T.C.
ULUDAĞ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

DIOPHANT DENKLEMLERİ VE ELİPTİK EĞRİLER

Musa DEMİRCİ

DOKTORA TEZİ
MATEMATİK ANABİLİM DALI

BURSA-2007

T.C.
ULUDAĞ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

DIOPHANT DENKLEMLERİ VE ELİPTİK EĞRİLER

Musa DEMİRCİ

Prof. Dr. İsmail Naci CANGÜL
(Danışman)

DOKTORA TEZİ
MATEMATİK ANABİLİM DALI

BURSA-2007

T.C.
ULUDAĞ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

DIOPHANT DENKLEMLERİ VE ELİPTİK EĞRİLER

Musa DEMİRCİ

DOKTORA TEZİ
MATEMATİK ANABİLİM DALI

Bu Tez 12/01/2007 tarihinde aşağıdaki jüri tarafından oybirliği/~~oy~~ ~~çokluğu~~ ile kabul edilmiştir.

Prof. Dr. İ. Naci CANGÜL
Danışman

Prof. Dr. Ahmet AVİNÇ

Doç. Dr. Osman BİZİM

Doç. Dr. Recep ŞAHİN

Yrd. Doç. Dr. Yılmaz ŞİMŞEK

ÖZET

Bu tezde, iki özel iki değişkenli ve üçüncü dereceden Diophant denklem sınıfı ele alınmıştır. Bunlar Bachet ve Frey eliptik eğrilerine karşılık gelen Diophant denklemleridir.

Eliptik eğriler için daha önce elde edilmiş olan sonuçlardan faydalanarak ve bunlara yenilerini ekleyerek karşılık gelen Diophant denklemlerinin çözümleri ile ilgili birçok sonuç belirlenmiştir. Basitleştirilmiş Weierstrass denkleminin özel birer hali olan $y^2 = x^3 + a^3$ Bachet eliptik eğrileri ve $y^2 = x^3 - n^2 x$ Frey eliptik eğrileri üzerindeki rasyonel noktaların sayısı, bu noktaların mertebeleri ve bu eğrilerin grup yapıları incelenmiştir. Eliptik eğri üzerindeki rasyonel noktalar, karşılık getirilen Diophant denklemlerinin çözümlerine karşılık geldiğinden bu elde edilen sonuçlar aynı zamanda bu Diophant denklemlerinin de çözümleri için de geçerli olurlar.

Tezin sıfırıncı ve birinci bölümlerinde, çalışmanın ikinci ve üçüncü bölümlerine temel oluşturacak kavramlar verilmiştir. Diophant denklemi ve eliptik eğri kavramları tanımlanmış ve aralarındaki ilişkiler ele alınmıştır. İkinci bölümde Bachet ve Frey Diophant denklemlerinin çözüm sayıları ile ilgili bazı sonuçlar verilmiştir. Üçüncü bölümde ise tanımlanan toplama işlemine göre bu denklemlerin çözüm kümelerinin grup yapıları ele alınmıştır.

ABSTRACT

In this thesis, two special classes of two variable cubic Diophantine equations, called Bachet and Frey equations, are considered in relation with some elliptic curve classes.

A new set of results related to the solutions of Diophantine equations corresponding to the ones obtained for elliptic curve classes is given. The number of rational points on Bachet elliptic curves $y^2 = x^3 + a^3$, and Frey elliptic curves $y^2 = x^3 - n^2 x$, which are just some special cases of simplified Weierstrass equation; their orders, and the group structure of them are considered. As the rational points on elliptic curves correspond to the solutions of the Diophantine equations, the results obtained for elliptic curves are also valid for the corresponding Diophantine equations.

In the first two chapters, the preliminary information necessary for the second and third chapters are recalled. The notions of Diophantine equations and elliptic curves are defined and the relations between them are obtained. In the second chapter, some results concerning the number of rational points on Bachet and Frey elliptic curves are given. In the third chapter, the group structure of the solution sets of these Diophantine equations under the addition operation are considered.

İÇİNDEKİLER

SİMGELER DİZİNİ

$\mathbb{Z}$	Tam sayılar kümesi
$\mathbb{Q}$	Rasyonel sayılar kümesi
$\mathbb{F}$	Cisim
$\mathbb{F}_p$	p elemanlı sonlu cisim
$\mathbb{F}_q$	Karakteristiği p olan q elemanlı sonlu cisim
$\mathbb{F}_p^*$	p elemanlı sonlu cisimin çarpımsal grubu: $\mathbb{F}_p - \{\bar{0}\}$
$\overline{\mathbb{F}}$	$\mathbb{F}$ cisminin cebirsel kapanışı
$\mathbb{F}[x, y]$	Katsayıları $\mathbb{F}$ cisminden alınan polinomlar halkası
$\mathbb{Z}[x]$	Katsayıları tam sayılar olan x'in polinomlarının halkası
$\mathbb{Z}_n$	n modunda kalan sınıflarının kümesi
$\mathbb{Z}_p$	p asal modundaki tam sayılar cismi
U_n	Birimlerin kümesi
Q_n	İkinci dereceden kalanların kümesi
K_p	p asal modunda üçüncü dereceden kalanların kümesi
$\chi(a)$	a'nın p asal modunda Legendre fonksiyonu
$\chi_3(a)$	a'nın p asal modunda üçüncü dereceden kalan karakteri
$\left(\frac{a}{p}\right)$	a'nın p asal modunda Legendre sembolü
E	Weierstrass eğrisi
E_a	Bachet eliptik eğrisi
$E \setminus \mathbb{F}$	Katsayıları $\mathbb{F}$ cisminden alınan E eğrisi
$E(\mathbb{F})$	$\mathbb{F}$ cismindeki E eğrisi üzerindeki noktaların kümesi
$E(\mathbb{F}_p)$	$\mathbb{F}_p$ sonlu cismindeki E eğrisi üzerindeki noktaların kümesi
$\#E(\mathbb{F}_p)$	$\mathbb{F}_p$ sonlu cismindeki E eğrisi üzerindeki noktaların sayısı
$E(\mathbb{F})_t$	$\mathbb{F}$ cismi üzerindeki E eğrisinin büküm noktalarının kümesi

$E(\mathbb{Q})$	$\mathbb{Q}$ cismi üzerindeki E eğrisinin noktalarının kümesi
$E(\mathbb{Q})_t$	$\mathbb{Q}$ cismi üzerindeki E eğrisinin büküm noktalarının kümesi
$E[n]$	E eğrisi üzerindeki n. mertebeden noktaların kümesi
$E(\mathbb{F})[n]$	$\mathbb{F}$ cismindeki E eğrisi üzerindeki n.mertebeden noktaların kümesi
$Kar(\mathbb{F})$	$\mathbb{F}$ cisminin karakteristiği
Q_p'	p asal modunda ikinci dereceden bir kalan olmayan kalanların kümesi
N	Nokta sayısı
$N_{p,a}$	Bachet eliptik eğrisi üzerindeki nokta sayısı
φ_q	q Frobenius endomorfizmi
t	Frobenius endomorfizminin izi
$j(E)$	E eğrisinin j-değişmezi
Δ	Weierstrass denkleminin diskriminantı
$C_n \times C_m$	n ve m mertebeli iki devirli grubun direkt çarpımı
$\mathbb{Q}[[T]]$	Katsayıları $\mathbb{Q}$'dan alınan kuvvet serileri halkası
θ	Sonsuzdaki nokta

0. GİRİŞ

0.1. Temel Bilgiler

Bu çalışmanın amacı, Diophant denklemleri ve bu denklemlerin belirli bir formu yardımıyla elde edilen eliptik eğriler ile bu eğrilerin çeşitleri ile ilgili inceleme yapmaktır.

Bu çalışmanın temel bilgiler kısmında I. G. Bashmakova "Diophantus and Diophantine Equations" , Y. Hellegouarch "Invitation to the Mathematics of Fermat – Wiles" , P. Ribenboim " Fermat's Last Theorem for Amateurs" ve G. E. Andrews " Number Theory" kitaplarından yararlanılmıştır.

Diophant denklemleri olarak adlandırılan denklemler genel olarak rasyonel katsayılı polinom denklemlerdir. Bu denklemlerle ilk olarak eski yunan matematikçilerinden Diophantus Alexandra'nın "Arithmetic" adlı kitabında karşılaşıldığı için bunlara Diophant denklemleri adı verilmiştir.

Bu problemlerin temellerini anlamak ve Diophant'ın metodlarını araştırmak için (indeterminate) belirsiz denklemler teorisinden ve cebirsel geometriden bazı kavramların ispatının incelenmesi ile başlanmalıdır. Günümüzde, belirsiz denklemlerin çözümü problemi aşağıdaki gibi formülize edilebilir;

n tane değişkenli m polinom verilsin (m < n), katsayıları belirli bir k cisminden alınan $f_1(x_1, x_2, ..., x_n)$, . . ., $f_m(x_1, x_2, ..., x_n)$ polinomlarının

$$\begin{aligned} f_1(x_1, x_2, ..., x_n) &= 0, \\ &\vdots \\ f_m(x_1, x_2, ..., x_n) &= 0, \end{aligned} \tag{1}$$

sistemindeki tüm rasyonel çözümlerinin $M(k)$ kümesi bulunur ve onun cebirsel yapısı hesaplanır. Tüm $x_i^{(0)} \in k$ ise $(x_1^{(0)}, ..., x_n^{(0)})$ çözümüne rasyonel denir.

$M(k)$ kümesi k cismine bağlıdır. Bu nedenle örneğin $x^2 + y^2 = 3$ denkleminin **Q** (Rasyonel sayılar) cisminde çözümü yoktur ancak $Q\sqrt{3}$ cisminde sonsuz çoklukta çözümü vardır yani, çözümler a ve b rasyonel sayılar iken $a + b\sqrt{3}$ formundaki sayıların kümesinden alınır.

Sayılar teorisi açısından en önemli durumlar $k = Q$ ve p asal iken k'nın $\bmod p$'deki kalan sınıflarının cismi olduğu durumlardır. Diophant bu durumlardan birincisini yani $k = Q$ olması durumunu ele almıştır.

Diophant'ın problemleri incelenirken öncelikle bir denklemde iki bilinmeyenin var olduğu durum ele alınır, yani $m = 1, n = 2$ iken

$$f(x, y) = 0 \qquad (2)$$

denklemiyle ilgilenilir.

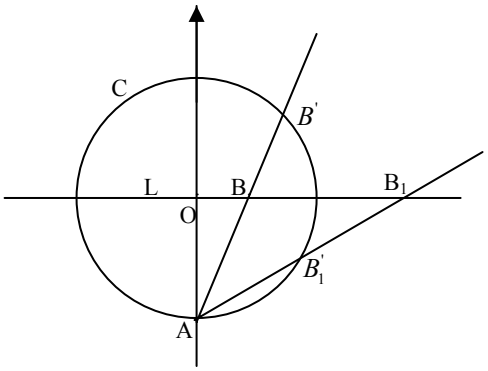
Bu denklem $R^{(2)}$ düzleminde bir Γ cebirsel eğrisini tanımlar. (2) denkleminin rasyonel çözümlerine Γ üzerindeki bir rasyonel nokta adı verilir.

İlk olarak (2) formundaki denklemlerin ya da denk olarak cebirsel eğrilerin sınıflandırılmasıyla ilgili biraz bilgi vermek gerekir. En doğal ve tarihsel olarak ilk zamanlarda bu sınıflandırma derece kavramını temel alıyordu.

(2) formundaki bir eğrinin derecesi $f(x, y)$ polinomunun terimlerindeki maksimal derecedir. Bu kavramın geometrik yorumu, n dereceli bir eğrinin ve bir doğrunun kesişimindeki noktaların sayısı n'dir. Bu noktaların sayısı sayıldığında bu noktaların katları da dikkate alınmalı ki bunlar arasında kompleks noktalar ve sonsuzdaki noktalar vardır. Örnek olarak $x^2 + y^2 = 1$ çemberi ve $x + y = 2$ doğrusu iki kompleks noktada kesişir, $x^2 - y^2 = 1$ hiperbolu ve $y = x$ doğruları sonsuzda iki noktada ve aynı hiperbol ve $x = 1$ doğrusu, 2 nin katlılığındaki bir noktada kesişir.

Diophant analizinin bakış açısından dereceye dayalı sınıflandırma daha önemli hale gelmiştir.

$C: x^2 + y^2 = 1$ çemberini ve rasyonel katsayılı herhangi bir doğruyu ele alalım, $L: y = 0$ denirse bu iki eğri üzerindeki rasyonel noktalar arasında $1:1$ eşleme vardır. Bunu göstermek için aşağıdaki yöntem kullanılabilir; C üzerinde sabit bir $A(0,-1)$ noktası ve L üzerindeki her bir B rasyonel noktayla birleştirilir AB doğrusu C çemberi ile C üzerindeki B' noktasında kesişir. Bunu aşağıdaki Şekil 0.1.1'de görebiliriz.



Şekil 0.1.1

Aşikâr olarak, herhangi bir rasyonel doğru ve rasyonel noktalı herhangi bir konik parça üzerindeki rasyonel noktalar arasında bu çeşit bir ilişki kurmak mümkündür. Bu gösterir ki Diophant analizi açısından dereceleri farklı olmasına rağmen C çemberi ve L doğrusu ayırt edilemezdir. Rasyonel noktalarının kümeleri denktir.

Cebirsel eğrilerin daha iyi bir sınıflandırılma işlemi bu eğrilerin cinslerine göre olur. Bu sınıflandırma yöntemi 19. yüzyılda Abel ve Riemann tarafından ortaya atıldı. Bu işlem için bir Γ eğrisi üzerindeki singüler noktalar ele alınır.

Γ eğrisinin (2) formundaki $f(x,y)$ polinomunun rasyonel sayılar cismi üzerinde indirgenemez olduğunu yani rasyonel katsayılı polinomların çarpımı olarak yazılamayacağını kabul edelim. Bir $p(x_0, y_0)$ noktasında Γ eğrisinin teğet doğrusu

$$k = -\frac{f_x(x_0, y_0)}{f_y(x_0, y_0)}$$

olmak üzere

$$y - y_0 = k.(x - x_0)$$

ile verilir.

f_x ya da f_y, p noktasında sıfırdan farklı ise, bu taktirde teğetin k katsayısı sonlu ve tanımlı bir değere sahiptir. Eğer $f_y(x_0, y_0) = 0$ ve $f_x(x_0, y_0) \neq 0$ ise bu durumda $k = \infty$ ve p noktasındaki teğet dikeydir.

Eğer p noktasındaki her iki kısmi türev de sıfıra eşit ise yani

$$f_x(x_0, y_0) = 0 \text{ ve } f_y(x_0, y_0) = 0$$

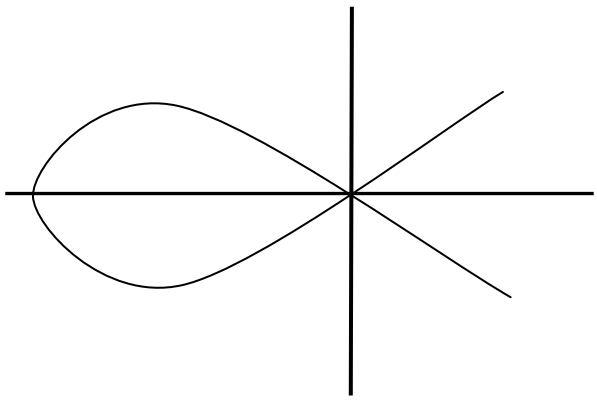
ise bu taktirde p noktasına singüler nokta denir.

Örnek olarak $(0,0)$ noktası $y^2 = x^2 + x^3$ eğrisinin singüler noktasıdır çünkü bu noktada kısmi türevler

$$f_x = -2x - 3x^2 \text{ ve } f_y = 2y$$

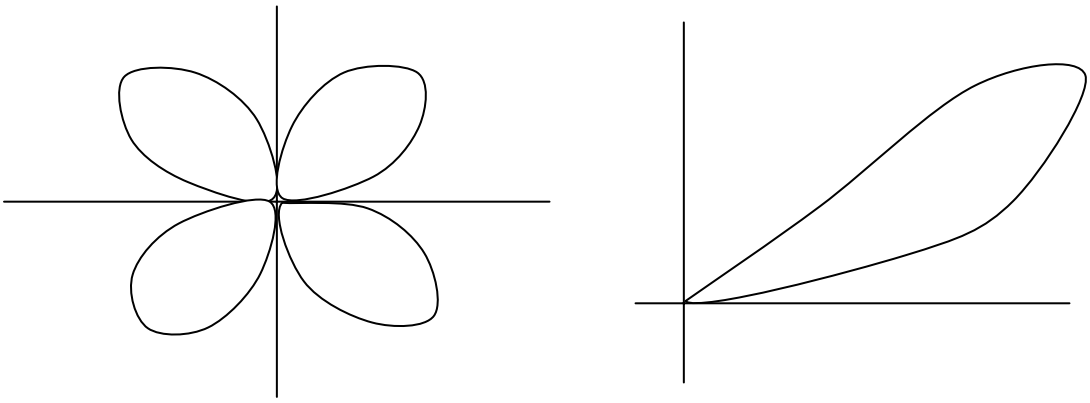
sıfıra eşit olur (yok olur).

Bir eğri üzerindeki en temel (basit) noktalar çift katlı (double point) noktalar, f_{xx}, f_{xy} ve f_{yy} kısmi türevlerinin en az birinin sıfır olmadığı noktalardır. Şekil 0.1.2 de iki farklı teğete sahip eğride bir çift katlı nokta (double point) olduğu görülebilir.



Şekil 0.1.2

Daha kompleks singüler noktalar Şekil 0.1.3'teki gibi gösterilir.



Şekil 0.1.3

Bir cebirsel eğri en çok sonlu sayıda singüler noktaya sahiptir. Gerçekten $f(x,y)$, Q üzerinde indirgenemez iken

$$f(x,y)=0$$

eğrinin denklemi olsun. Singüler noktaların koordinatları

$$f_x(x,y)=0,\ f_y(x,y)=0$$

denklemlerini ve (2) denklemini sağlamalıdır. Ancak bu üç cebirsel denklemden oluşan sistem yalnızca sonlu çoklukta çözüme sahip olabilir.

Şimdi, singüler noktaları iki katlı noktalar olan düzlem cebirsel eğrisinin cinsini tanımlayacağız (Genel durumda yani herhangi singüler noktaları olan herhangi bir cebirsel eğri alındığında tanım diğerlerine göre daha karmaşıktır. Burada ihtiyaç duymadığımız için bu genel tanım verilmeyecektir).

Γ, d tane iki katlı noktaya sahip olan bir düzlem cebirsel eğrisi olsun. Bu taktirde Γ'nın cinsi; n, Γ'nın derecesi olmak üzere

$$g=\frac{(n-1)(n-2)}{2}-d$$

formülü ile tanımlanan g tamsayısıdır. $g\geq 0$ olduğu gösterilebilir. Eğer Γ bir doğru ya da ikinci derece bir eğri ise formül p'nin 0 değeri için sağlanır, yani eğrilerin cinsleri aynıdır. Üçüncü dereceden bir eğri hiç iki katlı noktaya sahip değilse bu eğrinin

cinsi 1 dir, eğer cinsi 0 ise bu eğri iki katlı bir noktaya sahiptir. Örneğin, Fermat eğrisi olarak bilinen $x^3 + y^3 = 1$ eğrisinin cinsi 1'dir.

Cins kavramına göre sınıflandırma, bir eğrinin aritmetik özelliklerinin bütünüyle belirlenmesinde yetersiz kalır. Örneğin $x^2 + y^2 = 1$ ve $x^2 + y^2 = 3$ eğrilerinin her ikisinin de cinsi 0 dır. Ancak bunlardan birincisi sonsuz çoklukta rasyonel nokta bulundururken ikinci eğri hiç rasyonel nokta bulundurmaz. Diophantine analizi açısından yeterli olan eğrilerin sınıflandırılmasını bulmak için (2) formundaki denklemi çözerken φ ve ψ rasyonel fonksiyonlar iken (polinomların sayısı kadar)

$$x = \varphi(u,v),\ y = \psi(u,v) \tag{3}$$

değişken değiştirmelerini uygularız. (2) formundaki denkleme (3) deki değişkenler konulunca

$$G(u,v) = 0$$

denklemi elde edilir. Bu denklem bir Γ' eğrisi belirtir. Γ üzerindeki rasyonel noktalar, onların sonlu tanesi ihmal edilirse Γ' üzerindeki rasyonel noktalara taşınabilir ve tersine Γ' üzerindeki rasyonel noktaların da ters görüntülerinin Γ üzerindeki rasyonel noktalar olması için gerek ve yeter şart φ ve ψ fonksiyonlarının rasyonel katsayılı ve (3) deki denklemlerin terslerinin alınabiliyor olmasıdır. Yani

$$u = \varphi_1(x,y),\ v = \psi(x,y) \tag{4}$$

olacak şekilde rasyonel katsayılara sahip φ_1 ve ψ_1 rasyonel fonksiyonları bulmak mümkün olmalıdır. Eğer (3) ve (4) deki rasyonel katsayılara sahip denklemlerden faydalanarak Γ ve Γ' eğrileri arasında bir bağıntı kurmak mümkün ise bu taktirde eğrilere "*kendileri ve tersi rasyonel olarak denk eğriler*" denir ve bunu sağlayan dönüşümler "*kendisi ve tersi rasyonel dönüşümler*" olarak adlandırılır.

Örnek olarak, $\varphi(u,v)$ ve $\psi(u,v)$ lineer fonksiyonlar ise, yani

$$x = \varphi(u,v) = au + bv + c\,,$$

$$y = \psi(u,v) = a_1u + b_1v + c_1$$

ve

$$\begin{vmatrix} a & b \\ a_1 & b_1 \end{vmatrix} \neq 0$$

ise bu taktirde u ve v rasyonel katsayılara sahip x ve y'nin terimlerinde ifade edilebilir, yani tanımlanan dönüşümün kendisi ve tersi rasyoneldir. Aşağıdaki örnek biraz daha karmaşıktır. L eğrisi

$$\begin{aligned} y^2 &= x^4 - x^3 + 2x - 2 \\ &= (x-1)(x^3+2) \end{aligned} \tag{5}$$

şeklinde verilmiş olsun. $\varphi_3(u)$ bir kübik polinom iken L, $v^2 = \varphi_3(u)$ formundaki L' eğrisine, yani kendisi ve tersi rasyonel olan bir eğriye dönüştürülebilir. Bu işlemi tamamlamak için (5) denkleminin her iki tarafı $(x-1)^4$ ile bölünür ve

$$x - 1 = \frac{1}{u},\ \frac{y}{(x-1)^2} = v$$

konulursa (5) denklemi

$$v^2 = 3u^3 + 3u^2 + 3u + 1$$

haline dönüşür. Aynı zamanda u ve v denklemlerindeki x ve y ifadeleri

$$x = \frac{1+u}{u},\ y = \frac{v}{u^2}$$

şeklinde rasyonel olarak edilebilir ve tersine

$$u = \frac{1}{x-1},\ v = \frac{y}{(x-1)^2}$$

yani L ve L' eğrileri üzerinde kendisi ve tersi rasyonel dönüşüm tanımlanabilen denk eğrilerdir.

Sonlu sayıdaki noktanın ihmal edilmesi durumunda üzerlerinde kendisi ve tersi rasyonel dönüşüm tanımlanabilen denk iki eğri üzerindeki rasyonel noktaların M ve M' kümeleri arasında $1:1$ bir bağıntı kurmak mümkündür. Gözardı edilen noktalar (3) ve (4) deki denklemlerden en az birindeki hem pay hem de paydayı yok eden (sıfıra eşitleyen) noktalardır. İkinci örneğimizde,

$$v = \frac{y}{(x-1)^2}$$

fonksiyonun hem pay hem de paydası L üzerindeki $(1,0)$ noktasında sıfır olur. Bu ise L üzerindeki $(1,0)$ noktasına karşılık L''de hiçbir noktanın olmadığı anlamına gelir.

Diophant analizi açısından denk eğriler aynı görüntüye sahiptir. Ancak derecelerinin aynı olması gerekmez. Gösterilebilir ki üzerlerinde kendisi ve tersi rasyonel olan bir dönüşüm tanımlanan denk eğrilerin cinsleri eşittir. Başka bir ifadeyle kendisi ve tersi rasyonel olan dönüşümler altında ne n derecesi ne de iki katlı noktaların d sayısı değişmez. Bir eğrinin g cinsi bu büyüklüklerin bir fonksiyonudur ve o da değişmez. Tersi doğru değildir, yani cinsi eşit olan eğrilerin üzerlerinde kendileri ve tersleri rasyonel olan dönüşümlerin tanımlanması zorunlu değildir. Bu durum

$$x^2 + y^2 = 1 \text{ ve } x^2 + y^2 = 3$$

eğrileri ile ilgili bir önceki örnekten açıkça görülmektedir. Bu eğrilerin her ikisinin de cinsi 0 olmasına rağmen birinci eğri sonsuz çoklukta rasyonel noktaya sahipken ikincisinin hiç rasyonel noktası yoktur.

Böylece cinsi aynı olan eğriler, üzerlerinde kendileri ve tersleri rasyonel olan dönüşümler tanımlanabilen denk eğrilerin denklik sınıflarına ayrılır. Bu kavramların önemi Henri Poincaré tarafından ortaya konulmuştur. Henri Poincaré bu yüzyılın başlarında Diophant analizinin problemlerinin araştırılması ve sınıflandırma da çok temel, kendisi ve tersi rasyonel olan bir dönüşümlerin sınıfını yapmıştır.

Şimdi aşağıda verilen önemli bir duruma dikkat edelim. Eğer Γ en az bir rasyonel noktaya sahip bir kübik eğri ise bu taktirde bu eğrinin denklemini a ve b rasyonel sayılar iken kendisi ve tersi rasyonel olan dönüşümler yardımıyla

$$y^2 = x^3 + ax^2 + b \tag{6}$$

formundaki denkleme indirgenebilir.

0.2. Belirsiz Kübik Denklemler

Diophant dördüncü kitabında üçüncü ve dördüncü dereceden belirsiz denklemleri ele almıştır. Kübik eğriler rasyonel noktalar bulundursalar bile noktaların koordinatları rasyonel sayı bulundurmayabilir. Genel olarak tek değişkenli rasyonel fonksiyonların terimleri için de geçerli olan bir durumdur. Bununla birlikte, eğer kübik bir eğri üzerinde bir ya da iki rasyonel nokta biliyorsak onun üzerinde rasyonel noktaların toplamını bulabiliriz. Aslında, koordinatları $f_3(x, y) = 0$ denklemine sahip Γ

eğrisine y nin ilavesiyle elde edilen kübik denklem tanımlanabilen kübik denklemle üç noktada kesişen bir doğru mevcuttur. Bu

$$f_3(x,y)=0 \tag{7}$$

denkleminin köklerinden ikisi rasyonel ise üçüncüsü de rasyoneldir. Bu gözlemi aşağıdaki iki işlemin sonucu olarak değerlendirebiliriz.

1) Eğer P**,** Γ eğrisi üzerinde bir rasyonel nokta ise Γ'ya P'de teğet olan k rasyonel eğimli bir teğet çizilirse bu doğru Γ eğrisindeki rasyonel noktaların toplamında kesişir. (Gerçekten de eğrinin ve teğet dorğunun ortak çözümü yapılırsa iki rasyonel köke sahip bir kübik denklem elde edilir. Bu üçüncü noktanın da rasyonel olması anlamına gelir.)

2) Eğer P_1 ve P_2, Γ eğrisi üzerinde rasyonel noktalar ise bu taktirde P_1P_2 doğrusu Γ ile bu rasyonel noktaların toplamı noktasında kesişir. Bu iki işlemden Diophant'ın tanjant ve sekant metodları olarak bahsedeceğiz. Bu metodların nasıl işlediğini görmek için Diophant'ın problemine geri dönecek olunursa dördüncü kitaptaki 24. problem;

"Verilen bir sayıyı, çarpımları küpünden kendisinin
farkına eşit olacak şekilde iki sayıya bölmek"

şeklindedir. Burada;

6 sayısı verilsin. İlk sayıyı x olarak alalım. Bu taktirde ikincisi ise $6-x$ olacaktır.

Koşul $x_1x_2=y^3-y$ olarak sağlanır. Ancak $x_1x_2=6x-x^2$'dir. Bu ifade y^3-y'ye eşit olur. Böylece a keyfi bir sayı iken $y=ax-1$ oluşturalım, örneğin $a=2$ alınırsa

$$(2x-1)^3-(2x-1)=8x^3-12x^2+4x$$

haline gelir. Bu ifade $6x-x^2$ olur. Eğer her iki ifadedeki x'in katsayıları eşit olsaydı, x rasyonel olurdu. $3.2-2$'den 4 olur ancak 6 başlangıçta verilmiş değerdir. Bundan dolayı $3a-a$, 6'ya eşit olacak şekilde a'yı hesaplamalıyız. Sonraki aşamada $y=3x-1$ değeri konulduğunda

$$y^3-y=27x^3-27x^2+6x$$

elde edilir. Bu ifade $6x - x^2$ ye eşitlenmelidir. Sonrasında $x = \frac{26}{27}$ bulunur. Sonuç olarak

$$x_1 = \frac{26}{27}, x_2 = \frac{136}{27}$$

değerleri elde edilir.

Şimdi Diophant'ın metodunu bütün bir halde indirgemeyi deneyeceğiz. Keyfi bir a sayısı verilmiş olsun ve x ile $a - x$ bulunması istenen sayılar olsun.

$$x(a - x) = y^3 - y \tag{8}$$

olduğunu biliyoruz. Bu denklemi sağlayan rasyonel çözümlerden biri $(0,-1)$ dir. Diophant'ın yöntemine göre bu noktadan geçen bir

$$y = kx - 1 \tag{9}$$

doğrusunu (Diophant burada ilk olarak $k = 2$ almayı tercih etmiştir) ve bu doğrunun (8) deki eğri ile kesiştiği noktayı buluruz.

$$ax - x^2 = k^3x^3 - 3k^2x^2 + 2kx$$

denkleminde x rasyonel sayısı için denklem sağlandığından denklemde bu kullanıldığında

$$2k = a, \tag{10}$$

yani $k = \frac{a}{2}$ bulunur ki bu Diophant'ın elde ettiği bir sonuçtur. Böylece

$$x = \frac{3k^2 - 1}{k^3} = 2.\frac{3a^2 - 4}{a^3}$$

elde edilir.

(9) doğrusu ve (10) koşulunun önemini açıklamak için (a,b) rasyonel çözümüne sahip olan $f_3(a,b) = 0$ şeklindeki iki değişkenli keyfi bir kübik denkleme Diophant'ın yöntemi uygulanır. $P(a,b)$'den geçen bir doğru çizilirse

$$y - b = k(x - a) \tag{11}$$

ya da

$$x = a + t,\ y = b + kt \tag{12}$$

olur. Buradan

$$f_3(a+t,b+kt) = f_3(a,b) + tA(a,b) + ktB(a,b) + t^2C(a,b,k) + t^3D(a,b,k)$$
$$= 0$$

elde edilir. Ancak $f_3(a,b) = 0$ ve

$$A(a,b) + kB(a,b) = 0 \tag{13}$$

değerleri yerine konulursa

$$k = -\frac{A(a,b)}{B(a,b)} = -\left(\frac{\frac{\partial f_3}{\partial x}}{\frac{\partial f_3}{\partial y}}\right)(P)$$

değeri yani (9) doğrusunun $P(a,b)$ noktasındaki eğimi bulunur. Bu $P(a,b)$ noktası (9) doğrusunun (8) eğrisine teğet olduğu nokta olarak seçilmiş olması durumunda Diophant'ın (tanjant) teğet metodu kullanılabilir.

Diophant aynı metodu VI. kitabındaki 18. problemi çözmek için de kullanmıştır. Bu problem öncekilere benzer olarak

$$x^3 + y^3 = a^3 - b^3$$

şeklindedir. Ayrıca Diophant, kendisinin günümüze kadar ulaşmamış olan "Porisms" adlı kitabındaki daha başka problemleri de aynı yöntemle çözdüğünü ifade etmiştir.

Diophant'ın problemlerinin çözümlerindeki işlemlere baktığımızda $\frac{dy}{dx}$ teğeti ya da

$$\frac{dy}{dx} = -\left(\frac{\frac{\partial f_3}{\partial x}}{\frac{\partial f_3}{\partial y}}\right)$$

nin değeri olan k'nın hesaplanması için tamamıyla işlemsel bir metod kullanıldığını görebiliriz. Bu yöntem özellikle Fermat ve Descartes'ın türevin tanımı yönündeki çalışmalarında çok önemli bir rol oynamıştır ve tamamen cebirsel olarak düşünülen bu yöntem günümüzde cebirsel geometrideki bir çok problemin çözümü için de kullanılmaktadır.

Şimdi Diophant'ın sekant metodu olarak adlandırdığı ve IV. kitabındaki 26. problemin çözümünde kullandığı metodu inceleyelim.

Çarpımları ile herhangi birinin toplamı bir tam küp olan iki sayı bulalım.

$$x_1 = a^3 x \text{ ve } a = 2$$

alınırsa

$$x_1 = 8x$$

olur.

$$x_2 = x^2 - 1$$

olsun. Bu taktirde

$$x_1 . x_2 + x_1$$

in küp olması için ilk şart sağlanır. Geriye

$$x_1 . x_2 + x_2$$

nin de bir küp olduğunu göstermek kalıyor. Ancak

$$x_1 . x_2 + x_2 = 8x^3 + x^2 - 8x - 1$$

şeklinde bir ifadedir. Bu ifade $2x - 1$'in küpüne yani

$$8x^3 - 12x^2 + 6x - 1$$

değerine eşitlendiğinde

$$x = \frac{14}{13}$$

elde edilir. Buradan da

$$x_1 = \frac{112}{13} \text{ ve } x_2 = \frac{27}{169}$$

bulunur. Diophant'ın sekant metoduna devam edilirse ilk bilinmeyen $a^3 x$ ve ikincisi $x^2 - 1$ ile ifade edilir. Böylece problemin ilk şartı sağlanır ve ikincisi

$$a^3 x^3 + x^2 - a^3 x - 1 = y^3 \tag{14}$$

eşitliğinden bulunur. Diophant bu denklemde $y = ax - 1$ değişken değiştirmesini yaptığında

$$x = \frac{a^3 + 3a}{1 + 3a^2}$$

değerine ulaşmıştır. Burada Diophant tarafından kullanılan metod daha detaylı bir şekilde ele alındığında (14) denkleminin rasyonel çözümlerinden birinin $(0,-1)$ olduğu görülür. Bu noktadan geçen bir $y = kx - 1$ doğrusu çizilir ve bu doğrunun (14) ile kesiştiği nokta aşağıdaki denklemden bulunur;

$$\left(a^3 - k^3\right)x^3 + \left(1 + 3k^2\right)x^2 - \left(a^3 + 3k\right)x = 0 .$$

Önceki durumda, Diophant x in katsayısını sıfıra eşitlemiştir. Burada ise x^3 ün katsayısı sıfıra eşitlenir ve

$$a^3 - k^3 = 0,\ k = a$$

elde edilir.

Bu adımın geometrik önemi (14) deki denklem homojen koordinatlarda yazıldığında yani

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

alınırsa

$$a^3u^3 + u^2z - a^3uz^2 - z^3 = v^3 \qquad (15)$$

elde edilir. (15) de tanımlanan bu eğrinin $P_1(0,-1,1)$, $P_2(1,a,0)$ rasyonel noktalarına sahip olduğu ve bu noktaların tanımlanan eğri ile kesişen

$$v = au - z$$

doğrusu üzerinde olduğu görülür. (15) ile verilen eğri ile yukarıdaki bu doğrunun kesiştikleri üçüncü bir rasyonel nokta daha vardır. Böylece rasyonel noktaların birinin sonlu diğerinin ise sonsuzdaki nokta olması durumunda Diophant'ın sekant metodu olarak adlandırılan metodu kullandığı görülür.

Diophant IV. ve VI. kitabındaki diğer bazı problemlerde de teğet ve sekant metodlarını kullanmıştır.

0.3. Fermat ve Viéte'nin Çalışmalarında Kullanılan Diophant Metodları

Viéte'den önce herhangi birinin cebir ile ilgili oldukça sınırlı bilgiye sahip olduğu düşünülebilir. Dolayısıyla Viéte, Diophant'tan sonra calculus alanında en büyük katkıda bulunanlardan birisi olarak kabul edilmektedir.

Diophant'ın V. kitabındaki 16. problem "İki küpün toplamı iki küpün farkı olarak ifade edilebilir" şeklinde bir ifadeye sahiptir. Burada verilen aşikar olarak $a > b > 0$ iken pozitif x ve y sayıları için

$$x^3 + y^3 = a^3 - b^3$$

denklemidir. Viéte kendisine ait olan ve alışılmışın dışında "Zetetics" başlıklı kitabında Diophant'ın bu problemini ispatlamış ve buna benzer olarak aşağıdaki iki toplamsal problemi öne sürmüştür.

1. $x^3 - y^3 = a^3 + b^3 \qquad (x > y > 0,\ a > 0,\ b > 0)$

2. $x^3 - y^3 = a^3 - b^3 \qquad (x > y > 0,\ a > b > 0)$

Viéte, Diophant'ın teğet metodunu kullanarak her üç problemi de çözmüştür. Örneğin Viéte

$$x^3 + y^3 = a^3 - b^3$$

problemini çözmek için

$$x = t - b,\ y = a - kt$$

değişken dönüşümlerini yapmıştır ve bunu yaptıktan sonra

$$t^3\left(1 - k^3\right) + 3t^2\left(ak^2 - b\right) + 3t\left(b^2 - a^2k\right) = 0$$

elde etmiştir. Burada $b^2 - a^2k = 0$ alındığında $y = a - k(x + b)$ doğrusunun

$$x^3 + y^3 = a^3 - b^3$$

eğrisine teğet olduğu $(-b, a)$ noktasını veren eşitlik bulunmuş olur ve böylece

$$t = \frac{3a^3b}{a^3 + b^3}$$

x ve y için

$$x = b.\frac{2a^3 - b^3}{a^3 + b^3},$$

$$y = a.\frac{a^3 - 2b^3}{a^3 + b^3},$$

ifadeleri bulunur ki bu çözümün ancak $a^3 > 2b^3$ olması durumunda pozitif olacağını gösterir. Bu Diophant'ın

$$x^3 + y^3 = a^3 - b^3$$

denklemiyle bağlantılı olduğu iddiasına terstir. Yani "İki küpün farkı iki küp toplamı olarak ifade edilebilir" şeklindeki problemi çözmek için çaba harcayan ve

$$x^3 + y^3 = a^3 + b^3$$

denklemine benzer bir denklemin üstesinden gelmeye çalışan biri olan Fermat, Diophant ve Viéte'nin denklemlerine ilaveler yapmıştır. Buna göre eğer bu problem teğet metodu kullanılarak çözülecek olursa x ya da y'nin ikisinden birinin negatif olması zorluğu ortaya çıkar.

Fermat'nın bu güçlüklerin üstesinden gelmek için kullandığı metod teğet metodunun ardarda kullanılmasıydı. Fermat Diophant'ın "Arithmetic" adlı kitabındaki bir problemle ilgili yaptığı yorumda

$$4x^3 + 6x^2 + 4x + 1 = z^3$$

denklemini ele almıştır. Fermat burada basit bir işlemden sonra herhangi bir kişinin $x = -\frac{9}{22}$ değerini bulabileceğini ifade etmiştir. Aslında bu Diophant'ın teğet metodu uygulanarak elde edilen bir değerdir. Yani $z = \frac{4}{3}x + 1$ alınırsa x negatif olduğundan Fermat, $x = t - \left(\frac{9}{22}\right)$ değişken değişimi yapar, bir yok etme ve ardından bir kez daha teğet metodunu kullanır. Yapılan bu işlem sonuçta

$$4t^3 + At^2 + Bt + z_1^3 = 3$$

formunda bir denklem verir. Eğer $z = \left(\frac{B}{3z_1^2}\right)t + z_1$ değişken değiştirmesi uygulanırsa pozitif çözüm elde edilmiş olur.

Fermat'nın bu metodu Billy'nin "Inventum Nowum" adlı eserinde detaylı bir şekilde anlatılmıştır. Bu kitapta Billy, $f_n(x)$ rasyonel katsayılı n. dereceden bir polinom iken

$$y^2 = f_3(x),\ y^3 = f_3(x) \text{ ve } y^2 = f_4(x)$$

formundaki denklemler için bu metodun sonsuz çoklukta çözüm verdiğine dikkat çekmiştir. Diophant'ın iddiasına geri dönüldüğünde teğet metodunu Fermat'dan çok önceleri ortaya attığını söyleyebilir miyiz?

1621 yılında Bachet de Meziriac, Diophant'ın "Arithmetic" eserinin yeni bir çevirisini yayınlamıştır. Bu yeni çeviri Xylander's için daha iyiydi ve Latincenin yanısıra yunanca parçalarda bulunduruyordu. Bu baskı sadece çeviri kalitesinden dolayı değil aynı zamanda Bachet'in detaylı yorumları nedeniyle de gittikçe daha fazla kişi tarafından tanınmaya başladı.

Diophant'ın II. kitabındaki bir kareyi iki kare toplamına ayırma şeklinde olan 8. probleminin yanındaki boşluğa Fermat; bunun dışında bir küpü iki küpe parçalamanın ya da bir dördüncü dereceden bir ifadeyi iki tane dördüncü dereceden ifadeye ya da daha genel olarak ikinci dereceden farklı bir kuvvete sahip bir ifadeyi aynı dereceden iki ifadeye parçalamanın buradaki boşluğa sığamayacak kadar zekice bir ispatını bulduğunu yazmıştır. Bu ünlü ifade "Fermat'nın Son Teoremi" olarak bilinir. Bir kitap boşluğuna yazılı olan bu iddia Euler, Legendre, Dirichlet, Kummer ve diğer büyük matematikçiler tarafından araştırılan önemli bir iddiaydı ve bu araştırmalar sırasında matematikte yeni bir bilim dalı olarak ifade edebileceğimiz aritmetik ya da cebirsel sayılar cisminin aritmetiğinin kurulmuş olduğunu söyleyebiliriz.

Pierre Fermat 1601 yılında Fransa'nın güneyindeki Toulouse yakınlarında orta sınıf bir ailede dünyaya gelmişti. İyi bir eğitim almış Latince, İtalyanca ve İspanyolcayı çok iyi konuşabiliyor tüm bu dillerde ve ana dili Fransızcada çok etkileyici şiirler yazmıştır. Yunancayı çok iyi bildiği için bir çok çevirinin düzeltmelerini yapmış ve Helenizm üzerine oluşan tecrübesi ile tanınmaktadır. Yasalarla ilgili çalışmalarına bağlı olarak Toulouse kasabasının Parlamentosuna seçilmiş ve burada diğer bir çok parlamenter arkadaşı ya da esnaf akrabaları gibi sıradan bir yaşam sürmüştür. Dışarıdan çok sakin ve düzenli görünmesine rağmen özellikle matematiğe karşı çok büyük ilgisi varmış. Bu nedenle de Archimed, Apollon ve Diophant'ın gibi eski bilim adamlarının kitaplaını okumaktaydı. Fermat'nın ilk çalışmalarından biri Pappus tarafından sunulan Apollon'un kayıp risalesi olan "On Plane Loci"nin yeniden düzenlenmesidir. Zamanının bilim merkezlerinden uzakta yaşadığı için bulduğu sonuçları sürekli olarak mektuplar aracılığı ile sunmak zorunda kalmıştır. Yazdığı mektuplar onun matematiğin doğrularını öğrenme isteğini ve bu isteğin Fermat için öteden beri ne kadar engellenemez bir güçte olduğunu göstermektedir.

Fermat şüphesiz zamanının matematikçileri arasında önde yer alan birisiydi. Bu sayede sonsuz büyüklerin analizi olarak adlandırılan alanda olduğu gibi matematiğin bir çok alanında yeni genel metodlar ortaya atmıştır. Fermat ve Descartes analitik geometrinin temellerini atan kişilerdi yine Fermat Pascal ile birlikte olasılığın temellerini attılar, benzer şekilde günümüzde bilimlerin bir çoğunun gelişmesine katkısı olmuştur. Fermat, fiziksel olarak açıklanamayan olayların matematiksel uygulamaları ile de ilgilenmiştir. Özellikle optik alanında çalışmış ve kendisinden sonra adlandırılan küçük parçacık yasasını kullanarak homojen olmayan ortamlarda ışığın nasıl hareket ettiğini açıklamayı başarmıştır.

Fermat sayılar teorisini çok sevmekteydi ve bu alanda en iyi kendisiydi. Çok sayıdaki sorudan ilginç olanlarını seçebiliyor ve özel problemler ile ilgileniyordu. Öyle ki onun ilgilendiği bu temel problemler sayılar teorisini bir bilim dalı haline getirdi. Fermat'nın problemleri 18. ve 19. yüzyıllarda Euler ile başlayıp Hilbert ile biten bir süreçte en önemli matematikçiler tarafından çalışılmıştı.

Teoremden çok problem olarak bahsedilmesinin sebebi bir çoğunun Fermat tarafından ispatsız olarak ortaya atılmış olmasıdır. İddialarının ya ispatları için arkadaşlarına gönderdiği mektuplarda ya da Diophant'ın aritmetiğinin kendisindeki kopyasının kenar boşluklarına yazıyordu. Dördüncü dereceden sayılar için son teorem bir istisnadır ki ispatını Fermat yapmıştır. Fermat sayı teorik önermelerini ispatlamak için sonsuz indirgeme metodu olarak adlandırılan yöntemi kullanmıştır. Onun yeni bir metod tanımlamış olduğu, çağdaşı matematikçilere gönderdiği mektuplardan anlaşılmaktadır. Öyleki arkadaşlarına gönderdiği mektuplarda

"Kitapta verilen geleneksel metodlar böyle zor önermeleri ispatlamaya yeterli olmadığından, bunu başarmak için tamamen yeni bir yol buldum. Bu metoda sonsuz ya da belirsiz indirgeme metodu adını veriyorum. İlk olarak onu sadece aşağıdaki gibi olumsuz (negatif) önermeleri ispatlamak için kullandım… Bir karenin üç katı ile bir karenin birleşimi olan üçün katı şeklinde hiçbir sayı yoktur… Tamsayı katsayılı kenar uzunluğuna sahip olan ve alanı bir tam kare olan hiçbir dik üçgen yoktur. İspat "Reductio Ad Absurdum" yöntemiyle yapılır. Eğer tamsayı kenarlı ve alanı tam kare olan bir dik üçgen var olsaydı bu taktirde birinciden daha küçük ve aynı özellikte başka bir dik üçgende bulunur ki bu yeni dik üçgen de aynı özelliktedir. Böylece aynı

tartışmadan dolayı bu özellikte ikinciden daha küçük bir üçüncü daha bulunur ve devamında dördüncü, beşinci, ... gibi giderek azalan sayılar elde edilir. Ancak bir doğal sayı verilince daha küçük doğal sayılara doğru sonsuz bir azalma yoktur. Bundan dolayı alanı tam kare olan bir dik üçgen olmadığı sonucuna varılır"
şeklinde bir ifade yer almaktadır.

Kenar uzunlukları tamsayı verilen bir üçgenin alanı hakkında önermeye dikkat edilirse Fermat'nın metodunu göstermede kullandığı bu üçgenle ilgili önerme farkları kare olan hiç iki dördüncü dereceden iki sayının bulunmadığı ile alakalı önermeye denktir. Farkları dördüncü dereceden bir sayı olacak şekilde iki tane dördüncü dereceden sayı yoktur. Onun ispatı Fermat'nın günümüze kadar gelen sadece sayı teorik ispat türü olan indirgeme metoduyla yapılır. Daha sonra Euler son teoremin $n = 3$ ve $n = 4$ durumunu ispat etmek için indirgeme metodunu kullandı.

Günümüzde Fermat'nın indirgeme metodu Diophant analizi problemlerinin çalışılmasında vazgeçilmez bir araçtır. Ancak bu metodun bir eğri ya da manifold üzerindeki rasyonel noktalarla ilgili problemlerdeki kullanımı "*bir noktanın yüksekliği"* denilen yeni bir kavramın ortaya çıkmasını gerektirmiştir. Örneğin,

$$f(x, y) = 0$$

belirsiz denklemi verilmiş olsun. $f(x, y) = 0$ nin rasyonel çözümlerinin olmadığı ispatlanmak isteniyor. İspat için homojen koordinatlar kullanıldığında

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

olur ve

$$\Phi(u, v, z) = 0 \qquad (16)$$

denklemi elde edilir. (2) nin her rasyonel çözümü için (16) denkleminin bir tam çözümü vardır. Böylece (16) denkleminin hiç bir tam çözümünün olmadığını göstermek yeterlidir. Örnek olarak, eğer (2) denklemi

$$Ax^n + By^n = C,$$

formundadır. Bu taktirde (16) denklemi

$$Ax^n + By^n = Cz^n$$

formundadır. (16) denkleminin bir tam çözümü (u,v,z) olsun. Noktanın yüksekliği $|u|,|v|,|z|$ sayılarının en büyüğü olarak tanımlanır. Eğer h uzunluklu bir noktanın koordinatları (16) denklemini sağlıyor ise, bu taktirde boyu $h_1 < h$ özelliğindeki başka bir noktanın koordinatları da bu denklemi sağlayacaktır. h'tan daha küçük sonlu çoklukta pozitif tamsayı olduğundan, (16) denkleminin hiç tamsayı çözümü yoktur ve böylece (2) denkleminin hiç rasyonel çözümü yoktur.

Fermat'nın $f(x,y)=0$ formundaki ikinci derece ve üçüncü dereceden belirsiz denklemlerin karakterleri hakkındaki yorumu ise aşağıdaki şekildedir. Bu bağlamda tamamıyla söylenebilecek olan Fermat'nın Diophant'ın fikirlerini tamamıyla anlayabildiği ve sadece bir eğrinin geri çekilmesi için eklediği metodları ustalıkla uygulamış olduğudur. Kübik denklemlerin rasyonel çözümlerini bulma problemlerini, metodlarını açıklamaya uğraşan Fermat'dan sonra Billy'nin çalışmasında da yazıldığı gibi "*Arithmetic*"in Fermat'da bulunan kopyasının kenar boşluklarında bulunmuştur. "Doctriane Analyticae Inventum Nowum" başlıklı Billy'nin çalışması Fermat'nın biraraya getirilmiş çalışmalarını bulunduruyordu ve Diophant'ın metodlarını detaylı ve metodik bir yolla uygulamalarını bulunduruyordu ancak Billy yeni hiçbir şey ortaya koymamıştı.

0.4. Euler ve Jacobi'nin Çalışmalarında Kullanılan Diophant Denklemleri

İkinci ve üçüncü dereceden belirsiz denklemlerin çalışılması Diophant ile başlar. Bu çalışmaların birinci aşaması Euler (1707-1783) tarafından tamamlanmıştır.

Euler 18. yüzyılın en büyük matematikçisiydi. Matematikteki bu lider pozisyonunu korumak için kuvvetli genel metodları, derin fikirleri ya da katkıda bulunmadığı temel sonuçların olduğu herhangi bir alan neredeyse yok denebilir. Özellikle bu görüş Diophant analizi için doğrudur. "Algebra" adlı kitabında Euler

$$y^2 = ax^2 + bx + c \tag{17}$$

formundaki ve

$$y^2 = ax^3 + bx^2 + cx + d \tag{18}$$

formundaki denklemlerinin rasyonel çözümleri ile ilgili soruları sistemli bir şekilde analiz etmiştir ve iki durum arasındaki farkın kesin formülünü verdi. Böylece aşağıdaki gözlemle (18) formundaki denklemlerin incelenmesine başladı;

Önceden herhangi birinin yapamadığı bir şey ifade etmeliyiz, genel bir çözüm vermeye başlarız. Daha doğrusu x in sadece bir değerini bulmak için her bir işlem bize kolaylık sağlar. Halbuki önceden kullanılan metod bir seferde sonsuz çoklukta çözüm verir.

Dahası Diophant'ın teğet metodunun yardımıyla yeni bir çözümün nasıl elde edeceğini gösterdi. Euler'in tartışmaları her ne kadar geometrik terminoloji kullanmasa da tamamen analitikti.

Euler bazı kübik eğrilerin ikinci dereceden eğriler gibi davrandığını gözlemlemiştir. Yani x ve y bilinmeyenleri tek bir değişkenin rasyonel fonksiyonları olarak ifade edilebilir. Bunun gerçekleşmesi için Euler koşullar ifade etmiştir. Özel olarak (18) formunda denklem ele alındığında, sağ taraftaki

$$\begin{aligned} F_3(x) &= ax^3 + bx^2 + cx + d \\ &= a(x-\alpha)^2(x-\beta) \end{aligned}$$

polinomu katlı rasyonel köklere sahiptir. Euler bu koşulun yeterli olduğunu ispatladı ve bu durumda

$$y = k(x-\alpha)$$

değişikliği yardımıyla x ve y için rasyonel ifadeler elde etmenin mümkün olduğunu göstermiştir. Burada yerine koyma metodu kullanıldığında önce

$$k^2(x-\alpha)^2 = a(x-\alpha).(x-\beta)$$

eşitliğini, buradan da

$$x = \frac{k^2 + a\beta}{a},$$

$$y = k\frac{k^2 + a\beta + a\alpha}{a}$$

elde ederiz. Euler'in şartının $y^2 = F_3(x)$ eğrisinin iki katlı bir noktaya sahip olmasına yani cinsinin sıfır olmasına denk olduğunu göstermek kolaydır. Gerçekten de

$$y^2 = ax^3 + bx^2 + cx + d\,,$$

$$3ax^2 + 2bx + c = 0\,,$$

$$2y = 0$$

denklemleri singüler noktalar belirtir ki burada anlatılmak istenen iki katlı (double point) noktanın apsisinin

$$F_3(x) = ax^3 + bx^2 + cx + d$$

polinomunun bir kökü olması gerektiği ve onun türevi

$$F_3'(x) = 3ax^2 + 2bx + c = 0$$

ve bu nedenle $F_3(x)$'in bir katlı kökü olması sonucu çıkar. Bu kökün bulunması $F_3(x)$ ve $F_3'(x)$'e Euclid algoritmasının uygulanmasıyla bu kökün rasyonel olması gerektiği gerçeğini gösterir.

Daha sonra Poincaré, Euler'in şartının sadece gerek değil aynı zamanda yeter bir şart olduğunu da göstermiştir.

Euler ömrünün son yılında tekrar Diophant analizine döndü. Metodunu mükemmelleştirdi ve (18) formundaki eğri üzerinde verilmiş iki rasyonel nokta için Diophant'ın sekant metodunu ilk kez uyguladı. Euler özellikle,

$$F_3(\alpha) = f^2\,,\; F_3(\beta) = g^2 \tag{19}$$

almış ve

$$y = f + \frac{g-f}{\beta-\alpha}(x-\alpha)$$

ya da

$$y = g + \frac{g-f}{\beta-\alpha}(x-\beta)$$

değerini kullanmıştır. Bu (α,β) ve (β,g) noktalarından geçen doğruya denklemidir ve

$$F_3(x) = \left[f + \frac{g-f}{\beta-\alpha}(x-\alpha) \right]^2$$

denklemlerinden x in yeni bir rasyonel değeri elde edilir. Bunu yapmak için sadece (19)'daki eşitlikleri unutmamak gerekir.

Bu ifadelerin yer aldığı makaleler Euler'in ölümünden sonra 1830 yılında yayınlandı. Euler başka problemler ile ilgili makaleler de yazmıştır. Başlangıçta Diophant'ın problemleriyle bağlantısız ancak bu tür problemlerin yapısına yeni bir bakış açısı kazandıracak olanlar ile ilgilenmiştir. Eliptik integrallerin toplamı ile ilgili olan bu teorem Euler'in bulduğu en önemli teoremlerden biridir.

$$y^2 = ax^3 + bx^2 + cx + d$$

Γ olarak adlandırılan bir eğri ve $A(x, y)$, Γ üzerinde bir nokta olsun.

$$\Pi(A) = \int_{\infty}^{x} \frac{dx}{y}$$

olarak verilsin.

Euler'in ilk teoremi Γ üzerindeki herhangi $A(x, y)$ ve $B(x_1, y_1)$ noktaları için

$$\Pi(A) + \Pi(B) = \Pi(C) \tag{20}$$

şartını sağlayacak şekilde Γ üzerinde bir $C(x_2, y_2)$ noktasının olduğunu iddia etmektedir. Öyleki C nin koordinatları A ve B nin koordinatlarının rasyonel bir ifadesidir (yani bu noktaların rasyonel katsayılı bir fonksiyonu olarak ifade edilir).

Euler'in ikinci teoremi; A ve D, Γ üzerindeki noktalar ve n sayısı

$$\Pi(D) = n.\Pi(A) \tag{21}$$

olacak şekilde bir tamsayı ise bu taktirde D nin koordinatları A nın koordinatlarıyla rasyonel olarak ifade edilebilir. Özellikle $n = 2$ için

$$\Pi(D) = 2.\Pi(A)$$

elde edilir. (21) bağıntısı zaman zaman eliptik integrallerin çarpımı üzerindeki teorem olarak adlandırılır.

A ve B rasyonel noktalar ise C ve D de rasyoneldir. Bunun anlamı; Euluer'in teoremine göre Γ üzerinde bir ya da iki rasyonel nokta mevcut ise Γ üzerinde yeni bir rasyonel nokta elde edilebilir.

Euler'in toplam teoremi ve Diophant'ın analizi arasındaki ilişkiye ilk dikkat çeken ünlü alman matematikçisi Carl Gustav Jacob Jacobi'dir. Jacobi bu konuda "On the Use of Elliptic and Abelian Integrals in Diophantine Analysis" adında bir makale

yazmış ve bunu 19. yüzyılın en önemli matematik dergisi olan Crelle's Journal da 1834 yılında yayınlamıştır. Jacobi'nin çağdaşları makaleyi çok derin ve ilginç içeriğine rağmen çok önemsememişlerdir.

Jacobi makalesinin başlangıcında Euler ile ilgili olarak "Learned man" (bilgili adam) anlamına gelen kinayeli bir ifade kullanmıştır. Jacobi konu hakkındaki görüş ve düşüncelerini açık olarak ortaya koymuştur. Jacobi toplam (ekleme) teoremini formülüze etti ve Γ eğrisi üzerinde sonlu tane $A_1,...,A_s$ rasyonel noktaları verildiğinde $m_1,...,m_s$ herhangi tamsayılar iken

$$\Pi(A) = m_1\Pi(A_1) + ... + m_s\Pi(A_s)$$

bağıntısından faydalanarak Γ üzerinde yeni sonsuz çoklukta rasyonel nokta elde edilebileceğine dikkat çekmiştir. Benzer şekilde bir tek rasyonel noktayla başlayarak ve $\Pi(D) = 2.\Pi(A)$ bağıntısı kullanılarak rasyonel noktaların bir sonsuz dizisi elde edilmiştir. Bununla birlikte eğer $\pm 2, \pm 3, ..., n$ değerleri belirlenirse yeni noktalar elde etmeye ihtiyaç duyulur. Bu işlem sırasında bazı n değerleri için

$$n\Pi(A) = \Pi(A)$$

oluşturulabilir. Yani sonlu sayıdaki adımdan sonra başlangıçtaki noktaya dönülebilir. Jacobi bu olasılığın farkına varmış ve sınır şartlarını bulmuştur. Burada

$$n\Pi(A) = \Pi(A)$$

olacak şekilde bir n sayısının var olma şartını sağlayan noktalara "*sonlu mertebeli noktalar"* denilir.

Jacobi makalesinin sonunda bu sonuçların daha yüksek dereceli cebirsel eğriler için Euler'in toplam teoreminin Abel'in daha genel teoremleriyle yer değiştirmesi yoluyla genişletileceğini ifade etmiştir. Bu makalenin temel içeriğine bakılacak olunursa Jacobi'nin burada bir eliptik eğri üzerindeki rasyonel noktalar kümesinin yapısını bütünüyle keşfetmeye yaklaştığı görülebilir. Bu keşfi yapma aşamasında yüksek seviyede bilgiye sahip olduğundan yeni teknik bilgilere ihtiyaç duymamış sadece farklı bir bakış açısı geliştirmiştir. Bunu açıklamak için önce Γ eğrisi üzerindeki rasyonel noktaların *M* kümesini ele alalım. Eğer A ve B, *M* kümesinde iki nokta ise bu taktirde Euler teoremi gereğince *M'*de

$$\Pi(A) + \Pi(B) = \Pi(C)$$

olacak şekilde bir C noktası vardır. C noktası A ve B'nin toplamı olarak kabul edilir ve

$$A \oplus B = C$$

olarak yazılır. + yerine $\oplus$ işaretinin kullanılmasının sebebi sayıların toplamından daha farklı bir kavramdan bahsedilmesidir. Böylece M kümesi üzerinde bir ikili işlem tanımlanmış olur. Yani M kümesindeki herhangi iki A ve B elemanları ile yine M kümesindeki üçüncü bir C elemanı arasındaki bağlantıyı kurmanın kuralı tanımlanmış olur.

Modern matematikte boştan farklı bir S kümesi ile $\oplus$ toplam kuralının aşağıdaki şartları sağlaması durumunda grup yapısı elde edilir.

1) S**'**deki herhangi A, B ve C elemanları için;

$$(A \oplus B) \oplus C = A \oplus (B \oplus C)$$

2) S**,** her $A \in S$ için

$$A \oplus N = A$$

olacak şekildeki bir N etkisiz elemanı vardır.

3) S'deki her A elemanı için

$$A \oplus A' = N$$

olacak şekilde S'de bir A' elemanı vardır.

Eğer bunlara ek olarak S deki herhangi iki A ve B elemanları için

$$A \oplus B = B \oplus A$$

ise bu taktirde grup değişmeli ya da abelian diye adlandırılır. Dolayısıyla tamsayılar kümesi toplama işlemine göre pozitif rasyonel sayılar kümesi çarpma işlemi altında birer abelian gruptur. Determinantı sıfırdan farklı $2x2$ tipindeki matrislerin kümesi de çarpma işlemine göre değişmeli olmayan bir gruptur ve son örnekteki birim matris etkisiz eleman görevini üstlenmiştir.

Yapılan işlemin sayılardaki işlemlere benzerliğinden grup operasyonlarını sıklıkla toplam ya da çarpma işlemleri olarak adlandırılabilir. Böyle bir başlangıçtan sonra toplamsal ve çarpımsal terslerden bahsetmek doğaldır. Toplam terimi genellikle değişmeli gruplarla bağlantılı olarak konuşulur. Bu tür gruplarda bazen birim elemana sıfır elemanı da denilir.

M kümesinin $\oplus$ işlemiyle birlikte bir grup oluşturduğunu söyleyebilmek için aşağıdaki yol izlenir.

İşlemimizin birleşme özelliğini sağladığı, integraller üzerinde toplama işleminin birleşmeliliğinden;

$$[\Pi(A)+\Pi(B)]+\Pi(C)=\Pi(A)+[\Pi(B)+\Pi(C)]$$

olarak gösterilir. Geriye M kümesinin sıfır elemanının görevini üstlenen bir eleman bulundurduğunu ve M deki her bir elemanın toplamsal tersinin olduğunu göstermek kalır.

İlk olarak sıfır elemanını bulalım. Γ eğrisi üzerindeki rasyonel noktaların kümesi M ise yani M nin elemanları koordinatları sonlu rasyonel sayılar olan noktalar ise M nin hiç sıfır noktası yoktur. M üzerindeki noktaların toplamını konuşmak için sıfır elemanının rolünü üstlenecek ekstra bir θ noktasını M'ye ilave etmeliyiz. Böylece bu θ elemanı için

$$\Pi(\theta)=0$$

olmalıdır. Her bir A elemanı için toplamsal tersin bulunmasına dönüldüğünde eğer

$$\Pi(A)+\Pi(A')=0$$

ise $A\oplus A'=\theta$ olduğu kolaylıkla söylenebilir. Ancak bu durumda A' için x eksenine göre A'ya simetrik bir nokta alınmalıdır. Gerçektende A'nın koordinatları (x,y) ise A''nün koordinatları $(x,-y)$ dir. Bununla birlikte

$$\begin{aligned}\Pi(A') &= \int_{\infty}^{x}\frac{dx}{-y}\\ &= -\int_{\infty}^{x}\frac{dx}{y}\\ &= -\Pi(A)\end{aligned}$$

dır. Dikkat edildiğinde

$$\Pi(A)+\Pi(B)=\Pi(B)+\Pi(A)$$

yani $A\oplus B=B\oplus A$'dır. Bu ise grubun abelian olduğu anlamına gelir. Böylece Euler teoremiyle başlayıp Jacobi tarafından verilen bağlantı kullanılarak bir eliptik eğri üzerindeki rasyonel noktaların kümesini oluşturmak mümkündür. Bu küme eklenilen sonsuzdaki nokta ile birlikte bir değişmeli grup yapısına sahip olur. Jacobi tarafından

bahsedilen sonlu mertebeli noktalar sonlu mertebeli grup elemanlarına dönüşür. Bu Jacobi'nin gözlemlerinin modern bir ifadesidir.

19. yüzyılın ilk yarısındaki matematikçiler aritmetik işlemleri noktalara ya da sayılardan çok farklı diğer (nesnelere) objelere genişletmeyi düşünmemiştirler. Bu nedenden dolayı Jacobi, toplama işlemini A ve B noktaları için değil, $\Pi(A)$ ve $\Pi(B)$ integralleri için vermiştir.

0.5. Noktaları Toplama İşleminin Geometrik Anlamı

Euler'in toplama teoremi ile Diophant'ın teğet ve sekant metodları arasında bir bağlantı var mıdır? Her iki durumda da bir Γ eğrisi üzerindeki bir ya da iki rasyonel noktayla başlanır ve Γ üzerinde yeni bir rasyonel nokta elde edilir ne Euler ne de Jacobi yaşadıkları sürece böyle bir bağıntının ispatını ortaya koyamadılar.

Ele alınan soru biraz daha özelleştirilirse Euler'in teoreminden dolayı Γ eğrisi üzerinde A ve B gibi iki nokta verildiğinde

$$\Pi(C) = \Pi(A) + \Pi(B)$$

olacak şekilde bir C noktası bulunabilir. Diğer taraftan A ve B den geçen ve Γ eğrisi ile C' noktasında kesişen bir doğru çizilirse C ve C' noktaları arasındaki bağıntının olup olmadığı ile ilgili sorunun cevabı evet olacaktır. Bu bağlantı oldukça kolay birşekilde ifade edilebilir. Öyleki bu iki nokta x-eksenine göre birbirlerine simetriktirler. Yani C nin koordinatları (x_2, y_2) ise C' noktasının koordinatları $(x_2, -y_2)$ dir.

Şimdi bir eğri üzerindeki noktaların toplama işleminin geometrik anlamı açıkça; Γ üzerindeki A ve B noktalarının toplamı olan Γ eğrisi üzerindeki C noktası AB doğrusu ile Γ eğrisinin kesiştikleri noktanın x-eksenine göre simetriğidir.

Bu metod belirli bir A noktasının kendisi ile toplanması durumunu çözmede yetersiz kaldığı için $2A$ noktasını bulmak için bu metod kullanılamaz. Bu problemi aşmak için aşağıdaki yöntem kullanılabilir.

Diophant'ın ilk metodunu kullanarak A dan geçen ve bu A noktasında Γ eğrisine teğet olan bir doğru çizilir. Bu doğrunun Γ ile kesiştiği bir nokta olan D' noktası bulunur. D' noktası Euler'in

$$\Pi(D) = 2\Pi(A)$$

metoduyla elde edilen D noktasına simetriktir. Bu ise $2A$ noktasının ve daha genel olarak ta her n doğal sayısı için nA noktasının hesaplanabilir olduğunu gösterir.

Toplama işlemi bu şekilde tanımlandığında hangi nokta sıfır elemanının görevini üstlenecektir? Bu soruyu cevaplamak için homojen koordinatlar kullanılır. Eğer

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

alınırsa (18) denklemi

$$v^2 z = u^3 + auz^2 + bz^3 \tag{22}$$

haline gelir. (22) denkleminde $z = 0$ ise bu taktirde $u = 0$ dır ve v'nin keyfi olduğunu gösterir. Homojen koordinatlar çarpımsal bir sabit farkıyla tanımlandığından $v = 1$ alınır.

Eğri üzerindeki sonsuzdaki noktanın $(0,1,0)$ üçlüsüne karşılık geldiği, θ ile bu noktanın tanımlandığı ve θ' noktasının x -eksenine göre θ noktasının simetriği olduğu kabul edilir.

θ noktasının sıfır elemanının görevini üstlendiğini gösterelim. Her dikey $u = cz$ doğrusu θ noktasında kesişir. Gerçekten de $z = 0$ için $u = 0$ olur ve yine v, 1 e eşit olarak alınabilir.

A, Γ eğrisi üzerinde koordinatları (x_0, y_0) olan bir rasyonel nokta olsun. Bir önceki paragrafta ispatlandığı şekilde A dan ve θ dan geçen doğru düşey bir doğrudur. Yani denklemi

$$x = x_0$$

dır. Bu doğru Γ eğrisi ile A, θ ve A'nın x-eksenine göre simetriği olan $A'(x_0, -y_0)$ şeklindeki üç noktada kesişir. Verilen tanıma göre A ve θ' noktalarının toplamı A' ye simetriktir. Yani A'nın kendisidir. Bu ise

$$A \oplus \theta = A$$

anlamına gelir.

Sonuçta A noktasının toplamaya göre tersi $A'(x_0, -y_0)$ noktasıdır. A ve A' noktalarını birleştiren doğrunun dikey olduğunu ve böylece bu doğrunun Γ eğrisi ile θ noktasının kesiştiğini görmek mümkündür. Tanımdan A ve A' noktalarının toplamının θ'ya simetrik olan noktadır ki bu nokta kabulden dolayı θ ile çakışıktır. Böylece

$$A \oplus A' = \theta$$

dır. θ noktası için

$$\Pi(\theta) = \int_{\infty}^{\infty} \frac{dx}{y} = 0$$

olduğu bilinmektedir.

Böylece Euler'in toplam teoremi, sonsuzdaki noktanın sıfır elemanı görevini görmektedir.

Bir eliptik eğri üzerindeki noktaların toplamı Diophant'ın tanımladığı işlemlere dayandırılabilir. Daha özel olarak Γ eğrisi üzerinde

$$\Pi(A) \oplus \Pi(B) \oplus \Pi(C) = 0$$

tümü doğrusal olan üç nokta bulunduğundan ne Euler ne de Jacobi bahsetmemiştir. Euler bunu biliyor olabilirdi, ama Jacobi kesinlikle çok iyi biliyor olmalıydı. Başka bir deyişle kübik eğriler hakkında kesin bilgileri bilinmemekle birlikte her ikisinin de

$$y^2 = ax^4 + bx^3 + cx^2 + dx + e$$

gibi bir eğri için toplam teoremini tanımlamıştırlar. Ayrıca rasyonel noktalı

$$y^2 = ax^4 + bx^3 + cx^2 + dx + e$$

eğrileri için bu topam teoremi çok basit değildir ve geometrik anlamda tek türlü tanımlanmaz. Dahası ne Euler ne de Jacobi analitik ifadelerin geometrik açıklamasını yapamamıştır.

Bir eliptik eğri üzerindeki noktaların "toplamı" kavramının altında yatan mantık basit olmakla birlikte bu mantığın rasyonel noktaların kümesinin yapısının çalışılması için temel olmaya başlaması 70 yıl civarında sürmüştür. Bu kavram 1900'lü yılların başlarında Henri Poincaré tarafından ortaya atılmıştır.

1. ÖN BİLGİLER

Bu bölümde çalışmamızda kullanacağımız bazı temel kavramları tanımlayacağız ve bazı temel sonuçları vereceğiz. Bu sonuçların ispatları sayılar teorisi ile ilgili literatürde bulunabilir.

1.1 Diophant Denklemleri

1.1.1. Tanım. x ve y herhangi iki tamsayı olsun. x ve y'yi değişken kabul eden ve çözümleri de (x_0, y_0) sıralı tamsayı ikilileri olan tamsayı katsayılı denklemlere Diophant denklemleri denir. Yani katsayıları ve çözümleri tamsayılar olan denklemlere Diophant denklemleri denilmektedir.

Bu denklemlerin en bilinen hali a, b ve c tamsayılar olmak üzere $ax+by=c$ şeklindedir. Bu formdaki denklemlere lineer Diophant denklemleri adı verilir. Daha yüksek dereceli Diophant denklemleri de mevcuttur. Bunlara örnek olarak aşağıda tanımlanacak olan eliptik eğriler verilebilir. Bu tezin de konusu aynı zamanda bazı özel eliptik eğriler olan Diophant denklemlerini incelemektir.

1.1.2. Tanım. F karakteristiği 2 ve 3'ten farklı bir cisim olsun. $A, B \in F$ iken $4A^3 + 27B^2 \neq 0$ olmak üzere

$$y^2 = x^3 + Ax + B \in F[x]$$

ifadesi F cismi üzerinde bir eliptik eğri belirtir. Böyle bir eliptik eğriyi E ile göstereceğiz.

Bu denklemin sonsuzdaki noktayla birlikte tüm $(x, y) \in FxF$ çözümlerinin kümesi $E(F)$ ile tanımlanır ve E üzerindeki F-rasyonel noktalarının kümesi olarak adlandırılır.

1.1.3. Tanım. $\Delta(E) = -16\left(4A^3 + 27B^2\right)$ değeri E eliptik eğrisinin diskriminantı ve $j = -1728(4A)^3 / \Delta$ değeri j invaryantı olarak adlandırılır.

1.1.4. Tanım. $\bar{a} \in \mathbb{Z}_n^* = \mathbb{Z}_n - \{0\}$'ın çarpmaya göre tersi, $\overline{ab} = \overline{ba} = \bar{1}$ olacak şekilde bir $\bar{b} \in \mathbb{Z}_n^*$ elemanıdır. $\mathbb{Z}_n^*$ kümesinde çarpmaya göre tersi olan bir elemana "*birim (unit)*" denir ve $\mathbb{Z}_n^*$'daki birimlerin kümesi U_n ile gösterilir.

1.1.5. Yardımcı Teorem. $\bar{a} \in \mathbb{Z}_n^*$ elemanının bir birim olması için gerek ve yeter şart $(a, n) = 1$ olmasıdır.

Dolayısıyla bir cisimde 0 dışındaki tüm elemanlar birer birimdir.

1.1.6. Tanım. $\bar{g} \in \mathbb{Z}_n$ olsun. $\bar{g}$, U_n'i üretiyorsa g'ye n modunda bir "*ilkel kök*" denir. Bu durumda g'nin 0 ile $n-1$ arasındaki tüm kuvvetleri farklıdır ve bunlar U_n'deki tüm elemanları verir.

1.1.7. Örnek. 5 modunda $\bar{2}$ ve $\bar{3}$ ilkel köklerdir. Çünkü $U_5 = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ ve $\bar{1}^2 = \bar{1},\ \bar{2}^1 = \bar{2},\ \bar{2}^2 = \bar{4},\ \bar{2}^3 = \bar{3},\ \bar{2}^4 = \bar{1},\ \bar{3}^1 = \bar{3},\ \bar{3}^2 = \bar{4},\ \bar{3}^3 = \bar{2},\ \bar{3}^4 = \bar{1},\ \bar{4}^1 = \bar{4},\ \bar{4}^2 = \bar{1}$'dir.

1.1.8. Tanım. Bir $\bar{a} \in U_n$ verilsin. Eğer $\bar{a} = \bar{s}^2$ olacak şekilde bir $\bar{s} \in U_n$ varsa a'ya n modunda bir "*ikinci dereceden kalan*" denir ve bu şekildeki ikinci derece kalanların kümesi Q_n ile gösterilir.

1.1.9. Örnek. Küçük n'ler için U_n'deki tüm sayıların kareleri alınarak Q_n belirlenebilir. Örneğin $n = 7$ için $\bar{1}^2 \equiv \bar{1},\ \bar{2}^2 \equiv \bar{4},\ \bar{3}^2 \equiv \bar{2},\ \bar{4}^2 \equiv \bar{2},\ \bar{5}^2 \equiv \bar{4},\ \bar{6}^2 \equiv \bar{1} \pmod 7$ olduğundan $Q_7 = \{1, 2, 4\}$'tür.

1.1.10. Yardımcı Teorem. Q_n, U_n'in bir alt grubudur.

Verilen bir $\bar{a} \in U_n$ biriminin bir ikinci dereceden kalan olup olmadığını belirlemek için aşağıdaki tanımı vermek gerekir. n modunda asal olması durumunda

işlem kolaydır. $n=2$ ise $Q_2=\{\bar{1}\}$'dir ve $\bar{1}$ ikinci dereceden bir kalandır. O halde $n=p$'nin tek asal olması durumuyla başlayalım.

1.1.11. Tanım (Legendre Sembolü). p tek asal sayısı için bir a tam sayısının "*Legendre sembolü*"

$$(\frac{a}{p})=\begin{cases}0 & , \quad p\mid a \ ise\\ 1 & , \quad a\in Q_p \ ise\\ -1 & , \quad a\notin Q_p \ ise\end{cases}$$

şeklindedir. Literatürde $(\frac{a}{p})$ yerine bazen $\chi(a)$ da kullanılır.

1.1.12. Örnek. $p=7$ ise

$$(\frac{a}{7})=\begin{cases}0 & , \quad a\equiv 0\,(\text{mod } 7) ise\\ 1 & , \quad a\equiv 1,2 \ veya \ 4\ (\text{mod } 7)\ ise\\ -1 & , \quad a\equiv 3,5 \ veya \ 6\ (\text{mod } 7)\ ise\end{cases}$$

dir.

1.1.13. Tanım. p bir asal iken $x^3\equiv a\ (\text{mod } p)$ olacak şekilde bir $x\in\mathbb{Z}$ varsa $a\in\mathbb{Z}$'ye p modunda bir "*üçüncü dereceden kalan*" denir.

p modunda üçüncü dereceden kalanların kümesi K_p ile, K_p'nin $\mathbb{Z}_p^{\ *}=\mathbb{Z}_p-\{\bar{0}\}$'daki elemanlarının oluşturduğu küme $K_p^{\ *}$ ile gösterilir.

1.1.14. Teorem. $K_p^{\ *}$, $\mathbb{Z}_p$'deki çarpma işlemine göre bir gruptur ve aslında $\mathbb{Z}_p^{\ *}$'ın bir alt grubudur (Namlı 2001).

1.1.15. Teorem. $p\equiv 1(\text{mod } 3)$ bir asal olsun. ω birimin 1'den farklı olan kübik kökü olmak üzere $\omega=\frac{-1+\sqrt{-3}}{2}$ sayısı $\mathbb{Z}_p^{\ *}$'ın bir elemanıdır (Namlı 2001).

1.1.16. Sonuç. $p\equiv 1(\text{mod } 3)$ bir asal iken ω^2 elemanı da $\mathbb{Z}_p^{\ *}$'ın bir elemanıdır (Namlı 2001).

1.1.17. Tanım (Üçüncü Dereceden Kalan Karakteri). Bir p tek asal sayısı için bir "*a tam sayısının p modundaki kübik karakteri*" $\left(\frac{a}{p}\right)_3$ ile gösterilir ve

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

şeklinde tanımlanır. Bu karakter üçüncü dereceden kalanlar teorisinde, Legendre sembolünün ikinci dereceden kalan görevini yapar. Literatürde bazen $\left(\frac{a}{p}\right)_3$ yerine $\chi_3(a)$ gösterimi de kullanılır.

1.1.18. Teorem. p asal ve $p \equiv 1 \pmod 3$ olsun. $x^3 \equiv a \pmod p$ denkliğinin çözülebilmesi için gerek ve yeter şart $a^{\frac{p-1}{3}} \equiv 1 \pmod p$ olmasıdır (Namlı 2001).

1.1.19. Örnek. $\left(\frac{9}{7}\right)_3 = \left(\frac{2}{7}\right)_3 = 2^{\frac{7-1}{3}} = 2^2 = 4 \pmod 7$ $\omega \equiv 4 \pmod 7$ olduğundan $\left(\frac{9}{7}\right)_3 = \omega$'dır ve bu nedenle 9, 7 modunda üçüncü dereceden bir kalan değildir.

1.1.20. Örnek. $\left(\frac{15}{7}\right)_3 \equiv \left(\frac{1}{7}\right)_3 = 1^{\frac{7-1}{3}} = 1^2 \equiv 1 \pmod 7$ olup dolayısıyla 15, 7 modunda üçüncü dereceden bir kalandır. Yani $x^3 \equiv 15 \pmod 7$ denkliği çözülebilirdir. Gerçekten, $x^3 \equiv 15 \equiv 1 \pmod 7$, $x = 1$, $x = \omega$ ve $x = \omega^2$ bu denkliğin kökleridir. $\omega = \frac{-1+\sqrt{-3}}{2} \equiv 4 \pmod 7$ ve $\omega^2 \equiv 2 \pmod 7$ olduğundan bu denkliğin kökleri $x \equiv 1 \pmod 7$, $x \equiv 4 \pmod 7$ ve $x \equiv 2 \pmod 7$ şeklindedir.

1.1.21. Sonuç. $p \equiv 2 \pmod 3$ asal ise p modunda birbirinden farklı tam p tane üçüncü dereceden kalan vardır. Yani $\mathbb{Z}_p$'nin tüm elemanları üçüncü dereceden birer kalandır.

1.1.22. Örnek. $p=11$ olsun. $0^3\equiv 0,\ 1^3\equiv 1,\ 2\equiv 7^3,\ 3\equiv 9^3,\ 4\equiv 5^3 \pmod{11}$ ve $5\equiv 3^3,\ 6\equiv 8^3,\ 7\equiv 6^3,\ 8\equiv 2^3,\ 9\equiv 4^3,\ 10\equiv 10^3 \pmod{11}$'dir ve $\mathbb{Z}_{11}$'deki tüm sayılar üçüncü dereceden kalanlardır.

1.2. Eliptik Eğrilere Karşılık Gelen Diophant Denklemleri

1.2.1. Tanım. $a_1,a_2,a_3,a_4,a_6\in\mathbb{F}$ iken

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6 \tag{23}$$

şeklindeki bir denklem "*uzun Weierstrass normal formu"* olarak adlandırılır. Burada sonsuzdaki nokta olarak adlandırılan "θ" noktası vardır. Bu noktanın afin temsili $\theta=(\infty,\infty)$'dur.

1.2.2. Örnek. Weierstrass formundaki eğrilerin denklemlerinin bazı örnekleri aşağıda verilmiştir:

$$C_1: y^2=x^3$$
$$C_2: y^2=x^3+x^2$$
$$C_3: y^2=x^3+x$$

Üç eğrinin de iki tane $\mathbb{F}$-rasyonel noktası vardır: $P=(0,0)$ ve θ (Schmitt ve Zimmer 2003).

1.2.3. Tanım. $a_1,a_2,a_3,a_4,a_6\in\mathbb{F}$ katsayıları ile uzun Weierstrass normal formundaki bir denklemi ele alalım. Bu denklem için "*Tate değerleri"*

$$b_2=a_1^2+4a_2,$$
$$b_4=2a_4+a_1.a_3,$$
$$b_6=a_3^2+4a_6$$
$$b_8=a_1^2a_6+4a_2a_6-a_1a_3a_4+a_2a_3^2-a_4^2,$$
$$c_4=b_2^2-24b_4,$$
$$c_6=-b_2^3+36b_2b_4-216b_6.$$

şeklindedir. Ayrıca, "*diskriminant"*

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

ve "*j değişmezi"*

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

şeklindedir. Bu sabitler aşağıdaki bağıntıları sağlar:

$$4b_8 = b_2 b_6 - b_4^{\,2} \text{ ve } 12^3 \Delta = c_4^{\,3} - c_6^{\,2}$$

1.2.4. Tanım. C düzlemsel cebirsel eğrisi $f(x,y)=0$ polinom denklemiyle tanımlansın. Bu durumda $P=(x_0,y_0)\in C$ noktasının C eğrisinin bir *"singüler noktası"* olması için gerek ve yeter şart

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

olmasıdır. Eğer sadece birinci kısmi türevler sıfıra eşitleniyorsa singüler nokta katlı bir noktadır. Katlı noktanın iki farklı teğeti varsa *"düğüm (node)"*, iki teğeti çakışırsa *"çıkıntı (cusp)"* olarak adlandırılır. Singüler noktaları olmayan bir eğri *"singüler olmayan eğri"* olarak adlandırılır.

1.2.5. Önerme. Uzun Weierstrass normal formunda bir denklem yardımı ile verilen eğrileri aşağıdaki gibi sınıflandırabiliriz:

a) Eğri singüler değildir $\Leftrightarrow$ $\Delta \neq 0$. Diğer durumda eğri tek singüler noktayla singülerdir.

b) Eğrinin bir *düğümü* vardır $\Leftrightarrow$ $\Delta = 0$ ve $c_4 \neq 0$'dır.

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

1.2.2. Örnekte incelediğimiz C_1, C_2, C_3 eğrilerinin diskriminantları:

$$\Delta C_1 = 0,\ \Delta C_2 = 0,\ \Delta C_3 = -64$$

tür. Ayrıca

$$C_{1C_4} = 0,\ C_{2C_4} = 0,\ C_{3C_4} = -48$$

dir. Ayrıca $Kar(\mathbb{F}) = 2$ ise bu eğrilerin üçü de singülerdir ve birer çıkıntıları vardır. Eğer $Kar(\mathbb{F}) \neq 2$ ise C_1 eğrisinin bir çıkıntısı , C_2 eğrisinin bir düğümü vardır ve C_3 eğrisi singüler değildir. Tüm singüler durumlarda singüler nokta $P=(0,0)$'dır. Bunu kısmi türevlerine bakarak görebiliriz. Örnek olarak C_1 eğrisini ele alalım:

$$C_1 = f(x,y) = y^2 - x^3 = 0$$

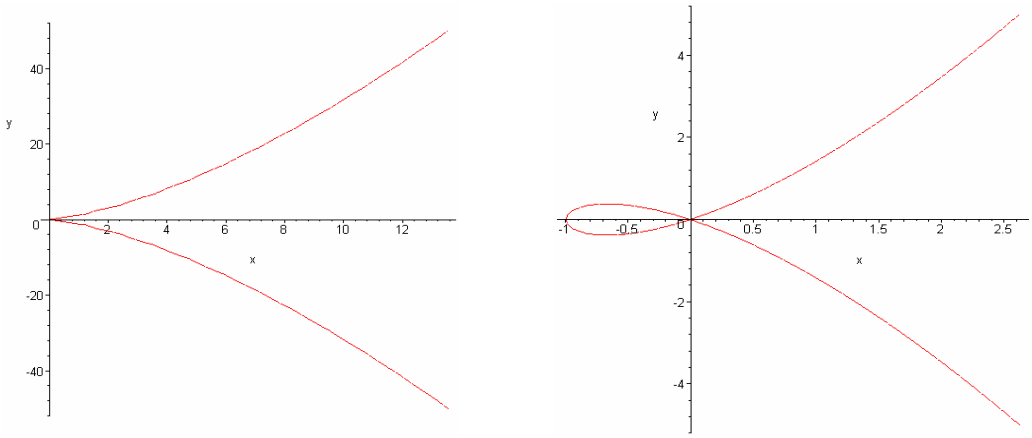
eğrisinin kısmi türevleri

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

dir. Buradan

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

denklemleri elde edilir. Karakteristik ne olursa olsun bu üç denklemin bir tek çözümü vardır. Bu da $x = y = 0$'dır (Schmitt ve Zimmer 2003).



$y^2 = x^3$ (Çıkıntı) $y^2 = x^3 + x^2$ (Düğüm)

Şekil 1.2.1

1.2.6. Tanım. Katsayıları $\mathbb{F}$ cisminden alınan, diskriminantı sıfırdan farklı uzun Weierstrass normal formundaki bir eğri sonsuzdaki nokta denilen özel bir nokta ile birlikte $\mathbb{F}$ üzerinde bir "*eliptik eğri*" olarak adlandırılır.

1.2.7. Tanım. E ve E' eliptik eğrileri

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

ve

$$E' : (y')^2 + a_1'x'y' + a_3'y' = (x')^3 + a_2'(x')^2 + a_4'x' + a_6' \quad ,$$

şeklinde verilsin. Bu eğriler arasındaki (ikisi de $\mathbb{F}$ cismi üzerinde tanımlı) değişken dönüşümlerine dikkat edersek, bir Weierstrass normal formunu diğerine resmeden dönüşümler bulmak isteriz. Tek değişken dönüşümü vardır. O da aşağıdaki formda olur:

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

Ters dönüşümü de

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

şeklindedir. Böyle dönüşümlere "*kendisi ve tersi rasyonel dönüşümler"* denilmektedir. Bu durumda

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

Weierstrass normal formundaki bu iki denklem arasında kendisi ve tersi rasyonel dönüşümler varsa bu iki denkleme "*izomorfturlar"* denilir.

1.2.8. Önerme. $E \setminus \mathbb{F}$ uzun Weierstrass normal formunda bir eğri olsun. O halde aşağıdaki varsayımlar altında $E \setminus \mathbb{F}$'nin belirtilen formda bir Weierstrass denklemine sahip olacak şekilde bir

$$x = u^2x' + r,\ \ y = u^3y' + u^2sx' + t \qquad (u \in \mathbb{F}^* \text{ ve } r,s,t \in \mathbb{F})$$

dönüşümü vardır.

a) Eğer $Kar(\mathbb{F}) \neq 2,3$ ise

$$y^2 = x^3 + a_4x + a_6 \tag{24}$$

$$\Delta = -16(4a_4^{\,3} + 27a_6^{\,2}),\ \ j = 1728\frac{4a_4^{\,3}}{4a_4^{\,3} + 27a_6^{\,2}}$$

olur.

b) Eğer $Kar(\mathbb{F}) = 3$ ve $j(E) \neq 0$ ise

$$y^2 = x^3 + a_2x^2 + a_6,$$

$$\Delta = -a_2{}^3 a_6,\ j = \frac{-a_2{}^3}{a_6}$$

olur.

Eğer $Kar(\mathbb{F}) = 3$ ve $j(E) = 0$ ise

$$y^2 = x^3 + a_4x + a_6,$$

$$\Delta = -a_4{}^3,\ j = 0$$

olur.

c) Eğer $Kar(\mathbb{F}) = 2$ ve $j(E) \neq 0$ ise

$$y^2 + xy = x^3 + a_2x^2 + a_6\ ,$$

$$\Delta = a_6,\ j = \frac{1}{a_6}$$

olur.

Eğer $Kar(\mathbb{F}) = 2$ ve $j(E) = 0$ ise

$$y^2 + a_3y = x^3 + a_4x + a_6\ ,$$

$$\Delta = a_3{}^4,\ j = 0$$

olur.

İspat. a) Eğer $Kar(\mathbb{F}) \neq 2$ ise (1) tipindeki Weierstrass denklemini kareye tamamlayarak basitleştirebiliriz. Denklemde $y + \frac{1}{2}(a_1x + a_3)$ yerine $\frac{1}{2}y$ yazarsak sonuç

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6 \tag{25}$$

olur.

Eğer $Kar(\mathbb{F}) \neq 2,3$ ise (25) denkleminde (x, y) yerine $\left(\frac{x - 3b_2}{36}, \frac{y}{108}\right)$ yazarsak sonuç

$$y^2 = x^3 - 27c_4x - 54c_6 \tag{26}$$

olur. Buradan $-27c_4 = A$ ve $-54c_6 = B$ konularak $E' : y^2 = x^3 + Ax + B$ gösterimi elde edilir.

b) (23) tipindeki bir Weierstrass denklemini alalım ve denklemin sol tarafını kareye tamamlayalım. Bu bize $\Delta = a_2{}^2 a_4{}^2 - a_2{}^3 a_6 - a_4{}^3$ ve $j = \dfrac{a_2{}^6}{\Delta}$ değişmezlerine sahip olan bir

$$y^2 = x^3 + a_2 x^2 + a_4 x + a_6$$

denklemini verir (Karakteristiğin 3 olduğunu unutmayalım). Eğer $j = 0$ ise, $a_2 = 0$'dır. Böylece istenilen denklem elde edilir. Diğer taraftan $j \neq 0$ ise $a_2 \neq 0$ ve böylece $x = x' + \dfrac{a_4}{a_2}$ ifadesi denklemde yerine konursa istenilen denklem elde edilir.

c) Tekrar (23) tipindeki Weierstrass denklemini alarak ispata başlayalım. Karakteristik 2 iken

$$j = \frac{a_1{}^{12}}{\Delta}$$

olduğu kolaylıkla hesaplanabilir. Eğer $j \neq 0$ ise $a_1 \neq 0$'dır. Bu durumda

$$x = a_1{}^2 x' + \frac{a_3}{a_1}\ ,\ y = a_1{}^3 y' + (a_1{}^2 a_4 + a_3{}^2)/a_1{}^3$$

ifadeleri denklemde yerine konursa istenilen denklemi elde ederiz. Benzer olarak $j = a_1 = 0$ olursa

$$x = x' + a_2\,,\ y = y'$$

ifadeleri denklemde yerine konursa istenilen denklem elde edilir.□

1.2.9. Teorem. $E \setminus \mathbb{F}$ bir eliptik eğri $(Kar(\mathbb{F}) \neq 2,3)$ olsun. Bu durumda

$$E' : y^2 = x^3 + Ax + B \qquad (A, B \in \mathbb{F}) \tag{27}$$

formunda $E' \setminus \mathbb{F}$ eğrisi için $\phi : E \to E'$ birasyonel dönüşümü vardır. O halde bu E' eğrisi**,** "*basitleştirilmiş Weierstrass normal formunda eğri"* olarak adlandırılır (Schmitt ve Zimmer 2003).

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

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

halini alacaktır.

$E : y^2 = x^3 + Ax + B$ eğrisinin tüm $(x, y) \in \mathbb{F}$ rasyonel çözümlerinin kümesi (sonsuzdaki o noktası ile birlikte) $E(\mathbb{F})$ ile gösterilir ve E üzerindeki *"$\mathbb{F}$-rasyonel noktalarının kümesi"* olarak adlandırılır.

Sadece kendisi ve tersi rasyonel dönüşümler basitleştirilmiş Weierstrass normal formunu

$$x = u^2 x', \; y = u^3 y'$$

dönüşümleri altında değişmez bırakır. Bu durumda

$$A = u^4 A', \quad B = u^6 B', \; u^{12}\Delta' = \Delta$$

dönüşümlerini elde ederiz.

1.2.10. Önerme. Weierstrass normal formundaki iki eliptik eğrinin $\overline{\mathbb{F}}$ üzerinde $(Kar(\mathbb{F}) \neq 2,3)$ izomorf olmaları için gerek ve yeter şart j-değişmezlerinin aynı olmasıdır.

İspat. Basitleştirilmiş Weierstrass normal formundaki eğrileri

$$E : y^2 = x^3 + Ax + B, \; E' : (y')^2 = (x')^3 + A'x' + B'$$

şeklinde ifade etmiştik. E'yi E''ne dönüştürecek

$$x = u^2 x', \; y = u^3 y'$$

şeklinde bir izomorfizm bulmak istiyoruz. $j = j'$ olduğundan

$$(4A)^3(4(A')^3 + 27(B')^2) = (4A')^3(4A^3 + 27B^2)$$
$$\Leftrightarrow A^3(B')^2 = (A')^3 B^2$$

Eğer $A = 0$ ise $B \neq 0$'dır. Böylece $A' = 0$ ve $B' \neq 0$'dır. Bu durumda $u = (\frac{B}{B'})^{\frac{1}{6}}$ alabiliriz. Eğer $B = 0$ ise $A \neq 0$'dır. Böylece $B' = 0$ ve $A' \neq 0$'dır. Bu durumda

$u = (\frac{A}{A'})^{\frac{1}{4}}$ alabiliriz. Eğer $AB \neq 0$ ise $A'B' \neq 0$'dır. Gerçekten $A'B' = 0$ ise $A' = 0$ ve $B' = 0$'dır. Böylece $\Delta' = 0$'dır. Bu ise bir istisnadır.

$$(A')^3 B^2 = A^3 (B')^2 \Leftrightarrow \frac{B^2}{(B')^2} = \frac{A^3}{(A')^3} \Leftrightarrow (\frac{B}{B'})^{\frac{1}{6}} = (\frac{A}{A'})^{\frac{1}{4}}$$

elde ederiz. Bu durumda

$$u = (\frac{A}{A'})^{\frac{1}{4}} = (\frac{B}{B'})^{\frac{1}{6}}$$

alabiliriz. □

1.2.11. Önerme. Her bir $j_0 \in \mathbb{F}$ değeri için j-değişmezi j_0 olan ve $\mathbb{F}$ üzerinde tanımlanabilecek bir tek eliptik eğri vardır.

Çizelge 1.2.1 (Schmitt ve Zimmer 2003)

$Kar(\mathbb{F})$	j_0	Eliptik eğri
$\neq 2,3$	0	$y^2 = x^3 + 1$
	12^3	$y^2 = x^3 + x$
	$\neq 0,12^3$	$y^2 = x^3 + 3\kappa x + 2\kappa$, $\kappa = \frac{j_0}{12 - j_0}$
2	0	$y^2 + y = x^3$
	$\neq 0$	$y^2 + xy = x^3 + x^2 + j_o^{-1}$
3	0	$y^2 = x^3 + x$
	$\neq 0$	$y^2 = x^3 + x^2 - j_0^{-1}$

1.3. Toplama Kuralı

Eliptik eğriler hakkında söylenebilecek en önemli husus şudur: Eğri üzerindeki noktalar toplamaya göre değişmeli grup oluşturur. $E \setminus \mathbb{F}$ eliptik eğrisi uzun Weierstrass normal formunda ve herhangi bir $\mathbb{F}$ cismi üzerinde olsun. E üzerindeki $\mathbb{F}$-rasyonel noktalarının kümesi $E(\mathbb{F}) = \{(x, y) \in E : x, y \in \mathbb{F}\} \cup \{o\}$ olsun. Eliptik eğrilerin sonlu ya da sonsuz çoklukta rasyonel noktaları vardır.

1.3.1. Teorem. Bir doğru bir eliptik eğriyi katlılıklarla birlikte tam olarak 3 noktada keser (Schmitt ve Zimmer 2003).

1.3.2. Teorem (Bézout). *m.* dereceden bir düzlem eğri ile *n.* dereceden bir düzlem eğri en çok $m.n$ tane noktada kesişir (Silverman 1992).

Bézout teoremi düzlem eğriler teorisinde temel teoremlerden biridir. Bézout'un teoreminin şu uygulamasını kullanacağız.

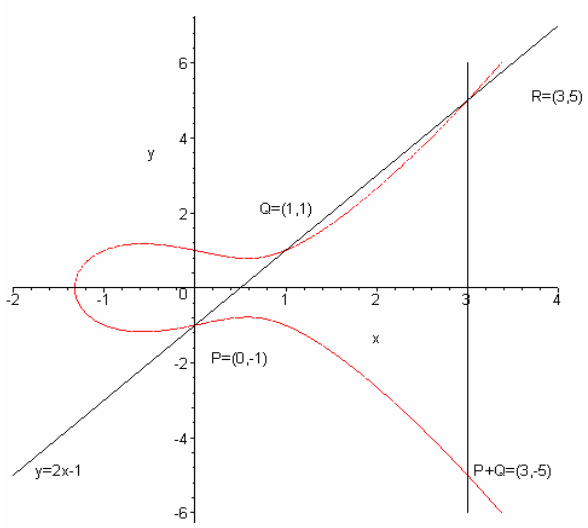
1.3.3.Teorem. C, C_1 ve C_2 kübik eğriler olsunlar. Varsayalım ki C, C_1 ve C_2'nin 8 kesişim noktasından geçsin. Bu durumda C, 9. kesişim noktasından da geçer (Silverman 1992).

1.3.4. Tanım. $E \setminus \mathbb{F}$ eliptik eğri $P_1, P_2 \in E(\mathbb{F})$ farklı olması gerekli olmayan iki nokta olsunlar. P_1 ve P_2'den geçen doğru (örneğin kesen) eliptik eğriyi üçüncü bir P_3' noktasında keser. P_3' ve θ'dan geçen doğruyu göz önüne alalım. Bu doğru eğriyi üçüncü nokta P_3'de keser. P_3'ü

$$P_1 + P_2 = P_3$$

şeklinde tanımlarız (Eğer $P_1 = P_2$ ise P_1'de E'ye teğet alınmak zorundadır). Yani eliptik eğriler üzerinde toplama bu şekilde gerçekleştirilir.

1.3.5. Örnek. $\mathbb{Q}$ cismi üzerinde $y^2 = x^3 - x + 1$ eliptik eğrisini ve bu eğri üzerinde $P = (0,-1)$ ve $Q = (1,1)$ noktalarını ele alalım. Aşağıda verilen şekle göre P ve Q noktalarını $y = 2x - 1$ doğrusu birleştirmektedir. O halde doğrunun eğri ile üçüncü kesişim noktası ortak çözümlenerek bulunabilir. $x = 0$ ve $x = 1$, P ve Q'nun apsisleri olduğuna göre üçüncü nokta $R = (3,5)$'dir. P'nin Q ile toplamı R'nin x-eksenine göre yansımasıdır. Yani $-R = P + Q = (3,-5)$'dir. (Mollin 2001)

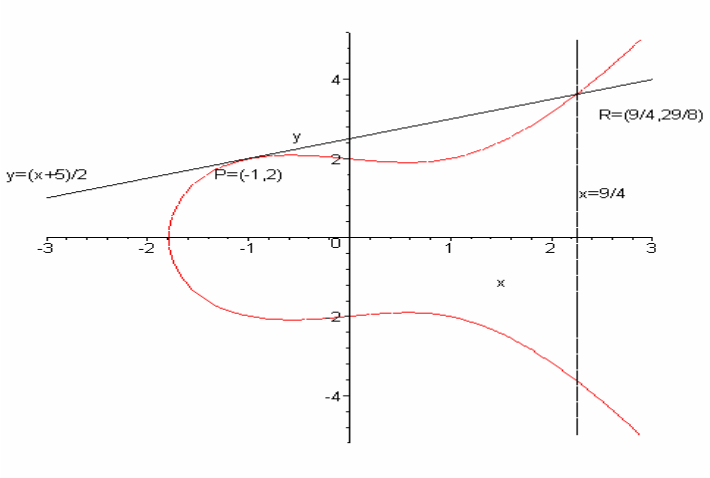


Şekil.1.3.1

1.3.6. Örnek. $\mathbb{Q}$ cismi üzerinde $y^2 = x^3 - x + 4$ eliptik eğrisini ve bu eğri üzerinde $P = (-1, 2)$ noktasını alalım. P noktasına kendisini ekleyelim (Yani $2P$'yi hesaplayalım). $2P$'yi hesaplayabilmek için P'de eğriye bir teğet alalım. İlk önce eğrinin x'e göre türevini alırız.

$$2yy' = 3x^2 - 1$$

P noktasını yukarıdaki denklemde yerine koyarsak $y' = m = \frac{1}{2}$'den teğetin eğimini bulmuş oluruz. Buradan da noktası ve eğimi belli doğru denkleminden P'den geçen teğet $y = \frac{x+5}{2}$ olur. Eğri ile teğetin ortak çözümünden de üçüncü kesişim noktası (ilk iki nokta P'dir) $R = (\frac{9}{4}, \frac{29}{8})$ bulunur. Böylece $P + P = 2P = -R$ eşitliğinden $-R = (\frac{9}{4}, \frac{-29}{8})$ olarak bulunur (Mollin 2001).



Şekil.1.3.2

1.3.7. Teorem. $E \setminus \mathbb{F}$, $\mathbb{F}$ üzerinde bir eliptik eğri olsun. $E(\mathbb{F})$ rasyonel noktalarının kümesi toplama işlemine göre değişmeli gruptur. Sonsuzdaki nokta "θ" bu grubun etkisiz elemanıdır.

$\mathbb{F}$ bir sayı cismi ise $E(\mathbb{F})$, E'nin $\mathbb{F}$ üzerinde "*Mordel-Weil grubu*" olarak adlandırılır.

İspat. Toplamanın aşağıdaki özelliklerini elde etmek kolaydır:

i) $P_1, P_2 \in E(\mathbb{F})$ için $P_1 + P_2 \in E(\mathbb{F})$'dir.

ii) Birim eleman: θ'dır. (Şekil.1.3.3)

iii) Değişme özelliği: $P_1 + P_2 = P_2 + P_1$

iv) Ters eleman özelliği: P ve θ'dan doğru ile eğrinin üçüncü kesişim noktası P' olsun. Bu durumda $P + P' = \theta$'dır. O halde $P' = -P$'dir. (Şekil.1.3.4)

Geriye toplamanın birleşme özelliğini göstermek kalır. $P_1, P_2, P_3 \in E(\mathbb{F})$ olsun.

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

olduğunu göstermeliyiz. Bunun için aşağıdaki doğruları (noktaları çakışırsa teğetler veya kesenler) tanımlayalım :

L_1 : Doğru P_1 ve P_2'den geçer. Bu doğru eğriyi üçüncü nokta olan $-(P_1 + P_2)$'de keser.

L_2: Doğru P_3 ve (P_1+P_2)'den geçer. Bu doğru eğriyi üçüncü nokta olan $-((P_1+P_2)+P_3)$'de keser.

L_3: Doğru (P_2+P_3) ve θ'dan geçer. Bu doğru eğriyi üçüncü nokta olan $-(P_2+P_3)$'de keser.

L_1': Doğru P_2 ve P_3'den geçer. Bu doğru eğriyi üçüncü nokta olan $-(P_2+P_3)$'de keser.

L_2': Doğru P_1 ve (P_2+P_3)'den geçer. Bu doğru eğriyi üçüncü nokta olan $-(P_1+(P_2+P_3))$'de keser.

L_3': Doğru (P_1+P_2) ve θ'dan geçer. Bu doğru eğriyi üçüncü nokta olan $-(P_1+P_2)$'de keser.

Bu durumda

$$C=L_1\cup L_2\cup L_3 \text{ ve } C'=L_1'\cup L_2'\cup L_3'$$

kübik eğrilerini tanımlarız. C ve E eğrilerinin ortak elemanları yoktur (Çünkü C üç doğrunun birleşimidir). Bézout teoreminin bir uygulaması böyle eğrilerin 9 ortak noktası olduğunu ifade eder. C ve E eğrileri için bu noktalar

$$\theta, P_1, P_2, P_3, (P_1+P_2), -(P_1+P_2), (P_2+P_3), -(P_2+P_3), -((P_1+P_2)+P_3).$$

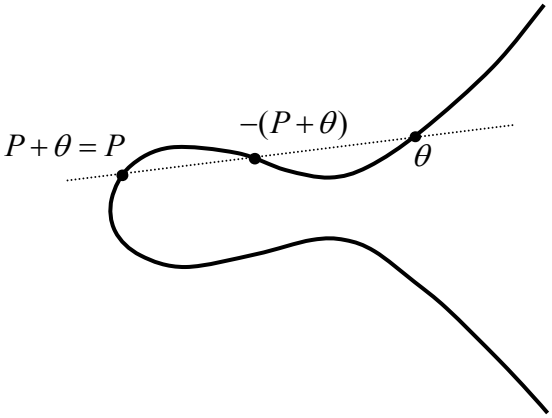
C' eğrisi C ve E eğrisinin ortak noktalarının ilk sekizinde kesişirler. Diğer taraftan C' nün E'de 9 ortak noktası vardır:

$$\theta, P_1, P_2, P_3, (P_1+P_2), -(P_1+P_2), (P_2+P_3), -(P_2+P_3), -(P_1+(P_2+P_3)).$$

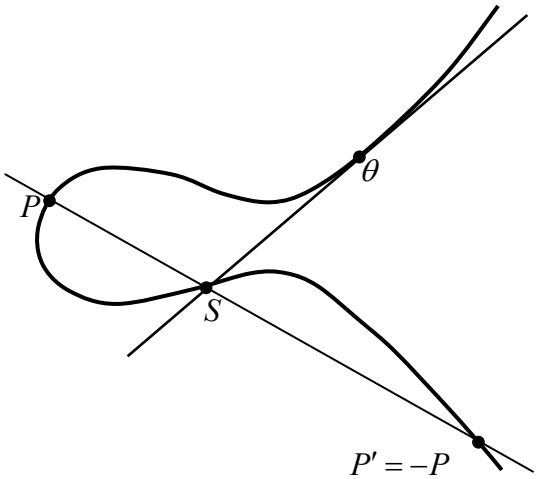
Böylece

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

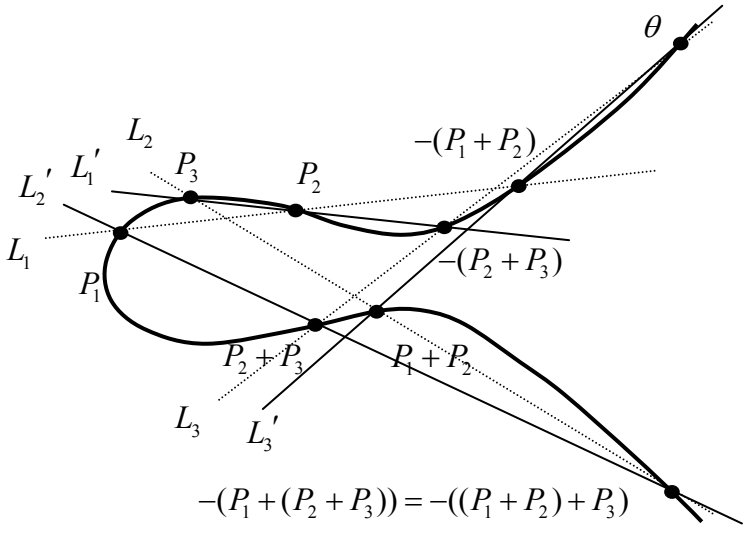
olur (Şekil.1.3.5).□



Şekil.1.3.3 (Birim eleman)



Şekil.1.3.4 (Ters eleman)



Şekil.1.3.5 (Birleşme özelliği)

1.3.8. Toplama Teoremi. $E\setminus\mathbb{F}$, $\mathbb{F}$ cismi üzerinde (23) tipinde bir eliptik eğri ve $P_1=(x_1,y_1)$, $P_2(x_2,y_2)\in E(\mathbb{F})$ olsun. Bu durumda

i) $-P_1=(x_1,-y_1-a_1x_1-a_3)$

ii) $x_1=x_2$ ve $y_2+y_1+a_1x_1+a_3=0$ ise örneğin $P_1=-P_2$ ise $P_1+P_2=\theta$'dır.

iii) $P_1\neq -P_2$ olsun. Eğer $x_1\neq x_2$ ise bu durumda

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

$$\nu=\frac{y_1x_2-y_2x_1}{x_2-x_1}=y_1-\lambda x_1$$

şeklinde ve eğer $x_1=x_2$ ise

$$\lambda=\frac{3x_1^{\,2}+2a_2x_1+a_4-a_1y_1}{2y_1+a_1x_1+a_3},$$

$$\nu=\frac{-x_1^{\,3}+a_4x_1+2a_6-a_3y_1}{2y_1+a_1x_1+a_3}=y_1-\lambda x_1,$$

şeklinde olur. Bu durumda

$$P_1+P_2=P_3=(x_3,y_3)$$

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

$$y_3=-(\lambda+a_1)x_3-\nu-a_3=\lambda(x_1-x_3)-y_1-a_1x_3-a_3.$$

şeklinde verilir (Schmitt ve Zimmer 2003).

Bilindiği gibi eliptik eğriler üzerindeki noktaların en genel temsili uzun Weierstrass normal formundaki afin temsildir. 1.3.8 Teoremde bu temsil için bir toplam formülü tanımladık. Bu temsil keyfi bir karakteristiğe sahip olan herhangi bir cisim için kullanılabilir. Şimdi (27) tipindeki Weierstrass eğrileri için toplam formülünü vereceğiz.

1.3.9. Tanım. $E\setminus\mathbb{F}$, (27) tipinde bir eliptik eğri ve $P_1\neq -P_2$ olacak şekilde $P_1=(x_1,y_1)$, $P_2=(x_2,y_2)\in E$ olsun. 1.3.8.Teorem gereği $P_1+P_2=(x_3,y_3)$

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

ve

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

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

ile verilir.

1.3.10. Örnek. $\mathbb{Q}$ cismi üzerinde $y^2 = x^3 + 17$ eliptik eğrisini ve bu eğri üzerinde $P_1 = (-1, 4)$ ve $P_2 = (2, 5)$ noktalarını alalım. $P_1 + P_2$'yi hesaplamak için ilk önce bu noktalardan geçen doğruyu buluruz. Bu doğru $y = \frac{1}{3}x + \frac{13}{3}$'dur. O halde eğim $\lambda = \frac{1}{3}$ olur. Sonrasında $x_3 = \lambda^2 - x_2 - x_1 = -\frac{8}{9}$ ve $y_3 = \lambda(x_1 - x_3) - y_1 = -\frac{109}{27}$ bulunur. Sonuç olarak $P_1 + P_2 = (x_3, y_3) = \left(-\frac{8}{9}, -\frac{109}{27}\right)$ olur (Silverman 1992).

İki noktadan geçen doğrunun eğimini verdik. Eğer doğrunun geçtiği iki nokta da aynı ise eğim nasıl hesaplanır? Varsayalım ki $P_0 = (x_0, y_0)$ olsun. $P_0 + P_0 = 2P_0$'ı bulmak istiyoruz. P_0'ı P_0'a birleştiren doğruya ihtiyacımız var. Fakat λ için verdiğimiz eğim formülünü kullanmayacağız. Bir P_0 noktasını kendisine eklemenin, P_0'ı P_0'a birleştiren ve P_0'da eğriye teğet olan doğruyu elde etmek anlamına geleceğini biliyoruz. $y^2 = f(x)$ bağıntısından türev yardımıyla

$$\lambda = \frac{dy}{dx} = \frac{f'(x)}{2y}$$

eğimi elde ederiz. Buradan da 1.3.9 Tanımdaki formülleri kullanarak $2P_0$'ın bileşenlerini buluruz.

1.3.11. Örnek. 1.3.10. Örnekteki $y^2 = x^3 + 17$ eliptik eğrisini ve bu eğri üzerindeki $P_1 = (-1, 4)$ noktasını alalım ve $2P_1$ noktasını hesaplayalım. $\lambda = \frac{dy}{dx} = \frac{f'(x_1)}{2y_1} = \frac{f'(-1)}{8} = \frac{3}{8}$ olur. Bu durumda ilk önce λ için bir değer elde ettik. 1.3.9 Tanımda verdiğimiz formülleri kullanırsak $2P_1 = \left(\frac{137}{64}, -\frac{2651}{512}\right)$ bulunur (Silverman 1992).

1.3.12. Tanım (Bachet'in İkiye Katlama Formülü). $y^2 = x^3 + a_2x^2 + a_4x + a_6$ kübik eğrisini ele alalım. Bu eğri üzerindeki bir P noktasının koordinatlarını kullanarak $2P$ için açık bir dönüşüm elde etmek istiyoruz. Bu kübik eğri için 1.3.8 Teoremde verdiğimiz $x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$ formülünü kullanırsak $a_1 = 0$ ve $x_1 = x_2$ olduğundan λ yerine de $\lambda = \dfrac{f'(x)}{2y}$ koyarsak $2P = (x_3, y_3)$ noktasının x_3 koordinatını şöyle formülleştirebiliriz:

$$x(2P) = \frac{x^4 - 2a_4x^2 - 8a_6x + a_4{}^2 - 4a_2a_6}{4x^3 + 4a_2x^2 + 4a_4x + 4a_6}$$

$2P$'nin x koordinatı için verilen bu formül *"İkiye katlama formülü (duplication formula)"* olarak adlandırılır. Aslında bu formül tüm singüler olmayan Weierstrass eğrileri yani eliptik eğriler için tanımlanabilir.

1.3.13. Tanım. E, $\mathbb{F}$ cismi üzerinde bir eliptik eğri ve belli bir $n \in \mathbb{N}$ için $nP = \theta$ olacak şekilde bir $P \in E(\mathbb{F})$ noktası olsun. Bu durumda P noktası *"büküm (torsion) noktası"* ya da "*sonlu mertebeli nokta*" diye adlandırılır. Bu şartı sağlayan en küçük n değerine P'nin mertebesi denir. θ noktası aşikar nokta olarak adlandırılır. P büküm noktası değilse *"sonsuz mertebeli nokta"* olarak adlandırılır.

Büküm noktalarının kümesi $E(\mathbb{F})_t$ ile gösterilir. $E(\mathbb{F})_t$, $E(\mathbb{F})$'in bir alt grubudur. $E(\mathbb{F})$'in *"büküm alt grubu"* olarak adlandırılır.

1.3.14. Örnek. $\mathbb{Q}$ cismi üzerinde $y^2 = x^3 - \dfrac{27}{4}$ eliptik eğrisini alalım. Bu eğrinin $\mathbb{Q}$'daki çözümleri $(3, \frac{9}{2}), (3, -\frac{9}{2})$ ve θ'dur. 1.3.12 Tanım gereği

$$x(2P) = \frac{x^4 + 54x}{4x^3 - 27}\Big|_{x=3} = \frac{81 + 162}{108 - 27} = 3$$

olur. Böylece $2P = P$ veya $2P = -P$'dir. $2P = P$ sonucu yanlıştır. Çünkü bu $P = \theta$ demektir. Böylece $2P = -P$ ve $3P = \theta$'dur. Diğer bir ifadeyle P'nin mertebesi 3'tür (Knapp 1992).

1.3.15. Örnek. $\mathbb{Q}$ sayı cismi üzerinde

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

eliptik eğrisini ele alalım. Bu eğrinin bir $\mathbb{Q}$ rasyonel noktası $P = (2,-3)$'tür.

$$2P = (0,-1),\ 3P = (-1,0),\ 4P = (0,1),\ 5P = (2,3),\ 6P = \theta.$$

Böylece $5P = -P$'dir. O halde P noktasının mertebesi 6'dır (Mollin 2001).

1.3.16. Örnek. $\mathbb{Q}$ üzerinde

$$E: y^2 = x^3 - 10x$$

eliptik eğrisini ele alalım.

$P = (-1,3)$, $Q = (0,0) \in E(\mathbb{Q})$'dur. $P + Q = (10,30)$ olur. Q'nun mertebesi 2'dir: Yani $2Q = \theta$'dur. Burada P noktası sonsuz mertebelidir ve

$$2P = (\frac{121}{36}, \frac{451}{216}), 3P = (\frac{-57121}{24649}, \frac{-12675843}{3869893}),$$

$$4P = (\frac{761815201}{29289744}, \frac{-20870873704079}{158516094528}) \ldots .$$

(Schmitt ve Zimmer 2003). Yukarıda görüldüğü gibi her toplamada bileşenler giderek karmaşıklaşmaktadır.

1.3.17. Nagel-Lutz Teoremi. E, $\mathbb{Q}$ üzerinde (5) tipinde bir eliptik eğri ve $P = (x_1, y_1) \in E(\mathbb{Q})_t$ ise bu durumda $x_1, y_1 \in \mathbb{Z}$'dir ve de ya $y_1 = 0$'dır (ki bu durumda P'nin mertebesi 2'dir) ya da $y_1 \neq 0$ ve $y_1^2 \mid (4A^3 + 27B^2)$'dir (Mollin 2001).

1.3.18. Sonuç. E, $\mathbb{Q}$ üzerinde bir eliptik eğri olsun. Bu durumda $E(\mathbb{Q})$'nun büküm alt grubu sonludur (Mollin 2001).

1.3.19. Örnek. $\mathbb{Q}$ cismi üzerinde $E: y = x^3 + 4$ eliptik eğrisi verilsin. Bu durumda $4A^3 + 27B^2 = 432$ olur. $P(x,y)$, $E(\mathbb{Q})$'da sonlu mertebeli bir nokta olsun. $0 = x^3 + 4$ denkleminin rasyonel çözümleri olmadığından $y \neq 0$'dır. Bu yüzden $y^2 \mid 432$ olur. Böylece $y = \pm 1, \pm 2, \pm 3, \pm 4, \pm 12$'dir. Sadece $y = \pm 2$ değerleri x'in rasyonel değerini verir. Böylece mümkün olan sonlu mertebeli noktalar

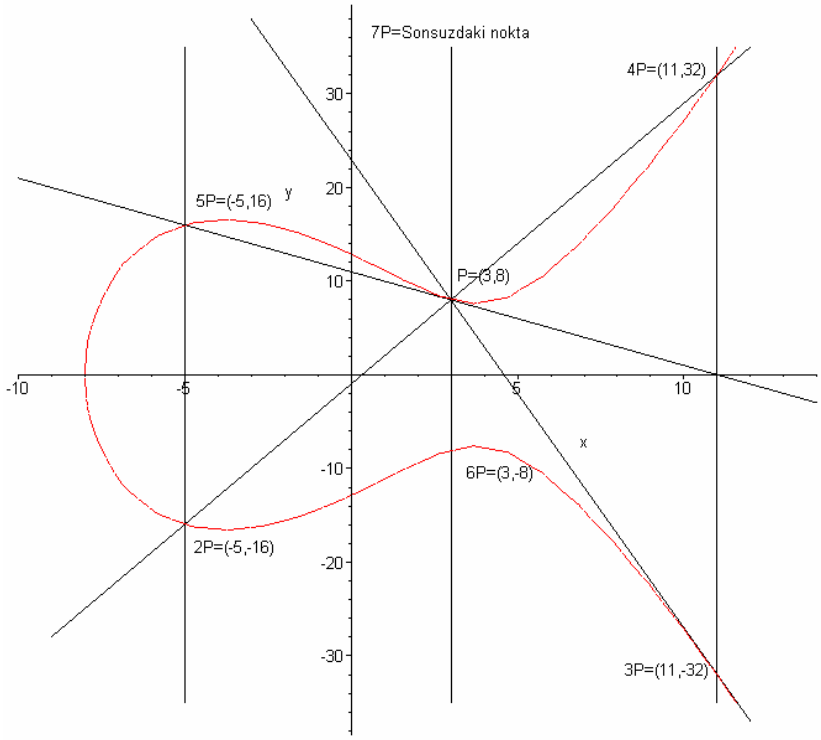
$(0,2),(0,-2)$'dir. Kolay bir hesaplama ile $3(0,\pm 2)=\theta$ olduğunu buluruz. $E(\mathbb{Q})$'nun büküm alt grubu 3 mertebeli devirli bir gruptur (Washington 2003).

1.3.20. Örnek. $\mathbb{Q}$ cismi üzerinde $E: y=x^3+8$ eliptik eğrisi verilsin. Bu durumda $4A^3+27B^2=1728$ olur. $y=0$ iken $x=-2$'dir. $(-2,0)$ noktasının mertebesi 2'dir. Eğer $y\neq 0$ ise bu durumda $y^2 \mid 1728$'dir. Buradan da $y \mid 24$ olur. Değişik ihtimalleri denersek $(1,\pm 3)$ ve $(2,\pm 4)$ noktalarını buluruz. Bununla birlikte

$$2(1,3)=(-\frac{7}{4},-\frac{13}{8}) \text{ ve } 2(2,4)=(-\frac{7}{4},\frac{13}{8})$$

dir. Bu noktaların koordinatları tam sayı olmadığından sonlu mertebeli değildirler. Bu yüzden $(1,3)$ ve $(2,4)$ sonlu mertebeli değildir. Buradan $E(\mathbb{Q})$'nun büküm alt grubunun $\{\theta,(-2,0)\}$ olduğu sonucu çıkar ($2(1,3)=-2(2,4)$ olduğundan dolayı $(1,3)+(2,4)=(-2,0)$ eşitliği açıkça görülür) (Washington 2003).

1.3.21. Örnek. $y^2=x^3-43x+166$ eliptik eğrisini ve bu eğri üzerinde $P=(3,8)$ noktasını ele alalım. Burada P noktasının katlarını alarak mertebesini hesaplayacağız. İlk olarak P'de teğetle başlayalım. P'deki teğet eğriyi $(-5,-16)$'da keser. Bunun da x-eksenine göre yansıması $2P=(-5,-16)$'dır. Bu durumda P ve $2P$'den geçen doğru eğriyi $(11,32)$'de keser. Bunun yansıması $3P=(11,-32)$ dir. $P=(3,8)$ ve $3P=(11,-32)$'den geçen doğru eğriyi $(11,-32)$'de tekrar keser. Bunun da x-eksenine göre yansıması $4P=(11,32)$'yi verir. P ve $4P$'den geçen doğru eğriyi $(-5,-16)$'da keser. Bunun x-eksenine göre yansıması $5P=(-5,16)$'dır. $5P$ ve P'den geçen doğru eğriyi $(3,8)$'de keser. Böylece $6P=(3,-8)$ x-eksenine göre yansımadır. Son olarak da P ve $6P$'den geçen doğru x-eksenine diktir. Böylece $7P=o$'dur (Mollin 2001).



Şekil.1.3.6

1.3.22. Tanım. $E \setminus \mathbb{F}$ bir eliptik eğri ve $n \in \mathbb{N}$ olsun.

$$E[n] = \{P \in E : nP = o\}$$

kümesine E'nin "*n-inci mertebeden noktalarının kümesi"* denir. E'nin $\mathbb{F}$-rasyonel olan n-inci mertebeden noktalarının kümesi

$$E(\mathbb{F})[n] = \{P \in E(\mathbb{F}) : nP = o\}$$

dır. Böylece $E[n] = E(\overline{\mathbb{F}})[n]$'dir.

Eliptik eğriler üzerinde ikinci ve üçüncü mertebeden noktalar diğerlerine göre daha önemlidir.

1.3.23. Önerme. E, $\mathbb{F}$ cismi üzerinde bir eliptik eğri olsun. $\mathbb{F}$'nin karakteristiği 2'den farklıysa

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

$\mathbb{F}$'nin karakteristiği 2 ise

$$E[2] \cong o \quad \text{veya} \quad \mathbb{Z}_2$$

dir (Washington 2003).

1.3.24. Teorem. E, $\mathbb{F}$ cismi üzerinde bir eliptik eğri ve $n \in \mathbb{Z}^+$ olsun. Eğer $\mathbb{F}$'nin karakteristiği n'i bölmezse veya sıfırsa

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

$\mathbb{F}$'nin karakteristiği $p > 0$ ise ve $p \mid n$ ise $p \nmid n'$ olacak şekilde $n = p^r n'$ olarak yazılabilir. O halde

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

dür.

1.3.25. Sonuç. $n = 3$ ve E, $\mathbb{F}$ cismi üzerinde bir eliptik eğri olsun. $E[3] \cong \mathbb{Z}_3 \times \mathbb{Z}_3$ veya bu grubun bir alt grubuna izomorftur. Yani bir eliptik eğri üzerindeki 3. mertebeden rasyonel noktaların sayısı karakteristiğe bağlı olarak 1, 3 ya da 9 olabilir (Washington 2003).

1.3.26. Mordell Teoremi. $A, B \in \mathbb{Q}$ olmak üzere E eliptik eğrisi

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

denklemiyle verilsin. $E(\mathbb{Q})$'daki her P noktası için, $n_1, n_2, ...n_r \in \mathbb{Z}$ iken

$$P = n_1.P_1 + n_2.P_2 + ...n_r.P_r$$

olacak şekilde bir $\{P_1, P_2, ..., P_r\}$ sonlu kümesi vardır. Diğer bir deyişle $E(\mathbb{Q})$ sonlu üreteçli bir gruptur (Mollin 2001).

1.3.27. Mazur Teoremi. $E \setminus \mathbb{Q}$ bir eliptik eğri olsun. Bu durumda ya $n \in \{1,2,3,4,5,6,7,8,9,10,12\}$ iken

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

olur, ya da $n \in \{1,2,3,4\}$ iken

$$E(\mathbb{Q})_t \cong \mathbb{Z} / 2\mathbb{Z} \times \mathbb{Z} / 2n\mathbb{Z}$$

dir (Mollin 2001).

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

1.3.28. Örnek. $E: y^2 = x^3 - x$ eliptik eğrisi verilsin. Bu eğri üzerindeki sonlu mertebeden noktaların kümesi $E(\mathbb{Q})_t = \{o, (0,0), (\pm 1, 0)\}$ dir. Bu kümenin her bir elemanı $2P = o$ şartını sağlar. Böylece $E(\mathbb{Q})_t$'nun grup yapısı

$$E(\mathbb{Q})_t \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

dir (Kato ve ark. 2000).

1.3.29. Örnek. $E: y^2 = x^3 + 1$ eliptik eğrisi bu eğri üzerinde $P = (2,3)$ verilsin. $2P = (0,1),\ 3P = (-1,0),\ 4P = (0,-1),\ 5P = (2,-3),\ 6P = o$ bulunur. O halde $E(\mathbb{Q})$'nin grup yapısı

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

dir (Kato ve ark. 2000).

1.3.30. Örnek. $E: y^2 = x^3 - 4$ eliptik eğrisi bu eğri üzerinde $P = (2,2)$ verilsin. $2P = (5,-11),\ 3P = (\frac{106}{9}, \frac{1090}{27})$ bulunur. O halde $E(\mathbb{Q})$'nun grup yapısı

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

dir, yani bir serbest gruptur. (Kato ve ark. 2000)

1.3.31. Önerme. $k \neq 0$ altıncı dereceden kökü olmayan bir tam sayı olsun. $\mathbb{Q}$ cismi üzerindeki

$$E_k: y^2 = x^3 + k \tag{28}$$

eliptik eğrisi *"Mordell eğrisi"* olarak adlandırılır. Bu durumda

$$E_k(\mathbb{Q})_t = \begin{cases} \{o, (m,0)\} \cong \mathbb{Z}/2\mathbb{Z} & -k = m^3 \neq 1, m \in \mathbb{Z} \ ise \\ \{o, (0, \pm n)\} \cong \mathbb{Z}/3\mathbb{Z} & k = n^2 \neq 1, n \in \mathbb{Z} \ ise \\ \{o, (12, \pm 36)\} \cong \mathbb{Z}/3\mathbb{Z} & k = -432 \ ise \\ \{o, (2, \pm 3), (0, \pm 1), (-1, 0)\} \cong \mathbb{Z}/6\mathbb{Z} & k = 1 \\ \{o\} & aksi\ takdirde \end{cases}$$

şeklinde ifade edilir (Schmitt ve Zimmer 2003).

Şimdi de (27) tipindeki denklemlerin tam sayı çözümlerini arayalım.

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

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

eliptik eğrisi yalnızca sonlu sayıda tam sayı bileşenli $P = (x, y)$ noktasına sahiptir. (Mollin 2001)

1.4. Sonlu Cisimler Üzerinde Eliptik Eğriler

E eliptik eğrisi $\mathbb{F}$ sonlu cismi üzerinde tanımlı olsun. $x, y \in \mathbb{F}$ olacak şekilde E üzerindeki (x, y) ikilileri sonlu çoklukta olduğundan $E(\mathbb{F})$ sonlu bir gruptur. Çalışmalarımızda p asal iken $\mathbb{F}_p$ sonlu cisim ve $q = p^n$, $n \geq 1$ iken $\mathbb{F}_q$ sembolü sonlu cisim genişlemesini temsil edecektir. İlk olarak bazı örnekleri inceleyelim.

1.4.1. Örnek. $E : y^2 = x^3 + x + 1$ eliptik eğrisi $\mathbb{F}_5$ üzerinde olsun. E üzerindeki noktaları saymak için x'in mümkün olan değerlerinin bir listesini yaparız. Bu durumda $x^3 + x + 1$'in 5 modundaki karekökleri olan y değerlerini bulmuş oluruz. Bu da E üzerindeki noktaları verir:

Çizelge 1.4.1

x	$x^3 + x + 1$	y	Noktalar
0	1	± 1	$(0,1), (0,4)$
1	3	-	-
2	1	± 1	$(2,1), (2,4)$
3	1	± 1	$(3,1), (3,4)$
4	4	± 2	$(4,2), (4,3)$
θ		θ	θ

Bu yüzden $E(\mathbb{F}_5)$'in mertebesi 9'dur. Kolay bir hesaplamayla $E(\mathbb{F}_5)$'in devirli olduğunu ve $(0,1)$ noktası ile üretildiğini gösterebiliriz (Washington 2003)

1.4.2. Örnek. $\mathbb{F}_7$ üzerinde $E : y^2 = x^3 + 2$ eliptik eğrisi olsun. Bu durumda $E(\mathbb{F}_7) = \{o, (0,3), (0,4), (3,1), (3,6), (5,1), (5,6), (6,1), (6,6)\}$ olur. Kolay bir hesaplamayla

bu P noktalarının tümünün $3P = o$ şartını sağladığını görebiliriz. Bundan dolayı bu grup $\mathbb{Z}_3 \times \mathbb{Z}_3$'e izomorftur. (Washington 2003)

1.4.3. Teorem. E, $\mathbb{F}_q$ sonlu cismi üzerinde bir eliptik eğri olsun. Bu durumda belli $n \geq 1$ ve $n_1, n_2 \geq 1$ tam sayıları için $n_1 \mid n_2$ olmak üzere bu eğri üzerindeki grup yapısı

$$E(\mathbb{F}_q) \cong \mathbb{Z}_n \text{ ya da } \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$$

olur.

İspat. Gruplar teorisindeki temel bir sonuca göre $i \geq 1$ için $n_i \mid n_{i+1}$ iken sonlu değişmeli bir grup $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times ... \mathbb{Z}_{n_r}$ devirli gruplarının direkt çarpımlarına izomorftur. Her bir i için $\mathbb{Z}_{n_i}$ grubu mertebeleri n_1'i bölen n_1 elemana sahip olduğundan mertebeleri n_1'i bölen n_1^r elemana sahip olan $E(\mathbb{F}_q)$ eğrilerini buluruz. 1.3.23. Teorem gereği bu şekilde en çok n_1^2 tane nokta vardır. ($\mathbb{F}_q$'nun cebirsel kapanışında kalan koordinatlara müsaade edilse bile**)**. Bu yüzden $r \leq 2$'dir. Bu arzu edilen sonuçtur. ($r = 0$ ise grup aşikardır ve bu durum teoremdeki $n = 1$ haline karşılık gelir.**)** □

1.5. Frobenius Endomorfizmi ve Süpersingüler Eğriler

1.5.1. Tanım. $E \setminus \mathbb{F}_q$, $\mathbb{F}_q$ sonlu cismi üzerinde bir eliptik eğri olsun. q-Frobenius endomorfizmi $\varphi_q : E \to E$

$$\varphi_q(x, y) = (x^q, y^q),\ \varphi_q(\theta) = \theta$$

olacak şekilde verilir.

1.5.2. Teorem. $E \setminus \mathbb{F}_q$ eliptik eğri ve φ_q q-Frobenius endomorfizmi olsun.

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

$$P \in E(\mathbb{F}_q) \Leftrightarrow \varphi_q(P) = P$$

olur.

b) $\varphi_q^{\,2} - t\varphi_q + q = 0$ olacak şekilde bir $t = t_q$ tam sayısı vardır. Yani tüm $P \in E$ 'ler için

$$\varphi_q^{\,2}(P) - t\varphi_q(P) + q.P = \theta$$

dır. (Burada t tamsayısı q -Frobenius endomorfizminin *"izi"* olarak adlandırılır.)

c) q -Frobenius endomorfizminin izi t, $E \setminus \mathbb{F}_q$ eliptik eğrisi üzerindeki rasyonel noktaların sayısını veren

$$\#E(\mathbb{F}_q) = q + 1 - t$$

formülünden bulunur (Schmitt ve Zimmer 2003).

1.5.3. Tanım. $\mathbb{F}_q$ karakteristiği p olan sonlu cisim ve $E \setminus \mathbb{F}_q$, $\mathbb{F}_q$ üzerindeki nokta sayısı $\#E(\mathbb{F}_q) = q + 1 - t$ ile verilen bir eliptik eğri olsun. Eğer $p \mid t$ ise bu eğri *"süpersingüler"* olarak adlandırılır. Eğer eğri süpersingüler değilse *"sıradan (ordinary)"* olarak adlandırılır. Başka bir ifadeyle $E[p] \cong \mathbb{Z}_p$ ise sıradan**,** $E[p] \cong \theta$ ise eğri süpersingüler olarak adlandırılır. Singülerlik ile süpersingülerlik birbirinden apayrı kavramlardır.

1.5.4. Yardımcı Teorem. Daha önce tanımladığımız $\mathbb{F}_p$ üzerindeki $E_k : y^2 = x^3 + k$ Mordell eğrisini ele alalım. Ayrıca p asal $p \nmid 6k$ ve $p \equiv 2 \pmod 3$ olsun. Bu durumda $E_k \setminus \mathbb{F}_p$ süpersingülerdir ve $\#E_k(\mathbb{F}_p) = p + 1$ 'dir (Schmitt ve Zimmer 2003).

Aşağıdaki sonuç sonlu cisimler üzerindeki bir eliptik eğrinin singüler olup olmadığını ifade etmenin basit bir yolunu verir.

1.5.5. Önerme. $E \setminus \mathbb{F}_q$ eliptik eğri, q, p asalının bir kuvveti ve $t = q + 1 - \#E(\mathbb{F}_q)$ olsun. Bu durumda E 'nin süpersingüler olması için gerek ve yeter şart $t \equiv 0 \pmod p$ olmasıdır. Bunun gerçekleşmesi için de gerek ve yeter şart $\#E(\mathbb{F}_q) \equiv 1 \pmod p$ olmasıdır. (Washington 2003)

1.5.6. Sonuç. Varsayalım ki $p \geq 5$ asal olsun. Bu durumda E'nin süpersingüler olması için gerek ve yeter şart $t = 0$ olmasıdır. Bu durum için de gerek ve yeter şart $\#E(\mathbb{F}_p) = p + 1$ olmasıdır. (Washington 2003)

1.5.7. Önerme. q tek, $q \equiv 2 \pmod 3$ ve $B \in \mathbb{F}_q^*$ olduğunu varsayalım. Bu durumda

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

ile verilen E eliptik eğrisi süpersingülerdir (Washington 2003).

1.6. Rasyonel Noktaların Sayısının Hesaplanması

$E \setminus \mathbb{F}_q$ eliptik eğri verilsin. (1) denkleminin $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$ çözümlerinin sayısını ya da buna denk olarak $E(\mathbb{F}_q)$'da kaç tane nokta olduğunu bulmak istiyoruz. x'in her bir değeri için y'nin en çok iki değeri vardır. O halde sonsuzdaki θ noktası dâhil bu eğri üzerinde en çok $2q + 1$ tane nokta vardır. Fakat rasgele seçilen bir elemanın ikinci dereceden bir kalan olma şansı %50 olduğundan bu sayı yarı yarıya azalacak ve q+1 olacaktır.

Aşağıdaki teoremi E. Artin tezinde konjektür olarak verdi. 1930'larda bu teorem Hasse tarafından ispatlandı.

1.6.1. Hasse Teoremi. $E \setminus \mathbb{F}_q$ eliptik eğri olsun. Bu durumda

$$| \#E(\mathbb{F}_q) - (q + 1) | = | t | \leq 2q$$

olur (Washington 2003).

1.6.2. Teorem. $E : y^2 = x^3 + Ax + B$ eliptik eğrisi $\mathbb{F}_q$ sonlu cismi üzerinde tanımlansın. Bu durumda

$$\#E(\mathbb{F}_q) = q + 1 + \sum_{x \in \mathbb{F}_q} \left(\frac{x^3 + Ax + B}{q}\right)$$

şeklindedir.

İspat. $x_0 \in \mathbb{F}_q$ için $x_0^3 + Ax_0 + B$'nin q modundaki değeri sıfırdan farklı ve ikinci dereceden bir kalan ise, E eğrisini sağlayan x_0 koordinatlı iki tane (x, y) ikilisi vardır. Eğer $x_0^3 + Ax_0 + B$'nin q modundaki değeri sıfır ise eğri üzerinde x_0 koordinatlı tek nokta vardır. Fakat ikinci dereceden bir kalan değilse bu koşulda nokta yoktur. Bu yüzden x koordinatı x_0 olan noktaların sayısı $1+(\frac{x^3+Ax+B}{q})$ tanedir. Bu ifadenin tüm $x_0 \in \mathbb{F}_q$'lar üzerinden toplamına sonsuzdaki nokta o'yu da eklersek nokta sayısı

$$\#E(\mathbb{F}_q) = 1 + \sum_{x \in \mathbb{F}_q} (1 + (\frac{x^3 + Ax + B}{q}))$$

olur. Sağdaki toplamdaki her bir terimden 1'i dışarıya alırsak bu şekilde arzu edilen formül elde edilir.□

1.6.3. Sonuç. q tek iken $A, B \in \mathbb{F}_q$ olmak üzere $x^3 + Ax + B$ bir polinom olsun. Bu durumda

$$|\sum_{x \in \mathbb{F}_q} (\frac{x^3 + Ax + B}{q})| \leq 2\sqrt{q}$$

olur.

İspat: $x^3 + Ax + B$'nin katlı kökü yoksa $y^2 = x^3 + Ax + B$ denklemi bir eliptik eğri belirtir. O halde 1.6.2 Teorem gereği şunu söyleyebiliriz:

$$q + 1 - \#E(\mathbb{F}_q) = -\sum_{x \in \mathbb{F}_q} (\frac{x^3 + Ax + B}{q})$$

Sonuç Hasse teoreminden görülür. □

1.6.4. Örnek. $\mathbb{F}_5$ üzerinde $E : y^2 = x^3 + x + 1$ eliptik eğrisi verilsin. 5 modunda ikinci dereceden kalanların kümesi, yani $Q_5 = \{1, 4\}$'tür. Bu yüzden

$$\begin{aligned} \#E(\mathbb{F}_5) &= 5 + 1 + \sum_{x=0}^{4} (\frac{x^3 + x + 1}{5}) \\ &= 6 + (\frac{1}{5}) + (\frac{3}{5}) + (\frac{1}{5}) + (\frac{1}{5}) + (\frac{4}{5}) \\ &= 6 + 1 - 1 + 1 + 1 + 1 = 9 \end{aligned}$$

olur (Washington 2003).

E, $\mathbb{F}_q$ sonlu cismi üzerinde tanımlanmış bir eliptik eğri ise bu eğri $r = 1, 2, ...$ için $\mathbb{F}_{q^r}$ cisim genişlemesi üzerinde de tanımlanabilir. O halde $\mathbb{F}_{q^r}$-noktalarını incelemek de anlamlıdır. Yani $y^2 = x^3 + Ax + B$ eğrisinin cisim genişlemeleri üzerindeki çözümlerini de inceleyebiliriz.

1.6.5. Tanım. E üzerindeki $\mathbb{F}_{q^r}$-noktalarının sayısı N_r ile gösterilsin. (Böylece $\mathbb{F}_q$ cismindeki nokta sayısı $N_1 = N$ dir). T bir değişken, $E \setminus \mathbb{F}_q$ bir eliptik eğri olmak üzere N_r sayılarından bir $Z\left(T; E \setminus \mathbb{F}_q\right)$ "*üretme serisi*" oluşturulur. $\mathbb{Q}[[T]]$'deki formal kuvvet serisi

$$Z\left(T; E \setminus \mathbb{F}_q\right) = e^{\sum \frac{N_r T^r}{r}}$$

şeklinde tanımlanır. Sağdaki serinin pozitif tamsayı katsayılı olduğu gösterilebilir. Bu kuvvet serileri $\mathbb{F}_q$ üzerindeki eliptik eğrinin "*zeta fonksiyonu*" olarak adlandırılır ve E'ye karşılık gelen önemli bir kavramdır.

"*Weil konjektürü*" (artık P.Deligne'nin bir teoremi de denilebilir) daha genel bir durumda zeta fonksiyonunun çok özel bir formu olduğunu belirtmektedir. Bir $E \setminus \mathbb{F}_q$ eliptik eğrisi için Weil aşağıdaki sonucu ispatlamıştır:

1.6.6. Weil Teoremi. $\mathbb{F}_q$, q elemanlı sonlu cisim, $E \setminus \mathbb{F}_q$ eliptik eğri olsun. O halde T değişkeninin Zeta fonksiyonu $t \in \mathbb{Z}$ iken

$$Z\left(T; E \setminus \mathbb{F}_q\right) = \frac{1 - tT + qT^2}{(1-T)(1-qT)} \tag{29}$$

şeklindeki bir rasyonel fonksiyondur. Bu t sayısının $N = N_1$ sayısıyla ilişkisi

$$N = q + 1 - t$$

şeklindedir. Ayrıca paydaki ikinci dereceden polinomun diskriminantı negatiftir. Dolayısıyla da mutlak değeri $\frac{1}{\sqrt{q}}$ olan iki $\frac{1}{\alpha}$ *ve* $\frac{1}{\beta}$ köküne sahiptir (Koblitz 1994).

1.6.7. Uyarı. (7)'nin payını $(1-\alpha T)(1-\beta T)$ şeklinde yazıp iki tarafın logaritmik türevini alırsak ve E üzerindeki $\mathbb{F}_{q^r}$ - noktalarının sayısı N_r ile gösterirsek

$$N_r = q^r + 1 - \alpha^r - \beta^r, \qquad r = 1, 2, ...$$

şeklindedir (Koblitz 1994).

1.7. Grup Mertebeleri Verilen Eliptik Eğrilerin Yapısı

Bu bölümde bir eliptik eğrinin eşleniği tanımlanmış ve sonlu cisimler üzerinde grup mertebeleri verilen eliptik eğrilerin grup yapıları ile ilgili bazı sonuçlar verilmiştir.

1.7.1. Tanım. $E \setminus \mathbb{F}_q$, $q = p^k$ ve $p > 3$ olmak üzere

$$E : y^2 = x^3 + a_4 x + a_6$$

basitleştirilmiş Weierstrass denklemiyle verilen bir eliptik eğri olsun. İkinci dereceden kalan olmayan bir $c \in F_q^*$ sabiti için

$$E_c : y^2 = x^3 + a_4 c^2 x + a_6 c^3$$

eğrisine E'nin *"c-eşleniği (twist)"* denir.

1.7.2. Önerme. $E \setminus \mathbb{F}_q$ bir eliptik eğri ve E' bu eğrinin eşleniği olmak üzere

a) $j(E) = j(E')$,

b) $\#E(\mathbb{F}_q) + \#E'(\mathbb{F}_q) = 2q + 2$.

İspat. a) Bu kısmı hesaplamak oldukça kolaydır.

b) E eğrisi üzerindeki rasyonel noktaların sayısı $N_1 = q+1+t$ ve eşleniği olan E' eğrisi üzerindeki rasyonel noktaların sayısı $N_2 = q+1-t$ olduğundan sonuç görülür. □

1.7.3. Önerme. E, $\mathbb{F}_q$'da (27) tipinde bir eliptik eğri ve belli bir n tamsayısı için

$$E(\mathbb{F}_q) \simeq \mathbb{Z}_n \times \mathbb{Z}_n$$

olsun. O zaman

a) $q = n^2 + 1$ veya

b) $q = n^2 \pm n + 1$ veya

c) $q = (n \pm 1)^2$

dir (Washington 2003).

İspat. Hasse teoremine göre $|t| \leq 2q$ iken $n^2 = q + 1 - t$'dir. Bu önermeyi ispatlamak için aşağıdaki yardımcı teoremi kullanacağız. Bu yardımcı teorem t ile ilgili kesin bir sınırlama verir.

1.7.4. Yardımcı Teorem. E, $\mathbb{F}_q$'da (5) tipinde bir eliptik eğri olsun. $\#E(\mathbb{F}_q) - (q+1) = t$ şeklinde tanımlı t Frobenius endomorfizminin izi için $t \equiv 2 \pmod{n}$**'**dir (Washington 2003).

$t \equiv 2 \pmod{n}$ olduğundan $t = 2 + kn$ olacak şekilde bir k tam sayısı vardır. Bu durumda

$$n^2 = q + 1 - t = q - 1 - kn$$

olur. O halde $q = n^2 + kn + 1$'dir. Hasse teoremine göre

$$|2 + kn| \leq 2\sqrt{q}$$

dur. Son eşitsizlikte her iki tarafın karesini alırsak

$$4 + kn + k^2 n^2 \leq 4q = 4(n^2 + kn + 1).$$

elde ederiz. Bu yüzden $|k| \leq 2$'dir. $k = 0, \pm 1, \pm 2$ değerleri 1.7.3 Önermedeki q değerlerinin listesini verir. Bu da 1.7.3 Önermesinin ispatını tamamlar. □

1.7.5. Yardımcı Teorem. $p \equiv 2 \pmod{3}$ tek asal olsun. $B \in \mathbb{F}_p^*$ iken $y^2 \equiv x^3 + B \pmod{p}$ eliptik eğrisi

$$E(\mathbb{F}_p) \cong C_{p+1}$$

olacak şeklinde $p+1$ mertebeli devirli grup yapısına sahiptir (Paillier 2000) .

Aslında $p \equiv 2 \pmod{3}$ yerine $p \equiv 5 \pmod{6}$ da alınabileceğine dikkat ediniz.

1.7.6. Örnek. $p = 17$ için $y^2 \equiv x^3 + 4^3 \pmod{17}$ eğrisi üzerindeki noktalar:

$$E(\mathbb{F}_{17}) = \{(0,8),(0,9),(2,2),(2,15),(4,3),(4,14),(5,6),(5,11),(6,5),(6,12),(7,4),(7,13),(8,7),$$

$(8,10),(11,1),(11,16),(13,0),o\}$ şeklindedir. Yani $\#E(\mathbb{F}_{17}) = 18$ 'dir. Bu eğrinin grup yapısı da $E(\mathbb{F}_{17}) \cong C_{18}$ olur.

2. BACHET VE FREY DIOPHANT DENKLEMLERİ

Birinci bölümde Weierstrass formundaki eliptik eğrilerin birer Diophant denklemi olduğunu gördük. Bu bölümde bu denklemlerin iki özel sınıfını ele alacağız. Bunlar Bachet Diophant denklemleri ve Frey Diophant Denklemleridir. Bu çalışmada Diophant denklemlerini sonsuz sayı cisimleri üzerinde değil F_p sonlu cisimleri üzerinde yapacağız. $y^2 = x^3 + Ax + B$ eliptik eğrilerinde uygun katsayı ve değişken değişiklikleri yapılmasıyla elde edilen bu denklemlerden Bachet Diophant denklemleri $y^2 = x^3 + a^3$ şeklinde ve Frey Diophant Denklemleri $y^2 = x^3 - n^2 x$ şeklinde ifade edilir.

2.1. Bachet Diophant Denklemleri

p asal iken karakteristiği 2 ve 3'ten farklı olan $\mathbb{F}_p$ sonlu cisminde tanımlı basitleştirilmiş Weierstrass normal formundaki

$$E : y^2 = x^3 + Ax + B \qquad (A, B \in \mathbb{F}_p, B \neq 0)$$

denklemini ele alalım. $A = 0$ durumunda elde ettiğimiz denklem

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

"*Bachet Diophant denklemleri*" (ya da Mordell denklemleri) olarak adlandırılır. Bu çalışmada $\mathbb{F}_p$ sonlu cisminde $B = a^3$ durumundaki

$$y^2 = x^3 + a^3 \qquad (a \in \mathbb{F}_p^*) \tag{30}$$

Bachet Diophant denklemlerini inceleyeceğiz. Bu bölümde verilen örneklerde denklemlerin çözüm sayısının hesaplanmasında Maple ve Visual Basic programları kullanılmıştır. Burada ilk olarak şu iki önemli sonucu verebiliriz.

2.1.1. Sonuç. $y^2 \equiv x^3 + a^3 \pmod{p}$ Bachet Diophant denklemi için j-değişmezi $j = 0$ ve diskriminantı $\Delta = -27.16.a^6$ bulunur.

2.1.2. Sonuç. $p \equiv 5 \pmod 6$ asal iken $y^2 \equiv x^3 + a^3 \pmod p$ Bachet Diophant denkleminin sağlayan noktaların üzerinde bulunduğu eğri "*süpersingüler*" dir. $p \equiv 1 \pmod 6$ iken ise "*süpersingüler*" değildir.

Bu kısımda Bachet Diophant Denklemlerinin çözüm sayıları ve bu çözümlerin elde edilmesiyle ilgili bazı sonuçlar ortaya koymaya çalışacağız. Ayrıca üçüncü dereceden kalanlar yardımıyla çözümlerin sayısını formülleştireceğiz.

2.2. Bachet Diophant Denklemlerinin Çözümlerinin Hesaplanması

Şimdi (30) denklemini ele alalım ve bunu E_a ile gösterelim. E_a denkleminin çözümü olan $\mathbb{F}_p$-rasyonel noktaların kümesini $E_a(\mathbb{F}_p)$, bu noktaların sayısını yani $\#E_a(\mathbb{F}_p)$ sayısını $N_{p,a}$ ile gösterelim. $y^2 \equiv u \pmod p$ denklemini sağlayan noktaların sayısının $1+\chi(u)$ olduğu bilinmektedir ve dolayısıyla $y^2 \equiv x^3 + a^3 \pmod p$ denklemini sağlayan noktaların sayısı sonsuzdaki noktayla beraber Hasse teoreminden

$$\begin{aligned} N_{p,a} &= 1 + \sum_{x \in \mathbb{F}_p} (1 + \chi(x^3 + a^3)) \\ &= p + 1 + \sum_{x \in \mathbb{F}_p} \chi(x^3 + a^3) \end{aligned}$$

şeklinde ifade edilir. (30) denkleminin $\mathbb{Z}_p$ cisminde en çok $2p+1$ tane çözüme sahip olduğu kolayca görülebilir. Yani $x, y \in \mathbb{Z}_p$ iken $2p$ tane (x, y) sıralı ikilisi ile birlikte sonsuzdaki nokta (30) denklemini sağlar. Bunun sebebi her bir $x \in \mathbb{F}_p$ için en çok iki tane $y \in \mathbb{F}_p$ vardır ve bunlar (30) denklemini sağlar.

Ancak $\mathbb{F}_p$'nin tüm elemanları ikinci dereceden kalan değildir. Aslında $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{\overline{0}\}$'daki elemanların sadece yarısı ikinci dereceden kalandır. Bundan dolayı $E_a(\mathbb{F}_p)$'deki noktaların sayısının en çok $p+1$ tane olması beklenir.

O halde $\mathbb{F}_p$ cisminde E_a denkleminin çözüm sayısının daha kesin formülü

$$N_{p,a} = p + 1 + \sum_{x \in \mathbb{F}_p} \chi(x^3 + a^3) \tag{31}$$

şeklindedir.

Şimdi sadece $\mathrm{p} \equiv 1 \pmod 6$ durumunu ele alacağız. $y^2 = x^3 + a^3$ denkleminin çözüm sayısına yönelik bazı hesaplamalara başlayalım. İlk olarak çözüm sayısını ikinci dereceden kalanlar yardımıyla yeniden ifade edeceğimiz şu teoremi verelim:

2.2.1. Teorem. $\mathrm{p} \equiv 1 \pmod 6$ bir asal olsun. $y^2 \equiv x^3 + a^3 \pmod p$ denkleminin çözümleri olan (x, y) rasyonel noktalarının sayısı

$$4 + \sum_{x \in \mathbb{F}_p} \rho(x)$$

toplamına eşittir ve burada

$$\rho(x) = \begin{cases} 2 & \chi(x^3 + a^3) = 1 \\ 0 & \chi(x^3 + a^3) \neq 1 \end{cases}$$

ile verilir. Formüldeki dört çözümden üçü aşikâr yani $y = 0$ durumundaki (x, y) ikilileri, dördüncüsü ise sonsuzdaki nokta olarak adlandırılan noktadır. Aynı zamanda denklemin çözümündeki y değerlerinin toplamı da p'ye eşittir.

İspat. $x \equiv 0, 1, 2, \ldots, p-1 \pmod p$ için $y^2 \equiv x^3 + a^3 \pmod p$ denkleminin çözümü olan (x, y) ikililerinin ikinci bileşeni olan y değerlerini bulalım. Eğer $y^2 \in Q_p$ ise $y \in U_p$'nin iki değeri vardır. Bu değerler x_0 ve $p - x_0$'dır. Eğer $y = 0$ ise $\omega^2 + \omega + 1 = 0$ olmak üzere $x = -a$, $x = -\omega a$ ve $x = -\omega^2 a$ gibi üç nokta daha vardır. (Burada $\mathrm{p} \equiv 1 \pmod 6$ için $\omega \in \mathbb{F}_p$'dir.) Bu üç değer aslında $a, a\omega, a\omega^2$'nin farklı dizilişinden başka bir şey değildir. Son olarak sonsuzdaki nokta da göz önüne alınırsa toplam 4 çözüm elde etmiş olunur. O halde sonuç buradan çıkar.

$\mathrm{p} \equiv 5 \pmod 6$ asal iken de $y^2 \equiv x^3 + a^3 \pmod p$ denkleminin çözümü olan (x, y) noktalarının sayısı

$$1 + \sum_{x \in F_p} \rho(x)$$

toplamına eşittir ve burada

$$\rho(x)=\begin{cases}2 & ,\ \chi(x^3+a^3)=1\\ 1 & ,\ \chi(x^3+a^3)=0\\ 0 & ,\ \chi(x^3+a^3)=-1\end{cases}$$

şeklinde tanımlanır. Formüldeki 1 sayısı sonsuzdaki noktayı ifade etmektedir. Ayrıca $y^2 \equiv x^3+a^3 \pmod{p}$ Bachet Diophant denkleminde $p \equiv 5 \pmod 6$ asal olması durumunda $p+1$ tane çözümün var olduğu bilinir..

2.2.2. Örnek. $y^2 \equiv x^3+2^3 \pmod{13}$ Bachet Diophant denkleminin aşikâr dört çözümü $(7,0),(8,0),(11,0)$ ve θ dur. Çünkü $y=0$ alınırsa $0 \equiv x^3+2^3 \pmod{13}$ denkleminde x in sırasıyla 7, 8 ve 11 değerleri bulunabilir ve bunlara bir de sonsuzdaki nokta olarak adlandırılan θ eklenirse aşikâr çözümler bulunmuş olur. Diğer çözümler ise formülden şöyle hesaplanabilir.

$Q_{13}=\{1,3,4,9,10,12\}$ olduğundan

$$\begin{aligned}\sum_{x\in\mathbb{F}_p}\rho(x) &= \rho(0)+\rho(1)+\rho(2)+\rho(3)+\rho(4)+\rho(5)+\rho(6)+\rho(7)+\rho(8)\\ &\quad +\rho(9)+\rho(10)+\rho(11)+\rho(12)\\ &=0+2+2+2+0+2+2+0+0+2+0+0+0\\ &=12\end{aligned}$$

$$4+\sum_{x\in\mathbb{F}_p}\rho(x)=16$$

dır. O halde bu eğri üzerinde toplam 16 tane nokta bulunur.

Hasse'nin teoremi yardımıyla verilen sonucu, ikinci dereceden kalanlar yerine p modundaki üçüncü dereceden kalanlar yardımıyla yeniden ifade edebiliriz.

2.2.3. Teorem. $p \equiv 1 \pmod 6$ bir asal olsun. $t=y^2-a^3$ olsun. Buna göre

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

şeklinde bir fonksiyon tanımlayalım. Bu takdirde $y^2 \equiv x^3+a^3 \pmod{p}$ denkleminin çözüm sayısı

$$1+\sum f(t)$$

toplamıyla verilir ve toplam tüm $y \in \mathbb{F}_p$ ler için alınır. Formüldeki 1 sayısı sonsuzdaki nokta içindir.

İspat. $p \mid t$ olsun. Bu takdirde $x^3 \equiv t \pmod{p}$ kongrüansı $x^3 \equiv 0 \pmod{p}$ haline gelir. O zaman tek çözüm $x \equiv 0 \pmod{p}$ olmasıdır. Dolayısıyla $f(t) = 1$ dir. İkinci olarak $t \notin K_p$ olsun. Buna göre t üçüncü dereceden kalan değildir ve $x^3 \equiv t \pmod{p}$ kongrüansının çözümü yoktur. $t \in K_p^*$ ise $p \equiv 1 \pmod 6$ ve $(p-1,3) = 3$ olduğundan $x^3 \equiv t \pmod{p}$ kongrüansı üç tane çözüme sahiptir.

2.2.4. Örnek. $y^2 \equiv x^3 + 6^3 \pmod{13}$ Bachet Diophant denkleminin çözüm sayısını üçüncü dereceden kalanlar yardımıyla verdiğimiz formülden şöyle hesaplarız: $K_{13} = \{0,1,5,8,12\}$ ve $t = y^2 - a^3$ $(y \in \mathbb{F}_p)$ olduğundan

$$\begin{aligned} 1 + \sum f(t) &= 1 + f(5) + f(6) + f(9) + f(12) + f(8) + f(4) + f(2) + f(2) + f(4) \\ &\quad + f(8) + f(1) + f(9) + f(6) \\ &= 1+3+0+0+3+3+0+0+0+0+3+3+0+0 \\ &= 16 \end{aligned}$$

dır. O halde bu denklemin çözüm kümesi16 nokta bulundurur.

Şimdi (30) denkleminin çözümü olan noktalardan apsisi 0 olanları ele alalım.

2.2.5. Teorem. $p \equiv 1 \pmod 6$ bir asal olsun. $y^2 \equiv x^3 + a^3 \pmod{p}$ denkleminin çözümleri arasında $a \in Q_p$ iken $x \equiv 0 \pmod{p}$ olan iki tane (x, y) sıralı ikilisi vardır. Eğer $a \notin Q_p$ ise eğri üzerinde $x \equiv 0 \pmod{p}$ olan (x, y) sıralı ikilisi yoktur.

İspat. $x \equiv 0 \pmod{p}$ için, $y^2 \equiv a^3 \pmod{p}$ olur. Bu kongrüansın çözümünün olması için gerek ve yeter koşul $\left(\frac{a^3}{p}\right) = \left(\frac{a}{p}\right) = 1$ olmasıdır. Yani a'nın p modunda ikinci dereceden kalan olmasıdır.

2.2.6. Örnek. $x \equiv 0 \pmod{13}$ için $4 \in Q_{13}$ olduğundan $y^2 \equiv x^3 + 4^3 \pmod{13}$ denkleminin çözümleri arasında $(0,5),(0,8)$ sıralı ikilileri vardır. Fakat $5 \notin Q_{13}$

olduğundan $y^2 \equiv x^3 + 5^3 \pmod{13}$ denkleminin çözümleri arasında $x \equiv 0 \pmod{13}$ için y değerleri mevcut değildir. Yani $(0, y)$ ikililerini bulmak mümkün değildir.

Bundan başka $a = 0,1,2,..., p-1 \pmod{p}$ ve $p \equiv 1 \pmod{6}$ bir asal iken $y^2 \equiv x^3 + a^3 \pmod{p}$ denklem sisteminin toplam çözüm sayısını ele alalım. $(a, p) = 1$ iken $y^2 \equiv x^3 + a^3 \pmod{p}$ denkleminin çözüm sayısının uygun bir k tam sayısı için $p+1-2k$ ya da $p+1+2k$ tane olduğunu biliyoruz.

Şimdi de E_a denklem sisteminin çözüm sayılarının toplamı ile ilgili şu sonucu verelim:

2.2.7. Teorem. $p \equiv 1 \pmod{6}$ bir asal ve $1 \le a \le p-1$ olsun. $N_{p,a} = \# E_a(\mathbb{F}_p)$ olsun. O zaman

$$\sum_{a=1}^{p-1} N_{p,a} = p^2 - 1$$

dir.

İspat. $1 \le a \le p-1$ için $(a, p) = 1$ olduğunu biliyoruz. O zaman p modunda a^3x^3 elemanlarının kümesi ile x^3'lerin kümesi aynıdır. Bu durumda

$$\sum_{x \in \mathbb{F}_p} \chi(x^3 + a^3) = \sum_{x \in \mathbb{F}_p} \chi(a^3x^3 + a^3)$$
$$= \chi(a^3) . \sum_{x \in \mathbb{F}_p} \chi(x^3 + 1)$$

olur. (30)'e göre

$$N_{p,a} - p - 1 = \chi(a^3).(N_{p,1} - p - 1)$$

alabiliriz. Her iki tarafın da 1'den $p-1$'e kadar olan toplamını aldığımızda

$$\sum_{a=1}^{p-1} N_{p,a} - p - 1 = \sum_{a=1}^{p-1} \chi(a^3).(N_{p,1} - p - 1)$$

olur. O zaman her iki taraf da 1 veya -1 olduğu için $\chi(a^3) = \chi(a)$ olduğunu kullanırsak

$$\sum_{a=1}^{p-1} N_{p,a} - \sum_{a=1}^{p-1} (p+1) = (N_{p,1} - p - 1).\sum_{a=1}^{p-1} \chi(a^3)$$
$$= (N_{p,1} - p - 1).\sum_{a=1}^{p-1} \chi(a)$$

ifadesini elde ederiz. Sonuç olarak biliyoruz ki

$$\sum_{a=1}^{p-1} \chi(a) = 0$$

dır. Buradan da

$$\sum_{a=1}^{p-1} N_{p,a} = p^2 - 1$$

olur.

2.2.8. Örnek. $y^2 \equiv x^3 + a^3 \pmod{13}$ Bachet Diophant denklemini ele alalım. $a = 1$ için $N_{p,a} = p + 1 + \sum_{x \in \mathbb{F}_p} \chi(x^3 + a^3)$ formülünden $N_{13,1} = 13 + 1 + \sum_{x \in \mathbb{F}_p} \chi(x^3 + 1^3) = 12$ dir. Benzer şekilde $N_{13,2} = 16$, $N_{13,3} = 12$, $N_{13,4} = 12$, $N_{13,5} = 16$, $N_{13,6} = 16$, $N_{13,7} = 16$, $N_{13,8} = 16$, $N_{13,9} = 12$, $N_{13,10} = 12$, $N_{13,11} = 16$, $N_{13,12} = 12$ olur. Sonuç olarak $\sum_{a=1}^{12} N_{13,a} = 13^2 - 1 = 168$ olur.

2.2.9. Sonuç. $\mathbb{F}_p$ cismi üzerindeki Bachet Diophant denklemlerinin çözüm sayılarıyla ilgili tüm sonuçlar, $r > 1$ doğal sayıları için $\mathbb{F}_{p^r}$ cismine genelleştirilebilir. (Demirci ve ark. 2005)

2.3. Frey Eliptik Eğrileri

p asal iken karakteristiği 2 ve 3'ten farklı olan $\mathbb{F}_p$ sonlu cisminde tanımlı basitleştirilmiş Weierstrass normal formundaki

$$E : y^2 = x^3 + Ax + B \qquad (A, B \in \mathbb{F}_p, A \neq 0)$$

denklemini ele alalım. $\mathbb{F}_p$ sonlu cisminde $A = -n^2$ ve $B = 0$ durumunda elde ettiğimiz

$$y^2 = x^3 - n^2 x \qquad (n \in \mathbb{F}_p^{\,*})$$

"*Frey Diophant denklemleri*" ni inceleyeceğiz. Bu bölümde de verdiğimiz örneklerde çözüm sayısının hesaplamalarında Maple ve Visual Basic programları kullanılmıştır.

Burada ilk olarak Bachet Diophant denklemlerin de olduğu gibi şu iki önemli sonucu verebiliriz.

2.3.1. Sonuç. $y^2 \equiv x^3 - n^2 x \pmod{p}$ Frey Diophant denkleminin için j-değişmezi $j = 1728$ ve diskriminantı $\Delta = 64.n^6$ dır.

2.3.2. Sonuç. $p \equiv 3 \pmod 4$ asal iken $y^2 \equiv x^3 - n^2 x \pmod{p}$ Frey Diophant denkleminin çözümü olan (x, y) ikililerinin üzerinde bulunduğu eliptik eğri "süpersingülerdir". $p \equiv 1 \pmod 4$ iken ise "süpersingüler değildir".

Bu bölümde Frey Diophant denkleminin çözüm sayıları ve bu denklemin çözümü olan (x, y) ikililerinin apsisleri toplamı ile ilgili bazı sonuçlar elde etmeye çalışacağız.

2.4. Frey Diophant Denklemlerinin Çözüm Sayılarının Hesaplanması

Şimdi $y^2 = x^3 - n^2 x$ denklemini ele alalım ve bunu E_n ile gösterelim. E_n denkleminin $\mathbb{F}_p$-rasyonel noktalarının kümesini $E_n(\mathbb{F}_p)$, bu noktaların sayısını yani $\#E_n(\mathbb{F}_p)$ sayısını $N_{p,n}$ ile gösterelim. $y^2 \equiv u \pmod{p}$ denklemini sağlayan noktaların sayısının $1 + \chi(u)$ olduğu bilinmektedir ve dolayısıyla $y^2 \equiv x^3 - n^2 x \pmod{p}$ denklemini sağlayan noktaların sayısı sonsuzdaki noktayla beraber Hasse teoreminden

$$\begin{aligned} N_{p,n} &= 1 + \sum_{x \in \mathbb{F}_p} (1 + \chi(x^3 - n^2 x)) \\ &= p + 1 + \sum_{x \in \mathbb{F}_p} \chi(x^3 - n^2 x) \end{aligned}$$

şeklinde ifade edilir. $y^2 = x^3 - n^2 x$ denkleminin $\mathbb{Z}_p$ cisminde en çok $2p+1$ tane çözüme sahip olduğu kolayca görülebilir. Yani $x, y \in \mathbb{Z}_p$ iken $2p$ tane (x, y) sıralı

ikilisi ile birlikte sonsuzdaki nokta $y^2 = x^3 - n^2 x$ denklemi sağlar. Bunun sebebi her bir $x \in \mathbb{F}_p$ için en çok iki tane $y \in \mathbb{F}_p$ var olmasıdır.

Ancak $\mathbb{F}_p$'nin tüm elemanları ikinci dereceden kalan değildir. Aslında $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{\overline{0}\}$'daki elemanların sadece yarısı ikinci dereceden kalandır. Bundan dolayı $E_n(\mathbb{F}_p)$'deki noktaların sayısının en çok $p+1$ tane olması beklenir.

O halde $\mathbb{F}_p$ cisminde E_n denkleminin çözüm sayısının daha kesin formülü

$$N_{p,n} = p + 1 + \sum_{x \in \mathbb{F}_p} \chi(x^3 - n^2 x)$$

şeklindedir.

$y^2 = x^3 - n^2 x$ üzerindeki noktaların sayısına yönelik bazı hesaplamalara başlayalım. İlk olarak şu teoremi verelim:

2.4.1. Teorem. p bir asal olsun. $n \in \mathbb{F}_p$ için $p-1$ tane $y^2 \equiv x^3 - n^2 x \pmod{p}$ Frey Diophant denklemi vardır.

İspat. Sabit bir n değeri alalım. Eğer $x \equiv 0 \pmod{p}$ ise $y \equiv 0 \pmod{p}$ olur. $x \equiv n \pmod{p}$ ve $x \equiv p - n \pmod{p}$ değerleri de aynı denklemi verir. Dolayısıyla ispat biter.

2.4.2. Örnek. $p = 7$ olsun. $n \in \mathbb{F}_7$ için 6 tane Diophant denklemi vardır. Bunlar $y^2 \equiv x^3 - 1^2 x \pmod{7}$, $y^2 \equiv x^3 - 2^2 x \pmod{7}$, $y^2 \equiv x^3 - 3^2 x \pmod{7}$, $y^2 \equiv x^3 - 4^2 x \pmod{7}$, $y^2 \equiv x^3 - 5^2 x \pmod{7}$ ve $y^2 \equiv x^3 - 6^2 x \pmod{7}$ denklemleridir

2.4.3. Teorem. p bir asal olsun. $1 \le n \le p-1$ olmak üzere $\frac{p-1}{2}$ tane birbirinden farklı $y^2 \equiv x^3 - n^2 x \pmod{p}$ Frey Diophant denklemi vardır.

İspat $y^2 \equiv x^3 - n^2 x \pmod{p}$ denkleminde $y = 0$ ise $x = 0$, $x = n$ ve $x = p - n$ bulunur. $1 \le n \le p-1$ için n ve p-n aynı denklik sınıfında oldukları için, 2.4.1. Teorem gereğince p-1 tane Frey Diophant denkleminin tam yarısı kadar, yani $\frac{p-1}{2}$ tane farklı denklem vardır.

2.4.4. Örnek. $p = 5$ olsun. $1 \le n \le 4$ olmak üzere $\frac{5-1}{2} = 2$ tane birbirinden farklı Diophant denklemi vardır. Bunlar ise $y^2 \equiv x^3 - 1^2 x \equiv x^3 - 4^2 x \pmod{5}$ ve $y^2 \equiv x^3 - 2^2 x \equiv x^3 - 3^2 x \pmod{5}$ denklemleridir.

2.4.5. Teorem. p bir asal olsun. $y^2 \equiv x^3 - n^2 x \pmod{p}$ denkleminin çözümlerinde bulunan (x, y) nokta ikilisinin apsisleri aynı olan rasyonel noktaların ordinatları toplamı p'dır.

İspat. $y^2 \equiv x^3 - n^2 x \pmod{p}$ denkleminde x'in 0, n ve p-n'den başka p-3 tane değeri vardır. O zaman bu x'ler için $y^2 \equiv x^3 - n^2 x \pmod{p}$ denkleminin çözümleri içinde ya 2 tane y değeri vardır ya da hiçbir y değeri yoktur. Eğer 2 tane y değeri varsa bunların toplamının p olduğu açıktır.

2.4.6. Örnek. $y^2 \equiv x^3 - 2^2 x \pmod{7}$ denklemini ele alalım. Bu denklemin çözümü olan (x, y) ikilileri $(0,0)$, $(2,0)$, $(5,0)$, $(1,2)$, $(1,5)$, $(3,1)$ ve $(3,6)$ dır. Burada apsisleri aynı olan noktaların ordinatları toplamı 7'dir.

$y^2 = x^3 - n^2 x$ denklemi iki durumda farklılık göstermektedir. Bunlar $p \equiv 1 \pmod{4}$ ve $p \equiv 3 \pmod{4}$ olduğu durumlardır.

2.5. $p \equiv 1 \pmod{4}$ Asal İken Frey Diophant Denklemlerinin Çözümleri

p'nin 4 modunda 1'e denk olduğu durumda, $y^2 = x^3 - n^2 x$ denkleminin çözümü olan nokta ikililerinin özellikleriyle ilgili elde edilen sonuçları verelim.

2.5.1. Teorem. $p \equiv 1 \pmod 4$ asal olsun. $1 \le n \le p-1$ olmak üzere $\frac{p-1}{2}$ tane $y^2 = x^3 - n^2 x \pmod p$ denkleminin $\frac{p-1}{4}$ tanesinin her birinde $x \in Q_p$ olan iki nokta, diğer yarısında da $x \in Q'_p$ olan iki nokta vardır.

İspat. $y^2 \equiv x^3 - n^2 x \pmod p$ denkleminde $y = 0$ için $x = 0$, $x = n$ ve $x = p - n$ olur. $n \in Q_p$ ise $p - n \in Q_p$ olacağından $x \in Q_p$ olur ki $|Q_p| = \frac{p-1}{2}$ olduğundan buradaki *n*'lerin sayısı Q_p'nin eleman sayısı kadar olur. O halde $\frac{p-1}{2}$ tane farklı eğri olur. $n \in Q_p$ ile $p - n \in Q_p$ aynı eğride yer aldığından tam $\left(\frac{p-1}{2}\right).\frac{1}{2} = \frac{p-1}{4}$ tane eğri $x \in Q_p$ elemanına sahiptir. Diğer yarısı da benzer şekilde bulunur.

2.5.2. Örnek. $p = 13$ olsun. $1 \le n \le 12$ olmak üzere $\frac{p-1}{2} = 6$ tane $y^2 = x^3 - n^2 x \pmod{13}$ denkleminin $\frac{p-1}{4} = 3$ tanesinin her birinde $x \in Q_p$ olan iki nokta, diğer yarısında da $x \in Q'_p$ olan iki nokta vardır. $p = 13$ için $Q_{13} = \{1,3,4,9,10,12\}$'dir. $y^2 \equiv x^3 - 1^2 x \equiv x^3 - 12^2 x \pmod{13}$ denkleminin çözümlerinden $(1,0)$ ve $(12,0)$ ikililerinin apsisleri olan $1, 12 \in Q_{13}$'tür. $y^2 \equiv x^3 - 3^2 x \equiv x^3 - 10^2 x \pmod{13}$ denkleminin çözümlerinden $(3,0)$ ve $(10,0)$ nokta ikilileri için $3, 10 \in Q_{13}$'tür. $y^2 \equiv x^3 - 4^2 x \equiv x^3 - 9^2 x \pmod{13}$ denkleminin çözümlerinden $(4,0)$ ve $(9,0)$ nokta ikilileri için $4, 9 \in Q_{13}$'tür.

2.5.3. Teorem. $p \equiv 1 \pmod 4$ bir asal olsun. Bu takdirde $x^3 \equiv t \pmod p$ denkliğinin x tam sayı çözümlerinin toplamı p modunda sıfıra denktir.

İspat $x^3 \equiv 1 \pmod{p}$ denkliğinin çözümleri $x \equiv 1, \omega, \omega^2 \pmod{p}$ dir ki burada $\omega = \dfrac{-1+\sqrt{3}\mathrm{i}}{2}$ birimin küp köküdür. Genel olarak $x^3 \equiv t \pmod{p}$'nin çözümleri x_0 bir özel çözüm olmak üzere $x \equiv x_0, x_0\omega, x_0\omega^2 \pmod{p}$ dir. Gerçekten de

$$(x_0\omega)^3 \equiv x_0^3\omega_0^3 \equiv x_0^3 \equiv t \pmod{p}$$

ve aynı şekilde

$$(x_0\omega^2)^3 \equiv x_0^3\omega^6 \equiv x_0^3(\omega^3)^2 \equiv x_0^3 \equiv t \pmod{p}$$

dir. Dolayısıyla bu çözümlerin toplamı

$$x_0 + x_0\omega + x_0\omega^2 = x_0 + x_0\omega + x_0(-1-\omega) = 0$$

dir. Eğer çözüm yoksa toplam 0 olarak düşünülebilir.

2.5.4. Teorem. $p \equiv 1 \pmod 4$ bir asal olsun. $y^2 \equiv x^3 - n^2x \pmod{p}$ denkleminin çözümü olan (x, y) sıralı ikililerinin sayısı

$$1 + \sum_{x \in \mathbb{F}_p} \rho(x)$$

toplamına eşittir ve burada

$$\rho(x) = \begin{cases} 2 & , \chi(x^3 - n^2x) = 1 \\ 1 & , \chi(x^3 - n^2x) = 0 \\ 0 & , \chi(x^3 - n^2x) = -1 \end{cases}$$

şeklinde ifade edilir. Aynı zamanda böyle y değerlerinin toplamı da p'ye eşittir.

İspat $p \equiv 1 \pmod 4$ asal olduğundan sonuç kolayca görülür.

2.5.5. Örnek. $y^2 \equiv x^3 - 10^2x \pmod{13}$ Frey Diophant denkleminin çözümü olan sekiz nokta ikilisi $(0,0)$, $(3,0)$, $(10,0)$, $(2,4)$, $(2,9)$, $(11,6)$, $(11,7)$ ve o'dur.

$Q_{13} = \{1,3,4,9,10,12\}$ olduğundan

$$\begin{aligned} \sum_{x \in \mathbb{F}_{13}} \rho(x) &= \rho(0) + \rho(1) + \rho(2) + \rho(3) + \rho(4) + \rho(5) + \rho(6) + \rho(7) + \rho(8) \\ &\quad + \rho(9) + \rho(10) + \rho(11) + \rho(12) \\ &= 1 + 0 + 2 + 1 + 0 + 0 + 0 + 0 + 0 + 0 + 1 + 2 + 0 \\ &= 7 \end{aligned}$$

$$1+\sum_{x\in\mathbb{F}_{13}}\rho(x)=8$$

dır. O halde bu denklemin toplam 8 tane çözümü vardır.

2.5.6. Teorem. $p\equiv 1 \pmod 4$ bir asal olsun. $y^2\equiv x^3-n^2x \pmod p$ denkleminin çözüm sayısı $\#E_n(\mathbb{F}_p)=N_{p,n}$ olsun. $r,s\in\mathbb{Z}$, r tek ve s çift, $p=r^2+s^2$ olmak üzere

a) $r+s\equiv 1 \pmod 4$ ise

i) $n\in Q_p$ ise $N_{p,n}=p+1-2r$

ii) $n\in Q'_p$ ise $N_{p,n}=p+1+2r$

b) $r+s\equiv 3 \pmod 4$ ise

i) $n\in Q_p$ ise $N_{p,n}=p+1+2r$

ii) $n\in Q'_p$ ise $N_{p,n}=p+1-2r$

dır.

2.5.7. Örnek. $p=17$ olsun. $y^2\equiv x^3-4^2x \pmod{17}$ Frey Diophant denkleminin çözümü olan 16 nokta $(0,0)$, $(4,0)$, $(13,0)$, $(1,6)$, $(1,11)$, $(3,8)$, $(3,9)$, $(6,1)$, $(6,16)$, $(11,4)$, $(11,13)$, $(14,2)$, $(14,15)$, $(16,7)$, $(16,10)$ ve o'dur.

r tek ve s çift tamsayı olmak üzere $p=r^2+s^2=17=1^2+4^2$ olduğundan $r=1$ ve $s=4$ bulunur. $r+s=1+4\equiv 1 \pmod 4$ ve $n=4\in Q_{17}$ olduğu için

$$N_{17,4}=p+1-2r=17+1-2.1=16$$

nokta sayısı 16 olarak bulunur.

2.5.8. Teorem. $p\equiv 3 \pmod 4$ asal olsun. $y^2\equiv x^3-n^2x \pmod p$ denkleminde

a) eğer $n\in Q_p$ ise $\dfrac{p-1}{2}$ tane $x\in Q_p$ değeri,

b) eğer $n\in Q_p$ ise $\dfrac{p+1}{2}$ tane $x\in\mathbb{F}_p\setminus Q_p$ değeri,

c) eğer $n\in Q'_p$ ise $\dfrac{p-1}{2}$ tane $x\in Q_p$ değeri,

d) eğer $n \in Q'_p$ ise $\frac{p+1}{2}$ tane $x \in \mathbb{F}_p \setminus Q_p$ değeri,

vardır.

İspat. Aşikârdır.

2.5.9. Örnek. $p = 11$ olsun. $y^2 \equiv x^3 - 3^2 x \pmod{11}$ denkleminin çözümü olan sayı ikililerinin arasında $(0,0)$, $(1,0)$, $(10,0)$, $(4,4)$, $(4,7)$, $(6,1)$, $(6,10)$, $(8,3)$, $(8,8)$, $(9,4)$ ve $(9,7)$ vardır. $y^2 \equiv x^3 - 7^2 x \pmod{11}$ denkleminde ise $(0,0)$, $(4,0)$, $(7,0)$, $(2,3)$, $(2,8)$, $(3,1)$, $(3,10)$, $(5,1)$, $(5,10)$, $(10,2)$ ve $(10,9)$ nokta ikilileri çözümler arasında yer alır. Şimdi n değerlerinin Q_{11}'de bulunup bulunmadığına göre x'in kaç tane değerinin Q_{11}'de bulunup bulunmadığına bakalım $Q_{11} = \{1,3,4,5,9\}$ olduğundan $y^2 \equiv x^3 - 3^2 x \pmod{11}$ denkleminin çözümleri olan $(1,0)$, $(4,4)$, $(4,7)$, $(9,4)$ ve $(9,7)$ sayı ikilerinin apsisleri, Q_{11}'de yer alır. $(0,0)$, $(10,0)$, $(6,1)$, $(6,10)$, $(8,3)$ ve $(8,8)$ nokta ikililerinin apsisleri ise yer almaz. Teoreme göre $n = 3 \in Q_{11}$ olduğundan, gerçekten de $\frac{p-1}{2} = 5$ tane $x \in Q_p$ değeri ve $\frac{p+1}{2} = 6$ tane de $x \in \mathbb{F}_p \setminus Q_p$ değeri vardır. $y^2 \equiv x^3 - 7^2 x \pmod{11}$ denklemi için ise $(4,0)$, $(3,1)$, $(3,10)$, $(5,1)$ ve $(5,10)$ noktalarının apsisleri, Q_{11}'de yer alır. $(0,0)$, $(7,0)$, $(2,3)$, $(2,8)$, $(10,2)$ ve $(10,9)$ noktalarının apsisleri ise yer almaz. Teoremin ifadesine göre, $n = 7 \notin Q_{11}$ olduğundan, $\frac{p-1}{2} = 5$ tane $x \in Q_p$ değeri ve $\frac{p+1}{2} = 6$ tane de $x \in \mathbb{F}_p \setminus Q_p$ değeri vardır.

2.5.10. Teorem. $p \equiv 3 \pmod 4$ asal olsun. Eğer $n \in K_p^*$ ve $y \equiv 0 \pmod p$ ise $y^2 \equiv x^3 - n^2 x \pmod p$ denkleminde apsisleri K_p'de kalan 3 sayı ikilisi vardır.

İspat. $y \equiv 0 \pmod p$ olsun. O zaman $x^3 \equiv n^2 x \pmod p$ ve $x(x-n)(x+n) \equiv 0 \pmod p$ olur. Buradan $x \equiv 0 \pmod p$, $x \equiv n \pmod p$ ve $x \equiv p - n \pmod p$ elde edilir. Tüm çözümlerin K_p'de olduğu aşikârdır.

2.5.11. Örnek. $p=19$ olsun. $y^2 \equiv x^3 - 11^2 x \pmod{19}$ denklemini ele alalım. Bu denklemin çözümü olan $(0,0)$, $(1,0)$ ve $(18,0)$ nokta ikililerinin ordinatları 0'dır. $K_{19} = \{0,1,7,8,11,12,18\}$ olduğundan bu noktaların apsislerinin K_p'de olduğu görülür.

2.5.12. Teorem. $p \equiv 3 \pmod 4$ bir asal olsun. $y^2 \equiv x^3 - n^2 x \pmod p$ denkleminin çözümü olan noktaların apsisleri toplamı

$$\sum_{x \in \mathbb{F}_p} (1 + \chi_p(x^3 - n^2 x)).x$$

formülüyle ifade edilir.

İspat.

$$\chi_p(t) = \begin{cases} 1 & x^2 \equiv t \pmod p \text{ çözümü var ise} \\ 0 & p \mid t \\ -1 & x^2 \equiv t \pmod p \text{ çözümü yok ise} \end{cases}$$

şeklinde tanımlandığından $1 + \chi_p(t) = 0,1$ ya da 2 olduğunu biliyoruz. $y \equiv 0 \pmod p$ iken $x^3 - n^2 x \equiv 0 \pmod p$ dir ve $p \mid 0$ iken $\chi_p(x^3 - n^2 x) = 0$ dır. Denklemin çözümü olan her bir $(x,0)$ noktası için $(1+0).x = x$ toplama eklenir. $x^3 - n^2 x = t$ olsun. $\left(\frac{t}{p}\right) = 1$ ise çözüm olan her bir (x,y) nokta için $(x,-y)$ noktası da bir çözümdür. Böylece her bir t için $(1+1).x = 2x$ toplama eklenir. Sonuç olarak $\left(\frac{t}{p}\right) = -1$ ise $x^2 \equiv t \pmod p$ 'nin hiç çözümü yoktur ve böyle (x,y) noktaları için $(1+(-1)).x = 0$ oluşu toplamla çelişir.

3. BACHET VE FREY DIOPHANT DENKLEMLERİNİN GRUP YAPILARI

3.1. Giriş

2. bölümde gördüğümüz iki tür Diophant denkleminin çözümleri kümesindeki toplama işlemine göre bir toplamsal abelian gruptur. Bu bölümde bu iki Diophant denklem türünün çözümlerinin oluşturduğu grupların yapısını inceleyeceğiz.

3.2. Bachet Diophant Denklemlerinin Grup yapıları

p asal olsun. $a \in \mathbb{F}_p^* = \mathbb{F}_p - \{0\}$ iken E_a Bachet Diophant denkleminin grup yapısını inceleyeceğiz. Bunu yaparken birinci bölümde bulunan " $p \equiv 2 \pmod 3$ tek asal olsun. $B \in \mathbb{F}_p^*$ iken $y^2 \equiv x^3 + B \pmod p$ denklemi

$$E(\mathbb{F}_p) \cong C_{p+1}$$

olacak şekilde $p+1$ mertebeli devirli grup yapısına sahiptir. (Paillier 2000)" yardımcı teoreminin ifadesinden faydalanacağız.

Aslında $p \equiv 2 \pmod 3$ yerine $p \equiv 5 \pmod 6$ da alınabileceğinden dolayı bu yardımcı teoremi kullanabiliriz. $E_a(\mathbb{F}_p) \cong C_{p+1}$, $p+1$ mertebeli devirli gruptur. Fakat $p \equiv 1 \pmod 6$ ise $E_a(\mathbb{F}_p)$'nin grup yapısını veren bilinen bir sonuç yoktur. Bu bölümde, $p \equiv 1 \pmod 6$ iken $E_a(\mathbb{F}_p)$'nin grup yapısını inceleyeceğiz. Bu grubun, C_n ve C_{nm} devirli gruplarının bir direkt çarpımına izomorf olduğunu göstereceğiz. Yani $m, n \in \mathbb{Z}$ için

$$E_a(\mathbb{F}_p) \cong \mathbb{Z}_n \times \mathbb{Z}_{nm}$$

dir. Ayrıca nokta sayısı, mertebe ve Frobenius endomorfizminin izi ile ilgili bazı sonuçları elde etmeye çalışacağız. $E_a(\mathbb{F}_p)$'nin mertebesini daha önceden $N_{p,a}$ ile gösterdik. Vereceğimiz sonuçların ifadesini kolaylaştırması açısından bundan sonra $N_{p,a}$ yerine bazen N kullanacağız. Nokta sayısını

$$N = n^2 m = p + 1 - t$$

şeklinde ifade edeceğiz. Burada t, Frobenius endomorfizminin izidir.

3.2.1. Teorem. E_a eliptik eğrilerinin belirttiği Diophant denklemleri için

$$N = n^2 m = p + 1 - t$$

şeklinde ifade edilirken $a \in Q_p$ olursa $t > 0$ ve diğer durumda $t < 0$ dır. (Yıldız ve ark. 2005)

3.3. $C_n \times C_{nm}$ Formundaki Grup Yapısına Uyan Bachet Eliptik Eğrileri

E_a eliptik eğrilerinin belirttiği Diophant denklemlerini ele alalım. Bu durumda $g \in Q_p'$ için

$$y^2 \equiv x^3 + g^3 a^3$$

kongrüans denkliği $y^2 \equiv x^3 + a^3$ kongrüans denkliğinin eşleniği olarak tanımlanır. Burada $a \in Q_p$ ise $ga \in Q_p'$ ve $a \in Q_p'$ ise $ga \in Q_p$ şeklindedir. (23) tipindeki herhangi bir denklem ile eşleniğinin t'lerinin işaretlerinin farklı olduğunu göstermek kolaydır. O halde aşağıdaki teoremi verebiliriz:

3.3.1. Teorem. $p \equiv 1 \pmod 6$ bir asal olsun. (23) tipindeki denkleminin çözümlerinin oluşturduğu $n^2 m = p + 1 - t$ mertebeli $C_n \times C_{nm}$ grubuna izomorf ise bunun eşleniği $r^2 s = p + 1 - t$ mertebeli $C_r \times C_{rs}$ grubuna izomorftur.(Yıldız ve ark. 2005)

3.3.2. Örnek. $y^2 \equiv x^3 + 2^3 \pmod{577}$ kongrüans denkliğini ele alalım. Bu denklemde $2 \in Q_{577}$, $N_{577,2} = 624$ ve çözümlerin oluşturduğu grup yapısı $C_4 \times C_{156}$ dır. $N = n^2 m = p + 1 - t$ bağıntısına göre $624 = 4^2.39 = 577 + 1 - t$ iken $t = -46$ olur. $y^2 \equiv x^3 + 10^3 \pmod{577}$ kongrüans denkliği için ise, $10 \in Q_{577}'$, $N_{577,10} = 532$ ve grup yapısı $C_2 \times C_{266}$ dır. Nokta sayısı formülüne göre $532 = 2^2.133 = 577 + 1 - t$ iken $t = 46$ bulunur.

3.3.3. Teorem. a) $p \equiv 1 \pmod{12}$ bir asal olsun. Bu durumda $t \equiv 2 \pmod{12}$ olması için gerek ve yeter şart $N \equiv 0 \pmod{12}$ ve $t \equiv 10 \pmod{12}$ olması için gerek ve yeter şart $N \equiv 4 \pmod{12}$ olmasıdır.

b) $p \equiv 7 \pmod{12}$ bir asal olsun. Bu durumda $t \equiv 4 \pmod{12}$ olması için gerek ve yeter şart $N \equiv 4 \pmod{12}$ ve $t \equiv 8 \pmod{12}$ olması için gerek ve yeter şart $N \equiv 0 \pmod{12}$ olmasıdır.

İspat. a) $p \equiv 1 \pmod{12}$ bir asal olsun. Bunu $n \in \mathbb{Z}$ iken $p = 1 + 12n$ şeklinde yazabiliriz. $t \equiv 2 \pmod{12}$'den $m \in \mathbb{Z}$ olmak üzere $t = 2 + 12m$ şeklinde ifade edebiliriz. Bunları nokta sayısı formülünde yerine koyarsak

$$\begin{aligned} t \equiv 2 \pmod{12} \Leftrightarrow N &= p + 1 - t \\ &= 1 + 12n + 1 - (2 + 12m) \\ &= 12(n - m) \\ \Leftrightarrow N &\equiv 0 \pmod{12} \end{aligned}$$

ve benzer olarak

$$\begin{aligned} t \equiv 10 \pmod{12} \Leftrightarrow N &= p + 1 - t \\ &= 1 + 12n + 1 - (10 + 12m) \\ &= -8 + 12(n - m) \\ \Leftrightarrow N &\equiv 4 \pmod{12} \end{aligned}$$

elde edilir. b) şıkkı da benzer yolla ispat edilir.

3.3.4. Örnek. $p = 1297 \equiv 1 \pmod{12}$ bir asal iken $y^2 \equiv x^3 + 123^3 \pmod{1297}$ kongrüans denkliğini ele alalım. $N_{1297,123} = 1252$ ve $t = 46 \equiv 10 \pmod{12}$ dir. Ayrıca $1252 \equiv 4 \pmod{12}$ dir. $y^2 \equiv x^3 + 42^3 \pmod{1297}$ kongrüans denkliği için ise $N_{1297,42} = 1344$ ve $t = -46 \equiv 2 \pmod{12}$ dir. Ayrıca $1344 \equiv 0 \pmod{12}$ dir.

$p \equiv 1 \pmod{6}$ asal iken Bachet Diophant denklemlerinin ve bunların eşleniklerinin çözümleri olan noktaların oluşturduğu grup tablosu aşağıda verilmiştir.

$p \le 127$ Asal Ve $p \equiv 1 \pmod 6$ İçin Bachet Eliptik Eğrilerine Karşılık Gelen Diophant Denklemlerinin Ve Eşleniklerinin Çözümleri Olan Noktaların Oluşturduğu Grupların Mertebe, Eleman Sayıları Ve Grup Yapısı Tablosu

p=7	Mertebe	Eleman sayısı	Mertebe	Eleman sayısı
	2	3	2	3
			3	2
			6	6
	$C_2 \times C_2$		$C_2 \times C_6$	

p=13	Mertebe	Eleman sayısı	Mertebe	Eleman sayısı
	2	3	2	3
	4	12	3	2
			6	6
	$C_4 \times C_4$		$C_2 \times C_6$	

p=19	Mertebe	Eleman sayısı	Mertebe	Eleman sayısı
	2	3	2	3
	3	2	7	6
	6	6	14	18
	$C_2 \times C_6$		$_2$ $C_2 \times C_{14}$	

p=31	Mertebe	Eleman sayısı	Mertebe	Eleman sayısı
	2	3	2	3
	7	6	3	8
	14	18	6	24
	$C_2 \times C_{14}$		$C_6 \times C_6$	

p=37	Mertebe	Eleman sayısı	Mertebe	Eleman sayısı
	2	3	2	3
	7	6	3	2
	14	18	4	12
			6	6
			12	24
	$C_2 \times C_{14}$		$C_4 \times C_{12}$	

p=43	Mertebe	Eleman sayısı	Mertebe	Eleman sayısı
	2	3	2	3
	3	8	13	12
	6	24	26	36
	$C_6 \times C_6$		$C_2 \times C_{26}$	

p=61	Mertebe	Eleman sayısı	Mertebe	Eleman sayısı
	2	3	2	3
	19	18	3	2
	38	54	4	12
			6	6
			12	24
	$C_2 \times C_{38}$		$C_4 \times C_{12}$	

p=67	Mertebe	Eleman sayısı	Mertebe	Eleman sayısı
	2	3	2	3
	3	2	13	12
	6	4	26	36
	7	6		
	14	18		
	21	14		
	42	36		
	$C_2 \times C_{42}$		$C_2 \times C_{26}$	

p=73	Mertebe	Eleman sayısı	Mertebe	Eleman sayısı
	2	3	2	3
	3	2	4	12
	6	6	8	48
	7	6		
	14	18		
	21	12		
	42	36		
	$C_2 \times C_{42}$		$C_8 \times C_8$	

p=79	Mertebe	Eleman sayısı	Mertebe	Eleman sayısı
	2	**3**	**2**	**3**
	3	**2**	**19**	**18**
	6	**6**	**38**	**54**
	7	**6**		
	14	**18**		
	21	**12**		
	42	**36**		
	$C_2 \times C_{42}$		$C_2 \times C_{38}$	

p=97	Mertebe	Eleman sayısı	Mertebe	Eleman sayısı
	2	**3**	**2**	**3**
	3	**2**	**4**	**12**
	6	**6**	**7**	**6**
	7	**6**	**14**	**18**
	14	**18**	**28**	**72**
	21	**12**		
	42	**36**		
	$C_2 \times C_{42}$		$C_4 \times C_{28}$	

p=103	Mertebe	Eleman sayısı	Mertebe	Eleman sayısı
	2	**3**	**2**	**3**
	3	**2**	**31**	**30**
	6	**6**	**62**	**90**
	7	**6**		
	14	**18**		
	21	**12**		
	42	**36**		
	$C_2 \times C_{42}$		$C_2 \times C_{62}$	

p=109	Mertebe	Eleman sayısı	Mertebe	Eleman sayısı
	2	**3**	**2**	**3**
	4	**12**	**3**	**8**
	7	**6**	**6**	**24**
	14	**18**	**9**	**18**
	28	**72**	**18**	**54**
	$C_4 \times C_{28}$		$C_6 \times C_{18}$	

p=127	Mertebe	Eleman sayısı	Mertebe	Eleman sayısı
	2	**3**	**2**	**3**
	37	**36**	**3**	**8**
	74	**108**	**6**	**24**
			9	**18**
			18	**54**
	$C_2 \times C_{74}$		$C_6 \times C_{18}$	

3.4. Frey Diophant Denklemlerinin Grup Yapısı

p asal olsun. $n \in \mathbb{F}_p^* = \mathbb{F}_p - \{0\}$ iken E_n Frey Diophant denklemlerinin çözümlerinin grup yapısını inceleyeceğiz. p'nin 4 modunda 1'e ve 3'e denk oluşuna göre iki ayrı sınıflandırma yapmak mümkündür. $E_n(\mathbb{F}_p)$'nin genel olarak grup yapısını veren bilinen bir sonuç yoktur. Bu nedenle de iki grupta değerlendirme yapılmıştır. $p \equiv 3 (\text{mod } 4)$ ise $E_n(\mathbb{F}_p) \cong \mathbb{Z}_2 \times \mathbb{Z}_{\frac{p+1}{2}}$, $p+1$ mertebeli bir gruptur. Fakat bu bölümde yalnızca $p \equiv 1 \text{ (mod 4)}$ ise $\mathbb{Z}_a$ ve $\mathbb{Z}_{a.b}$ devirli gruplarının bir direkt çarpımına izomorf olduğunu göstereceğiz. Yani $a, b \in \mathbb{N}$ için

$$E_n(\mathbb{F}_p) \cong \mathbb{Z}_a \times \mathbb{Z}_{a.b}$$

dir. Ayrıca nokta sayısı, mertebe ve Frobenius endomorfizminin izi ile ilgili bazı sonuçları elde etmeye çalışacağız. $N_{p,n}$ ile $E_n(\mathbb{F}_p)$'nin mertebesi gösterilmektedir. bundan sonra $N_{p,n}$ yerine bazen N kullanılacaktır. Dolayısıyla nokta sayısı

$$N = a^2 b = p + 1 - t$$

şeklinde ifade edilecektir. Burada t, Frobenius endomorfizminin izidir. Bu bölümde verilen örneklerde nokta sayısı ve mertebe hesaplamalarında Maple ve Visual Basic programları kullanılmıştır.

3.5. $p \equiv 1 \pmod 4$ Asal İken Frey Diophant Denklemlerinin Grup Yapısı

E_a eliptik eğrilerinin belirttiği Diophant denklemlerini ele alalım. Bu durumda $g \in Q_p'$ için

$$y^2 \equiv x^3 - g^2 n^2 x$$

kongrüans denkliği $y^2 \equiv x^3 - n^2 x$ kongrüans denkliğinin eşleniği olarak tanımlanır. Burada $n \in Q_p$ ise $gn \in Q_p{}'$ ve $n \in Q_p{}'$ ise $gn \in Q_p$ şeklindedir. $y^2 = x^3 - n^2 x$ $(n \in \mathbb{F}_p{}^*)$ tipindeki herhangi bir denklem ile eşleniğinin t'lerinin işaretlerinin farklı olduğunu göstermek kolaydır. O halde aşağıdaki teorem verilebilir.

3.4.2. Teorem. $p \equiv 1 \pmod 4$ bir asal olsun. $y^2 = x^3 - n^2 x$ $(n \in \mathbb{F}_p{}^*)$ denkleminin çözümlerinin oluşturduğu grup $a^2 b = p + 1 - t$ mertebeli $\mathbb{Z}_a \times \mathbb{Z}_{a.b}$ grubuna izomorf ise bunun eşleniği $d^2 e = p + 1 + t$ mertebeli $\mathbb{Z}_d \times \mathbb{Z}_{d.e}$ grubuna izomorftur.

3.4.3. Örnek. $y^2 \equiv x^3 - 1^2 x \pmod{541}$ kongrüans denkliğini ele alalım. Bu eğri için $1 \in Q_{541}$, $N_{577,2} = 584$ ve grup yapısı $\mathbb{Z}_2 \times \mathbb{Z}_{292}$'dır. $N = a^2 b = p + 1 - t$ bağıntısına göre $584 = 2^2.146 = 541 + 1 - t$ iken $t = -42$ olur. $y^2 \equiv x^3 - 539^2 x \pmod{541}$ kongrüans denkliği için ise, $539 \in Q'_{541}$, $N_{541,539} = 500$ ve grup yapısı $\mathbb{Z}_{10} \times \mathbb{Z}_{50}$'dır. Nokta sayısı formülüne göre $500 = 10^2.5 = 541 + 1 - t$ iken $t = 42$ bulunur.

3.4.4. Teorem.

a) $p \equiv 1 \pmod 8$ bir asal olsun. Bu durumda

i) $t \equiv 2 \pmod 8$ olması için gerek ve yeter şart $N \equiv 0 \pmod 8$

ii) $t \equiv 6 \pmod 8$ olması için gerek ve yeter şart $N \equiv 4 \pmod 8$

olmasıdır.

b) $p \equiv 5 \pmod 8$ bir asal olsun. Bu durumda

i) $t \equiv 2 \pmod 8$ olması için gerek ve yeter şart $N \equiv 4 \pmod 8$

ii) $t \equiv 6 \pmod 8$ olması için gerek ve yeter şart $N \equiv 0 \pmod 8$

olmasıdır.

İspat a) $p \equiv 1 \pmod 8$ bir asal olsun. Bunu $n \in \mathbb{Z}$ iken $p = 1 + 8n$ şeklinde yazabiliriz. $t \equiv 2 \pmod 8$'den $m \in \mathbb{Z}$ olmak üzere $t = 2 + 8m$ şeklinde ifade edebiliriz. Bunları nokta sayısı formülünde yerine koyarsak

$$t \equiv 2 \pmod 8 \Leftrightarrow N = p+1-t$$
$$= 1+8n+1-(2+8m)$$
$$= 8(n-m)$$
$$\Leftrightarrow N \equiv 0 \pmod 8$$

ve benzer olarak

$$t \equiv 6 \pmod 8 \Leftrightarrow N = p+1-t$$
$$= 1+8n+1-(6+8m)$$
$$= -4+8(n-m)$$
$$\Leftrightarrow N \equiv 4 \pmod 8$$

elde edilir. b) şıkkı da benzer yolla ispat edilir.

3.4.5. Örnek. $p = 281 \equiv 1 \pmod 8$ bir asal iken $y^2 \equiv x^3 - 14^2 x \pmod{281}$ kongrüans denkliği ele alındığında. $N_{281,14} = 272$ ve $t = 10 \equiv 2 \pmod 8$ ve $N = 272 \equiv 0 \pmod 8$ 'dır. Şimdi de $p = 461 \equiv 5 \pmod 8$ bir asal olmak üzere $y^2 \equiv x^3 - 433^2 x \pmod{461}$ kongrüans denkliğini ele alalım. $N_{461,433} = 500$ ve $t = -38 \equiv 2 \pmod 8$ ve $N = 500 \equiv 4 \pmod 8$ 'dır.

3.4.6. Teorem. $p \equiv 1 \pmod 4$ bir asal olsun. Bu durumda t, 4 ile bölünemez.

İspat Tersine t'nin 4 ile bölündüğünü varsayalım. Bu durumda $k \in \mathbb{Z}$ için $t = 4k$ ve $n \in \mathbb{N}$ için $p = 1+4n$ yazarsak $N = 1+4n+1-4k$ elde ederiz. Bu da $N \equiv 2 \pmod 4$ oluşunu gerektirir. Fakat N, 4 modunda 2'ye denk olamaz. $N \equiv 0 \pmod 4$ 'tür. Bu da varsayımla çelişir. Bu yüzden t, 4 ile bölünemez.

3.4.7. Örnek. $p = 397 \equiv 1 \pmod 4$ bir asal iken $y^2 \equiv x^3 - 43^2 x \pmod{397}$ kongrüans denkliğini ele alalım. $N_{397,43} = 360$ 'dır. $N = p+1-t$ formülünden $t = 38$ bulunur. $4 \nmid 38$ 'dir. Ayrıca $y^2 \equiv x^3 - 103^2 x \pmod{257}$ kongrüans denkliği de incelenirse $N_{257,103} = 260$ 'tır. Sonuç olarak nokta sayısı formülünden $t = -2$ bulunur. Yine $4 \nmid -2$ 'dır.

3.4.8. Sonuç. $p \equiv 1 \pmod 4$ asal olsun. Bu durumda $N \equiv 0$ veya $N \equiv 4 \pmod 8$ olur.

3.4.9. Örnek. $y^2 \equiv x^3 - 289^2 x \pmod{389}$ kongrüans denkliğini ele alalım. Nokta sayısı $N_{389,289} = 424$'tür. O halde $N \equiv 0 \pmod 4$'dır. $y^2 \equiv x^3 - 33^2 x \pmod{389}$ kongrüans denkliği için ise $N_{389,33} = 356$'tır. O halde $N \equiv 4 \pmod 8$'dır.

Böylece $p \equiv 1 \pmod 4$ asal iken $\mathbb{F}_p$ sonlu cisimleri üzerindeki $y^2 = x^3 - n^2 x$ Frey Diophnat Denklemlerinin çözümlerinin oluşturdukları grupların hangi gruba izomorf olduğunu ifade edebiliyoruz. Ancak diğer hallerde için grup yapısı hakkında bir şey söyleyemiyoruz. $p \equiv 1 \pmod 4$ bir asal olmak üzere E_n eğrisi karşılık gelen Frey Diophant denkleminin çözüm noktalarının oluşturduğu grup yapısının $E_n(\mathbb{F}_p) \cong \mathbb{Z}_a \times \mathbb{Z}_{a.b}$ olduğu ve bunun eşleniğinin de $\mathbb{Z}_d \times \mathbb{Z}_{d.e}$ olduğunu ifade edebiliriz.

Çalışmada, $p \equiv 1 \pmod 4$ bir asal olmak üzere $\mathbb{F}_p$ sonlu cisimleri üzerindeki $E_n : y^2 = x^3 - n^2 x$ eğrisine karşılık gelen denklemin çözümü olan noktaların grup yapısı ile ilgili tablo aşağıda verilmiştir.

$p \le 113$ Asal Ve $p \equiv 1 \pmod 4$ İçin Frey Eliptik Eğrilerine Karşılık Gelen Diophant Denklemlerinin Ve Eşleniklerinin Çözümleri Olan Noktaların Oluşturduğu Grupların Mertebe, Eleman Sayıları Ve Grup Yapısı Tablosu

	$n \in Q_p$		$n \notin Q_p$	
p=5	**Mertebe**	**Eleman sayısı**	**Mertebe**	**Eleman sayısı**
	2	**3**	**2**	**3**
	4	**4**		
	$C_2 \times C_4$		$C_2 \times C_2$	

p=13	**Mertebe**	**Eleman sayısı**	**Mertebe**	**Eleman sayısı**
	2	**3**	**2**	**3**
	4	**4**	**5**	**4**
			10	**12**
	$C_2 \times C_4$		$C_2 \times C_{10}$	

p=17	Mertebe	Eleman sayısı	Mertebe	Eleman sayısı
	2	3	2	3
	4	12	5	4
			10	12
	$C_4 \times C_4$		$C_2 \times C_{10}$	

p=29	Mertebe	Eleman sayısı	Mertebe	Eleman sayısı
	2	3	2	3
	4	4	5	4
	5	4	10	12
	10	12		
	20	16		
	$C_2 \times C_{20}$		$C_2 \times C_{10}$	

p=37	Mertebe	Eleman sayısı	Mertebe	Eleman sayısı
	2	3	2	3
	4	4	3	8
	5	4	6	24
	10	12		
	20	16		
	$C_2 \times C_{20}$		$C_6 \times C_6$	

	$n \in Q_p$		$n \notin Q_p$	
p=41	Mertebe	Eleman sayısı	Mertebe	Eleman sayısı
	2	3	2	3
	4	12	13	12
	8	16	26	36
	$C_4 \times C_8$		$C_2 \times C_{26}$	

p=53	Mertebe	Eleman sayısı	Mertebe	Eleman sayısı
	2	3	2	3
	4	4	17	16
	5	4	34	49
	10	12		
	20	16		
	$C_2 \times C_{20}$		$C_2 \times C_{34}$	

p=61	Mertebe	Eleman sayısı	Mertebe	Eleman sayısı
	2	3	2	3
	3		13	
	4	4	26	
	6			
	12			
	$C_6 \times C_{12}$		$C_2 \times C_{26}$	

p=73	Mertebe	Eleman sayısı	Mertebe	Eleman sayısı
	2	3	2	3
	4	12	17	
	5		34	
	10			
	20			
	$C_4 \times C_{20}$		$C_2 \times C_{34}$	

p=89	Mertebe	Eleman sayısı	Mertebe	Eleman sayısı
	2	3	2	3
	4	12	5	
	5		10	
	10		25	
	20		50	
	$C_4 \times C_{20}$		$C_2 \times C_{50}$	

p=97	Mertebe	Eleman sayısı	Mertebe	Eleman sayısı
	2	3	2	3
	4	12	29	
	5		58	
	10			
	20			
	$C_4 \times C_{20}$		$C_2 \times C_{58}$	

p=101	Mertebe	Eleman sayısı	Mertebe	Eleman sayısı
	2	3	2	3
	4	4	5	
	13		10	
	26			
	52			
	$C_2 \times C_{52}$		$C_{10} \times C_{10}$	

p=109	Mertebe	Eleman sayısı	Mertebe	Eleman sayısı
	2	3	2	3
	4	4	29	
	13		58	
	26			
	52			
	$C_2 \times C_{52}$		$C_2 \times C_{58}$	

p=113	Mertebe	Eleman sayısı	Mertebe	Eleman sayısı
	2	3	2	3
	4	12	5	
	8		10	
	16		25	
			50	
	$C_8 \times C_{16}$		$C_2 \times C_{50}$	

EKLER

>\# y^2=x^3+a^3 (mod p) EĞRİSİ ÜZERİNDEKİ RASYONEL NOKTA SAYISINI HESAPLAMA#

```
> restart;
> p:=prime;a:=int;n:=posint;l:int;
> hesapla:=proc(p,a);
> n:=p+1;
>  for x from 0 to p-1 do
>   with(numtheory):
>    l:=legendre(x^3+a^3,p);
>    n:=n+l;
>  end do;
> end proc;
> hesapla(p,a);
```

ÖRNEK

```
> #y^2=x^3+24^3 (mod 1723) Eğrisi Üzerindeki Rasyonel Nokta
Sayısını Hesaplama#
> restart;
> p:=prime;a:=int;n:=posint;l:int;
> hesapla:=proc(p,a);
> n:=p+1;
>  for x from 0 to p-1 do
>   with(numtheory):
>    l:=legendre(x^3+a^3,p);
>    n:=n+l;
>  end do;
> end proc;
```

Warning, `n` is implicitly declared local to procedure `hesapla`

Warning, `x` is implicitly declared local to procedure `hesapla`

Warning, `l` is implicitly declared local to procedure `hesapla`

```
hesapla := proc(p, a)
local n, x, l;
    n := p + 1;
    for x from 0 to p - 1 do
        with(numtheory); l := legendre(x^3 + a^3, p); n := n + l
    end do
end proc
```

```
> hesapla(1723,24);
```

Warning, the protected name order has been redefined and unprotected

1764

```
> # P MODUNDA İKİNCİ DERECEDEN KALANLARI HESAPLAMA#
> restart;
> p:=prime;x:=int;s:=int;
> hesapla:=proc(p);
>  for x from 1 to p-1 do
>   with(numtheory):
>       s:=mroot(x,2,p);
>   if s<>FAIL then
>    print(x);
>   end if;
>  end do;
> end proc;
> hesapla(p);
```

ÖRNEK

```
>#Q31'i Hesaplama#
> restart;
> p:=prime;x:=int;s:=int;
> hesapla:=proc(p);
>  for x from 1 to p-1 do
>   with(numtheory):
```

```
>       s:=mroot(x,2,p);
>   if s<>FAIL then
>    print(x);
>   end if;
>  end do;
>end proc;
>hesapla(31);
```

$p := prime$

$x := int$

$s := int$

Warning, `x` is implicitly declared local to procedure `hesapla`

Warning, `s` is implicitly declared local to procedure `hesapla`

hesapla := **proc**(*p*)
local *x*, *s*;
    for *x* **to** *p* − 1 **do**
        with(*numtheory*); *s* := mroot(*x*, 2, *p*); **if** *s* ≠ *FAIL* **then** print(*x*) **end if**
    end do
end proc

Warning, the protected name order has been redefined and unprotected

1

2

4

5

7

8

9

10

14

16

18

19

20

25

28

```
> # p=1 (mod 6) ASALLARI LİSTELER #
>restart;
>asallistele:=proc(n);
>x:=int;a:=prime;i:=int;
> for i from 1 while ithprime(i)< n do
> with(numtheory):
>   a:=ithprime(i);
> x:=a mod 6;
>  if x = 1 then
>     lprint(a);
>    end if;
> end do;
>end proc;
>asallistele(n);
```

```
> # p=5 (mod 6) ASALLARI LİSTELER #
>restart;
>asallistele:=proc(n);
>x:=int;a:=prime;i:=int;
> for i from 1 while ithprime(i)< n do
> with(numtheory):
>   a:=ithprime(i);
> x:=a mod 6;
>  if x = 5 then
>     lprint(a);
>    end if;
> end do;
>end proc;
>asallistele(n);
```

```
> #y^2=x^3+a^3 (mod p) EĞRİSİNDEKİ NOKTALARIN MERTEBELERİNİ
BULMA#
```

```
> restart;
> mertebe:=proc(x1,y1,p);
>x:=int;y:=int;x2:=int;y2:=int;
> n:=2;
> if y1<>0 then
>    n:=n+1;
>    m:=((3*x1^2)/(2*y1)) mod p;
>    x:=(m^2-x1-x1) mod p;
>    y:=(m*(x1-x)-y1) mod p;
>    #print([x,y],"mertebe:",n);
>    x2:=x;y2:=y;
>    while x<>x1 or y<>p-y1 do
>          n:=n+1;
>         m:=((y-y1)/(x-x1)) mod p;
>         x:=(m^2-x-x1) mod p;
>         y:=(m*(x2-x)-y2) mod p;
>        #print([x,y],"mertebe:",n);
>         x2:=x;y2:=y;
>    end do;
>print("mertebe:",n);
> else  print("mertebe:",n);
>end if;
>end proc;
>hesapla:=proc(p,a);
> xgec:=int;ygec:=int;l:=int;
> for xgec from 0 to p-1 do
>  with(numtheory);
>  l:=xgec^3+a^3;
>  ygec:=msqrt(l,p);
>  if   ygec<>FAIL  then
>      if ygec<>0 then
>   print([xgec,ygec],[xgec,-ygec]);
>      else
>   print([xgec,ygec]);
```

```
>   end if;
>  mertebe(xgec,ygec,p);
>   end if;
> end do;
>end proc;
>hesapla(p,a);
```

ÖRNEK

```
>#y^2=x^3+4^3 (mod 19) EĞRİSİNDEKİ NOKTALARIN MERTEBELERİNİ
BULMA#
>restart;
>mertebe:=proc(x1,y1,p);
>x:=int;y:=int;x2:=int;y2:=int;
>n:=2;
>if y1<>0 then
>    n:=n+1;
>    m:=((3*x1^2)/(2*y1)) mod p;
>    x:=(m^2-x1-x1) mod p;
>    y:=(m*(x1-x)-y1) mod p;
>    #print([x,y],"mertebe:",n);
>    x2:=x;y2:=y;
>    while x<>x1 or y<>p-y1 do
>          n:=n+1;
>         m:=((y-y1)/(x-x1)) mod p;
>         x:=(m^2-x-x1) mod p;
>         y:=(m*(x2-x)-y2) mod p;
>        #print([x,y],"mertebe:",n);
        x2:=x;y2:=y;
>    end do;
>print("mertebe:",n);
>else  print("mertebe:",n);
>end if;
>end proc;
```

```
`Warning, \`x\` is implicitly declared local to procedure \`mertebe\`\n`
`Warning, \`y\` is implicitly declared local to procedure \`mertebe\`\n`
`Warning, \`x2\` is implicitly declared local to procedure \`mertebe\`\n`
`Warning, \`y2\` is implicitly declared local to procedure \`mertebe\`\n`
`Warning, \`n\` is implicitly declared local to procedure \`mertebe\`\n`
`Warning, \`m\` is implicitly declared local to procedure \`mertebe\`\n`
mertebe := proc(x1, y1, p)
local x, y, x2, y2, n, m;
    x := int;
    y := int;
    x2 := int;
    y2 := int;
    n := 2;
    if y1 ≠ 0 then
        n := n + 1;
        m := (3/2×x1^2/y1) mod p;
        x := (m^2 – 2×x1) mod p;
        y := (m×(x1 – x) – y1) mod p;
        x2 := x;
        y2 := y;
        while x ≠ x1 or y ≠ p – y1 do
            n := n + 1;
            m := (y – y1)/(x – x1) mod p;
            x := (m^2 – x – x1) mod p;
            y := (m×(x2 – x) – y2) mod p;
            x2 := x;
            y2 := y
        end do ;
        print("mertebe:", n)
    else print("mertebe:", n)
    end if
end proc
> hesapla:=proc(p,a);
>xgec:=int;ygec:=int;l:=int;
> for xgec from 0 to p-1 do
> with(numtheory);
> l:=xgec^3+a^3;
```

```
> ygec:=msqrt(l,p);
> if   ygec<>FAIL  then
>if ygec<>0 then
 >print([xgec,ygec],[xgec,-ygec]);
 >else
 >print([xgec,ygec]);
>end if;
>mertebe(xgec,ygec,p);
> end if;
> end do;
> end proc;
```

Warning, `xgec` is implicitly declared local to procedure `hesapla`

Warning, `ygec` is implicitly declared local to procedure `hesapla`

Warning, `l` is implicitly declared local to procedure `hesapla`

```
hesapla := proc(p, a)
local xgec, ygec, l;
    xgec := int;
    ygec := int;
    l := int;
    for xgec from 0 to p - 1 do
        with(numtheory);
        l := xgec^3 + a^3;
        ygec := msqrt(l, p);
        if ygec ≠ FAIL then
            if ygec ≠ 0 then print([xgec, ygec], [xgec, –ygec])
            else print([xgec, ygec])
            end if;
            mertebe(xgec, ygec, p)
        end if
    end do
end proc
```

```
> hesapla(19,4);
```

Warning, the protected name order has been redefined and unprotected

[0, 8], [0, -8]

"mertebe:", 3

[8, 5], [8, -5]
"mertebe:", 6
[10, 0]
"mertebe:", 2
[12, 5], [12, -5]
"mertebe:", 6
[13, 0]
"mertebe:", 2
[15, 0]
"mertebe:", 2
[18, 5], [18, -5]
"mertebe:", 6

 # Eliptik Eğri Üzerindeki Noktaların Mertebelerini Hesaplar # Visual Basic

```
Sub Makro1()
        j = 2
        Do While Sheets(1).Cells(j, 1) <> "son"
          i = 2
          x1 = Sheets(1).Cells(j, 1)
          y1 = Sheets(1).Cells(j, 2)
          k = Sheets(1).Cells(j, 3)
          a = Sheets(1).Cells(j, 4)
          If y1 <> 0 Then
            i = i + 1
            m1 = (3 * x1 * x1 + a)
            m2 = (2 * y1)
            Sheets(2).Cells(1, 1) = m1
            Sheets(2).Cells(1, 2) = m2
            Sheets(2).Cells(2, 1) = "=MOD(R[-1]C,R[-1]C[1])"
            Do While Sheets(2).Cells(2, 1) <> 0
              m1 = m1 + k
              Sheets(2).Cells(1, 1) = m1
              Sheets(2).Cells(1, 2) = m2
             Sheets(2).Cells(2, 1) = "=MOD(R[-1]C,R[-1]C[1])"
```

```
Loop
m = m1 / m2
Sheets(3).Cells(1, 1) = m
Sheets(3).Cells(2, 1) = "=MOD(R[-1]C,'1'!RC[2])"
m = Sheets(3).Cells(2, 1)
x = m * m - x1 - x1
y = m * (x1 - x) - y1
Sheets(3).Cells(1, 2) = x
Sheets(3).Cells(2, 2) = "=MOD(R[-1]C,'1'!RC[1])"
Sheets(3).Cells(1, 3) = y
Sheets(3).Cells(2, 3) = "=MOD(R[-1]C,'1'!RC[0])"
x = Sheets(3).Cells(2, 2)
y = Sheets(3).Cells(2, 3)
x2 = x
y2 = y

Do While x <> x1 Or y <> (k - y1)
   i = i + 1
   m1 = y - y1
   m2 = x - x1
   Sheets(2).Cells(1, 1) = m1
   Sheets(2).Cells(1, 2) = m2
   Sheets(2).Cells(2, 1) = "=MOD(R[-1]C,R[-1]C[1])"
   Do While Sheets(2).Cells(2, 1) <> 0
      m1 = m1 + k
      Sheets(2).Cells(1, 1) = m1
      Sheets(2).Cells(1, 2) = m2
      Sheets(2).Cells(2, 1) = "=MOD(R[-1]C,R[-1]C[1])"
   Loop
   m = m1 / m2
   Sheets(3).Cells(1, 1) = m
   Sheets(3).Cells(2, 1) = "=MOD(R[-1]C,'1'!RC[2])"
   m = Sheets(3).Cells(2, 1)
   x = m * m - x - x1
   y = m * (x2 - x) - y2
```

```
            Sheets(3).Cells(1, 2) = x
            Sheets(3).Cells(2, 2) = "=MOD(R[-1]C,'1'!RC[1])"
            Sheets(3).Cells(1, 3) = y
            Sheets(3).Cells(2, 3) = "=MOD(R[-1]C,'1'!RC[0])"
            x = Sheets(3).Cells(2, 2)
            y = Sheets(3).Cells(2, 3)
            x2 = x
            y2 = y

        Loop
        Sheets(1).Cells(j, 5) = i
    End If
    j = j + 1
    Loop

End Sub

Sub xolus()
    ' xolus Makro
    'Sheets("nokta belirle").Columns("A:A").Select
    'Selection.ClearContents
    Sheets("nokta belirle").Cells(1, 1) = "x"
    Sheets("grafik veri").Cells(1, 1) = "x"
    Sheets("grafik veri").Cells(1, 2) = "y"
    td = Sheets("nokta belirle").Cells(2, 2)
    gg = 1
    sat = 2
    j = 2
    For md = 0 To td - 1
        Sheets("nokta belirle").Cells(md + 2, 2) = td
        Sheets("nokta belirle").Cells(md + 2, 1) = md
        Sheets("nokta belirle").Cells(md + 2, 5) = md ^ 3 + a * md + Sheets("nokta
    belirle").Cells(2, 4)
        Sheets("nokta belirle").Cells(md + 2, 6) = "=MOD(R[0]C[-1],RC[-4])"
```

```
ag = Sheets("nokta belirle").Cells(md + 2, 6)
   For yf = 0 To td - 1
      For ch = 0 To td - 1
         If ((yf * yf) - ch * td) = ag Then
            gg = gg + 1
            Sheets(1).Cells(gg, 1) = Sheets("nokta belirle").Cells(2 + md, 1)
            Sheets(1).Cells(gg, 2) = yf
            Sheets(1).Cells(gg, 3) = Sheets("nokta belirle").Cells(2, 2)
            Sheets(1).Cells(gg, 4) = Sheets("nokta belirle").Cells(2, 3)
            i = 2
            x1 = Sheets(1).Cells(gg, 1)
            y1 = Sheets(1).Cells(gg, 2)
            k = Sheets(1).Cells(gg, 3)
            a = Sheets(1).Cells(gg, 4)
            Sheets(1).Cells(2, 2 * gg + 3) = x1
            Sheets(1).Cells(2, 2 * gg + 4) = y1
            Sheets("grafik veri").Cells(sat, 1) = x1
            Sheets("grafik veri").Cells(sat, 2) = y1
            sat = sat + 1
            Sheets(1).Cells(1, 2 * gg + 3) = "x"
            Sheets(1).Cells(1, 2 * gg + 4) = "y"
            Sheets(1).Cells(i, 6) = 1

         If y1 <> 0 Then
               i = i + 1
               m1 = (3 * x1 * x1 + a)
               m2 = (2 * y1)
               Sheets(2).Cells(1, 1) = m1
               Sheets(2).Cells(1, 2) = m2
               Sheets(2).Cells(2, 1) = "=MOD(R[-1]C,R[-1]C[1])"
               Do While Sheets(2).Cells(2, 1) <> 0
               m1 = m1 + k
                  Sheets(2).Cells(1, 1) = m1
                  Sheets(2).Cells(1, 2) = m2
                  Sheets(2).Cells(2, 1) = "=MOD(R[-1]C,R[-1]C[1])"
```

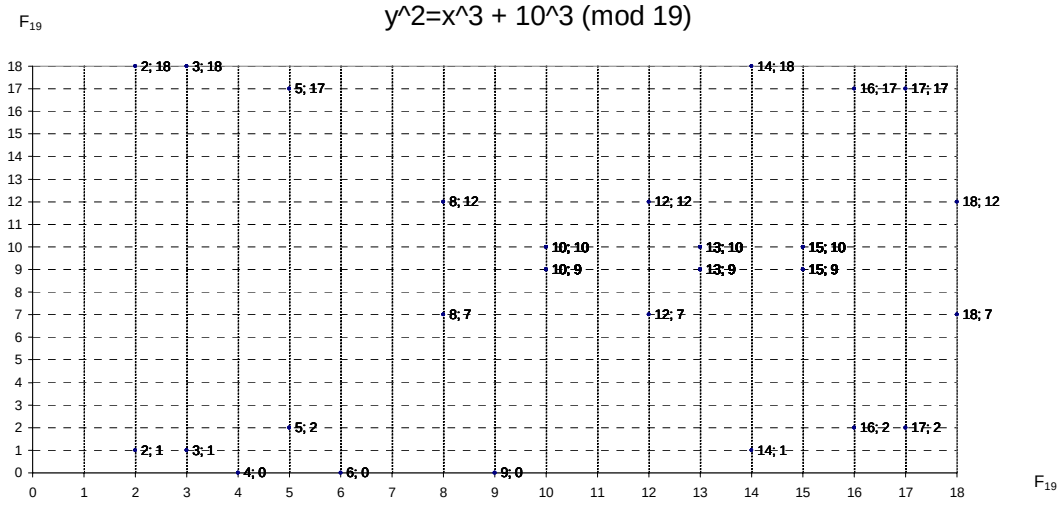
```
Loop
m = m1 / m2
Sheets(3).Cells(1, 1) = m
Sheets(3).Cells(2, 1) = "=MOD(R[-1]C,'1'!RC[2])"
m = Sheets(3).Cells(2, 1)
x = m * m - x1 - x1
y = m * (x1 - x) - y1
Sheets(3).Cells(1, 2) = x
Sheets(3).Cells(2, 2) = "=MOD(R[-1]C,'1'!RC[1])"
Sheets(3).Cells(1, 3) = y
Sheets(3).Cells(2, 3) = "=MOD(R[-1]C,'1'!RC[0])"
x = Sheets(3).Cells(2, 2)
y = Sheets(3).Cells(2, 3)
Sheets(1).Cells(i, 2 * gg + 3) = x
Sheets(1).Cells(i, 2 * gg + 4) = y
Sheets(1).Cells(i, 6) = i - 1
Sheets("grafik veri").Cells(sat, 1) = x
Sheets("grafik veri").Cells(sat, 2) = y
sat = sat + 1
x2 = x
y2 = y
Do While x <> x1 Or y <> (k - y1)
   i = i + 1
   m1 = y - y1
   m2 = x - x1
   Sheets(2).Cells(1, 1) = m1
   Sheets(2).Cells(1, 2) = m2
   Sheets(2).Cells(2, 1) = "=MOD(R[-1]C,R[-1]C[1])"
   Do While Sheets(2).Cells(2, 1) <> 0
      m1 = m1 + k
      Sheets(2).Cells(1, 1) = m1
      Sheets(2).Cells(1, 2) = m2
      Sheets(2).Cells(2, 1) = "=MOD(R[-1]C,R[-1]C[1])"
   Loop
```

```
                m = m1 / m2
                Sheets(3).Cells(1, 1) = m
                Sheets(3).Cells(2, 1) = "=MOD(R[-1]C,'1'!RC[2])"
                m = Sheets(3).Cells(2, 1)
                x = m * m - x - x1
                y = m * (x2 - x) - y2
                Sheets(3).Cells(1, 2) = x
                Sheets(3).Cells(2, 2) = "=MOD(R[-1]C,'1'!RC[1])"
                Sheets(3).Cells(1, 3) = y
                Sheets(3).Cells(2, 3) = "=MOD(R[-1]C,'1'!RC[0])"
                x = Sheets(3).Cells(2, 2)
                y = Sheets(3).Cells(2, 3)
                x2 = x
                y2 = y
              Sheets(1).Cells(i, 6) = i - 1
              Sheets(1).Cells(i, 2 * gg + 3) = x
              Sheets(1).Cells(i, 2 * gg + 4) = y
              Sheets("grafik veri").Cells(sat, 1) = x
              Sheets("grafik veri").Cells(sat, 2) = y
              sat = sat + 1
              Loop
              Sheets(1).Cells(j, 5) = i
            Else
              Sheets(1).Cells(j, 5) = 2
            End If
          j = j + 1
        End If
      Next
    Next
Next
End Sub
```

ÖRNEK

$y^2 \equiv x^3 + 10^3 \pmod{19}$ eliptik eğrisi üzerindeki noktaları, bu noktaların kuvvetlerini ve mertebelerini bulunuz.

x	y	MOD	a	MERTEBE	KUVVET	x	y	x	y	x	y	x	y	x	y	x	y	x	y	x	y	x	y	x	y	x	y	x	y	x	y	x	y	x	y	x	y	x	y
2	1	19	10	14	1	2	1	2	18	3	1	3	18	4	0	5	2	5	17	6	0	8	7	8	12	9	0	10	9	10	10	12	7	12	12	13	9	13	10	14	1	14	18	15	9
2	18	19	10	14	2	13	9	13	10	10	9	10	10			15	10	15	9			10	9	10	10			15	9	15	10	15	9	15	10	10	9	10	10	15	9	15	10	13	9
3	1	19	10	14	3	5	2	5	17	17	2	17	17			8	7	8	12			2	18	2	1			13	10	13	9	3	18	3	1	15	10	15	9	16	2	16	17	10	10
3	18	19	10	14	4	10	9	10	10	15	9	15	10			13	10	13	9			15	9	15	10							13	9	13	10					13	9	13	10		
4	0	19	10	2	5	8	12	8	7	12	12	12	7			2	1	2	18			5	2	5	17							17	2	17	17					18	12	18	7		
5	2	19	10	14	6	15	10	15	9	13	10	13	9			10	9	10	10			13	10	13	9							10	10	10	9					10	10	10	9		
5	17	19	10	14	7	9	0	9	0	4	0	4	0			9	0	9	0			9	0	9	0							4	0	4	0					6	0	6	0		
6	0	19	10	2	8	15	9	15	10	13	9	13	10			10	10	10	9			13	9	13	10							10	9	10	10					10	9	10	10		
8	7	19	10	14	9	8	7	8	12	12	7	12	12			2	18	2	1			5	17	5	2							17	17	17	2					18	7	18	12		
8	12	19	10	14	10	10	10	10	9	15	10	15	9			13	9	13	10			15	10	15	9							13	10	13	9					13	10	13	9		
9	0	19	10	2	11	5	17	5	2	17	17	17	2			8	12	8	7			2	1	2	18							3	1	3	18					16	17	16	2		
10	9	19	10	4	12	13	10	13	9	10	10	10	9			15	9	15	10			10	10	10	9							15	10	15	9					15	10	15	9		
10	10	19	10	4	13	2	18	2	1	3	18	3	1			5	17	5	2			8	12	8	7							12	12	12	7					14	18	14	1		
12	7	19	10	14																																									
12	12	19	10	14																																									
13	9	19	10	4																																									
13	10	19	10	4																																									
14	1	19	10	14																																									
14	18	19	10	14																																									
15	9	19	10	4																																									
15	10	19	10	4																																									
16	2	19	10	14																																									
16	17	19	10	14																																									
17	2	19	10	14																																									
17	17	19	10	14																																									
18	7	19	10	14																																									
18	12	19	10	14																																									



KAYNAKLAR

Andrews, G. E. 1971. Number Theory. Dover Publications Inc, New York, 259 p.

Andrews, G. E. 1961. An Asymptotic Expression for the Number of Solution of a General Class of Diophantine Equations. Transactions of the American Mathmetical Society, Vol 99 (2): 272-277

Baker, A. 1968. Contribution to the Theory of Diophantine Equations. II. The Diophantine Equation $y^2 = x^3 + k$. Philosophical Transactions of the Royal Society of London, Vol 263, (1139): 193-208

Bashmakova, I., G. 1997. Diophantus And Diophantine Equations. The Mathematical Association of America, Washington DC, 90 p.

Bremner, A. 1975. An Equation of Mordell. Mathematics of Computation, Volume 29, Number 131, July: 925-928.

Çelik, B. 2004. Maple ve Maple ile Matematik. Nobel Yayın Dağıtım, Yenişehir. Ankara, 561 s.

Davis, M. 1972. On The Number of Solution of Diophantine Equations. Proceedings of The American Mathmetical Society, 35 (2): 552-554.

Demirci, M., G. Soydan, İ. N. Cangül. 2005. Rational points on the elliptic curves $y^2 \equiv x^3 + a^3 \pmod{p}$ in F_p where $p \equiv 1 \pmod 6$ is prime. Rocky J. of Maths, (basımda).

Grinstead, C. M. 1978. On a Method of Solving a Class of Diophantine Equations. Mathematics of Computation, Vol 32, (143): 936-940

Hellegouarch, Y. 2002. Invitation to the Mathematics of Fermat-Wiles. Academic Press, London,381 p.

Kato, K., N. Kurokawa, T. Saito. 2000. Number Theory 1 Fermat's Dream. American Mathematical Society, United States of America, 154 p.

Kim, D., J. K. Koo, M. H. Kim. 2005. Congruence Equations of $ax^i + by^j \equiv c$ and $ax^i + by^j + dz^t \equiv c \pmod{p}$ when $p = 2q + 1$ with p ve q Odd Primes. Communications of the Korean Mathmetical Society, Vol 20, (3): 467-485

Knapp, A. W. 1992. Elliptic Curves. Princeton University Pres, New Jersey, 427 p.

Koblitz, N. 1994. A Course in Number Theory and Cryptography. Springer-Verlag New york Inc, 235 p.

Le Veque, W., J. 1997. Fundamentals Of Number Theory. Dover Publications, New York, 280 p.

Mason, R.C. 1999. Diophantine Equations Over Function Field. Cambridge University Press, Cambridge, 125 p.

Mollin, R. A. 2001. An Introduction to Cryptography. Chapman&Hall/CRC, United States of America, 373 p.

Namlı, D. 2001. Kübik Rezidüler. Doktora Tezi. Balıkesir Üniversitesi (yayımlanmamış), Balıkesir, 74 s.

Ribenboim, P. 1999. Fermat's Last Theorem for Amateurs. Springer-Verlag, New York Inc, 407 p.

Silverman, J. H. 1986. The Arithmetic of Elliptic Curves. Springer-Verlag, New York Inc, 400 p.

Silverman, J. H., J. Tate. 1992. Rational Points on Elliptic Curves. Springer-Verlag, New York Inc, 281 p.

Smart, N. P. 1998. The Algorithmic Resolution of Diophantine Equations, London Mathematical Society, Cambridge, 243 p.

Soydan, G. 2005. Sonlu Cisimler Üzerinde Bachet Eliptik Eğrileri. Doktora Tezi. Uludağ Üniversitesi (yayımlanmamış), Bursa, 82 p.

Yıldız İkikardeş, N. 2006. Sonlu Cisimler Üzerinde Frey Eliptik Eğrileri. Doktora Tezi. Balıkesir Üniversitesi (yayımlanmamış), Balıkesir, 91 p.

İNDEKS

ÖZGEÇMİŞ

08. 01. 1978 yılında Sakarya'da doğmuş olan Musa DEMİRCİ ilk ve orta okulu Adapazarı İsmet İnönü İlköğretim Okulu'nda, liseyi ise Adapazarı Ali Dilmen Lisesi'nde bitirmiştir. 1995 yılında Muğla Üniversitesi Fen-Edebiyat Fakültesi Matematik Bölümü'nü kazanmış 1997 yılında Uludağ Üniversitesi Fen-Edebiyat Fakültesi Matematik Bölümü'ne yatay geçiş yapmıştır. 2000 yılında mezun olup aynı yıl Uludağ Üniversitesi Fen Bilimleri Enstitüsü'nde Yüksek Lisansına başlamıştır. Yine 2000 yılında Uludağ Üniversitesi Fen Edebiyat Fakültesi Matematik Bölümü'nde Arş. Gör. Kadrosunda göreve başlamıştır. 2002 yılında Uludağ Üniversitesi Fen Bilimleri Enstitüsü'nde Doktora çalışmasına başlamış olan Musa DEMİRCİ halen Fen-Edebiyat Fakültesi'ndeki görevine devam etmektedir.

TEŞEKKÜR

Çok uzun olmasa da akademik yaşantımın başından itibaren daima sabrı, desteği ve bilgisi ile örnek aldığım danışman hocam Sayın Prof. Dr. İsmail Naci CANGÜL'e içtenlikle teşekkür ederim.

Ayrıca lisans üstü eğitimimin başlangıcından itibaren birlikte çalıştığımız arkadaşlarım Dr. Gökhan SOYDAN ve Öğr. Gör. Dr. Nazlı YILDIZ İKİKARDEŞ, size de teşekkürler...

Bugün, bir Doktora çalışması yapabilecek bir aşamaya gelmemde maddi, manevi desteklerini eksik etmeyen anneme, babama ve ağabeyime de teşekkürü borç bilirim.

Tüm bunların yanı sıra bu uzun ve uzun olduğu kadar da yorucu çalışma döneminde sonsuz desteğini, sabrını, sevgisini hiçbir zaman eksik etmeyen ve bana daima güvenen sevgili eşim Elif'e çok teşekkür ederim. Bu çalışmanın başlangıcında dünyaya geldiği için belki de bu döneminde biraz ihmal etmiş olduğum canım oğlum Osman Sina'ya da bana çalışma azmi verdiği için sonsuz teşekkürler…