod{16}$ ise de $C_p(\mathbf{Q})$ nun rankı 0 dır.

Bu açıklamalara göre, C_{37} ve C_{173} için rankın 1, $C_{43}(\mathbf{Q})$ ve $C_{167}(\mathbf{Q})$ nun rankının 0 olduğu ifade edilmiş olur.

Buraya kadar, rankın 0 veya 1 olmasıyla ilgili örnekler incelenmiş oldu; rankı 2, 3 veya 4 olan örnekler de bulunabilir, ama rankı büyük olan eğrileri belirlemek oldukça zordur. Ve ayrıca, rankı keyfi büyüklükte olan bir eliptik eğrinin var olup olmadığı sorusu henüz tam olarak cevaplandırılamamıştır. Mestre (Mestre, 1992) adlı bir matematikçi 14 Nisan 1992 tarihinde;

$$b = -20981194451128309649475399485,$$

$$c = 26653992551590286206010035905960909459942897$$

olmak üzere;

$$y^2 + xy = x^3 + bx + c$$

nin belirlediği eliptik eğri üzerindeki rasyonel noktalar grubu için rankın 15 olduğunu ispatlamış ve bu tarihten sonra; rankı 16 veya 16 dan büyük olan bir eliptik eğri bulunamamıştır.

Aşağıdaki çizelgede verilen eğriler için $C(\mathbf{Q})$ nun sonlu mertebeli elemanlarından oluşan $\text{tors}C(\mathbf{Q})$ grubunun hangi gruba izomorf olduğu verilmiştir.

Çizelge 2.2.1 : Verilen eğriler için $\text{tors}\mathcal{C}(\mathbf{Q})$ grupları

$\mathcal{C}_f(\mathbf{Q})$	$\text{tors } \mathcal{C}_f(\mathbf{Q})$	D_f
$y^2 = x^3 + 2$	0	$-2^6 3^3$
$y^2 = x^3 + x$	$\mathbf{Z}_2$	-2^6
$y^2 = x^3 + 4$	$\mathbf{Z}_3$	$-2^8 3^3$
$y^2 = x^3 + 4x$	$\mathbf{Z}_4$	-2^{12}
$y^2 = x^3 - y - x^2$	$\mathbf{Z}_5$	-11
$y^2 = x^3 + 1$	$\mathbf{Z}_6$	$-2^4 3^3$
$y^2 = x^3 + 2x^2 + xy - 2y$	$\mathbf{Z}_7$	$-2^7 13$
$y^2 = x^3 - 6x^2 - 7xy + 6y$	$\mathbf{Z}_8$	$+2^8 3^4 17$
$y^2 = x^3 + 6x^2 - 3xy - 6y$	$\mathbf{Z}_9$	$-2^9 3^5$
$y^2 = x^3 - 18x^2 + 7xy + 36y$	$\mathbf{Z}_{10}$	$-2^5 3^{10} 11^2$
$y^2 = x^3 - 210x^2 - 43xy + 210y$	$\mathbf{Z}_{12}$	$+ 2^{12} 3^6 5^3 7^4 13$
$y^2 = x^3 - x$	$\mathbf{Z}_2 \oplus \mathbf{Z}_2$	$+2^6$
$y^2 = x^3 + 5x^2 + 4x$	$\mathbf{Z}_4 \oplus \mathbf{Z}_2$	$+2^8 3^2$
$y^2 = x^3 - 3x^2 - 5xy + 6y$	$\mathbf{Z}_6 \oplus \mathbf{Z}_2$	$+2^2 3^6 5^2$
$y^2 = x^3 + 337x^2 + 20736x$	$\mathbf{Z}_8 \oplus \mathbf{Z}_2$	$+ 2^{20} 3^8 5^4 7^2$

2.7. Tekil Kübik Eğriler

Bu kısımda, tekil (singular) kübik eğriler incelenecek ve bu tür eğriler üzerindeki rasyonel noktalarla, tekil olmayan (eliptik) eğriler üzerindeki rasyonel noktaların farklı özelliklere sahip oldukları açıklanacaktır.

$\mathcal{C}$ bir tekil kübik eğri, S de bu eğrinin bir tekil noktası olsun. Tekil nokta tanımından, S den geçen ve $\mathcal{C}$ ile kesişen her doğrunun S noktasındaki katlılığının en az 2 olduğu açıktır. S' de $\mathcal{C}$ üzerinde ikinci bir tekil nokta olmak üzere, S ve S' den geçen L doğrusunun $\mathcal{C}$ ile kesişiminin (katlılık sayılmak üzere) en az dört nokta olduğu görülür; fakat, daha önce açıklandığı üzere, bir doğruyla bu doğruyu içermeyen bir kübik eğrinin, katlılık sayılmak üzere, en fazla üç ortak noktası olması gerektiğinden dolayı, $\mathcal{C}$ nin en fazla bir tekil noktası olabileceği sonucuna varılır.

$\mathcal{C}$ nin bir tekil eğri olması durumunda da; bu eğri üzerindeki tekil olmayan noktalar kümesiyle, eliptik eğrilerde olduğu gibi, bir grup yapısı oluşturulabilir. Bunun için,

$$\mathcal{C}_{ns} = \{P \in \mathcal{C} : P, \mathcal{C} \text{ nin tekil noktası değil}\}$$

olarak tanımlandığında, rasyonel koordinatlı noktaların $\mathcal{C}_{ns}$ nin bir alt kümesini oluşturacağı; yani, $\mathcal{C}_{ns}(\mathbf{Q}) \subseteq \mathcal{C}_{ns}$ olacağı açıktır. Genel olarak (orijin noktası bir tekil nokta olmadığı zaman), $\mathcal{O}$ olarak orijin noktası seçilir. $P, R \in \mathcal{C}_{ns}$ için bu noktaların toplamı, $P + R$, eliptik eğrilerdeki gibi geometrik olarak tanımlandığında, $\langle \mathcal{C}_{ns}, + \rangle$, $\mathcal{O}$ birim elemanlı bir Abel grubu olur. Ayrıca, $\mathcal{O} \in \mathcal{C}_{ns}(\mathbf{Q})$ olması durumunda; $\mathcal{C}_{ns}(\mathbf{Q})$ grubu $\mathcal{C}_{ns}$ nin bir altgrubunu oluşturur. Burada, $\mathcal{C}_{ns}$ kübik eğrisinin daha önce sözü edilen, Weierstrass Normall Formunda ifade edilebileceği ve toplam formüllerinin cebirsel olarak da elde edilebileceği açıktır.

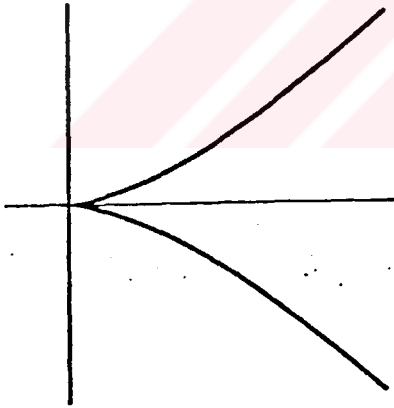
Örneğin, $y^2 = x^3$ ün belirlediği eğri için $S = (0,0)$ noktası, katlılığı 3 olan bir tekil noktadır ve burada toplam formülleri; $P = (x_1, y_1)$, $R = (x_2, y_2)$ ve $\nu = \frac{y_1 x_2 - x_1 y_2}{x_2 - x_1}$ olmak üzere

$$P + R = (x_1, y_1) + (x_2, y_2) = \left(\frac{\nu^2}{x_1 \cdot x_2}, \frac{\nu^3}{y_1 \cdot y_2} \right)$$

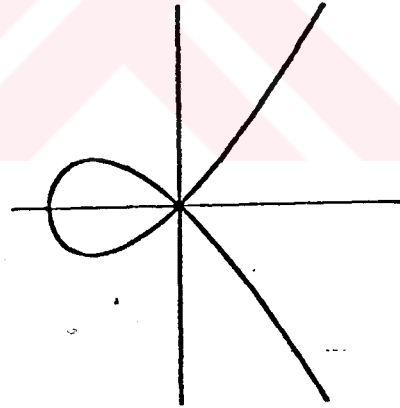
olur.

Bu bölümün 5. kesiminde, C nin bir eliptik eğri olması durumunda, Mordell Teoremi'nden, $C(\mathbb{Q})$ nun sonlu üretilmiş olduğu ifade ve ispat edilmişti. Bu kısımda ise, C nin bir kübik eğri olması durumunda $C_{ns}(\mathbb{Q})$ nun nasıl bir grup olduğu belirlenmeye çalışılacaktır.

Tekil olan kübik eğrilerde, tekil nokta olan S için iki durum söz konusudur. Bunlardan birincisi, S noktasının çift katlı bir nokta olması durumu; buna örnek olarak, $C : y^2 = x^3 + x^2$ eğrisinde $(0,0)$ noktası düşünülebilir (Şekil 2.7.1. (b)). İkinci olarak da; S noktasının üç katlı bir nokta olması durumudur, bu da $C' : y^2 = x^3$ örneğinde de kolayca görülebileceği gibi, $(0,0)$ noktası olarak düşünülebilir (Şekil 2.7.1. (a)). Sözü edilen bu iki eğriyle ilgili olan aşağıdaki teorem, tekil bir eğri üzerindeki rasyonel noktalar grubunun sonlu üretilip üretilmediği konusuna açıklık getirmektedir.



Şekil 2.7.1. (a) $y^2 = x^3$



Şekil 2.7.1. (b) $y^2 = x^3 + x^2$

Teorem 2.7.1 (a) : C kübik eğrisi $y^2 = x^3 + x^2$ nin belirlediği tekil eğri ve $\mathbb{Q}^* = \{r \in \mathbb{Q} : r \neq 0\}$ olsun. Bu durumda;

$$\phi : C_{ns}(\mathbb{Q}) \longrightarrow \mathbb{Q}^*,$$

$$\phi(P) = \begin{cases} \frac{y-x}{y+x} & , P = (x, y) \\ 1 & , P = \mathcal{O} \end{cases}$$

ile tanımlanan dönüşüm bir grup izomorfizmidir.

(b) : C , $y^2 = x^3$ ün belirlediği tekil eğri ise,

$$\phi : C_{ns}(\mathbf{Q}) \longrightarrow \mathbf{Q} ,$$

$$\phi(P) = \begin{cases} \frac{x}{y} & , \quad P = (x, y) \\ 0 & , \quad P = \mathcal{O} \end{cases}$$

ile tanımlanan ϕ dönüşümü bir grup izomorfizmidir.

İspat (a) : $C : y^2 = x^3 + x^2$ için

$$\phi : C_{ns}(\mathbf{Q}) \longrightarrow \mathbf{Q}^* ,$$

$$\phi(P) = \begin{cases} \frac{y-x}{y+x} & , \quad P = (x, y) \\ 1 & , \quad P = \mathcal{O} \end{cases}$$

dönüşümünün iyi tanımlı olmasında $x + y \neq 0$ olması gerekir, bu da $(0,0)$ noktası bir tekil nokta olduğundan dolayı, $\forall x, y \in C_{ns}$ için $x + y \neq 0$ olması nedeniyle bir sorun oluşturmaz.

Ayrıca; ϕ dönüşümüne karşılık

$$\psi : \mathbf{Q}^* \longrightarrow C_{ns}(\mathbf{Q}) ,$$

$$\psi(t) = \begin{cases} \left(\frac{4t}{(1-t)^2}, \frac{4t(1+t)}{(1-t)^3} \right) & , \quad t \neq 1 \\ \mathcal{O} & , \quad t = 1 \end{cases}$$

dönüşümü tanımlandığında, $\phi(\psi(t)) = t$ ve $\psi(\phi(P)) = P$ olduğundan dolayı, ϕ dönüşümünün tersi ψ olur. Böylece ϕ nin bire-bir ve örten bir dönüşüm olduğu gösterilmiş olur.

ϕ dönüşümünün bir grup izomorfizmi olduğunu göstermek için, ϕ veya ψ den herhangi birinin bir grup homomorfizmi olduğunu göstermek yeterlidir. Buradan hareketle;

$$\begin{aligned} \psi\left(\frac{1}{t}\right) &= \left(\frac{4t^{-1}}{(1-t^{-1})^2}, \frac{4t^{-1}(1+t^{-1})}{(1-t^{-1})^3} \right) \\ &= \left(\frac{4t}{(1-t)^2}, -\frac{4t(1+t)}{(1-t)^3} \right) \\ &= -\psi(t) \end{aligned}$$

özelliklerinden ve C_{ns} üzerindeki üç noktanın toplamının birim olması için gerek ve yeter şart, bunların doğrudaş olması gerektiğinden yararlanarak, ψ nin bir homomorfizm olduğu aşağıdaki gibi ispatlanabilir.

1^0) $t_1, t_2 \in \mathbf{Q}^* \setminus \{1\}$ ise $t_3 = \frac{1}{t_1 t_2}$ olmak üzere, $i = 1, 2, 3$ için $\psi(t_i) = \left(\frac{4t_i}{(1-t_i)^2}, \frac{4t_i(1+t_i)}{(1-t_i)^3} \right)$ dir. Bu durumda, $P_i = \psi(t_i) = (x_i, y_i)$ olsun. P_1 ve P_2 den

geçen doğru denklemi $(x_2 - x_1)(y - y_1) = (y_2 - y_1)(x - x_1)$ olduğundan dolayı, $(x, y) = (x_3, y_3)$ için $t_1.t_2.t_3 = 1$ eşitliği gözönünde bulundurularak, $P_i = (x_i, y_i)$ koordinatları doğru denkleminde yerleştirilip gerekli düzenlemeler yapıldığında,

$$x_1y_2 - x_2y_2 + x_2y_3 - x_3y_2 + x_3y_1 - x_1y_3 = \frac{32(t_1 - t_2)(t_1 - t_3)(t_2 - t_3)(t_1.t_2.t_3 - 1)}{(1 - t_1)^3(1 - t_2)^3(1 - t_3)^3} = 0$$

elde edilir. Bu da, P_1 , P_2 ve P_3 ün doğrudan olduğunu dolayısıyla,

$$\psi(t_1.t_2) = \psi\left(\frac{1}{t_3}\right) = -\psi(t_3) = \psi(t_1) + \psi(t_2)$$

eşitliğinin sağlandığını ispatlar.

2^0) $t_1 = 1$ veya $t_2 = 1$ ise (kabul edelim ki, $t_1 = 1$ olsun),

$$\psi(t_1.t_2) = \mathcal{O} + \psi(t_2) = \psi(t_1) + \psi(t_2)$$

eşitliğinin sağlanacağı açıktır.

Bu da, ϕ nin bir izomorfizm olduğunu kanıtlar.

(b) : $\mathcal{C} : y^2 = x^3$ ve

$$\phi : \mathcal{C}_{ns}(\mathbb{Q}) \longrightarrow \mathbb{Q} \quad \text{için}$$

$$\phi(P) = \begin{cases} \frac{x}{y} & , \quad P = (x, y) \\ 0 & , \quad P = \mathcal{O} \end{cases}$$

dönüşümünün bir grup izomorfizmi olduğunun ispatı (a) şikkındaki ispata benzer şekilde yapılır (Silverman ve Tate 1992).

Teorem 2.7.1 in bir sonucu olarak, $\langle \mathbb{Q}, + \rangle$ ve $\langle \mathbb{Q}^*, \bullet \rangle$ grupları sonlu üretilmiş olmadığından dolayı, $\mathcal{C}_{ns}$ eğrileri üzerindeki rasyonel noktalar grubunun da sonlu üretilmediği kolayca anlaşılabilir, en azından teoremdeki iki tekil eğri için, bu eğriler üzerindeki rasyonel noktalar grubunun farklı özelliklere sahip olduğu gösterilmiş olur. Ayrıca, bu sayede tekil kübik eğriler üzerindeki rasyonel noktalar grubunun, özellikleri çok iyi bilinen $\mathbb{Q}^*$ veya $\mathbb{Q}$ çarpımsal grubu formunda olması nedeniyle, çalışmalarımızda tekil olmayan (eliptik) eğriler üzerindeki rasyonel noktalar grubuna neden bu kadar çok önem verdiğimiz anlaşılmış olur.

2.8. Sonlu Cisimler Üzerinden Eliptik Eğriler

Bu bölümde, $(\text{mod } p)$ ye göre tamsayılar cismi olan ve F_p ile gösterilen asal cisim veya onun bir sonlu genişlemesi üzerinden eliptik eğriler incelenecektir. Tabii ki; bu tip eğrilerin, geometrik olarak, gözönünde canlandırılabilmesi oldukça güçtür.

Genel olarak, F_q , F_p nin $q = p^e$ elemanlı bir cisim genişlemesi ve $f(x, y)$ tamsayı katsayılı bir polinom olmak üzere,

$$C(F_q) = \{ (x_0, y_0) : x_0, y_0 \in F_q \text{ ve } f(x_0, y_0) \equiv 0 \pmod{p} \}$$

kümesine F_q içinde $f(x, y)$ nin belirlediği eğri ve (x_0, y_0) çözümlerine de bu eğrinin noktaları adı verilir. Eğer (x_0, y_0) noktasının koordinatları F_p içinde ise, bu nokta bir rasyonel nokta olarak adlandırılır. Özel olarak, p sayısı m ve n den her ikisini birden bölmek üzere, $mx + ny + s \equiv 0 \pmod{p}$ yi sağlayan (x_0, y_0) ikilileri kümesi $(\text{mod } p)$ ye göre bir doğruyu oluşturur.

Tekil nokta ve projektif nokta kavramlarının, sonsuz cisimlerdeki bu kavramlarla hemen hemen aynı olduğu birinci bölümde açıklanmıştı. Bu iki durum arasındaki tek farklılık, birisinde hesaplamaların $(\text{mod } p)$ dikkate alınarak yapılmasıdır.

Tanım 2.8.1 : $f(x, y) \in F_p[x, y]$ derecesi 3 olan bir polinom olmak üzere; eğer $f(x, y)$ F_p üzerinden indirgenemez ve $f(x, y)$ nin projektif koordinatlarda belirlediği eğrinin hiç tekil noktası yok ise $C(F_p)$ ye F_p üzerinden bir eliptik eğri denir.

F_p üzerinden bir eliptik eğri örneğine aşağıdaki birkaç açıklamadan sonra yer verilecektir. Ayrıca, bundan sonraki gösterimlerde, bazen fazla karışıklığa neden olmamak üzere, $(\text{mod } p)$ ye göre kongruanslar eşitliklerle ifade edilecektir, kısacası $' \equiv '$ yerine $' = '$ gösterimi kullanılacaktır. Buna dikkat edilmelidir.

Kısaca şunu belirtelim ki, daha önce verilen bilgilere dayanarak; $a, b, c \in F_p$ olmak üzere,

$$C : y^2 \equiv x^3 + ax^2 + bx + c \pmod{p}$$

nin bir eliptik eğri tanımlaması için gerek ve yeter şartın $p \geq 3$ ve diskriminantın $D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 \not\equiv 0 \pmod{p}$ olması gerektiği sonucuna varılır.

Eğer, C , F_p cismi üzerinden bir eliptik eğri ise, bu eğri üzerindeki noktalar kümesinde, $(\text{mod } p)$ dikkate alınarak, daha önce tanımlanan toplama işlemine benzer bir işlemin tanımlanmasıyla, $(\forall A, B \in C(F_p) \text{ için } A + B = \mathcal{O} * (A * B))$ bu kümenin bir değişmeli grup oluşturduğu görülür (Niven, Zuckerman ve Montgomery 1991).

Daha önce olduğu gibi, burada da verilen bir $f(x, y) = 0$ kübik denkleminin homojenleştirilmesi sonucunda elde edilecek olan $F(X, Y, Z) = 0$ denkleminde, $Z = 0$ a karşılık gelen nokta (veya noktalar) yine C nin sonsuzdaki noktası olarak adlandırılacak ve $\mathcal{O}$ ile gösterilecektir.

$x_1, y_1, x_2, y_2 \in \mathbb{F}_p$ olmak üzere $P_1 = (x_1, y_1)$ ve $P_2 = (x_2, y_2)$ $\mathcal{C}$ eliptik eğrisi üzerinde iki nokta olsun. Bu durumda, $P_3 = P_1 + P_2 = (x_3, y_3)$ noktasının koordinatları aşağıdaki formüllerle hesaplanabilir (burada $P_1 \neq \mathcal{O}$, $P_2 \neq \mathcal{O}$ ve $P_1 \neq P_2$ ve $P_1 + P_2 \neq \mathcal{O}$ kabul edilmektedir); P_1 ve P_2 noktalarından geçen doğru denklemi,

$$\lambda = \begin{cases} (y_2 - y_1) \cdot (x_2 - x_1)^{-1} & , \quad x_1 \neq x_2 \pmod{p} \\ (3x_1^2 + 2ax_1 + b)(2y_1)^{-1} & , \quad P_1 = P_2 \end{cases}$$

ve

$$\nu \equiv y_1 - \lambda x_1 \equiv y_2 - \lambda x_2 \pmod{p}$$

olmak üzere, $y \equiv \lambda x + \nu \pmod{p}$ biçimindedir. Burada $(x_2 - x_1)^{-1}$ ile $(x_2 - x_1)$ in $\pmod{p}$ ye göre tersi ifade edilmektedir. Benzer ifade $(2y_1)^{-1}$ için de geçerlidir. Böylece, P_3 ün koordinatları;

$$x_3 \equiv \lambda^2 - a - x_1 - x_2 \pmod{p} \text{ ve } y_3 \equiv -\lambda x_3 - \nu \pmod{p}$$

olarak formüle edilebilir.

Fazla teoriye girmeden önce, aşağıda sonlu bir cisim üzerinden bir eliptik eğri örneği verilerek, bu eğri üzerindeki rasyonel noktalar grubu belirlenmiştir.

Örnek 2.8.1 : $\mathbb{F}_5$ cismi üzerinden $\mathcal{C} : y^2 = x^3 + x + 1$ in belirlediği eğrinin bir eliptik eğri olup olmadığını anlamak için öncelikle; $p \geq 3$ ve $f(x)$ in diskriminantının p ye bölünüp bölünmediğini belirlemek gerekir. Burada, $p \geq 3$ ve

$$\begin{aligned} D &= -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 \\ &= -4b^3 - 27c^2 = -31 \not\equiv 0 \pmod{5} \end{aligned}$$

olması nedeniyle $\mathcal{C}$ nin $\mathbb{F}_5$ üzerinden bir eliptik eğri olduğu sonucuna varılır.

$\mathbb{F}_5$ cismi üzerinden, bu eğri üzerindeki rasyonel noktalar grubu yani $\mathcal{C}(\mathbb{F}_5)$ belirlenmek isteniyorsa; $\mathbb{F}_5$ içinde x ve y koordinatları için sonlu sayıda durum söz konusu olması nedeniyle, önce $x = 0, 1, 2, 3$ ve 4 için $f(x)$ hesaplanır ve $f(x)$ in alacağı bu değerlerden hangilerinin bir tamkare olduğu incelenerek çözüm bulunur; yani,

$$\begin{aligned} f(0) &\equiv f(2) \equiv f(3) \equiv 1 \pmod{5} \\ f(1) &\equiv 3 \pmod{5} \\ f(4) &\equiv 4 \pmod{5} \end{aligned}$$

ve $\mathbb{F}_5$ içinde tamkare olan sayılar, sadece;

$$\begin{aligned} (\mp 1)^2 &\equiv 1 \pmod{5} \\ (\mp 2)^2 &\equiv 4 \pmod{5} \end{aligned}$$

olması nedeniyle,

$$\mathcal{C}(\mathbb{F}_5) = \{\mathcal{O}, (0, \mp 1), (2, \mp 1), (-2, \mp 1), (-1, \mp 1)\}$$

den ibarettir. Burada, yukarıda sözü edilen toplam formülleri kullanılarak; $P = (x_1, y_1) = (0, 1)$ noktası için; $2P = (x_3, y_3)$ koordinatları,

$$\begin{aligned}\lambda &\equiv (3x_1^2 + 2ax_1 + b)(2y_1)^{-1} \pmod{5} \\ &\equiv (3 \cdot 0^2 + 2 \cdot 0 \cdot 0 + 1)(2 \cdot 1)^{-1} \pmod{5} \\ &\equiv 3 \pmod{5}, \\ \nu &\equiv y_1 - \lambda x_1 \equiv 1 - 2 \cdot 0 \equiv 1 \pmod{5} \text{ olduğundan;} \\ x_3 &\equiv \lambda^2 - a - x_1 - x_2 \equiv 4 \pmod{5}, \\ y_3 &\equiv -\lambda \cdot x_3 - \nu \equiv (-2) \cdot 4 - 1 \equiv 2 \pmod{5}\end{aligned}$$

ve böylece, $2P = (4, 2)$ olarak hesaplanır. Bu işlemlerin tekrarlanmasıyla da

$$3P = (2, 1), 4P = (3, -1), \dots$$

olması nedeniyle; $\#C(F_5) = 9$ olduğu dikkate alınacak olursa; $P = (0, 1)$ noktasının $C(F_5)$ i ürettiği sonucuna varılır. Bu da, verilen C eğrisi için

$$C(F_5) \cong Z_9$$

olduğunu gösterir.

$C(F_p)$ nin sonlu elemanlı olması nedeniyle, sonlu üretilmiş olacağı açıktır. Buna rağmen; $C(F_p)$ nin eleman sayısını, özel eğriler hariç tam olarak belirlemede kullanılabilecek olan herhangi bir formül henüz geliştirilememiştir. Bu nedenle, aşağıda sadece özel eğriler için $C(F_p)$ yi hesaplamada kullanılacak olan bazı özellik ve teoremlere yer verilmiştir.

F_p üzerinden bir doğrunun denklemi $y \equiv mx + s \pmod{p}$ olmak üzere bu doğru üzerindeki rasyonel noktalar tam olarak belirlenebilir. Çünkü, F_p içinde x in alacağı her değer için y belirlenmiş olur, böylece doğru üzerinde p tane rasyonel noktanın olduğu görülür, buna sonsuzdaki $Y \equiv mX + sZ \pmod{p}$ denkleminde $[1, m, 0]$ a karşılık gelen noktanın da eklenmesiyle, verilen doğru üzerinde toplam $p + 1$ tane rasyonel noktanın olması gerektiği sonucuna varılır.

$p \neq 0$ ve $f(x)$ katsayıları F_p içinde olan bir polinom olmak üzere, $C(F_p)$ üzerindeki rasyonel noktaların sayısı belirlenmek istenirse, daha önce de olduğu gibi, $x_0 = 0, 1, \dots, p - 1$ için $f(x_0)$ hesaplanır. Eğer; $f(x_0) \equiv 0 \pmod{p}$ ise $y = 0$ bir çözüm olur. Diğer yandan, sayılar kuramından, F_p cisminin $1, 2, \dots, p - 1$ elemanlarından yarısının tamkare yarısının ise tamkare olmadığı hatırlanacak olursa, $f(x_0) \not\equiv 0 \pmod{p}$ için $y^2 \equiv f(x_i) \pmod{p}$ yi sağlayan en fazla $\frac{p-1}{2}$ tane çözüm bulunabileceği ve bu tür her çözüm için de; y nin iki değer alabiliyor olmasından dolayı; toplam en fazla p tane rasyonel çözüm bulunabilir. Buna sonsuzdaki noktanın da eklenmesiyle,

$$\#C(F_p) = p + 1 + \epsilon$$

olur ki; burada hata terimi olarak adlandırılan ϵ nun p den çok küçük olacağı açıktır. Ayrıca, burada $f(x)$ in derecesi ile ilgili herhangi bir kısıtlama olmadığından dolayı, bu ifade; eliptik eğriler için de geçerlidir.

Böylece; $\mathcal{C} : y^2 \equiv f(x) \pmod{p}$ eğrisi üzerindeki rasyonel noktaların sayısının bir doğru üzerindeki rasyonel noktaların sayısından çok fazla olmadığı sonucu ortaya çıkar. $\mathcal{C}$ eğrisi üzerindeki rasyonel noktaların sayısını belirlemede oluşan hata terimini için bir tahmin veren aşağıdaki teoreme geçmeden önce, teoremden sözü edilecek olan genus kavramına kısa bir açıklık getirilmesi gerekir: $f(x,y) \in \mathbb{C}[x,y]$, $\deg f = d$ olsun. Eğer, $f(x,y)$ polinomu $\mathbb{C}$ üzerinden indirgenemez ve $\mathcal{C}_f(\mathbb{C})$ tekil olmayan bir eğri ise, $g = \frac{(d-1)(d-2)}{2}$ sayısına verilen eğrinin *genusu* adı verilir. Buna göre, herhangi bir eliptik eğrinin genusu 1 dir.

Teorem 2.8.1 (Hasse - Weil) : $\mathbb{F}_p$ sonlu cismi üzerinden tanımlanan, indirgenemez ve tekil olmayan $\mathcal{C}$ eğrisinin genusu g olsun. Bu durumda, $\mathcal{C}$ nin koordinatları $\mathbb{F}_p$ içinde olan noktalarının sayısı, $|\epsilon| \leq 2.g.\sqrt{p}$ olmak üzere,

$$\#\mathcal{C}(\mathbb{F}_p) = p + 1 + \epsilon$$

dur (Seigel ve Tate 1992).

$\mathcal{C} ; \mathbb{F}_p$ sonlu cismi üzerinden bir eliptik eğri olmak üzere, Hasse-Weil Teoremi, $\mathcal{C}$ nin genusu 1 olduğu için,

$$-2\sqrt{p} \leq \mathcal{C}(\mathbb{F}_p) - p - 1 \leq 2\sqrt{p}$$

olması gerektiğini ifade eder. Daha önceden belirtildiği gibi, her $\mathcal{C}$ eğrisi için $\#\mathcal{C}(\mathbb{F}_p)$ yi tam olarak belirleyecek olan bir kriterin bulunamaması nedeniyle; bazı matematikçiler özel eğriler için $\#\mathcal{C}(\mathbb{F}_p)$ yi hesaplayabilmek için yorucu çalışmalar yapmışlardır. Bu matematikçilerden biri de Gauss'dur. Gauss, $\mathbb{F}_p$ cismi üzerinden

$$x^3 + y^3 \equiv 1 \pmod{p} \quad (2.8.1)$$

biçimindeki Fermat denkleminin projektif koordinatlarda belirlediği eğri üzerindeki rasyonel noktaların sayısını belirleyebilmek için aşağıda verilen teoremi ispatlamıştır. (2.8.1). denklemin projektif koordinatlarda karşılık gelen denklem

$$X^3 + Y^3 + Z^3 \equiv 0 \pmod{p} \quad (2.8.2)$$

olsun. Burada aşıkâr çözüm olan $(0,0,0)$ noktasının projektif düzleme ait olmaması nedeniyle; rasyonel bir çözüm olarak sayılmayacağı ve ayrıca; $a \neq 0$ olmak üzere (x_0, y_0, z_0) çözümü ile (ax_0, ay_0, az_0) çözümlerine, projektif düzlemin tanım gereği, tek bir çözüm gözüyle bakılabileceği unutulmamalıdır.

Teorem 2.8.2 (Gauss) : $x, y, z \in \mathbb{F}_p$ olmak üzere; M_p , (2.8.2) denkleminin projektif çözümleri sayısı olsun. Bu durumda,

(a) $p \not\equiv 1 \pmod{3}$ ise $M_p = p + 1$ dir.

(b) $p \equiv 1 \pmod{3}$ ise $\exists A, B \in \mathbb{Z}$ öyle ki $4p = A^2 + 27B^2$ dir. Burada; A ve B sayıları, işaretlerinin değiştirilmesi, dışında tek türlü belirlidir. Ek olarak, A nın işareti $A \equiv 1 \pmod{3}$ olacak şekilde belirlenecek olursa, $M_p = p + 1 + A$ dir.

Burada, $p \equiv 1 \pmod{3}$ olması durumunda; $4p = A^2 + 27B^2$ denklemi; $A^2 \equiv \mp 1 \pmod{3}$ olacağından dolayı A nın işaretinin uygun seçilmesiyle $A \equiv 1 \pmod{3}$ ifadesinin elde edilebileceğini gösterir.

Teoremin ispatına geçmeden önce F_p sonlu cismi ile ilgili bir hatırlatma yapılabilir; bu da $F_p^* = \{1, 2, \dots, p-1\}$ in $p-1$ elemanlı, çarpımsal bir devirli grup olmasıdır.

İspat (a) : $p \not\equiv 1 \pmod{3}$ ise, F_p^* in mertebesi (yani, $p-1$) 3 ile bölünmez. Böylece,

$$\begin{aligned} k: F_p^* &\longrightarrow F_p^* \\ x &\longrightarrow k(x) = x^3 \end{aligned}$$

dönüşümü bir izomorfizm olur. Çünkü, $\forall x, y \in F_p^*$ için,

(i) $k(xy) = x^3 y^3 = k(x).k(y)$ olduğundan k bir homomorfizmdir.

(ii) $k(x) = 1$ ise, $x^3 = 1$ ve $3 \nmid p-1$ olması nedeniyle, $x = 1$ olmalıdır. Bu da; k nın bire-bir olduğunu gösterir. Buna ek olarak, tanım ve görüntü kümelerinin aynı ve sonlu olması nedeniyle de, k nın örten olacağı açıktır.

Böylece, $0^3 \equiv 0 \pmod{3}$ olduğu da gözönüne alınarak, F_p nin her elemanının tek bir küp köke sahip olduğu söylenebilir. $x^3 + y^3 + z^3 \equiv 0 \pmod{p}$ nin çözümleri sayısı ile $x+y+z \equiv 0 \pmod{p}$ nin çözümleri sayısının aynı olması gerektiğini gösterir. $x+y+z \equiv 0 \pmod{p}$ projektif düzlemde bir doğru denklemdir ve hatırlanacağı gibi bu doğru üzerindeki rasyonel noktalar sayısının F_p üzerinden $p+1$ olduğu daha önce incelenmişti; böylece $M_p = p+1$ olduğu sonucuna varılır.

(b) : $p \equiv 1 \pmod{3}$ ise, $\exists m \in \mathbb{Z}$ öyle ki $p = 3m + 1$ dir. 3 ün F_p^* in mertebesini bölmesi nedeniyle

$$\begin{aligned} k: F_p^* &\longrightarrow F_p^* \\ x &\longrightarrow k(x) = x^3 \end{aligned}$$

dönüşümü bir homomorfizmdir (uyarı; bire-bir ve örten değildir). $\mathcal{R} = \text{Gör } k = \{x^3 : x \in F_p^*\}$ olmak üzere, $\mathcal{R}$ nin F_p^* in bir alt grubu olacağı açıktır. k dönüşümünün çekirdeği, $u \in F_p^*$ ve $u^3 \equiv 1 \pmod{p}$ olmak üzere, $1, u, u^2$ gibi üç elemandan oluşmaktadır.

Örneğin, $p = 13$ için, $\mathcal{R} = \{\mp 1, \mp 5\}$ ve Çek $k = \{1, 3, 9\}$ olur. $\mathcal{R}$ nin elemanları *kübik rezidüler* olarak adlandırılır. F_p^* içinde $\mathcal{R}$ nin belirlediği üç eşkümeden $\mathcal{R}$ nin dışındaki ikisi $\mathcal{S}$ ve $\mathcal{T}$ ise, $s \in F_p^* \setminus \mathcal{R}$ olmak üzere $\mathcal{S} = s\mathcal{R}$ ve $\mathcal{T} = s^2\mathcal{R}$ olarak ifade edilebilir. $p = 13$ örneğinde; $s = 2$ seçilirse; $\mathcal{S} = 2\mathcal{R} = \{\mp 2, \mp 10\}$ ve $\mathcal{T} = 2^2.\mathcal{R} = \{\mp 4, \mp 7\}$.

$\mathcal{R}$, $\mathcal{S}$ ve $\mathcal{T}$ nin bu şekilde belirlenmesiyle; F_p nin kesişmeyen kümelerin birleşimi şeklinde, $F_p = \{0\} \cup \mathcal{R} \cup \mathcal{S} \cup \mathcal{T}$, ifade edilebileceği kolayca görülebilir. Ayrıca burada, eşkümelerin eleman sayısının eşit olması gerektiğinden dolayı; $\mathcal{R}$, $\mathcal{S}$ ve $\mathcal{T}$ nin herbirinin eleman sayısı m dir. Diğer yandan, $\forall x \in \mathcal{R}$ için $-x \in \mathcal{R}$

olacağından, $\mathcal{R} = -\mathcal{R}$ ve $s \in \mathbb{F}_p^* \setminus \mathcal{R}$ için, $\mathcal{S} = s\mathcal{R} = -s\mathcal{R} = -\mathcal{S}$, $\mathcal{T} = s^2\mathcal{R} = -s^2\mathcal{R} = -\mathcal{T}$ olur. Bu açıklamaların ışığı altında, M_p sayısını $\mathcal{R}$, $\mathcal{S}$ ve $\mathcal{T}$ ye bağlı olarak ifade edebilmek için yeni bir sembole ihtiyaç duyulmaktadır. Bu da; $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z} \subseteq \mathbb{F}_p$ cisminin alt kümeleri olmak üzere; $[\mathcal{X}, \mathcal{Y}, \mathcal{Z}]$ veya $[\mathcal{X}\mathcal{Y}\mathcal{Z}]$ sembolü $x \in \mathcal{X}$, $y \in \mathcal{Y}$, $z \in \mathcal{Z}$ ve $x + y + z = 0$ ı sağlayan (x, y, z) üçlülerinin sayısı yani,

$$[\mathcal{X}, \mathcal{Y}, \mathcal{Z}] = [\mathcal{X}\mathcal{Y}\mathcal{Z}] = \#\{(x, y, z) : x \in \mathcal{X}, y \in \mathcal{Y}, z \in \mathcal{Z}, x + y + z = 0\}$$

olsun. “ Bu sembolün terimleri içinde M_p çözümlerinin sayısı ne kadardır ?” sorusunun cevabı, iki adımda verilebilir:

x , y ve z nin hiçbirisi sıfır olmamak üzere, $x^3 + y^3 + z^3 \equiv 0 \pmod{p}$ nin çözümleri düşünüldüğünde, üç tane sıfırdan farklı küpün toplamını sıfır olacak şekilde ifade etmenin sayısının $[\mathcal{R}\mathcal{R}\mathcal{R}]$ olacağı açıktır. Fakat, burada her küp için üç tane mümkün durum söz konusu olacağından dolayı da; x , y ve z sıfırdan farklı olmak üzere, (3.2.2) nin çözümleri sayısı $27 \cdot [\mathcal{R}\mathcal{R}\mathcal{R}]$ olur. $a \neq 0$ için (x, y, z) ve (ax, ay, az) çözümlerinde herhangi bir kısıtlama yapılmadığından dolayı, a nın alabileceği değer sayısı $p - 1$ olması nedeniyle, istenen projektif çözümler sayısı

$$\frac{27[\mathcal{R}\mathcal{R}\mathcal{R}]}{p-1} = \frac{27[\mathcal{R}\mathcal{R}\mathcal{R}]}{3m} = \frac{9[\mathcal{R}\mathcal{R}\mathcal{R}]}{m}$$

olmalıdır.

x , y , z sayılarından birisi sıfır olduğunda, örneğin $z = 0$ olduğunda, (2.8.2) nin acaba kaç tane projektif çözümü vardır? Bu durumda, $(0, 0, 0)$ çözümü projektif bir çözüm olmadığından, ne x ne de y sıfır olamaz. Dolayısıyla, $\forall x \in \mathbb{F}_p^*$ için $y^3 = -x^3$ ün daha önce söz edildiği gibi; $-x$, $-ux$ ve $-u^2x$ olan üç tane çözümü olması nedeniyle; $(x, y, 0)$ biçimindeki çözüm sayısı $3 \cdot (p - 1)$ olmalıdır. $z = 0$ için yapılan işlemler x , y için de düşünülecek olursa; toplam $9 \cdot (p - 1)$ çözüm olur ama (x, y, z) ile (ax, ay, az) nin aynı nokta olması nedeniyle de; sözü edilen çözüm sayısı $\frac{9 \cdot (p-1)}{p-1} = 9$ olarak elde edilir.

Son olarak, yukarıdaki iki hesabın birleştirilmesiyle, M_p nin

$$M_p = \frac{9[\mathcal{R}\mathcal{R}\mathcal{R}]}{m} + 9 = 9 \cdot \left(\frac{[\mathcal{R}\mathcal{R}\mathcal{R}]}{m} + 1 \right)$$

biçiminde olduğu görülür.

$[\mathcal{X}\mathcal{Y}\mathcal{Z}]$ sembolünün sağladığı özelliklerden birkaçı aşağıdaki gibidir:

$$\otimes \quad \mathcal{Z} \cap \mathcal{W} = \emptyset \text{ ise } [\mathcal{X}\mathcal{Y}(\mathcal{Z} \cap \mathcal{W})] = [\mathcal{X}\mathcal{Y}\mathcal{Z}] + [\mathcal{X}\mathcal{Y}\mathcal{W}] \text{ dir.}$$

$$\otimes \quad [\mathcal{X}\mathcal{Y}\mathcal{Z}] = [\mathcal{X}\mathcal{Z}\mathcal{Y}] = [\mathcal{Y}\mathcal{X}\mathcal{Z}] = [\mathcal{Y}\mathcal{Z}\mathcal{X}] = [\mathcal{Z}\mathcal{X}\mathcal{Y}] = [\mathcal{Z}\mathcal{Y}\mathcal{X}] \text{ dir.}$$

$$\otimes \quad \text{a } \mathcal{X} = \{ax : x \in \mathcal{X}\} \text{ olmak üzere, } a \neq 0 \text{ için } [\mathcal{X}\mathcal{Y}\mathcal{Z}] = [a\mathcal{X}, a\mathcal{Y}, a\mathcal{Z}] \text{ dir.}$$

$\mathbb{F}_p = \{0\} \cup \mathcal{R} \cup \mathcal{S} \cup \mathcal{T}$ kesişmeyen kümelerin birleşimi şeklinde ve $[\mathcal{R}\mathcal{R}\mathbb{F}_p] = m^2$ olması nedeniyle,

$$[\mathcal{R}\mathcal{R}\{0\}] + [\mathcal{R}\mathcal{R}\mathcal{R}] + [\mathcal{R}\mathcal{R}\mathcal{S}] + [\mathcal{R}\mathcal{R}\mathcal{T}] = m^2$$

olur. $s \in \mathcal{S}$ ve $t \in \mathcal{T}$ için,

$$\begin{aligned} [\mathcal{R}\mathcal{R}\mathcal{S}] &= [s\mathcal{R}, s\mathcal{R}, s\mathcal{R}] = [\mathcal{S}\mathcal{S}\mathcal{T}] \text{ ve} \\ [\mathcal{R}\mathcal{R}\mathcal{T}] &= [t\mathcal{R}, t\mathcal{R}, t\mathcal{R}] = [\mathcal{T}\mathcal{T}\mathcal{S}] \end{aligned}$$

olması nedeniyle,

$$[\mathcal{R}\mathcal{R}\{0\}] + [\mathcal{R}\mathcal{R}\mathcal{R}] + [\mathcal{S}\mathcal{S}\mathcal{T}][\mathcal{T}\mathcal{T}\mathcal{S}] = m^2 \quad (2.8.3)$$

$$[\{0\}\mathcal{T}\mathcal{S}] + [\mathcal{R}\mathcal{T}\mathcal{S}] + [\mathcal{S}\mathcal{T}\mathcal{S}][\mathcal{T}\mathcal{T}\mathcal{S}] = m^2 \quad (2.8.4)$$

eşitliğin sağlandığı görülür. $\mathcal{S} \cap \mathcal{T} = \emptyset$ ve $-\mathcal{S} = \mathcal{S}$ olduğundan, $[\{0\}\mathcal{T}\mathcal{S}] = 0$ ve ayrıca, $-\mathcal{R} = \mathcal{R}$ olması nedeniyle de; $[\mathcal{R}\mathcal{R}\{0\}] = m$ eşitlikleri kullanılarak; (2.8.3) ve (2.8.4) ün eşitlenmesiyle; $m + [\mathcal{R}\mathcal{R}\mathcal{R}] = [\mathcal{R}\mathcal{T}\mathcal{S}]$ ve böylece,

$$M_p = \frac{9 \cdot [\mathcal{R}\mathcal{T}\mathcal{S}]}{m}$$

formülü elde edilir. Burada, $[\mathcal{R}\mathcal{T}\mathcal{S}]$ nin belirlenmesiyle M_p nin belirlenebileceği gerçeğinden hareketle ispatın geri kalan kısmında, $[\mathcal{R}\mathcal{T}\mathcal{S}]$ nin hesaplanabileceği bir metod geliştirilecektir.

$\xi = e^{\frac{2\pi i}{p}}$ olmak üzere birimin p -inci kökleri, $1 = \xi^0, \xi^1, \dots, \xi^{p-1}$ olduğu hatırlanacak olursa, burada $\xi^a = \xi^b \iff a \equiv b \pmod{p}$ ve ayrıca $\xi^{a+b} \equiv \xi^a \cdot \xi^b \pmod{p}$ özelliklerinin sağlanacağı kolayca görülebilir.

Bu açıklamalardan sonra,

$$\alpha_1 = \sum_{r \in \mathcal{R}} \xi^r, \quad \alpha_2 = \sum_{s \in \mathcal{S}} \xi^s, \quad \alpha_3 = \sum_{t \in \mathcal{T}} \xi^t$$

olarak tanımlandığında, $\alpha_1, \alpha_2, \alpha_3$ sayıları birimin m farklı kökünün toplamı olur ve bunlar *Kübik Gauss Toplamları* olarak adlandırılır. α_i lerin herhangi ikisinin, örneğin α_2 ile α_3 ün, çarpımı

$$\alpha_2 \cdot \alpha_3 = \sum_{s \in \mathcal{S}} \xi^s \cdot \sum_{t \in \mathcal{T}} \xi^t = \sum_{s \in \mathcal{S}, t \in \mathcal{T}} \xi^{s+t} = \sum_{x \in \mathcal{F}} \mathcal{N}_x \xi^x$$

biçiminde ifade edilebilir ve burada; $\mathcal{N}_x, s \in \mathcal{S}, t \in \mathcal{T}$ olmak üzere, $s + t = x$ i sağlayan (s, t) ikililerinin sayısını göstermektedir.

$$r \in \mathcal{R} \text{ için, } \mathcal{N}_x = [\mathcal{S}\mathcal{T}\{-x\}] = [r\mathcal{S}, r\mathcal{T}, \{-rx\}] = [\mathcal{S}\mathcal{T}\{-rx\}] = \mathcal{N}_x$$

olduğundan, $\mathcal{N}_x$ in sadece $\mathcal{R}, \mathcal{S}$ veya $\mathcal{T}$ ye bağlı olması gerektiği sonucuna varılır. Böylece,

$$m \cdot \mathcal{N}_x = [\mathcal{S}, \mathcal{T}, \mathcal{R}_x] = \begin{cases} [\mathcal{S}\mathcal{T}\mathcal{R}] & , x \in \mathcal{R} \\ [\mathcal{S}\mathcal{T}\mathcal{S}] & , x \in \mathcal{S} \\ [\mathcal{S}\mathcal{T}\mathcal{T}] & , x \in \mathcal{T} \end{cases}$$

olur. a, b, c tamsayıları $[\mathcal{S}\mathcal{T}\mathcal{R}] = m \cdot a, [\mathcal{S}\mathcal{T}\mathcal{S}] = m \cdot b$ ve $[\mathcal{S}\mathcal{T}\mathcal{T}] = m \cdot c$ olacak şekilde tanımlanacak olursa,

$$M_p = 9 \cdot a \text{ ve } \alpha_2 \alpha_3 = a \alpha_1 + b \alpha_2 + c \alpha_3$$

olduğu görülür. a nın belirlenebilmesi için, $\alpha_3\alpha_1$ ve $\alpha_1\alpha_2$ benzer şekilde hesaplanarak

$$\alpha_3\alpha_1 = a\alpha_2 + b\alpha_3 + c\alpha_1,$$

$$\alpha_1\alpha_2 = a\alpha_3 + b\alpha_1 + c\alpha_2$$

eşitlikleri elde edilir. Diğer yandan,

$$0 = (\xi^p - 1) = (\xi - 1).(\xi^{p-1} + \xi^{p-2} + \dots + 1)$$

ve $\xi \neq 1$ olması nedeniyle,

$$\xi^{p-1} + \xi^{p-2} + \dots + 1 = 0$$

dan, $\alpha_1 + \alpha_2 + \alpha_3 = -1$ olduğu açıktır. Yukarıda belirlenen, $\alpha_i\alpha_j$ çarpımları taraf tarafa toplanacak olursa;

$$\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = (a + b + c)(\alpha_1 + \alpha_2 + \alpha_3) = -(a + b + c)$$

ve ayrıca,

$$\begin{aligned} m(a + b + c) &= [STR] + [STS] + [STT] \\ &= [ST(\mathcal{R} \cup \mathcal{S} \cup \mathcal{T})] \\ &= [STF_p] - [ST\{0\}] = m^2 \end{aligned}$$

eşitliğinden yararlanarak,

$$\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = -m$$

olduğu görülür. Böylece;

$$\alpha_1^2 + \alpha_2^2 + \alpha_3^2 = (\alpha_1 + \alpha_2 + \alpha_3)^2 - 2(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) = 1 + 2m$$

olur. $\alpha_1\alpha_2\alpha_3$ çarpımı

$$\begin{aligned} \alpha_1(\alpha_2\alpha_3) &= \alpha_1(a\alpha_1 + b\alpha_2 + c\alpha_3), \\ \alpha_2(\alpha_1\alpha_3) &= \alpha_2(a\alpha_2 + b\alpha_3 + c\alpha_1), \\ \alpha_3(\alpha_1\alpha_2) &= \alpha_3(a\alpha_3 + b\alpha_1 + c\alpha_2) \end{aligned}$$

eşitliklerinin taraf tarafa toplanmasıyla, $k = 2a - b - c = 3a - m$ olmak üzere,

$$3\alpha_1\alpha_2\alpha_3 = a(1 + 2m) + (b + c)(-m) = a + k.m$$

biçiminde ifade edilebilir. Burada, k nın belirlenmesi durumunda, $M_p = 9.a = 3(k + m) = 3k + p - 1$ olması nedeniyle, M_p nin de belirlenmiş olacağı açıktır.

$$F(t) = (t - \alpha_1).(t - \alpha_2).(t - \alpha_3) = t^3 + t^2 - mt - \frac{a + km}{3}$$

olsun. $F(t)$ nin, $\mathcal{D}_f$ ile gösterilecek olan diskriminantı, $\alpha_i \alpha_j$ çarpımları yardımıyla hesaplanabilir; çünkü,

$$\begin{aligned}
 \sqrt{\mathcal{D}_f} &= (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3) \\
 &= \alpha_2 \alpha_3 (\alpha_2 - \alpha_3) + \alpha_3 \alpha_1 (\alpha_3 - \alpha_1) + \alpha_1 \alpha_2 (\alpha_1 - \alpha_2) \\
 &= (a\alpha_1 + b\alpha_2 + c\alpha_3)(\alpha_2 - \alpha_3) + (a\alpha_2 + b\alpha_3 + c\alpha_1)(\alpha_3 - \alpha_1) \\
 &\quad + (a\alpha_3 + b\alpha_1 + c\alpha_2)(\alpha_1 - \alpha_2) \\
 &= (b - c)(\alpha_1^2 + \alpha_2^2 + \alpha_3^2 - \alpha_1 \alpha_2 - \alpha_1 \alpha_3 - \alpha_2 \alpha_3) \\
 &= (b - c)(1 + 3m) \\
 &= (b - c)p
 \end{aligned}$$

dir.

$i = 1, 2, 3$ için $\beta_i = 1 + 3\alpha_i$ olarak tanımlandığında,

$$\begin{aligned}
 \beta_1 + \beta_2 + \beta_3 &= 0, \\
 \beta_1 \beta_2 + \beta_1 \beta_3 + \beta_2 \beta_3 &= -3p, \\
 \beta_1 \beta_2 \beta_3 &= 3k - 2
 \end{aligned}$$

olur. Kökleri β_i olan denklem $G(t)$ ile gösterilecek olursa;

$$G(t) = (t - \beta_1)(t - \beta_2)(t - \beta_3) = t^3 - 3pt - (3k - 2)p$$

olacağından, $A = 3k - 2$ için M_p nin teoremden sözü edilen biçimde, yani

$$M_p = 3k + p - 1 = p + 1 + A$$

olarak yazılabileceği sonucuna varılır. İspatın tam olarak yapılabilmesi için, $A = 3k - 2$ nin teoremden ifade edilen koşulları sağladığını göstermek gerekir.

$\mathcal{D}_g$, $G(t)$ polinomunun diskriminantı olmak üzere, kübik denklemler için diskriminant formülünden

$$\begin{aligned}
 \mathcal{D}_g &= -4(-3p)^3 - 27(A.p)^2 \\
 &= 4.27p^3 - 27A^2p^2
 \end{aligned}$$

olur. Diğer yandan; $\beta_i - \beta_j = 3(\alpha_i - \alpha_j)$ olması nedeniyle

$$\mathcal{D}_g = 27^2 \cdot \mathcal{D}_f$$

olmalıdır. $\mathcal{D}_g$ için elde edilen bu iki eşitlikten,

$$4.27p^3 - 27A^2p^2 = 27^2 \cdot \mathcal{D}_f = 27^2 \cdot (b - c)^2 \cdot p^2$$

elde edilir. Bu eşitliğin her iki tarafının p^2 ile sadeleştirilmesiyle, $B = b - c$ olmak üzere,

$$4p = A^2 + 27B^2$$

ve

$$A = 3k - 2 \equiv 1 \pmod{3}$$

olduğu görülür.

Buraya kadar yapılan ispatta, $A, B \in \mathbb{Z}$ olmak üzere, $4p$ nin $4p = A^2 + 27B^2$ biçiminde ifade edilebileceği, $A \equiv 1 \pmod{3}$ ve $M_p = p+1+A$ olduğu gösterilmiş oldu. İspatın bitirilmesi için de; A ve B nin, işaret farkıyla, tektürlü belirli olduğu gösterilmelidir.

Kabul edelim ki, $4p$ nin $4p = A_1^2 + 27B_1^2$ gibi başka bir ifadesi daha olsun. Bu durumda,

$$\begin{aligned} 4p(B_1^2 - B^2) &= (A^2 + 27B^2)B_1^2 - (A_1^2 + 27B_1^2)B^2 \\ &= (AB_1 + A_1B)(AB_1 - A_1B) \end{aligned}$$

olur ve p sayısının eşitliğin sol tarafındaki ifadeyi bölmesi nedeniyle, p nin sağ taraftaki çarpanlardan birisini bölmesi gerekir. $p|(AB_1 - A_1B)$ olsun. $4p$ için verilen iki ifadenin çarpımı ile,

$$16p^2 = (A^2 + 27B^2)(A_1^2 + 27B_1^2) = A^2A_1^2 + 27B^2A_1^2 + 27B_1^2A^2 + 27^2B^2B_1^2$$

ve buradan

$$16p^2 - (AA_1 + 27BB_1)^2 = 27(AB_1 - A_1B)^2$$

elde edilir. $p|(AB_1 - A_1B)$ olması nedeniyle de;

$$16 - \left(\frac{AA_1 + 27BB_1}{p}\right)^2 = 27\left(\frac{AB_1 - A_1B}{p}\right)^2$$

eşitliği gerçekleşir. Bu eşitliğin sol tarafı 16 dan küçük bir sayı, sağ tarafı ise 27 nin pozitif bir katı olacağından dolayı; eşitlik sadece iki tarafın da sıfır olması durumunda söz konusu olur. Burada, $AB_1 - A_1B = 0$ olacağından, $\lambda = \frac{A_1}{A} = \frac{B_1}{B}$ için $A_1 = \lambda A$, $B_1 = \lambda B$ eşitlikleri,

$$A^2 + 27B^2 = 4p = A_1^2 + 27B_1^2$$

denkleminde yerleştirildiğinde; $\lambda^2 = 1$ ve böylece $\lambda = \mp 1$ olabileceği görülür. $\lambda = \mp 1$ için $A = \mp A_1$ ve $B = \mp B_1$ olması nedeniyle; $p|(AB_1 - A_1B)$ durumunda ispat biter. Diğer yandan, $p|(AB_1 + A_1B)$ için de benzer işlemler yapılarak

$$16p^2 - (AA_1 + 27BB_1)^2 = 27(AB_1 + A_1B)^2$$

eşitliği elde edilir. Burada, p eşitliğin sağ tarafındaki ifadeyi böldüğünden, $p|(AA_1 + 27BB_1)$ olmalıdır. Bu durum yukarıda incelendiğinden dolayı, ispat bitmiş olur.

$p \equiv 1 \pmod{3}$ olacak şekildeki küçük p asal sayıları için; $4p = A^2 + 27B^2$ yi sağlayan A ve B tamsayıları kolayca bulunabilir. Böylece, M_p belirlenmiş olur. Küçük p lere karşılık gelen A , B ve M_p değerleri ile ilgili bir çizelgeye aşağıda yer verilmiştir.

Çizelge 2.8.1 Küçük p asal sayıları için A , B ve M_p değerleri

p	A	B	$M_p = A + p + 1$
7	1	1	9
13	-5	1	9
19	7	1	27
31	4	2	36
4027	-104	14	3924

Burada, M_p lerin 9 un bir katı olması durumu bir tesadüf değildir. Çünkü, Gauss Teoremi'nin ispatı hatırlanacak olursa, M_p , $a \in \mathbf{Z}$ olmak üzere, $M_p = 9.a$ biçiminde ifade edilmişti.



3. BULGULAR VE TARTIŞMA

Bu tez çalışmasında $\mathcal{C}(\mathbf{R})$ bir eliptik eğri ve $\mathcal{O} \in \mathcal{C}(\mathbf{Q})$ olmak üzere, öncelikle $\mathcal{C}(\mathbf{Q})$ grubunun $\mathcal{C}(\mathbf{R})$ nin bir altgrubu olduğu kanıtlandı. Daha sonra, $\mathcal{C}(\mathbf{Q})$ grubunun sonlu nokta kullanılarak üretilebileceğini ifade eden Mordell Teoremi'nin, ispatında ileri derecede cebirsel sayılar teorisi kullanıldığı ve ispat biçimi beşinci bölümde yapılan ispata benzer olduğu için bu çalışmada, $\mathcal{C}(\mathbf{Q})$ nun mertebesi iki olan bir noktasının varlığı kabul edilerek Mordell Teoremi ispatlandı. Böylece, Sonlu üretilmiş Abel Gruplarının Temel Teoremi'nden, uygun bir $r \in \mathbf{N}$, $i = 1, 2, \dots, s$ için p_i bir asal sayı ve $v_i \in \mathbf{N}$ olmak üzere

$$\mathcal{C}(\mathbf{Q}) \cong \underbrace{\mathbf{Z} \oplus \mathbf{Z} \oplus \dots \oplus \mathbf{Z}}_{r \text{ tane}} \oplus \mathbf{Z}_{p_1^{v_1}} \oplus \mathbf{Z}_{p_2^{v_2}} \oplus \dots \oplus \mathbf{Z}_{p_s^{v_s}}$$

biçiminde olacağı elde edildi.

$\mathcal{C}(\mathbf{Q})$ nun yapısı ve sahip olduğu özelliklerle ilgili olarak yapılan çalışmalarda, $\mathcal{C}(\mathbf{Q})$ nun rankı olarak adlandırılan yukarıdaki r sayısının en fazla 15 olması durumunda eliptik eğri örneklerinin bulunabildiği; fakat, $r > 16$ için henüz bir eliptik eğri örneğine rastlanılmadığı görülmüştür. Kısacası, r nin alabileceği maksimum değer henüz kesin olarak belirlenememiştir. Bu konuda çalışmalar devam etmektedir.

Diğer yandan, $\mathcal{C}(\mathbf{Q})$ nun mertebesi sonlu olan noktalarından oluşan ve burkulma (torsion) grubu olarak adlandırılan, $\mathbf{Z}_{p_1^{v_1}} \oplus \mathbf{Z}_{p_2^{v_2}} \oplus \dots \oplus \mathbf{Z}_{p_s^{v_s}}$ grubu ile ilgili olarak elde edilen sonuçlardan bazıları şunlardır:

a) Nagell-Lutz Teoremi kullanılarak $\mathcal{C}(\mathbf{Q})$ nun mertebesi sonlu olan bütün noktaları belirlenebilir, dolayısıyla da $\text{tors } \mathcal{C}(\mathbf{Q})$ nun bütün noktaları belirlenebilir.

b) Mazur Teoremi ile herhangi bir eliptik eğri için $\text{tors } \mathcal{C}(\mathbf{Q})$ gruplarının izomorf olacağı 15 grup elde edilerek Nagell-Lutz Teoremi yardımıyla, $\text{tors } \mathcal{C}(\mathbf{Q})$ nun izomorf olduğu grup tam olarak belirlenebilir.

4. SONUÇ

Sayılar teorisinde önemli problemlerden biri katsayıları tamsayı olan polinom denklemlerin, yani Diophantus denklemlerinin tam veya rasyonel çözümlerini belirlemektir.

Yukarıdaki özelliklere sahip bir $f(x, y) = \sum_{i+j \leq 3} a_{ij} x^i y^j = 0$ denklemi ele alındığında, bu denklemin bütün tam veya rasyonel çözümlerini belirlemek dahi o kadar kolay değildir. Bu nedenle, $f(x, y) = 0$ ın belirlediği eğri eğer bir eliptik eğri ise, eğri üzerinde bir rasyonel nokta belirlendikten sonra Mordell Teoremi'nden yararlanarak diğer tüm rasyonel noktalar üretilebilir. Dolayısıyla, bu durumda $f(x, y) = 0$ ın tüm tam veya rasyonel çözümleri belirlenmiş olur.

Diğer yandan, eğer $f(x, y) = 0$ ın belirlediği eğri bir eliptik eğri değil (yani, tekil kübik eğri) ise tekil nokta dışındaki herhangi bir rasyonel nokta kullanılarak teğet ve kiriş yöntemiyle başka rasyonel noktalar elde edilebilir.

Verilen tekil kübik eğrinin sonlu üretilmiş bir Abel grubu olup olmadığı henüz tam olarak ($y^2 = x^3$, $y^2 = x^3 + x^2$ dışında) belirlenemediğinden dolayı, eğri üzerindeki tüm rasyonel noktaları tam olarak belirlemek zordur. Fakat, kübik eğrilerin büyük bir çoğunluğunu oluşturan eliptik eğriler için, bu problem çözülmüştür.

Sonuç olarak denilebilir ki, eğer tekil kübik eğriler üzerindeki tüm rasyonel noktaları verebilecek bir yöntem geliştirilebilirse, iki değişkenli ve derecesi üç olan Diophantus denklemlerinin tüm rasyonel (dolayısıyla, tamsayı) çözümleri belirlenmiş olur.

5. ÖZET

Katsayıları rasyonel sayılar olan $f(x, y) = \sum_{i+j \leq 3} a_{ij} x^i y^j = 0$ kübik denklemi, uygun dönüşümlerle, Weierstrass normal formu olarak bilinen

$$y^2 = g(x) = x^3 + ax^2 + bx + c \quad a, b, c \in \mathbb{Q} \quad (5.1)$$

biçimine dönüştürülebilir. Eğer burada $g(x) = 0$ ın farklı karmaşık kökleri var ise, (5.1) denkleminin belirlediği eğriye $\mathbb{Q}$ üzerinden bir eliptik eğridir denir.

Bir eliptik eğri üzerinde bulunan herhangi iki, P ve R noktasından geçen doğru bu eğriyi tektürlü belirli üçüncü bir noktada keser. İşte bu noktanın x -eksenine göre simetriği olan nokta, verilen iki noktanın toplamı, yani $P + R$ noktası olarak tanımlanır. Toplama işleminin bu şekilde tanımlanmasıyla, eliptik eğri üzerindeki noktalar kümesi birim elemanı eğrinin sonsuzdaki noktası olan bir Abel grubu oluşturur.

Verilen eliptik eğri üzerindeki bir $P = (x, y)$ noktası için eğer $x, y \in \mathbb{Q}$ ise bu noktaya eğrinin bir rasyonel noktası denir. Eğer eğrinin sonsuzdaki noktası bir rasyonel nokta olarak ele alınırsa, rasyonel noktalardan oluşan küme verilen eliptik eğri üzerindeki noktalar grubunun bir altgrubunu oluşturur. Bu tezin amacı, bu altgrubun yapısını ve özelliklerini incelemektir. Bu bağlamda akla gelebilecek sorulardan biri şudur: Acaba bu altgrup sonlu mudur, veya sonlu üretilmiş bir Abel grubu mudur? Bu sorunun yanıtı, evettir. Bu sorunun yanıtı, söz konusu grubun sonlu üretilmiş Abel grubu olduğunu ifade eden Mordell Teoremidir. Tezin birinci bölümünde, konu ile ilgili ön bilgiler verilmiş ve gösterimler tanıtılmıştır. Tezin ikinci bölümünde yükseklik kavramı ve bazı homomorfizm dönüşümlerinden yararlanarak, Mordell Teoremi'nin ispatına (mertebesi iki olan bir rasyonel noktanın varlığı durumunda) yer verilmiş ve bununla ilgili bir kaç örnek yapılmıştır.

Sonlu Üretilmiş Abel Gruplarının Temel Teoremi'nden yararlanarak, bir eliptik eğri üzerindeki rasyonel noktalar grubunu incelemek yerine bu grubun izomorf olduğu ve $\mathbb{Z}$ ile $\mathbb{Z}_{p_i, v_i}$ lerin dolaysız toplamından oluşan grubu belirleyebilmek yeterlidir. Çünkü, $\mathbb{Z}$ ile $\mathbb{Z}_{p_i, v_i}$ lerin yapıları ve özellikleri çok iyi bilindiği için rasyonel noktalar grubu hakkında birçok sonuç kolayca elde edilmiş olur.

Birinci bölümde ifade edilen Nagell-Lutz ve Mazur teoremleri yardımıyla rasyonel noktalar grubunun mertebesi sonlu olan noktalarından oluşan grubun tam olarak belirlenebildiği görülmüştür. Bununla beraber, bu grubun rankı olarak adlandırılan r sayısı ile ilgili olarak, bugüne kadar, $r > 15$ olan herhangi bir eliptik eğri örneği bulunamamıştır.

Sadece $\mathbb{R}$ veya $\mathbb{Q}$ cismi için değil de herhangi bir $\mathbb{F}$ cismi (sonlu veya sonsuz) üzerinden eliptik eğriler düşünülebileceğinden dolayı, üçüncü bölümde sonlu cisimler

zerinden eliptik eęri kavramının tanımı verilmiřtir. Bu tr eliptik eęriler iin de rasyonel nokta kavramı tanımlanarak zel bir eliptik eęri iin bu eęri zerindeki rasyonel noktaların sayısını veren Gauss Teoremi ifade ve ispat edilmiřtir.



6. SUMMARY

It is well known that by suitable transformations a cubic equation of the form

$$f(x, y) = \sum_{i+j \leq 3} a_{ij} x^i y^j = 0$$

with rational coefficients can be transformed into an equation of the following form which is referred to as Weierstrass Normal Form:

$$y^2 = g(x) = x^3 + ax^2 + bx + c; \quad a, b, c \in \mathbb{Q} \quad (6.1)$$

If the equation $g(x) = 0$ has distinct complex roots, then the curve given by the equation (6.1) is called an elliptic curve over $\mathbb{Q}$.

If P and R are two points on an elliptic curve, then the line joining these two points intersects the curve in a uniquely determined third point. The symmetric partner of this point about the x -axis is defined to be the sum $P + R$ of the points P and R . With this definition of addition, the set of points on the elliptic curve becomes an Abelian group whose identity element is the point at infinity of the elliptic curve.

Given an elliptic curve and a point $P = (x, y)$ on it; if $x, y \in \mathbb{Q}$, then P is called a rational point of the curve. If the point at infinity is considered as a rational point, then the set of rational points constitutes a subgroup of the group of points on the elliptic curve. The aim of this thesis is to investigate the structure and properties of this subgroup. One of the questions that one might ask, in this context, is whether or not this subgroup is finite or finitely generated. The answer to this question is Mordell's Theorem which states that the subgroup of rational points is a finitely generated Abelian group.

In the first chapter of the thesis we give the preliminaries and introduce the notations. In the second chapter, we give the proof of Mordell's Theorem (under the assumption that there is a rational point of order two) where we use the concept of height and also some homomorphic mappings. We also give some examples in connection with Mordell's Theorem.

Since the Fundamental Theorem of Finitely Generated Abelian groups gives the structure of such groups completely; one can say that the structure of the group of rational points of an elliptic curve is completely described by Mordell's Theorem.

By means of Nagel-Lutz Theorem and Mazur's Theorem the we have stated in the first chapter, it is possible to determine the subgroup of elements of finite order in the group of rational points of elliptic curves over $\mathbb{Q}$. However, not much is known about the rank r of this group, and so far, no example is given for an elliptic curve with $r > 15$.

In the third chapter of the thesis, we give the definition of elliptic curves over

finite fields. We introduce the concept of rational points in that case also, and we reproduce the proof of a theorem of Gauss which gives the number of rational points of a particular elliptic curve over a finite field.



7. KAYNAKLAR

- BREMNER, A. and CASSELS, J.W.S. 1984.** On the equation $Y^2 = X(X^2 + p)$. Math. Comp. 42 , pp. 257-264.
- KNAPP, A.W. 1992.** Elliptic Curves. Princeton University Press, pp. 1-121, New Jersey.
- KOBLITZ, N. 1987.** A Course in Number Theory and Cryptography, New York.
- MENEZES, A. and VANSTONE S. 1990.** The Implementation of Elliptic Curve Cryptosystems. Dept. of Combinatorics and Optimization, University of Waterloo, pp. 2-13, Ontario, Canada.
- MENSTRE, J.F. January 1992.** Private communication.
- NIVEN, I. , ZUCKERMAN, H.S. and MONTGOMERY, H.L. 1991.** An Introduction to the theory of numbers. pp. 249-287, New York.
- SIEGEL, C.L. 1926.** The Integer Solutions of the equation $y^2 = ax^n + bx^{n-1} + \dots + k$. Math. Soc. 1, pp. 66-68, London.
- SILVERMAN, J.H. and TATE, J. 1992.** Rational points on Elliptic Curves. Springer-Verlag, pp. 1-144, New York, Inc.
- WEIL, A. , 1949.** Number of solutions of equations over finite fields. Bull. Amer. Math. Soc. 55, pp. 497-508, America.

ÖZGEÇMİŞ

Sevda SEZER, 1971 yılında Bitlis'te doğdu. İlk, orta, lise öğrenimini Antalya'da tamamladı. 1990 yılında girdiği Akdeniz Üniversitesi Fen Fakültesi Matematik Bölümünden 1994 yılında Matematikçi olarak mezun oldu. Ekim 1994-Ocak 1997 yılları arasında, Akdeniz Üniversitesi Fen Bilimleri Enstitüsü, Matematik Anabilim Dalında Yüksek Lisans Öğrenimini tamamladı.

Nisan 1996 dan itibaren Akdeniz Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalında Araştırma Görevlisi olarak görev yapmaktadır.

