T.C.
BALIKESİR ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI

SONLU CİSİMLER ÜZERİNDE FREY ELİPTİK EĞRİLERİ

DOKTORA TEZİ

Nazlı YILDIZ İKİKARDEŞ

Balıkesir, Nisan – 2006

T.C.
BALIKESİR ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI

SONLU CİSİMLER ÜZERİNDE FREY ELİPTİK EĞRİLERİ

DOKTORA TEZİ

Nazlı YILDIZ İKİKARDEŞ

Balıkesir, Nisan – 2006

T.C.
BALIKESİR ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI

SONLU CİSİMLER ÜZERİNDE FREY ELİPTİK EĞRİLERİ

DOKTORA TEZİ

Nazlı YILDIZ İKİKARDEŞ

Bu çalışma 2005/08 nolu proje ile Balıkesir Üniversitesi Rektörlüğü Bilimsel Araştırma Projeleri Birimi tarafından desteklenmiştir.

Balıkesir, Nisan – 2006

T.C.
BALIKESİR ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI

SONLU CİSİMLER ÜZERİNDE FREY ELİPTİK EĞRİLERİ

DOKTORA TEZİ

Nazlı YILDIZ İKİKARDEŞ

Tez Danışmanı : Prof. Dr. İsmail Naci CANGÜL

İkinci Danışman : Yrd. Doç. Dr. Dilek NAMLI

Sınav Tarihi : 13. 04. 2006

Jüri Üyeleri : Prof. Dr. İsmail Naci CANGÜL (Danışman-U.Ü.)

Doç. Dr. Osman BİZİM (U.Ü.)

Doç. Dr. Ahmet Sinan ÇEVİK (BA.Ü.)

Yrd. Doç. Dr. Setenay DOĞAN (U.Ü.)

Yrd. Doç. Dr. Recep ŞAHİN (BA.Ü.)

Balıkesir, Nisan – 2006

ÖZET

SONLU CİSİMLER ÜZERİNDE FREY ELİPTİK EĞRİLERİ

Nazlı YILDIZ İKİKARDEŞ
Balıkesir Üniversitesi, Fen Bilimleri Enstitüsü,
Matematik Anabilim Dalı

(Doktora Tezi / Tez Danışmanı : Prof. Dr. İsmail Naci CANGÜL)
(İkinci Danışman : Yrd. Doç. Dr. Dilek NAMLI)

Balıkesir, 2006

Bu çalışmada, p asal iken $\mathbb{F}_p$ sonlu cisimlerinde basitleştirilmiş Weierstrass denkleminin özel bir hali olan $y^2 = x^3 - n^2 x$ Frey eliptik eğrileri üzerindeki nokta sayısı, noktaların mertebeleri ve bu eğrilerin grup yapıları incelenmiştir.

Bu çalışma beş bölümden oluşmaktadır. Giriş bölümü olan birinci bölümde çalışma tanıtılmıştır.

İkinci bölümde, çalışma boyunca gerekli olan temel tanım ve teoremler verilmiştir.

Üçüncü bölümde, $y^2 = x^3 - n^2 x$ Frey eliptik eğrilerinin nokta sayıları ile ilgili bazı sonuçlar verilmiştir.

Dördüncü bölümde, $y^2 = x^3 - n^2 x$ Frey eliptik eğrisinin $\mathbb{F}_p$ sonlu cismi üzerindeki grup yapısı incelenmiştir. Grup yapısının, p 'nin 4 modunda 1'e ve 3'e denk olmasına göre iki tip olduğundan bahsedilmiştir. $p \equiv 1 \pmod 4$ bir asal olmak üzere E_n eğrisi üzerindeki rasyonel noktaların grup yapısının, $a, b \in \mathbb{N}^+$ olmak üzere $E_n(\mathbb{F}_p) \cong \mathbb{Z}_a \times \mathbb{Z}_{a.b}$ olduğu gösterilmiştir. Bu eğrilerin grup yapısı incelenirken nokta sayısına da bakılmıştır. Ayrıca n 'nin Q_p 'de bulunup bulunmayışına göre grubun dördüncü mertebeden elemana sahip olup olmayacağı gösterilmiştir.

Beşinci bölümde, tezde elde edilen sonuçlar verilmiştir.

ANAHTAR SÖZCÜKLER : sonlu cisimler üzerinde eliptik eğriler / rasyonel noktalar / kübik denklemler / Frey eliptik eğrileri.

ABSTRACT

THE FREY ELLIPTIC CURVES ON FINITE FIELDS

Nazlı YILDIZ İKİKARDEŞ
Balıkesir University, Institute of Science, Department of Mathematics

(Ph. D. Thesis / Supervisor: Prof. Dr. İsmail Naci CANGÜL)
(Second Supervisor: Asst. Prof. Dr. Dilek NAMLI)

Balıkesir, 2006

In this thesis, the number of rational points, their orders, and the group structure of them, on Frey elliptic curves $y^2 = x^3 - n^2 x$ which are the special case of simplified Weierstrass equation over finite fields $\mathbb{F}_p$ where p is prime, are studied.

This study consists of five chapters. In the first chapter, which is the introductory chapter of this thesis, the thesis is introduced.

In the second chapter, the necessary definitions and results are recalled.

In the third chapter, some new results concerning the number of points on the Frey elliptic curves $y^2 = x^3 - n^2 x$ are given.

In the fourth chapter, the group structures of the Frey elliptic curves $y^2 = x^3 - n^2 x$ on finite fields $\mathbb{F}_p$ are obtained. It is shown that the group structure of these curves can be of two types according to that p is a prime congruent to 1 or 3 modulo 4. It has been shown that, in the former case, the group structure of rational points on the curve E_n is isomorphic to $E_n(\mathbb{F}_p) \cong \mathbb{Z}_a \times \mathbb{Z}_{a.b}$, where $a, b \in \mathbb{N}^+$. While considering the group structure of these curves, the number of rational points is also studied. Further, it has also been shown that whether the group has elements of order 4 according to whether n is in Q_p or not.

In the fifth chapter, the results obtained in the thesis are recalled.

KEY WORDS: elliptic curves over finite fields / rational points / cubic equations / Frey elliptic curves.

İÇİNDEKİLER

SEMBOL LİSTESİ

Simge	Adı
$\mathbb{Z}$	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_n	Frey 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
$N_{p,n}$	Frey eliptik eğrisi üzerindeki nokta sayısı

φ_q	q Frobenius endomorfizmi
t	Frobenius endomorfizminin izi
$j(E)$	E eğrisinin j-değişmezi
Δ	Weierstrass denkleminin diskriminantı
$C_a \times C_b$	a ve b mertebeli iki devirli grubun direkt çarpımı
$\mathbb{Q}[[T]]$	Katsayıları $\mathbb{Q}$'dan alınan kuvvet serileri halkası

ŞEKİL LİSTESİ

ÇİZELGE LİSTESİ

ÖNSÖZ

Çalışmalarımızın başlangıcından bugüne kadar desteğini hissettiğim, engin bilgileri sayesinde hep bir adım daha ileriye gittiğim, her yönüyle örnek almaya çalıştığım, yoğun çalışmaları arasında bana zaman ayırıp, katkılarını esirgemeyen, değerli danışman hocam Prof. Dr. İsmail Naci CANGÜL' e,

çok şeyler paylaştığımız değerli çalışma grubu arkadaşlarım Gökhan SOYDAN ve Musa DEMİRCİ' ye,

sayesinde birçok şey kazandığım değerli hocam Yrd. Doç. Dr. Dilek NAMLI' ya,

her türlü yardımını gördüğüm oda arkadaşım Devrim ÜZEL' e,

beni bugünlere getiren ve hala kahrımı çeken kıymetli annem ve babama,

benim için herkesin ve her şeyin ötesinde olan sevgili eşim Sebahattin' e,

sonsuz teşekkürler…

Balıkesir, 2006 Nazlı YILDIZ İKİKARDEŞ

1. GİRİŞ

Bu çalışmada, p asal iken $\mathbb{F}_p$ sonlu cisimlerinde basitleştirilmiş Weierstrass denkleminin özel bir hali olan Frey eliptik eğrilerinin nokta sayıları ve grup yapısı incelenmiştir.

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

tipindeki denklemlere eliptik eğriler (veya kübik denklemler) denir. Aslında eliptik eğri isimlendirilmesi biraz aldatıcıdır. Çünkü burada bir elips söz konusu değildir. Yalnızca belli tip denklemler söz konusudur. Bu denklemlere eliptik eğriler denilmesinin sebebi, eski zamanlarda elipslerin çevrelerini ve gezegen yörüngelerinin uzunluğunu hesaplamakta kullanılmış olmalarıdır.

Eliptik eğrileri ilginç kılan özellik; çözümü çok kolay olan denklemlerle, çözümü zor ve neredeyse imkansız olan denklemler arasında bir yerde bulunmalarıdır. Genel eliptik eğrilerdeki a, b ve c değerleri değiştirilerek her biri farklı özelliklere sahip, fakat hepsi de çözülebilen, sonsuz sayıda denklem üretilebilir.

Eliptik eğrilerle ilk ilgilenenler Yunanlı matematikçiler olmuştur. Diophantus, *Arithmetika* adlı eserinin büyük bir kısmını bunların özelliklerini incelemeye ayırmıştır. Muhtemelen Diophantus'dan ilham alan Fermat da bu zor konuya el atmıştır. Daha sonra da Fermat'nın son teoremi doğmuştur.

Matematik tarihindeki en ünlü problemlerden biri olan Fermat'nın son teoremi, sayılar teorisinin temel yapı taşlarından biridir. Bu teorem $n \geq 3$ tam sayıları için

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

denklemini sağlayacak sıfırdan farklı x, y, z tam sayı çözümleri olmadığını ifade eder.

Fermat'nın bu son teoremi yaklaşık 3 yüzyıl boyunca birçok ünlü matematikçiyi meşgul etmiştir. 1984 sonbaharında Almanya'daki bir sempozyumda Gerhard Frey, Fermat'nın Son Teoreminin ispatlanabileceği konusunda bir sunum yapmıştır. Frey'e göre, Taniyama-Shimura varsayımı ispatlanabilirse Fermat'nın Son Teoremi de ispatlanabilecekti. Frey, Fermat'nın Son Teoremi yanlışsa, yani en az bir tamsayılı çözüm varsa neler olacağından bahsediyordu. Bunun nasıl bir şey olacağını kendisi de bilmediğinden aranan sayıların yerine A, B ve C harflerini koydu:

$$A^N + B^N = C^N$$

Daha sonra kurgusal olarak çözülmüş denklemini şu hale getirdi:

$$y^2 = x(x - A^N)(x + B^N)$$

Frey bunun bir eliptik eğri olduğunu söyledi. Dolayısıyla eğer Taniyama-Shimura varsayımının doğru olduğu ispat edilecek olursa, her eliptik eğri mutlaka modüler olacaktı. Her eliptik eğri mutlaka modüler ise, Frey'in eliptik eğrisi mevcut değildir, yani böyle bir eliptik denklem yoksa Fermat'nın denkleminin çözümü yoktur. Öyleyse "Fermat'nın son teoremi doğrudur" denile bilinirdi.

Daha sonra Ken Ribet, Fermat ile Taniyama-Shimura arasındaki bağlantıya son şeklini kazandırmıştır. Nihayet 1993 yılında, Fermat'nın son teoremini ispatlamayı hayatının tutkusu haline getiren Andrew Wiles, bu rüyayı gerçekleştirmiştir.

1920'lerde Siegel tarafından, kübik bir denklemin sonlu sayıda tam sayı çözümleri olduğu ispatlanmıştır. Baker-Coates, 1970'te tam sayı çözümleri için bir üst sınır vermişlerdir.

Kübik denklemlerin sonsuz çoklukta da olabilecek rasyonel çözümleri, çözümlerin sonlu bir kümesi ile başlanarak geometrik bir işlemin tekrarlı uygulamasıyla bulunabilir. Böyle üretilmiş sonlu kümelerin var olduğu 1901'de Poincaré tarafından ortaya atılmıştır. 1922'de L. J. Mordell, $\mathbb{Q}$ sayı cisminde tanımlı eliptik eğriler üzerindeki rasyonel noktaların grubunun daima sonlu üreteçli olduğunu ispatladı. 1928'de ise Weil sayı cisimlerine ve yüksek cinse sahip eğrilere karşılık gelen durumlara genelleştirmiştir. Mordell teoremi, rasyonel çözümlerin kümesi için sonlu bir üreteç kümesi bulmaya yardımcı olan bir yöntemdir. Fakat Mordell'in metodunun, bir üreteç kümesi verdiği henüz ispatlanamamıştır. Daha sonra 1974'te, $\mathbb{Q}$ sayı cisminde tanımlı eliptik eğriler üzerindeki sonlu mertebeli rasyonel noktaların, devirli grup veya iki devirli grubun direkt çarpımına izomorf olduğu, Barry Mazur tarafından ispatlanmıştır.

Son otuz yıldır eliptik eğriler, sayılar teorisi ve kriptografi gibi alanlarda giderek artan bir önem kazanmıştır. 1980'li yıllardan itibaren eliptik eğriler kriptografide, çarpanlara ayırma ve asallık testlerinde kullanılmaya başlanmıştır. Benzer şekilde 1980'li ve 1990'lı yıllarda Fermat'nın son teoreminin ispatında, kullanılan en önemli kavram eliptik eğriler olmuştur.

Çalışmanın birinci bölümü, tezin amacının verildiği ve tezin bölümlerinin tanıtıldığı giriş bölümüdür.

İkinci bölümde, yani ön bilgiler bölümünde, ilerleyen bölümlere temel oluşturacak bazı tanım ve teoremlere yer verilmiştir. Bu bölümde, ikinci ve üçüncü dereceden kalan kavramları, normal formlar, toplama kuralı, sonlu cisimler üzerindeki eliptik eğriler, eliptik eğrilerin nokta sayılarının hesaplanmasında önemli bir yeri olan Frobenius endomorfizmi, süpersingüler eğriler, rasyonel noktaların sayısının hesaplanmasıyla ilgili teoremler ve son olarak grup mertebesi verilen eliptik eğrilerin grup yapısından bahsedilmiştir.

Üçüncü bölümde basitleştirilmiş Weierstrass normal formundaki $y^2 = x^3 + Ax + B$ eliptik eğrilerinin n, A, B, birer tam sayı olmak üzere $A = -n^2$ ve $B = 0$ özel hali olan

$$E_n : y^2 = x^3 - n^2 x$$

Frey eliptik eğrileri ele alınmıştır. Bu eğrilerin $p \equiv 1 \pmod 4$ ve $p \equiv 3 \pmod 4$ asal olmak üzere $\mathbb{F}_p$ sonlu cisimleri üzerindeki nokta sayıları ve bu noktaların mertebeleri incelenmiştir. E_n eliptik eğrisi üzerindeki rasyonel noktaların sayısının, sonsuzdaki nokta ile beraber

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

olduğu gösterilmiştir.

Dördüncü bölümde $y^2 = x^3 - n^2 x$ Frey eliptik eğrisinin $\mathbb{F}_p$ sonlu cismi üzerindeki grup yapısı incelenmiştir. Burada p'nin 4 modunda 1 ve 3'e denk olmasına göre iki durum söz konusudur. $p \equiv 1 \pmod 4$ bir asal olmak üzere E_n eğrisi üzerindeki rasyonel noktaların grup yapısının $E_n(\mathbb{F}_p) \cong \mathbb{Z}_a \times \mathbb{Z}_{a.b}$ olduğu gösterilmiştir.

t, frobenius endomorfizminin izini göstermek üzere E_n eğrisi üzerindeki rasyonel noktaların sayısının

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

olduğu ifade edilmiştir. Ayrıca p asal sayısının 8 modundaki sınıflandırmasına göre t'ler de sınıflandırılmıştır. Son olarak $p \equiv 1 \pmod 4$ asal iken n'nın Q_p'nin elemanı olup olmamasına göre nokta sayısının bir sınıflandırması yapılmıştır. Son derece önemli bir yere sahip olan dördüncü mertebeden elemanlar incelenmiştir.

Beşinci bölümde de, tezde elde edilen sonuçlar verilmiş ve önerilerde bulunulmuştur.

2. ÖN BİLGİLER

Bu bölümde çalışmamızda kullanacağımız bazı temel kavramları ve teoremleri vereceğiz.

2.1 İkinci ve Üçüncü Dereceden Kalanlar

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

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

2.1.3 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 U_n'deki tüm elemanları verir [2].

2.1.4 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.

2.1.5 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 [3].

2.1.6 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.

2.1.7 Yardımcı Teorem Q_n, U_n'in bir alt grubudur [1].

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.

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

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

şeklindedir. Literatürde $\left(\frac{a}{p}\right)$ yerine bazen $\chi(a)$ da kullanılır [4].

2.1.9 Örnek $p=7$ ise

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

dir.

2.1.10 Teorem p bir asal olsun. Eğer

a) $p \equiv 1 \pmod 4$ ise $-1 \in Q_p$,

b) $p \equiv 3 \pmod 4$ ise $-1 \notin Q_p$ [1].

2.1.11 Teorem p bir asal olsun. Eğer

a) $p \equiv 1 \pmod 4$ ise $m \in Q_p$ ise $p - m \in Q_p$,

b) $p \equiv 3 \pmod 4$ ise $m \in Q_p$ ise $p - m \notin Q_p$ [1].

2.1.12 Tanım p bir asal iken $x^3 \equiv a \pmod p$ olacak şekilde bir $x \in \mathbb{Z}$ varsa $a \in \mathbb{Z}$'ye p modunda bir "*üçüncü dereceden kalan*" denir [5].

p modunda üçüncü dereceden kalanların kümesini K_p ile, K_p'nin $\mathbb{Z}_p^* = \mathbb{Z}_p - \{\bar{0}\}$ daki elemanlarının kümesini de K_p^* ile gösterelim.

2.1.13 Teorem K_p^*, $\mathbb{Z}_p$'deki çarpma işlemine göre bir gruptur ve aslında $\mathbb{Z}_p^*$'ın bir alt grubudur [5].

2.1.14 Teorem $p \equiv 1 \pmod 3$ 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 [5].

2.1.15 Sonuç $p \equiv 1 \pmod 3$ bir asal iken ω^2 elemanı da $\mathbb{Z}_p^*$'ın bir elemanıdır [5].

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

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

şeklinde tanımlanır [5]. Bu karakter üçüncü dereceden kalanlar teorisinde, Legendre sembolünün ikinci dereceden kalan görevini yapar. Literatürde bazen $\left(\frac{a}{p}\right)_3$ yerine $\chi_3(a)$ da kullanılır. Euler kriterinde k = 3 konulursa aşağıdaki sonuç elde edilir:

2.1.17 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 [5].

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

2.1.19 Örnek $\left(\frac{1}{7}\right)_3 = 1^{\frac{7-1}{3}} = 1^2 \equiv 1 \pmod 7$, dolayısıyla 1, 7 modunda üçüncü dereceden bir kalandır. Yani $x^3 \equiv 1 \pmod 7$ denkliği çözülebilirdir. Gerçekten, $x^3 \equiv 1 \pmod 7$, $x = 1$, $x = \omega$ 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 $x \equiv 2 \pmod 7$'dir.

2.1.20 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 bir kalandır [5].

2.1.21 Örnek $p = 17$ olsun. Mod 17'de, $0^3 \equiv 0$, $1^3 \equiv 1$, $2^3 \equiv 8$, $3^3 \equiv 10$, $4^3 \equiv 13$, $5^3 \equiv 6$, $6^3 \equiv 12$, $7^3 \equiv 3$, $8^3 \equiv 2$, $9^3 \equiv 15$, $10^3 \equiv 14$, $11^3 \equiv 5$, $12^3 \equiv 11$, $13^3 \equiv 4$, $14^3 \equiv 7$, $15^3 \equiv 9$, $16^3 \equiv 16$'dır ve $\mathbb{Z}_{17}$'deki tüm sayılar üçüncü dereceden kalanlardır.

2.1.22 Teorem $p \equiv 1 \pmod 3$ asal ise p modundaki farklı üçüncü dereceden kalanların sayısı $\frac{p+2}{3}$'tür [5].

2.2. Normal Formlar

Eliptik eğriler çeşitli normal formlarda ifade edilebilir. Bu bölümde Weierstrass normal formlarını ve bu formdaki denklemlerle ilgili bazı sabitlerle birasyonel dönüşümleri tanımlayacağız.

2.2.1 Tanım A^2 afin düzlem iken **s**abit olmayan $f(x,y) \in \mathbb{F}[x,y]$ polinomunun $\mathbb{F}$ cisminin $\overline{\mathbb{F}}$'daki köklerinin kümesi

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

$\mathbb{F}$ üzerinde *"düzlemsel afin cebirsel eğri"*dir. C eğrisi üzerindeki rasyonel sayı bileşenli (x,y) noktaları *"$\mathbb{F}$-rasyonel noktalar"* olarak adlandırılır. C'deki $\mathbb{F}$-rasyonel noktaların kümesini

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

şeklinde tanımlarız. Düzlemsel afin cebirsel eğrilere örnek olarak, Weierstrass denklemleri verilebilir [6].

2.2.2 Tanım $C = C(f)$, $\mathbb{F}$ cismi üzerinde düzlemsel afin cebirsel eğri olsun. $C \setminus \mathbb{F}$ fonksiyon cismi, $\mathbb{F}[x,y]/(f)$ bölüm cismidir. $\mathbb{F}(C)$ ile gösterilir [6].

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

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (2.2.1)$$

şeklindeki bir denkleme "*uzun Weierstrass normal formu"* denir. Burada sonsuzdaki nokta olarak adlandırılan "o" noktasının afin temsili $o=(\infty,\infty)$ dur [6].

2.2.4 Örnek Weierstrass formundaki eğrilere bazı örnekler 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 o [6].

2.2.5 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"*

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

dır. Ayrıca, "*diskriminant"*

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

ve " *j değişmezi"*

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

dır [6]. Bu sabitler aşağıdaki bağıntıları sağlar:

$$4b_8 = b_2b_6 - b_4^2 \text{ ve } 12^3\Delta = c_4^3 - c_6^2$$

2.2.6 Tanım C düzlemsel cebirsel eğrisi $f(x,y)=0$ polinom denklemiyle tanımlansın. Bu durumda $P=(x_0,y_0)\in C$ noktasının, C'nin 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 [6].

2.2.7 Önerme Uzun Weierstrass normal formunda bir denklem 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 [7].

2.2.4.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 bir çıkıntısı 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:

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

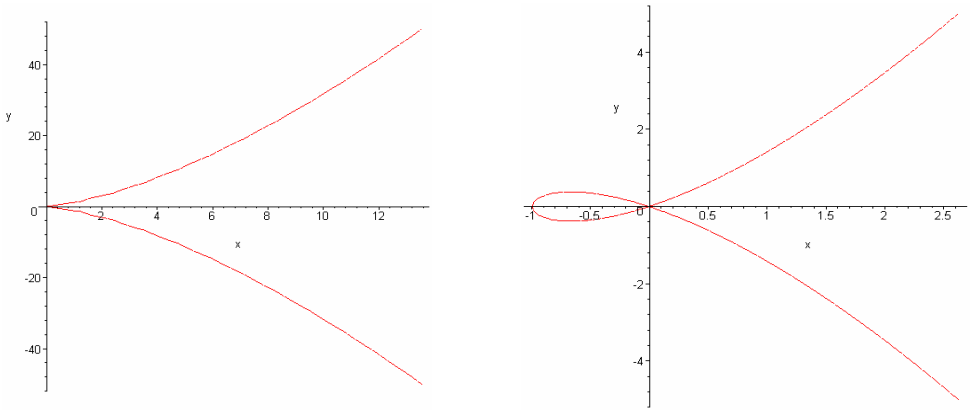
eğrisinin kısmi türevleri

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

dir. Karakteristik ne olursa olsun bu üç denklemin

$$\begin{aligned} y^2 - x^3 &= 0 \\ -3x^2 &= 0 \\ 2y &= 0 \end{aligned}$$

bir tek çözümü vardır. Bu da $x = y = 0$ dır [6].



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

Şekil 2.2.1

2.2.8 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 [6].

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

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

ve

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

şeklinde verilsin. Bu eğriler arasındaki değişken dönüşümlerine dikkat edersek, bir Weierstrass normal formunu diğerine resmeden dönüşümler bulmak gerekir. Tek değişken dönüşümü vardır. O da şu 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 "*birasyonel"* denilmektedir. Bu durumda

$$\begin{aligned}
ua' &= a_1 + 2s,\\
u^2a_2' &= a_2 - sa_1 + 3r - s^2,\\
u^3a_3' &= a_3 + ra_1 + 2t,\\
u^4a_4' &= a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st,\\
u^6a_6' &= a_6ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1,\\
u^2b_2' &= b_2 + 12r,
\end{aligned}$$

$$u^4 b_4' = b_4 + r b_2 + 6r^2,$$
$$u^6 b_6' = b_6 2r b_4 + r^2 b_2 + 4r^3,$$
$$u^8 b_8' = b_8 + 3r b_6 + 3r^2 b_4 + r^3 b_2 + 3r^4,$$
$$u^4 c_4' = c_4,$$
$$u^6 c_6' = c_6,$$
$$u^{12}\Delta' = \Delta,$$
$$j' = j.$$

Weierstrass normal formundaki bu iki denklemin arasında birasyonel dönüşümler varsa bu iki denkleme "*izomorfturlar"* denilir [6].

2.2.10 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

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

dönüşümü vardır: [6]

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

$$y^2 = x^3 + a_4 x + a_6 \tag{2.2.2}$$
$$\Delta = -16(4a_4{}^3 + 27a_6{}^2)\;,\; j = 1728\frac{4a_4{}^3}{4a_4{}^3 + 27a_6{}^2}$$

olur.

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

$$y^2 = x^3 + a_2 x^2 + a_6\,,$$
$$\Delta = -a_2{}^3 a_6\,,\; j = \frac{-a_2{}^3}{a_6}$$

olur.

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

$$y^2 = x^3 + a_4 x + a_6 ,$$
$$\Delta = -a_4{}^3 , \; j = 0$$

olur.

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

$$y^2 + xy = x^3 + a_2 x^2 + a_6 ,$$
$$\Delta = a_6 , \; j = \frac{1}{a_6}$$

olur.

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

$$y^2 + a_3 y = x^3 + a_4 x + a_6 ,$$
$$\Delta = a_3{}^4 , \; j = 0$$

olur.

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

$$E' : y^2 = x^3 + Ax + B \qquad (A, B \in \mathbb{F}) \qquad (2.2.3)$$

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 [6].

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 birasyonel dönüşümler basitleştirilmiş Weierstrass normal formunu

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

dönüşümleri altında değişmez bırakır. Bu durumda

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

dönüşümlerini elde ederiz.

2.2.12 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 [6].

2.2.13 Önerme j-değişmezi j_0 olan her bir $j_0 \in \mathbb{F}$ için $\mathbb{F}$ üzerinde tanımlanabilecek bir eliptik eğri vardır [6].

Çizelge 2.2.1

$Kar(\mathbb{F})$	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	$y^2 = x^3 + x$
	$\neq 0$	$y^2 = x^3 + x^2 - j_0^{-1}$

2.3. Toplama Kuralı

Eliptik eğriler hakkında en önemli gerçek, eğri üzerindeki noktaların toplamaya göre değişmeli bir grup oluşturmasıdır. $E \setminus \mathbb{F}$ 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.

2.3.1 Teorem Bir doğru bir eliptik eğriyi katlılıklarla birlikte tam olarak 3 noktada keser [6].

2.3.2 Bézout Teoremi *m.* dereceden bir düzlem eğri ile *n.* dereceden bir düzlem eğri en çok *m.n* tane noktada kesişir [7].

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

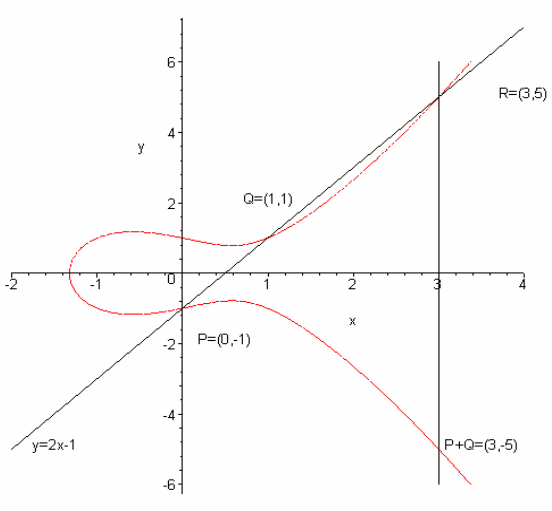
2.3.3 Teorem C, C_1 ve C_2 kübik eğriler olsunlar. Varsayalım ki C, C_1 ve C_2'nin 8 kesişim noktasından geçsin. Bu durumda C, 9. kesişim noktasından geçer [7].

2.3.4 Tanım $E \setminus \mathbb{F}$ eliptik eğri $P_1, P_2 \in E(\mathbb{F})$ farklı olması gerekli olmayan iki nokta olsun. P_1 ve P_2'den geçen doğru (örneğin kesen) eliptik eğriyi üçüncü bir P_3' noktasında keser. P_3' ve o'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.) [6].

2.3.5 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 [8].

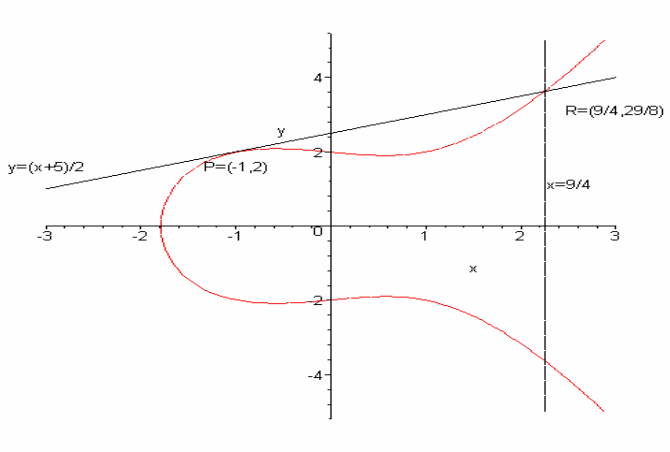


Şekil.2.3.1

2.3.6 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 [8].



Şekil.2.3.2

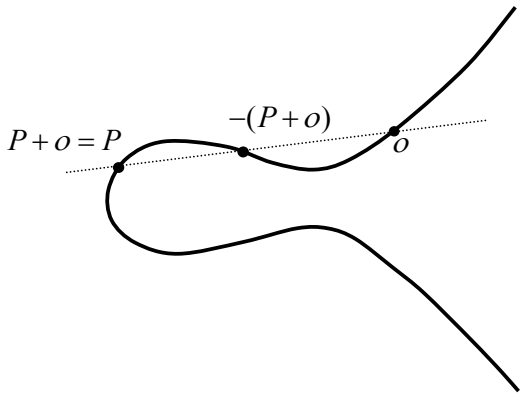
2.3.7 Teorem $E \setminus \mathbb{F}$, $\mathbb{F}$ üzerinde bir eliptik eğri olsun. $E(\mathbb{F})$ rasyonel noktalarının kümesi toplama işlemine göre değişmeli gruptur. Sonsuzdaki nokta "o" bu grubun etkisiz elemanıdır [6].

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

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. 2.3.6. Teoremde uzun olan Weierstrass normal formundaki eliptik eğriler için toplama formülü vereceğiz.

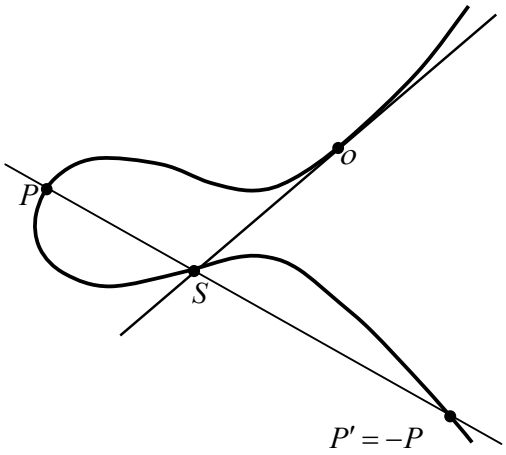
ii) Birim eleman: o (Şekil.2.3.3)



Şekil.2.3.3 Birim eleman

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

iv) Ters eleman özelliği: P ve o'dan doğru ile eğrinin üçüncü kesişim noktası P' olsun. Bu durumda $P + P' = o$ dır. O halde $P' = -P$ dir. (Şekil.2.3.4)



Şekil.2.3.4 Ters eleman

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 (noktaların çakışırsa teğetler veya kesenler) tanımlayalım :

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

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

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

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

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

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

Bu durumda

$$C=L_1\cup L_2\cup L_3 \ , \ C'=L_1'\cup L_2'\cup L_3'$$

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

$$o, P_1, P_2, P_3, (P_1 + P_2), -(P_1 + P_2), (P_2 + P_3), -(P_2 + P_3), -((P_1 + P_2) + P_3).$$

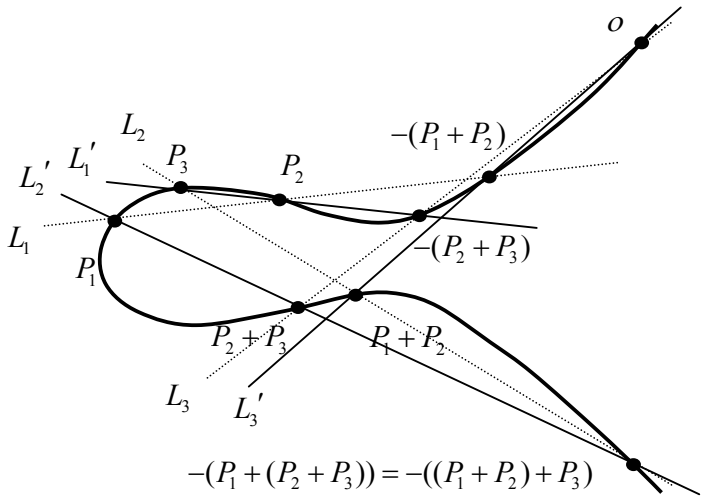
C' eğrisi C ve E eğrisinin ortak noktalarının ilk sekizinde kesişirler. Diğer taraftan C' nün E'de 9 ortak noktası vardır:

$$o, P_1, P_2, P_3, (P_1 + P_2), -(P_1 + P_2), (P_2 + P_3), -(P_2 + P_3), -(P_1 + (P_2 + P_3)).$$

Böylece

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

olur (Şekil.2.3.5).



Şekil.2.3.5 Birleşme özelliği

2.3.8 Toplama Teoremi $E \setminus \mathbb{F}$, $\mathbb{F}$ cismi üzerinde (2.2.1) tipinde bir eliptik eğri olsun. $P_1 = (x_1, y_1)$, $P_2(x_2, y_2) \in E(\mathbb{F})$ 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 $P_1 + P_2 = o$ 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 [6].

Bilindiği gibi eliptik eğriler üzerindeki noktaların en genel temsili uzun Weierstrass normal formundaki afin temsildir. 2.3.8 Teoremde bu temsil için bir toplam formülü tanımlanmıştır. Bu temsil keyfi bir karakteristikteki herhangi bir cisim için kullanılır. Şimdi (2.2.3) tipindeki Weierstrass eğrileri için toplam formülünü vereceğiz.

2.3.9 Tanım $E \setminus \mathbb{F}$, (2.2.3) 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. 2.3.8 Teorem gereği $P_1 + P_2 = (x_3, y_3)$

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

ve

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

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

ile verilir [8].

2.3.10 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. Sonra da $x_3 = \lambda^2 - x_2 - x_1 = -\frac{8}{9}$ 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 [7].

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 ihtiyaç vardır. Fakat λ için verilen eğim formülü kullanılamaz. 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 edilir. Buradan da 2.3.9 Tanım'daki formülleri kullanarak $2P_0$'ın bileşenlerini buluruz.

2.3.11 Örnek 2.3.10. 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 edilmişti. 2.3.9 Tanımda verilen formülleri kullanırsak $2P_1 = \left(\frac{137}{64}, -\frac{2651}{512}\right)$ bulunur [7].

2.3.12 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 2.3.8 Teoremde verilen $x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$ formülünü kullanırsak $a_1 = 0$ ve $x_1 = x_2$ olduğundan λ yerine de $\lambda = \frac{f'(x)}{2y}$ koyarsak $2P = (x_3, y_3)$ noktasının x_3 koordinatını şöyle formülize ederiz:

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

$2P$'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 [7].

2.3.13 Tanım E, $\mathbb{F}$ cismi üzerinde bir eliptik eğri ve belli bir $n \in \mathbb{N}$ için $nP = o$ 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. o 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 [8].

2.3.14 Örnek $\mathbb{Q}$ cismi üzerinde $y^2 = x^3 - \frac{27}{4}$ eliptik eğrisini alalım. Bu eğrinin $\mathbb{Q}$'daki çözümleri $(3, \frac{9}{2}), (3, -\frac{9}{2})$ ve o'dur. 2.3.12 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 $P = o$ demektir. Böylece $2P = -P$ ve $3P = o$ dur. Diğer bir ifadeyle P'nin mertebesi 3'tür [9].

2.3.15 Örnek $\mathbb{Q}$ sayı cismi üzerinde

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

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

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

Böylece $5P = -P$ dir. O halde P noktasının mertebesi 6'dır [8].

2.3.16 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: $2Q = o$. P noktası sonsuz mertebelidir.

$$2P = (\frac{121}{36}, \frac{451}{216}),\ 3P = (\frac{-57121}{24649}, \frac{-12675843}{3869893}),$$
$$4P = (\frac{761815201}{29289744}, \frac{-20870873704079}{158516094528})\ldots$$

[6]

Yukarıda görüldüğü gibi her toplamada bileşenler giderek karmaşıklaşır.

2.3.17 Nagel-Lutz Teoremi E, $\mathbb{Q}$ üzerinde (2.2.3) tipinde bir eliptik eğri ve $P = (x_1, y_1) \in E(\mathbb{Q})_t$ ise bu durumda $x_1, y_1 \in \mathbb{Z}$ ve ya $y_1 = 0$ (bu durumda P'nin mertebesi 2'dir.) ya da $y_1 \neq 0$ ve $y_1^2 \mid (4A^3 + 27B^2)$ 'dir [8].

2.3.18 Sonuç E, $\mathbb{Q}$ üzerinde bir eliptik eğri olsun. Bu durumda $E(\mathbb{Q})$'nun büküm alt grubu sonludur [8].

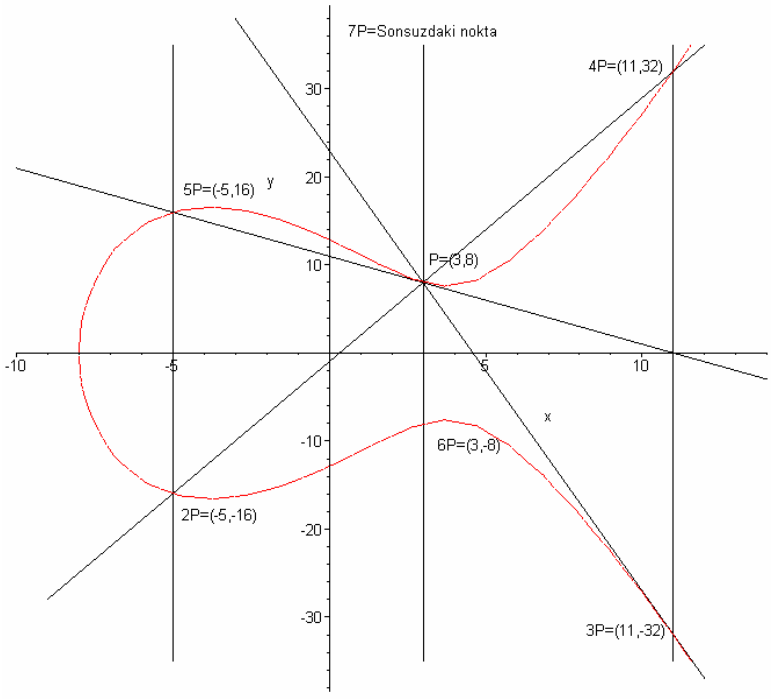
2.3.19 Örnek $\mathbb{Q}$ cismi üzerinde $E: y = x^3 + 4$ eliptik eğrisi verilsin. Bu durumda $4A^3 + 27B^2 = 432$ olur. $P(x, y)$, $E(\mathbb{Q})$'da sonlu mertebeli bir nokta olsun. $0 = x^3 + 4$ denkleminin rasyonel çözümleri olmadığından $y \neq 0$'dır. Bu yüzden $y^2 \mid 432$ olur. Böylece $y = \pm 1, \pm 2, \pm 3, \pm 4, \pm 12$'dir. Sadece $y = \pm 2$, x'in rasyonel değerini verir. Böylece mümkün olan sonlu mertebeli noktalar $(0, 2), (0, -2)$'dir. Kolay bir hesaplama ile $3(0, \pm 2) = o$ olduğunu buluruz. $E(\mathbb{Q})$'nun büküm alt grubu 3 mertebeli devirli bir gruptur [10].

2.3.20 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 $\{o,(-2,0)\}$ olduğu sonucu çıkar (Uyarı: $2(1,3)=-2(2,4)$ olduğundan dolayı $(1,3)+(2,4)=(-2,0)$ eşitliği açıkça görülür.) [10].

2.3.21 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 [8].



Şekil.2.3.6

2.3.22 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 [8].

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

2.3.23 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 [10].

2.3.24 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 $n = p^r n'$'dür. O halde

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

dür [10].

2.3.25 Sonuç E bir eliptik eğri olsun. n ile çarpma olarak tanımlanan E'nin endomorfizması n^2 derecelidir [10].

2.3.26 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 [8].

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

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

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 [8].

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

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

dir [11].

2.3.29 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 [11].

2.3.30 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 [11].

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

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

eliptik eğrisi yalnızca sonlu sayıda tam sayı bileşenli $P = (x, y)$ noktasına sahiptir [12].

2.4 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.

2.4.1 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 2.4.1

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	$(4,2),(4,3)$
o		o	o

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 [10].

2.4.2 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 [10].

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

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

olur [10].

2.5 Frobenius Endomorfizmi ve Süpersingüler Eğriler

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

$$\varphi_q(x, y) = (x^q, y^q), \quad \varphi_q(o) = o$$

olacak şekilde verilir [10].

2.5.2 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

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

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 [6].

2.5.3 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**,** $E[p] \cong o$ ise süpersingüler olarak adlandırılır. Singülerlik ile süpersingülerlik birbirinden apayrı kavramlardır [10]

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

2.5.4 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 [10].

2.5.5 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 [10].

2.6 Rasyonel Noktaların Sayısını Hesaplama

$E \setminus \mathbb{F}_q$ eliptik eğri verilsin. (2.2.1) 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 o noktası dahil bu eğri üzerinde en çok $2q+1$ tane nokta vardır. Fakat rasgele seçilen bir elemanın ikinci dereceden bir kalan olma şansı yüzde elli olduğundan bu sayı yarı yarıya azalacak ve $q+1$ olacaktır.

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

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

olur [13, 14, 15, 16, 17, 18].

2.6.2 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 [9].

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

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

olur [9].

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

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

olur [10].

E, $\mathbb{F}_q$ sonlu cismi üzerinde tanımlanmış bir eliptik eğri ise bu eğri $r = 1, 2, \ldots$ 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.

2.6.5 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 [15].

"*Weil konjektürü*" 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:

2.6.6 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

$$Z\left(T; E \setminus \mathbb{F}_q\right) = \frac{1 - tT + qT^2}{(1-T)(1-qT)} \tag{2.6.1}$$

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 [15].

2.6.7 Uyarı (2.6.1)'nın 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

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

şeklindedir [15].

2.7 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.

2.7.1 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 $c \in \mathbb{F}_q^*$ sabiti için

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

eğrisine E'nin *"c-eşleniği (twist)"* denir [19].

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

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

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

dir [10, 20].

2.7.3 Yardımcı Teorem E, $\mathbb{F}_q$'da (2.2.3) tipinde bir eliptik eğri olsun. $t = (q+1) - \#E(\mathbb{F}_q)$ şeklinde tanımlı t Frobenius endomorfizminin izi için $t \equiv 2 \pmod{n}$'dir [10].

2.7.4 Önerme E, $\mathbb{F}_q$'da (2.2.3) 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 [10, 21].

3. F_p SONLU CİSİMLERİNDEKİ $y^2=x^3-n^2x$ FREY ELİPTİK EĞRİLERİ ÜZERİNDEKİ RASYONEL NOKTALAR

3.1 Frey Eliptik Eğrileri

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

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

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

$$y^2 = x^3 - n^2 x \qquad (n \in \mathbb{F}_p^{\,*}) \tag{3.1.1}$$

"*Frey eliptik eğrileri*"ni inceleyeceğiz. Bu bölümde verdiğimiz örneklerde nokta sayısı hesaplamalarında Maple ve Visual Basic programları kullanılmıştır [22]. Burada ilk olarak şu iki önemli sonucu verebiliriz.

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

3.1.2 Sonuç $p \equiv 3 \pmod 4$ asal iken $y^2 \equiv x^3 - n^2 x \pmod{p}$ Frey eliptik eğrisi "süpersingülerdir". $p \equiv 1 \pmod 4$ iken ise "süpersingüler değildir" [23].

Bu bölümde Frey eliptik eğrilerinin üzerindeki nokta sayıları ve bu noktaların apsisleri toplamı ile ilgili bazı sonuçlar elde etmeye çalışacağız.

3.2 Frey Eliptik Eğrilerinin Nokta Sayılarının Yeniden Hesaplanması

Şimdi (3.1.1) eğrisini ele alalım ve bunu E_n ile gösterelim. E_n eğrisindeki $\mathbb{F}_p$-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. (3.1.1) eliptik eğrisinin $\mathbb{Z}_p$ cisminde en çok $2p+1$ tane noktaya sahip olduğu kolayca görülebilir. Yani $x, y \in \mathbb{Z}_p$ iken $2p$ tane (x, y) nokta çifti ile birlikte sonsuzdaki nokta (3.1.1) denklemini sağlar. Bunun sebebi her bir $x \in \mathbb{F}_p$ için en çok iki tane $y \in \mathbb{F}_p$ vardır ve bunlar (3.1.1) denklemini sağlar.

Ancak $\mathbb{F}_p$'nin tüm elemanları ikinci dereceden kalan değildir. Aslında $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{\bar{0}\}$'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 eğrisi üzerindeki nokta sayısının daha kesin formülü

$$N_{p,n} = p + 1 + \sum_{x \in \mathbb{F}_p} \chi(x^3 - n^2 x) \qquad (3.1.2)$$

şeklindedir.

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

3.2.1 Teorem p bir asal olsun. $n \in \mathbb{F}_p$ için p-1 tane $y^2 \equiv x^3 - n^2 x \pmod{p}$ eğrisi 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 eğriyi verir. Dolayısıyla ispat biter. ■

3.2.2 Örnek $p = 7$ olsun. $n \in \mathbb{F}_7$ için 6 tane eliptik eğri 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 $y^2 \equiv x^3 - 6^2 x \pmod{7}$ eğrileridir.

3.2.3 Teorem p bir asal olsun. $1 \le n \le p-1$ olmak üzere $\frac{p-1}{2}$ tane *birbirinden farklı* $y^2 \equiv x^3 - n^2 x \pmod{p}$ eliptik eğri vardır.

İspat $y^2 \equiv x^3 - n^2 x \pmod{p}$ eğrisinde $y = 0$ ise $x = 0$, $x = n$ ve $x = p - n$ bulunur. $1 \le n \le p-1$ için n ve p -n aynı eğride oldukları için, Teorem 3.2.1.'e göre p-1 tane eliptik eğrinin tam yarısı kadar, yani $\frac{p-1}{2}$ tane farklı eliptik eğri vardır. ■

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

3.2.5 Teorem p bir asal olsun. $y^2 \equiv x^3 - n^2 x \pmod{p}$ eliptik eğrisinde apsisleri aynı olan rasyonel noktaların ordinatları toplamı p' dır.

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

3.2.6 Örnek $y^2 \equiv x^3 - 2^2 x \pmod{7}$ eğrisini ele alalım. Bu eğrideki rasyonel noktalar $(0,0)$, $(2,0)$, $(5,0)$, $(1,2)$, $(1,5)$, $(3,1)$ ve $(3,6)$ dır. Burada apsisleri aynı olan noktaların ordinatları toplamı 7'dir.

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

3.3 $p \equiv 1 \pmod{4}$ Asal İken Frey Eliptik Eğrilerindeki Rasyonel Noktalar

p'nin 4 modunda 1'e denk olduğu durumda, (3.1.1) eğrisinde, rasyonel noktaların özellikleriyle ilgili elde edilen sonuçları verelim.

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

İspat $y^2 \equiv x^3 - n^2 x \pmod{p}$ eğrisinde $y = 0$ için $x = 0$, $x = n$ ve $x = p - n$ olur. 2.1.11. Teoreme göre $n \in Q_p$ 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 elemanı 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. ■

3.3.2 Örnek $p=13$ olsun. $1 \le n \le 12$ olmak üzere $\frac{p-1}{2}=6$ tane $y^2 = x^3 - n^2 x \pmod{13}$ eğrisinin $\frac{p-1}{4}=3$ 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. $y^2 \equiv x^3 - 1^2 x \equiv x^3 - 12^2 x \pmod{13}$ eliptik eğrisinde $(1,0)$ ve $(12,0)$ noktaları için $1, 12 \in Q_{13}$'tür. $y^2 \equiv x^3 - 3^2 x \equiv x^3 - 10^2 x \pmod{13}$ eliptik eğrisinde $(3,0)$ ve $(10,0)$ noktaları için $3, 10 \in Q_{13}$'tür. $y^2 \equiv x^3 - 4^2 x \equiv x^3 - 9^2 x \pmod{13}$ eliptik eğrisinde $(4,0)$ ve $(9,0)$ noktaları için $4, 9 \in Q_{13}$'tür. $y^2 \equiv x^3 - 2^2 x \equiv x^3 - 11^2 x \pmod{13}$ eliptik eğrisinde $(2,0)$ ve $(11,0)$ noktaları için $2, 11 \notin Q_{13}$'tür. $y^2 \equiv x^3 - 5^2 x \equiv x^3 - 8^2 x \pmod{13}$ eliptik eğrisinde $(5,0)$ ve $(8,0)$ noktaları için $5, 8 \notin Q_{13}$'tür. $y^2 \equiv x^3 - 6^2 x \equiv x^3 - 7^2 x \pmod{13}$ eliptik eğrisinde $(6,0)$ ve $(7,0)$ noktaları için $6, 7 \notin Q_{13}$'tür.

3.3.3 Teorem $p \equiv 1 \pmod 4$ asal olsun. $y^2 \equiv x^3 - n^2 x \pmod p$ eğrisinde, eğer $n \in Q_p$ ise $x \in Q_p$ olan 2 tane x değeri vardır. Bunların toplamı p ile bölünür. Ayrıca ordinatları ise 0'dır.

İspat Teorem 2.1.11'den görülür. ■

3.3.4 Örnek $p=13$ olsun. $y^2 \equiv x^3 - 9^2 x \pmod{13}$ eğrisini ele alalım. Burada $n = 9 \in Q_{13}$'tür. $Q_{13} = \{1, 3, 4, 9, 10, 12\}$ olduğundan, $x \in Q_p$ olan noktalar $(1,0)$ ve $(12,0)$'dır. Apsisleri toplamı 0'dır. Ayrıca ordinatları da 0'dır.

3.3.5 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. ■

3.3.6 Teorem $p \equiv 1 \pmod 4$ bir asal olsun. $0 \le x \le p-1$ olacak şekilde herhangi bir x tam sayısı alalım. O zaman bir $1 \le n \le p-1$ için

$$j(p) = \sum_{x=0}^{p-1} (1 + \chi(x^3 - n^2x)).x$$

$p \mid j(p)$ dir. Özellikle

$$k(p) = \sum_{x=0}^{p-1} \chi(x^3 - n^2x).x$$

toplamı p ile bölünür.

İspat Her y değeri için $t = y^2 + n^2 x$ olsun. O zaman $x^3 \equiv t \pmod{p}$ denkliğinin çözümlerinin toplamı, Teorem 3.3.5 gereği sıfıra denktir. Tüm y değerleri için bu geçerlidir. Böylece tüm apsislerin toplamı sıfıra denktir. ■

3.3.7 Örnek $p = 17$ olsun. $0 \le x \le 16$ olacak şekilde bir herhangi bir x tam sayısı alalım. O zaman $1 \le n \le 16$ için $n = 2$ olmak üzere,

$$\begin{aligned} j(17) &= \sum_{x=0}^{16} (1 + \chi(x^3 - 2^2 x)).x \\ &= (1 + \chi(0^3 - 2^2.0)).0 + (1 + \chi(1^3 - 2^2.1)).1 \\ &\quad + (1 + \chi(2^3 - 2^2.2)).2 + (1 + \chi(3^3 - 2^2.3)).3 \\ &\quad + (1 + \chi(4^3 - 2^2.4)).4 + (1 + \chi(5^3 - 2^2.5)).5 \\ &\quad + (1 + \chi(6^3 - 2^2.6)).6 + (1 + \chi(7^3 - 2^2.7)).7 \\ &\quad + (1 + \chi(8^3 - 2^2.8)).8 + (1 + \chi(9^3 - 2^2.9)).9 \\ &\quad + (1 + \chi(10^3 - 2^2.10)).10 + (1 + \chi(11^3 - 2^2.11)).11 \\ &\quad + (1 + \chi(12^3 - 2^2.12)).12 + (1 + \chi(13^3 - 2^2.13)).13 \\ &\quad + (1 + \chi(14^3 - 2^2.14)).14 + (1 + \chi(15^3 - 2^2.15)).15 \\ &\quad + (1 + \chi(16^3 - 2^2.16)).16 \end{aligned}$$

$$\begin{aligned} j(17) &= (1+0).0 + (1-1).1 + (1+0).2 + (1+1).3 \\ &\quad + (1-1).4 + (1-1).5 + (1-1).6 + (1+1).7 \\ &\quad + (1+1).8 + (1+1).9 + (1+1).10 + (1-1).11 \\ &\quad + (1-1).12 + (1-1).13 + (1+1).14 + (1+0).15 \\ &\quad + (1-1).16 \end{aligned}$$

$$\begin{aligned} j(17) &= 0 + 0 + 2 + 2.3 + 0 + 0 + 0 + 2.7 + 2.8 \\ &\quad + 2.9 + 2.10 + 0 + 0 + 0 + 2.14 + 1.15 + 0 \\ &= 119 \end{aligned}$$

$17 \mid 119$ 'dur. Özellikle

$$
\begin{aligned}
k(17) &= \sum_{x=0}^{16} \chi(x^3 - 2^2 x).x \\
&= (\chi(0^3 - 2^2.0)).0 + (\chi(1^3 - 2^2.1)).1 \\
&\quad + (\chi(2^3 - 2^2.2)).2 + (\chi(3^3 - 2^2.3)).3 \\
&\quad + (\chi(4^3 - 2^2.4)).4 + (\chi(5^3 - 2^2.5)).5 \\
&\quad + (\chi(6^3 - 2^2.6)).6 + (\chi(7^3 - 2^2.7)).7 \\
&\quad + (\chi(8^3 - 2^2.8)).8 + (\chi(9^3 - 2^2.9)).9 \\
&\quad + (\chi(10^3 - 2^2.10)).10 + (\chi(11^3 - 2^2.11)).11 \\
&\quad + (\chi(12^3 - 2^2.12)).12 + (\chi(13^3 - 2^2.13)).13 \\
&\quad + (\chi(14^3 - 2^2.14)).14 + (\chi(15^3 - 2^2.15)).15 \\
&\quad + (\chi(16^3 - 2^2.16)).16
\end{aligned}
$$

$$
\begin{aligned}
k(17) &= 0.0 + (-1).1 + 0.2 + 1.3 + (-1).4 \\
&\quad + (-1).5 + (-1).6 + 1.7 + 1.8 + 1.9 \\
&\quad + 1.10 + (-1).11 + (-1).12 + (-1).13 \\
&\quad + 1.14 + 0.15 + (-1).16
\end{aligned}
$$

$$
\begin{aligned}
k(17) &= 0 - 1 + 0 + 3 - 4 - 5 - 6 + 7 + 8 + 9 \\
&\quad + 10 - 11 - 12 - 13 + 14 + 0 - 16 \\
&= -17
\end{aligned}
$$

$17 \mid -17$ 'dır.

3.3.8 Teorem $p \equiv 1 \pmod 4$ bir asal olsun. $y^2 \equiv x^3 - n^2 x \pmod p$ eğrisi üzerindeki (x, y) rasyonel noktalarının sayısı

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

toplamına eşittir ve burada

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

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

İspat $p \equiv 1 \pmod 4$ asal olmak üzere Teorem 2.1.11'den ispat kolayca görülür. ■

3.3.9 Örnek $y^2 \equiv x^3 - 10^2 x \pmod{13}$ Frey eliptik eğrisi üzerindeki sekiz nokta $(0,0)$, $(3,0)$, $(10,0)$, $(2,4)$, $(2,9)$, $(11,6)$, $(11,7)$ ve o'dur. Şimdi formülden şöyle hesaplayalım:

$Q_{13} = \{1,3,4,9,10,12\}$ 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 eğri üzerinde toplam 8 tane nokta bulunur.

3.3.10 Teorem $p \equiv 1 \pmod 4$ bir asal olsun. $y^2 \equiv x^3 - n^2 x \pmod p$ eğrisindeki rasyonel sayıların 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.

3.3.11 Örnek $p=17$ olsun. $y^2 \equiv x^3 - 4^2 x \pmod{17}$ Frey eliptik eğrisi üzerindeki 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. Şimdi teoreme göre şöyle hesaplayalım:

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.

3.4 $p \equiv 3 \pmod 4$ Asal İken Frey Eliptik Eğrilerindeki Rasyonel Noktalar

Şimdi de 4 modunda 3'e denk olan p asalları için, (3.1.1) eğrisinde, rasyonel noktaların özellikleriyle ilgili elde edilen sonuçları verelim.

3.4.1 Teorem $p \equiv 3 \pmod 4$ asal olsun. $y^2 \equiv x^3 - n^2 x \pmod p$ eğrisinde $x \in \mathbb{F}_p$'in $\frac{p+3}{2}$ tane farklı değeri vardır. Sabit bir x için iki farklı y değeri vardır ve bu y'lerin toplamı p'dir.

İspat Denkliğimizi $x^3 \equiv y^2 + n^2 x \pmod p$ biçiminde tekrar yazalım. $y \equiv 0 \pmod p$ için $x \equiv 0, n, p-n \pmod p$ olur. $y \neq 0 \pmod p$ için $y^2 + n^2 x$'in

her değeri y'nin t ve p-t gibi iki değerini verir. $p \equiv 3 \pmod 4$ asal iken 2.1.11 Teoreme göre $m \in Q_p$ iken $p-m \in Q'_p$ olduğundan $|Q_p| = \frac{p-1}{2}$ ifadesinden $\left(\frac{p-1}{2}\right) - 1 = \frac{p-3}{2}$ tane değer elde ederiz. $y \equiv 0 \pmod p$ için de 3 farklı x değerini de eklersek $\frac{p-3}{2} + 3 = \frac{p+3}{2}$ tane farklı x değeri bulunur. ■

3.4.2 Örnek $p = 7$ olsun. $y^2 \equiv x^3 - 3^2 x \pmod 7$ eğrisinde $(0,0)$, $(3,0)$, $(4,0)$, $(2,2)$, $(2,5)$, $(6,1)$ ve $(6,6)$ noktaları yer almaktadır. Görüldüğü gibi $x \in \mathbb{F}_7$'in $\frac{p+3}{2} = 5$ tane farklı değeri vardır. Sabit $x = 6$ için $y = 1$ ve $y = 6$ gibi iki farklı değeri vardır ve bu y'lerin toplamı $p = 7$ 'dır.

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

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

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

c) eğer $n \in Q'_p$ ise $\frac{p-1}{2}$ 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 Aşikardır.

3.4.4 Örnek $p = 11$ olsun. $y^2 \equiv x^3 - 3^2 x \pmod{11}$ eğrisinde $(0,0)$, $(1,0)$, $(10,0)$, $(4,4)$, $(4,7)$, $(6,1)$, $(6,10)$, $(8,3)$, $(8,8)$, $(9,4)$ ve $(9,7)$ noktaları vardır. $y^2 \equiv x^3 - 7^2 x \pmod{11}$ eğrisinde ise $(0,0)$, $(4,0)$, $(7,0)$, $(2,3)$, $(2,8)$, $(3,1)$, $(3,10)$, $(5,1)$, $(5,10)$, $(10,2)$ ve $(10,9)$ noktaları bulunmaktadır. 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 $y^2 \equiv x^3 - 3^2 x \pmod{11}$ eğrisi için $(1,0)$, $(4,4)$, $(4,7)$, $(9,4)$ ve $(9,7)$ noktalarının apsisleri, Q_{11}'de yer alır. $(0,0)$, $(10,0)$, $(6,1)$, $(6,10)$, $(8,3)$ ve $(8,8)$ noktalarının apsisleri ise yer almaz. Teoreme göre bakarsak, $n = 3 \in Q_{11}$ 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. $y^2 \equiv x^3 - 7^2 x \pmod{11}$ eğrisi 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. Teoreme göre bakarsak, $n = 7 \notin Q_{11}$ 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.

3.4.5 Teorem $p \equiv 3 \pmod 4$ asal olsun. Eğer $n \in K_p^*$ ve $y \equiv 0 \pmod p$ ise $y^2 \equiv x^3 - n^2 x \pmod p$ eğrisinde apsisleri K_p'de kalan 3 nokta 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 aşikardır. ■

3.4.6 Örnek $p = 19$ olsun. $y^2 \equiv x^3 - 11^2 x \pmod{19}$ eğrisini ele alalım. Burada $(0,0)$, $(1,0)$ ve $(18,0)$ noktalarının ordinatları 0'dır. $K_{19} = \{0,1,7,8,11,12,18\}$ olduğundan bu noktaların apsislerinin K_p'de olduğu görülür.

3.4.7 Teorem $p \equiv 3 \pmod 4$ bir asal olsun. $y^2 \equiv x^3 - n^2 x \pmod p$ eğrisi üzerindeki rasyonel 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 $x^3-n^2x\equiv 0 \pmod p$ dir ve $p\mid 0$ iken $\chi_p(x^3-n^2x)=0$ dır. Eğri üzerindeki her bir $(x,0)$ noktası için $(1+0).x=x$ toplama eklenir. $x^3-n^2x=t$ olsun. $\left(\frac{t}{p}\right)=1$ ise eğri üzerindeki her bir (x,y) noktası için $(x,-y)$ noktası da eğri üzerindedir. 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. ■

3.4.8 Örnek $y^2\equiv x^3-5^2x \pmod{11}$ Frey eliptik eğrisi üzerindeki rasyonel noktalar $(0,0)$, $(5,0)$, $(6,0)$, $(1,3)$, $(1,8)$, $(7,5)$, $(7,6)$, $(8,2)$, $(8,9)$, $(9,3)$ ve $(9,8)$ noktalarıdır. Teorem yardımıyla bu noktaların apsisleri toplamını bulalım.

$Q_{11}=\{1,3,4,5,9\}$ olduğundan

$$\begin{aligned}\sum_{x\in\mathbb{F}_{11}}(1+\chi_{11}(x^3-5^2x)).x &= (1+\chi_{11}(0)).0+(1+\chi_{11}(9)).1+(1+\chi_{11}(2)).2\\ &\quad+(1+\chi_{11}(7)).3+(1+\chi_{11}(8)).4+(1+\chi_{11}(0)).5\\ &\quad+(1+\chi_{11}(0)).6+(1+\chi_{11}(3)).7+(1+\chi_{11}(4)).8\\ &\quad+(1+\chi_{11}(9)).9+(1+\chi_{11}(2)).10\\ &=0+2+0+0+0+5+6+14+16+18+0\\ &=61\end{aligned}$$

dır.

3.4.9 Teorem $p \equiv 3 \pmod 4$ bir asal olsun. $y^2 \equiv x^3 - n^2 x \pmod p$ eğrisindeki rasyonel sayıların sayısı $\# E_n(\mathbb{F}_p) = N_{p,n} = p+1$'dır.

İspat [11] nolu kaynakta $k = n^2$ durumundaki ispatı bulunabilir. Şimdi biz ikinci bir ispatını verelim. $p \equiv 3 \pmod 4$ asal olmak üzere $y^2 \equiv x^3 - n^2 x \pmod p$ eğrisinde 3.4.1 Teoreme göre, $\frac{p+3}{2}$ tane farklı $x \in \mathbb{F}_p$ değeri vardır. $y \equiv 0 \pmod p$ için $x \equiv 0 \pmod p$, $x \equiv n \pmod p$ ve $x \equiv p - n \pmod p$ çözümleri aşikardır. Bunları bu x değerlerinden çıkarırsak $\frac{p+3}{2} - 3 = \frac{p-3}{2}$ tane farklı değer kalır. Her bir $x \in \mathbb{F}_p$ için, ordinatları toplamı p olan iki farklı nokta elde ettiğimize göre bunu 2 ile çarparsak $2.\frac{p-3}{2} = p-3$ tane nokta elde ederiz. Daha sonra çıkardığımız 3 değeri tekrar eklersek $p-3+3 = p$ tane nokta elde ederiz. Tabi ki bir de sonsuzdaki nokta o olduğundan nokta sayısı $p+1$ olur. ■

3.4.10 Örnek $p = 23$ olsun. $y^2 \equiv x^3 - 14^2 x \pmod{23}$ eğrisini ele alalım. Bu eğri üzerindeki noktalar $(0,0)$, $(9,0)$, $(14,0)$, $(1,9)$, $(1,14)$, $(4,4)$, $(4,19)$, $(6,11)$, $(6,12)$, $(7,11)$, $(7,12)$, $(8,5)$, $(8,18)$, $(10,11)$, $(10,12)$, $(11,7)$, $(11,16)$, $(18,2)$, $(18,21)$, $(20,3)$, $(20,20)$, $(21,4)$, $(21,19)$ ve o'dur. Teoreme göre de rasyonel noktaların sayısı $\# E_{14}(\mathbb{F}_{23}) = N_{23,14} = 23+1 = 24$'tür.

3.4.11 Teorem $p \equiv 3 \pmod 4$ bir asal olsun. $y^2 \equiv x^3 - n^2 x \pmod p$ eğrisi üzerindeki (x, y) rasyonel noktalarının sayısı

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

toplamına eşittir ve burada

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

şeklinde ifade edilir. Aynı zamanda böyle y değerlerinin toplamı da p modunda 0'a denktir.

İspat $x \equiv 0, 1, 2, ..., p-1 \pmod{p}$ için $y^2 \equiv x^3 - n^2 x \pmod{p}$ eğrisi üzerindeki y değerlerini bulalım. Eğer $y^2 \in Q_p$ ise $y \in U_p$'nin iki değeri vardır. 3.4.9 Teoreme göre $p+1$ tane nokta vardır. $(0,0)$, $(n,0)$ ve $(p-n,0)$ noktaları hariç diğer noktaların ordinatları sıfırdan farklıdır. Bunlar ordinatları toplamı p olan nokta çiftleri oldukları için x'in tüm olası değerlerinin sayısı 3.4.1 Teoreme göre $\frac{p+3}{2}$'dir. Yukarıdaki üç noktayı çıkarırsak $\frac{p-3}{2}$ tane nokta çifti elde ederiz. Dolayısıyla $\frac{p-3}{2}$ tanesi Q_p'nin elemanı olur. Yani $4+\left(\frac{p-3}{2}\right).2 = p+1$ olur. O halde sonuç buradan çıkar. ■

3.4.12 Örnek $p = 7$ olsun. $y^2 \equiv x^3 - 6^2 x \pmod{7}$ eğrisinde $(0,0)$, $(1,0)$, $(6,0)$, $(4,2)$, $(4,5)$, $(5,1)$ ve $(5,6)$ noktaları yer almaktadır. $Q_7 = \{1,2,4\}$ olduğundan

$$\begin{aligned}\sum_{x \in \mathbb{F}_7} \rho(x) &= \rho(0) + \rho(1) + \rho(2) + \rho(3) + \rho(4) + \rho(5) + \rho(6) \\ &= 0 + 0 + 0 + 0 + 2 + 2 + 0 \\ &= 4\end{aligned}$$

$$4 + \sum_{x \in \mathbb{F}_7} \rho(x) = 4 + 4 = 8$$

dır. O halde bu eğri üzerinde toplam 8 tane nokta bulunur. Ayrıca buradaki noktaların ordinatları toplamı da $0+0+0+2+5+1+6 = 14 \equiv 0 \pmod{7}$ olarak bulunur.

3.4.13 Teorem p bir asal ve $1 \le n \le p-1$ olsun. $E_n(\mathbb{F}_p)$'deki rasyonel noktaların sayısı $N_{p,n} = \# E_n(\mathbb{F}_p)$ olsun. O zaman

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

dır.

İspat $p \equiv 3 \pmod 4$ bir asal olsun. 3.2.1 Teoreme göre, $n \in \mathbb{F}_p^*$ için *p-1* tane eliptik eğri vardır. Herhangi bir *n* değeri için eğride sonsuzdaki nokta *o* hariç *p* tane nokta olduğundan

$$\begin{aligned}\sum_{n=1}^{p-1} N_{p,n} &= (p-1).p + (p-1) \\ &= p^2 - 1\end{aligned}$$

bulunur.

$p \equiv 1 \pmod 4$ bir asal olsun. 3.3.10 Teoreme göre,

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

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

dir. $|Q_p| = |Q'_p| = \dfrac{p-1}{2}$ tane olduğunu biliyoruz. O halde

$$\begin{aligned}\sum_{n=1}^{p-1} N_{p,n} &= \left(\frac{p-1}{2}\right).(p+1 \pm 2r) + \left(\frac{p-1}{2}\right).(p+1 \mp 2r) \\ &= \left(\frac{p-1}{2}\right).(2p+2) \\ &= (p-1).(p+1) \\ &= p^2 - 1\end{aligned}$$

olur. ■

3.4.14 Örnek $y^2 \equiv x^3 - n^2 x \pmod{13}$ eliptik eğrisini ele alalım. $1 \le n \le 12$ için nokta sayısı 3.3.10 Teoreme göre hesaplanırsa, $N_{13,1} = 8$ $N_{13,2} = 20$, $N_{13,3} = 8$, $N_{13,4} = 8$, $N_{13,5} = 20$, $N_{13,6} = 20$, $N_{13,7} = 20$, $N_{13,8} = 20$, $N_{13,9} = 8$, $N_{13,10} = 8$, $N_{13,11} = 20$, $N_{13,12} = 8$ olur. Sonuç olarak $\sum_{n=1}^{12} N_{13,n} = 13^2 - 1 = 168$ olur.

3.4.15 Örnek $y^2 \equiv x^3 - n^2 x \pmod{11}$ eliptik eğrisini ele alalım. $1 \le n \le 10$ için nokta sayısı 3.4.9 Teoreme göre $p+1$ olduğundan, $N_{11,n} = 11+1 = 12$ olur. Sonuç olarak $\sum_{n=1}^{10} N_{11,n} = 11^2 - 1 = 120$ olur.

3.4.16 Sonuç $\mathbb{F}_p$ cismi üzerindeki Frey eliptik eğrilerinin nokta sayılarıyla ilgili tüm sonuçlar, $r > 1$ doğal sayıları için $\mathbb{F}_{p^r}$ cismine genelleştirilebilir.

Yukarıdaki sonucu ve 2.6.6 Weil Teoremini kullanarak:

3.4.17 Örnek $\mathbb{F}_5$ cisminde tanımlı $y^2 = x^3 - 2^2 x$ Frey eliptik eğrisi üzerindeki noktaları bulalım. Burada $N_1 = 4$ tane nokta vardır. Bunlar $(0,0)$ $(2,0)$, $(3,0)$ ve sonsuzdaki noktadır. $N_{p,n} = p + 1 - t$ formülünden $N_{p,n} = N_1$ olduğundan $t = 2$ bulunur.

Şimdi $r = 2$ için $\mathbb{F}_{25}$ cismi üzerindeki nokta sayısını hesaplayalım. İlk olarak 2.6.6 Weil Teoremi ve 2.6.7 Uyarıya göre

$$1 - 2T + 5T^2 = 0$$

ikinci derece denkleminden $\alpha = -1 - 2i$ ve $\beta = -1 + 2i$ bulunur. Sonuç olarak da $\mathbb{F}_{25}$ cismi üzerindeki nokta sayısı

$$N_r = p^r + 1 - \alpha^r - \beta^r$$

formülünden $N_2 = 56$ bulunur. Benzer olarak $\mathbb{F}_{125}$ cismi üzerindeki nokta sayısı $N_3 = 220$ olarak hesaplanır.

3.4.18 Örnek $\mathbb{F}_7$ cisminde tanımlı $y^2 = x^3 - 3^2 x$ Frey eliptik eğrisi üzerindeki noktaları bulalım. Burada $N_1 = 8$ tane nokta vardır. Bunlar $(0,0)$, $(3,0)$, $(4,0)$, $(2,2)$, $(2,7)$, $(6,1)$, $(6,6)$ ve sonsuzdaki noktadır.

Şimdi $r = 2$ için $\mathbb{F}_{49}$ cismi üzerindeki nokta sayısını hesaplayalım. Yani N_2'yi

$$N_2 = 7^2 + 1 - \alpha^2 - \beta^2$$

bulmaya çalışalım. Eşlenik kökler α ve β'yı bulmak için $N_{p,n} = p + 1 - t$ denklemini ele alalım. $8 = 7 + 1 - t$ eşitliğinden $t = 0$ bulunur. O halde $1 + 7T^2 = 0$ denkleminin kökleri $\frac{\pm i}{\sqrt{7}}$'dir. Yani $\alpha = \sqrt{7}i$ ve $\beta = -\sqrt{7}i$ olur. Sonuç olarak nokta sayısı

$$N_r = \begin{cases} 7^r + 1 & , \ r \ tek \ ise \\ 7^r + 1 - 2.(-7)^{\frac{r}{2}} & , \ r \ çift \ ise \end{cases}$$

şeklinde ifade edilebilir. Bu durumda $N_2 = 7^2 + 1 - 2.(-7)^{\frac{2}{2}} = 64$ olur. Benzer olarak $N_3 = 7^3 + 1 = 343$ ve $N_4 = 2303$ bulunur.

4. F_p SONLU CİSİMLERİ ÜZERİNDEKİ $y^2=x^3-n^2x$ FREY ELİPTİK EĞRİLERİNİN GRUP YAPISI

4.1 Giriş

p asal olsun. $n \in \mathbb{F}_p^* = \mathbb{F}_p - \{0\}$ iken E_n Frey eliptik eğrilerinin 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 grup yapısını veren bilinen bir sonuç yoktur. $p \equiv 3 \pmod 4$ 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 $p \equiv 1 \pmod 4$ 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. $E_n(\mathbb{F}_p)$'nin mertebesini daha önceden $N_{p,n}$ ile gösterdik. Vereceğimiz sonuçların ifadesini kolaylaştırması açısından bundan sonra $N_{p,n}$ yerine bazen N kullanacağız. Nokta sayısını

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

şeklinde ifade edeceğiz. Burada t, Frobenius endomorfizminin izidir. Bu bölümde verdiğimiz örneklerde nokta sayısı ve mertebe hesaplamalarında Maple ve Visual Basic programları kullanılmıştır [22].

4.1.1 Teorem p asal olsun. E_n eliptik eğrileri için

$$N \equiv 0 (\text{mod } 4)$$

dır.

İspat $p \equiv 1 \text{ (mod 4)}$ asal olsun. Bu durumda 3.3.10 Teoreme göre $r, s \in \mathbb{Z}$, r tek ve s çift, $p = r^2 + s^2$ olmak üzere $N = p + 1 \mp 2r$ olduğunu biliyoruz. O halde

$$\begin{aligned} N &= p + 1 \mp 2r \\ &= r^2 + s^2 + 1 \mp 2r \\ &= (r \mp 1)^2 + s^2 \end{aligned}$$

r tek ve s çift olduğundan $(r \mp 1)^2 + s^2 \equiv 0 (\text{mod } 4)$ olur.

$p \equiv 3 (\text{mod } 4)$ asal olsun. Bu durumda 3.4.9 Teoreme göre $N = p + 1$ dir. $k \in \mathbb{Z}$ olmak üzere $p = 4k + 3$ yazarsak,

$$\begin{aligned} N &= p + 1 \\ &= 4k + 3 + 1 \\ &= 4(k + 1) \\ &\equiv 0 (\text{mod } 4) \end{aligned}$$

elde edilir. Böylece ispat biter.■

4.1.2 Örnek $p = 29$ olsun. $y^2 \equiv x^3 - 2^2 x \text{ (mod } 29)$ eğrisini ele alalım. $p = r^2 + s^2 = 29 = 5^2 + 2^2$ olmak üzere $r = 5$ ve $s = 2$ bulunur. 3.3.10 Teoreme göre, $r + s = 5 + 2 \equiv 3 \text{ (mod } 4)$ ve $n = 2 \in Q'_{29}$ olduğundan

$$N_{29,2} = p + 1 - 2r = 29 + 1 - 2.5 = 20 \equiv 0 \text{ (mod } 4)$$

bulunur.

4.1.3 Örnek $p = 23$ olsun. $y^2 \equiv x^3 - 14^2 x \pmod{23}$ eğrisini ele alalım. 3.4.9 Teoreme göre,

$$N_{23,14} = p + 1 = 23 + 1 = 24 \equiv 0 \pmod{4}$$

bulunur.

4.1.4 Sonuç $p > 3$ asal olsun. $E_n(\mathbb{F}_p)$'de 2. mertebeden 3 tane eleman vardır [11].

4.2 $p \equiv 1 \pmod 4$ Asal İken Frey Eliptik Eğrilerinin Grup Yapısı

E_n eğrisini ele alalım. Bu durumda $g \in Q_p'$ için

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

eğrisi $y^2 \equiv x^3 - n^2 x$ eğrisinin eşleniği olarak tanımlanır. Burada $n \in Q_p$ ise $gn \in Q_p'$ ve $n \in Q_p'$ ise $gn \in Q_p$ şeklindedir. (3.1.1) tipindeki herhangi bir eğri ile eşleniğinin t'lerinin işaretlerinin farklı olduğunu göstermek kolaydır. O halde aşağıdaki teoremi verebiliriz:

4.2.1 Teorem $p \equiv 1 \pmod 4$ bir asal olsun. (3.1.1) tipindeki eğri $a^2 b = p + 1 - t$ 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 .

4.2.2 Örnek $y^2 \equiv x^3 - 1^2 x \pmod{541}$ eliptik eğrisini 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. $y^2 \equiv x^3 - 539^2 x \pmod{541}$ eğrisi 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.

4.2.3 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

$$\begin{aligned} t \equiv 2 \pmod 8 \Leftrightarrow N &= p+1-t \\ &= 1+8n+1-(2+8m) \\ &= 8(n-m) \\ \Leftrightarrow N &\equiv 0 \pmod 8 \end{aligned}$$

ve benzer olarak

$$\begin{aligned} t \equiv 6 \pmod 8 \Leftrightarrow N &= p+1-t \\ &= 1+8n+1-(6+8m) \\ &= -4+8(n-m) \\ \Leftrightarrow N &\equiv 4 \pmod 8 \end{aligned}$$

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

4.2.4 Örnek $p = 281 \equiv 1 \pmod 8$ bir asal iken $y^2 \equiv x^3 - 14^2 x \pmod{281}$ eliptik eğrisini ele alalım. $N_{281,14} = 272$ 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 iken $y^2 \equiv x^3 - 433^2 x \pmod{461}$ eliptik eğrisini ele alalım. $N_{461,433} = 500$ ve $t = -38 \equiv 2 \pmod 8$ ve $N = 500 \equiv 4 \pmod 8$ 'dır.

4.2.5 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. Çünkü Teorem 4.1.1.'e göre, $N \equiv 0 \pmod 4$ 'tür. Bu da varsayımımızla çelişir. Bu yüzden t, 4 ile bölünemez. ■

4.2.6 Örnek $p = 397 \equiv 1 \pmod 4$ bir asal iken $y^2 \equiv x^3 - 43^2 x \pmod{397}$ eliptik eğrisini ele alalım. $N_{397,43} = 360$ 'dır. $N = p + 1 - t$ formülünden $t = 38$ bulunur. $4 \nmid 38$ 'dir. Ayrıca $y^2 \equiv x^3 - 103^2 x \pmod{257}$ eğrisini de incelersek $N_{257,103} = 260$ 'tır. Nokta sayısı formülünden $t = -2$ bulunur. Yine $4 \nmid -2$ 'dır.

4.2.7 Sonuç $p \equiv 1 \pmod 4$ asal olsun. Bu durumda $N \equiv 0$ veya $N \equiv 4 \pmod 8$ olur.

4.2.8 Örnek $y^2 \equiv x^3 - 289^2 x \pmod{389}$ eliptik eğrisini ele alalım. Nokta sayısı $N_{389,289} = 424$ 'tür. O halde $N \equiv 0 \pmod 4$ 'dır. $y^2 \equiv x^3 - 33^2 x \pmod{389}$ eğrisi için ise $N_{389,33} = 356$ 'tır. O halde $N \equiv 4 \pmod 8$ 'dır.

4.2.3 Teoremden şu sonucu verebiliriz:

4.2.9 Sonuç $p \equiv 1 \pmod 4$ bir asal ise $t \equiv \mp 2 \pmod 8$ olur.

Şimdi de $2r = |t|$ olacak şekilde bir r tam sayısı tanımlayalım. Yani $2r = |p+1-N|$ olsun. Bundan sonraki hesaplamalarımızda r ve t ile ilgili sonuçlar elde edeceğiz. (3.1.1) tipindeki eğri için $t = 2r$ ise eşleniği için $t = -2r$ 'dir. İlk olarak (3.1.1) tipindeki Frey eliptik eğrisi ve eşleniği üzerindeki rasyonel noktaların sayısı hakkında aşağıdaki sonucu verebiliriz.

4.2.10 Teorem

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

i) $t = 2r$ olmak üzere $r \equiv 1 \pmod 4$ ise (3.1.1) tipindeki eğri için $N \equiv 0 \pmod 8$ ve bu eğrinin eşleniği için $t = -2r$ ve $N \equiv 4 \pmod 8$ olur.

ii) $t = 2r$ olmak üzere $r \equiv 3 \pmod 4$ ise (3.1.1) tipindeki eğri için $N \equiv 4 \pmod 8$ ve bu eğrinin eşleniği için $t = -2r$ ve $N \equiv 0 \pmod 8$ olur.

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

i) $t = 2r$ olmak üzere $r \equiv 1 \pmod 4$ ise (3.1.1) tipindeki eğri için $N \equiv 4 \pmod 8$ ve bu eğrinin eşleniği için $t = -2r$ ve $N \equiv 0 \pmod 8$ olur.

ii) $t = 2r$ olmak üzere $r \equiv 3 \pmod 4$ ise (3.1.1) tipindeki eğri için $N \equiv 0 \pmod 8$ ve bu eğrinin eşleniği için $t = -2r$ ve $N \equiv 4 \pmod 8$ olur.

İspat $p \equiv 1 \pmod 8$ asal olsun. $n \in \mathbb{Z}$ için $p = 1 + 8n$ yazalım. $t \equiv 2 \pmod 8$ ve $t = 2r$ olmak üzere $r \equiv 1 \pmod 4$ 'dir. Şimdi $m \in \mathbb{Z}$ için $t = 2 + 8m$ yazalım. O halde

$$\begin{aligned} N &= p + 1 - t = 1 + 8n + 1 - 2 - 8m \\ &= 8(n - m) \end{aligned}$$

olur. Bu da $N \equiv 0 \pmod 8$ oluşunu gerektirir. Diğer kısımlar benzer şekilde ispatlanabilir.■

4.2.11 Örnek $p = 73 \equiv 1 \pmod 8$ bir asal iken $y^2 \equiv x^3 - 12^2 x \pmod{73}$ eliptik eğrisini ele alalım. $N_{73,12} = 80$ ve $t = -6$ olur. $t = 2r$ olduğundan $r = -3 \equiv 1 \pmod 4$ 'dir. O halde $N \equiv 0 \pmod 8$ 'dir. Bu eğrinin bir eşleniği olan $y^2 \equiv x^3 - 29^2 x \pmod{73}$ eğrisi üzerindeki nokta sayısının $N_{73,29} = 68$ olduğunu buluruz. Nokta sayısı formülünden $t = 6$ bulunur. $t = -2r$ olduğundan $r = -3 \equiv 1 \pmod 4$ bulunur. O halde $N \equiv 4 \pmod 8$ 'dir.

4.3 Frey Eliptik Eğrileri Üzerindeki 4. Mertebeden Elemanlar

Bu bölümde E_n Frey eliptik eğrilerinde 4. mertebeden eleman bulunma koşulları belirlenecek ve bunlarla ilgili bazı sonuçlar elde edilecektir. $p \equiv 1 \pmod 4$ bir asal olduğunda, E_n Frey eliptik eğrileri için iki tip grup yapısı vardır:

a) 4. mertebeden eleman içeren grup yapısı,
b) 4. mertebeden eleman içermeyen grup yapısı.

4.3.1 Sonuç

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

i) $r \equiv 1 \pmod 4$ ise (3.1.1) tipindeki eğri için $t = 2r$ ve $N \equiv 0 \pmod 8$ olur. Ayrıca $E_n(\mathbb{F}_p)$ 'nin 4. mertebeden elemanı vardır. Bu eğrinin eşleniği için $t = -2r$ ve $N \equiv 4 \pmod 8$ olur. Bu da grubun 4. mertebeden eleman bulundurmamayı gerektirir.

ii) $r \equiv 3 \pmod 4$ ise (3.1.1) tipindeki eğri için $t = 2r$ ve $N \equiv 4 \pmod 8$ olur. Ayrıca $E_n(\mathbb{F}_p)$ 'nin 4. mertebeden elemanı yoktur. Bu eğrinin eşleniği için $t = -2r$ ve $N \equiv 0 \pmod 8$ olur. Bu da grubun 4. mertebeden eleman bulundurmasını gerektirir.

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

i) $r \equiv 1 \pmod 4$ ise (3.1.1) tipindeki eğri için $t = 2r$ ve $N \equiv 4 \pmod 8$ olur. Bu yüzden de $E_n(\mathbb{F}_p)$'nin 4. mertebeden elemanı yoktur. Bu eğrinin eşleniği için $t = -2r$ ve $N \equiv 0 \pmod 8$ olur. Bu da grubun 4. mertebeden eleman bulundurmasını gerektirir.

ii) $r \equiv 3 \pmod 4$ ise (3.1.1) tipindeki eğri için $t = 2r$ ve $N \equiv 0 \pmod 8$ olur. Ayrıca $E_n(\mathbb{F}_p)$'nin 4. mertebeden elemanı vardır. Bu eğrinin eşleniği için $t = -2r$ ve $N \equiv 4 \pmod 8$ olur. Bu yüzden de grubun 4. mertebeden elemanı yoktur.

4.3.2 Örnek $p = 349 \equiv 5 \pmod 8$ bir asal iken $y^2 \equiv x^3 - 71^2 x \pmod{349}$ eliptik eğrisini ele alalım. $N_{349,71} = 340$, $t = 10$ ve $r = 5 \equiv 1 \pmod 4$'dır. O halde $N = 340 \equiv 4 \pmod 8$ olur. Bu yüzden de eğrinin 4. mertebeden elemanı yoktur. Bu eğrinin bir eşleniği olan $y^2 \equiv x^3 - 16^2 x \pmod{349}$ eliptik eğrisini alırsak $N_{349,16} = 360$, $t = -10$ ve $r = 5 \equiv 1 \pmod 4$ olur. O halde $N = 360 \equiv 0 \pmod 8$'dır. Bu da 4. mertebeden eleman bulundurmasını gerektirir. Bunlar da $(82, 269)$, $(82, 80)$, $(267, 43)$ ve $(267, 306)$ noktalarıdır.

Frey eliptik eğrilerinin p modunda sınıflandırılmasında 4. mertebeden elemanlar çok önemli bir yer tutmaktadır. Şimdi 4. mertebeden eleman sayısının 4 veya 12 olduğunu gösterelim.

4.3.3 Teorem $p \equiv 1 \pmod 4$ bir asal olsun. Eğer E_n eğrisi üzerindeki nokta sayısı $N \equiv 0 \pmod 4$ ise eğri üzerinde 4. mertebeden 4 ya da 12 tane nokta vardır.

İspat 2.3.24 Teorem ve 2.3.25 Sonuç gereği E_n eğrisi üzerinde sonsuzdaki nokta ile birlikte en çok 16 nokta vardır. Bu noktalar için mümkün olan 14 farklı grup tipi vardır [24]. Fakat 4.1.4 Sonuçtan biliyoruz ki 2. mertebeden yalnız 3 nokta içeren bir grup yapısı söz konusudur. Bu durumu ele aldığımızda olabilecek grup

tipleri 5'e düşer. Bunların 4. mertebeden elemanlarının mertebelerini incelediğimizde 4 ya da 12 olduğu kolayca görülür. ■

4.3.4. Örnek $y^2 \equiv x^3 - 33^2 x \pmod{37}$ eliptik eğrisini ele alalım. Nokta sayısı $N_{37,33} = 40 \equiv 0 \pmod 4$ olur. Bu eğri üzerinde 4. mertebeden 4 eleman vardır: $(13,18)$, $(13,19)$, $(24,3)$ ve $(24,34)$. $y^2 \equiv x^3 - 5^2 x \pmod{41}$ eliptik eğrisi için ise $N_{41,5} = 32 \equiv 0 \pmod 4$ 'dır. Bu eğri üzerinde 4. mertebeden 12 eleman vardır: $(2,9)$, $(2,32)$, $(4,13)$, $(4,28)$, $(8,5)$, $(8,36)$, $(33,4)$, $(33,37)$, $(37,6)$, $(37,35)$, $(39,1)$ ve $(39,40)$.

4.3.5 Sonuç $p \equiv 1 \pmod 4$ bir asal olsun. Bu durumda

a) $p \equiv 1 \pmod 8$ ise $E_n(\mathbb{F}_p)$ 'nin 4. mertebeden 12 tane elemanı vardır. Bunun eşleniğinin ise 4. mertebeden elemanı yoktur.

b) $p \equiv 5 \pmod 8$ ise $E_n(\mathbb{F}_p)$ 'nin 4. mertebeden 4 tane elemanı vardır. Bunun eşleniğinin ise 4. mertebeden elemanı yoktur.

İspat 4.3.1 Sonuçtan kolayca görülür.■

4.3.6 Örnek $y^2 \equiv x^3 - 55^2 x \pmod{457}$ eliptik eğrisini ele alalım. $p = 457 \equiv 1 \pmod 8$ 'dir. Bu eğri üzerinde 4. mertebeden 12 eleman vardır: $(54,91)$, $(54,366)$, $(115,331)$, $(115,126)$, $(225,345)$, $(225,112)$, $(232,131)$, $(232,326)$, $(342,24)$, $(342,433)$, $(403,135)$ ve $(403,322)$. $y^2 \equiv x^3 - 24^2 x \pmod{509}$ eliptik eğrisi için ise $p = 509 \equiv 5 \pmod 8$ olur. O halde bu eğri üzerinde 4. mertebeden 4 eleman vardır: $(98,155)$, $(98,354)$, $(411,336)$ ve $(411,179)$.

4.3.7 Teorem $p \equiv 1 \pmod 4$ bir asal olsun. E_n eğrisinde

a) Eğer $n \in Q_p$ ise $E_n(\mathbb{F}_p)$ 'nin 4. mertebeden 4 ya da 12 tane elemanı vardır,

b) Eğer $n \in Q'_p$ ise $E_n(\mathbb{F}_p)$ 'nin 4. mertebeden elemanı yoktur.

İspat 4.3.1 Sonuç ve 4.3.5 Sonuçtan görülür. ■

4.3.8 Örnek $y^2 \equiv x^3 - 12^2 x \pmod{61}$ eğrisinde $12 \in Q_{61}$ olduğundan 4. mertebeden 4 tane eleman vardır. $y^2 \equiv x^3 - 32^2 x \pmod{73}$ eğrisinde ise $32 \in Q_{73}$ olduğundan 4. mertebeden 12 tane eleman vardır. $y^2 \equiv x^3 - 68^2 x \pmod{73}$ eğrisinde $68 \in Q'_{73}$ olduğundan 4. mertebeden eleman yoktur.

4.3.9 Teorem $p \equiv 1 \pmod 4$ bir asal olsun. E_n eğrisinde

a) $n \in Q_p$ olması için gerek ve yeter şart $N \equiv 0 \pmod 8$,

b) $n \in Q'_p$ olması için gerek ve yeter şart $N \equiv 4 \pmod 8$ 'dır.

İspat 4.3.1 Sonuç ve 4.3.7 Teoremden görülür. ■

4.3.10 Örnek $y^2 \equiv x^3 - 14^2 x \pmod{113}$ eğrisinde $14 \in Q_{113}$ olduğundan $N = 128 \equiv 0 \pmod 8$ 'dır. $y^2 \equiv x^3 - 21^2 x \pmod{137}$ eğrisinde ise $21 \in Q'_{137}$ olduğundan $N = 116 \equiv 4 \pmod 8$ elde edilir.

4.3.11 Teorem $p \equiv 1 \pmod 4$ bir asal olsun. E_n eğrisinde

a) $N \equiv 0 \pmod 8$ ise $E_n(\mathbb{F}_p)$ 'nin 4. mertebeden 4 ya da 12 tane elemanı vardır,

b) $N \equiv 4 \pmod 8$ ise $E_n(\mathbb{F}_p)$ 'nin 4. mertebeden elemanı yoktur.

İspat 4.3.7 Teorem ve 4.3.9 Teoremden kolayca görülür. ■

4.3.12 Örnek $y^2 \equiv x^3 - 10^2 x \pmod{13}$ eliptik eğrisini ele alalım. $N = 8 \equiv 0 \pmod 8$ 'dır. Bu eğri üzerinde 4. mertebeden 4 tane eleman vardır: $(2,4)$, $(2,9)$, $(11,6)$ ve $(11,7)$. $y^2 \equiv x^3 - 4^2 x \pmod{17}$ eliptik eğrisi için ise $N = 16 \equiv 0 \pmod 8$ olur. Bu eğri üzerinde ise 4. mertebeden 12 tane eleman vardır: $(1,6)$, $(1,11)$, $(3,8)$, $(3,9)$, $(6,1)$, $(6,16)$, $(11,4)$, $(11,13)$, $(14,2)$, $(14,15)$, $(16,7)$ ve $(16,10)$. Şimdi de $y^2 \equiv x^3 - 14^2 x \pmod{17}$ eliptik eğrisi için $N = 20 \equiv 4 \pmod 8$ olduğundan bu eğride 4. mertebeden eleman yoktur.

4.3.13 Teorem p bir asal olsun. x'in 1 ile p arasında $x^3 - x \equiv 0 \pmod{p}$ şartını sağlayan 3 değeri vardır.

İspat $x(x-1)(x+1) \equiv 0 \pmod{p}$ denkliğinin 3 tane çözümü olduğu açıktır. Bunlar $x \equiv 0 \pmod{p}$, $x \equiv 1 \pmod{p}$ ve $x \equiv p-1 \pmod{p}$ değerleridir. ■

4.3.14 Teorem $p \equiv 1 \pmod{4}$ asal olsun. Bu durumda

$$\sum_{x \in \mathbb{F}_p} \chi(x^3 - x) \equiv 2 \pmod{4}$$

olur.

İspat Her bir $x \in \mathbb{F}_p$ için $x^3 - x$'in p tane değeri hesaplanabilir. 4.3.13 Teorem gereği bu değerlerden üçü 0'dır. $x^3 - x$'in kalan p-3 değeri $\frac{p-3}{2}$ tane ikili şeklinde gruplandırılabilir. $p \equiv 1 \pmod{4}$ iken $\frac{p-3}{2}$ tektir. Gerçekten $k \in \mathbb{Z}$ için $p = 1 + 4k$ yazarsak $\frac{p-3}{2} = 2k - 1$ olur. Varsayalım ki bu ikililerden s tanesi Q_p'de $2k - 1 - s$ tanesi de Q_p''ünde olsun. Bir ikili Q_p'de ise $\sum_{x \in \mathbb{F}_p} \chi(x^3 - x)$ toplamına 2 eklenir. Eğer Q_p' nde ise toplama (-2) eklenir. Bu yüzden

$$\begin{aligned} \sum_{x \in \mathbb{F}_p} \chi(x^3 - x) &= 3.0 + s.(+2) + (2k - 1 - s).(-2) \\ &= 4(s - k) + 2 \end{aligned}$$

ifadesi sonucu gerektirir. ■

4.3.15 Örnek $p=17$ olsun. $Q_{17}=\{1,2,4,8,9,13,15,16\}$ olduğuna göre, bu durumda,

$$\begin{aligned}\sum_{x\in\mathbb{F}_{17}}\chi(x^3-x) &= \chi(0)+\chi(0)+\chi(6)+\chi(7)+\chi(9)+\chi(1)+\chi(6)\\ &\quad+\chi(13)+\chi(11)+\chi(6)+\chi(4)+\chi(11)+\chi(16)\\ &\quad+\chi(8)+\chi(10)+\chi(11)+\chi(0)\\ &=0+0-1-1+1+1-1+1-1-1+1-1+1+1-1-1+0\\ &=-2\equiv 2 \pmod 4\end{aligned}$$

4.3.16 Sonuç $p\equiv 1 \pmod 4$ asal olsun. Eğer $N\equiv 0 \pmod 4$ ise $t\equiv 2 \pmod 4$ dır.

İspat. $N=p+1-t=p+1+\sum_{x\in\mathbb{F}_p}\chi(x^3-n^2x)$ iken $t=-\sum_{x\in\mathbb{F}_p}\chi(x^3-n^2x)$ olduğu bilinir. 4.1.1 Teoremden sonuç görülür. ■

4.3.17 Örnek $y^2\equiv x^3-27^2x \pmod{409}$ eliptik eğrisini ele alalım. $N=416\equiv 0 \pmod 4$ olduğundan $N=p+1-t$ formülünü kullanarak $416=409+1-t$, $t=-10$ ve $t=-10\equiv 2 \pmod 4$ elde edilir.

5. SONUÇLAR

Bu çalışmada, p asal iken $\mathbb{F}_p$ sonlu cisimleri üzerindeki $E_n : y^2 = x^3 - n^2 x$ Frey eliptik eğrilerinin nokta sayıları ve grup yapısı hakkında bilgi vermek amaçlanmıştır.

Çalışmanın 3.1 kısmında Frey eliptik eğrilerinden bahsedilmiştir.

3.2 bölümünde, $\mathbb{F}_p$ sonlu cisimlerinde, herhangi bir p asalı için Frey eliptik eğrilerinin sayılarını ve bu eğrideki noktaların apsisleri ve ordinatlarıyla ilgili durumları açıklayan teoremler verilmiştir. Bunların ispatları yapılmıştır.

3.3 bölümünde, p'nin 4 modunda 1'e denk olduğu durumda, $y^2 = x^3 - n^2 x$ eğrisinde, rasyonel noktaların özellikleriyle ilgili elde edilen teoremler verilmiş ve ispatlanmıştır.

3.4 bölümünde ise, p'nin 4 modunda 3'e denk olduğu durumda, $y^2 = x^3 - n^2 x$ eğrisinde, rasyonel noktaların özellikleriyle ilgili elde edilen teoremler ifade ve ispat edilmiştir.

4.1 bölümünde, $\mathbb{F}_p$ sonlu cisimleri üzerindeki $y^2 = x^3 - n^2 x$ Frey eliptik eğrilerinin grup yapısı ifade edilmiştir. Nokta sayısının p asalı için $N \equiv 0 \pmod 4$ olduğunu veren bir teorem ifade ve ispat edilmiştir.

4.2 bölümünde, $p \equiv 1 \pmod 4$ bir asal olmak üzere E_n eğrisi üzerindeki rasyonel noktaların grup yapısının $E_n(\mathbb{F}_p) \cong \mathbb{Z}_a \times \mathbb{Z}_{a.b}$ olduğu ve bunun eşleniğinin $\mathbb{Z}_d \times \mathbb{Z}_{d.e}$ olduğu bir teoremle ifade edilmiştir. t'nin 8 modundaki durumlarına göre,

E_n eğrisi üzerindeki rasyonel noktaların sayısının aldığı dört farklı durum teoremle ifade edilmiş ve ispatlanmıştır.

4.3 bölümünde, $p \equiv 1 \pmod 4$ bir asal olmak üzere E_n eğrisi üzerindeki 4. mertebeden elemanlar incelenmiştir. Grup yapısının, 4. mertebeden eleman içeren ya da içermeyen olmak üzere iki türlü olduğu görülmüştür. 4. mertebeden eleman varsa, bunların sayısının 4 veya 12 olduğu ifade edilmiştir. n'nın Q_p'nin elemanı olup olmamasına göre nokta sayısının bir sınıflandırması yapılmıştır. p, n, t ve N arasındaki tüm ilişkiler belirlenmiştir. Bunlar teorem olarak ifade edilip ispatlanmıştır.

Çalışmada, $p \equiv 1 \pmod 4$ bir asal olmak üzere $\mathbb{F}_p$ sonlu cisimleri üzerindeki $E_n : y^2 = x^3 - n^2 x$ eliptik eğrisinin grup yapısı ile ilgili sonuçlar elde edilmiştir. Ayrıca $p \equiv 3 \pmod 4$ durumundaki eğrilerin grup yapısı da çalışılabilir.

EK A : "$y^2 = x^3 - n^2 x \pmod{p}$ EĞRİSİ ÜZERİNDEKİ NOKTALARIN MERTEBELERİNİ BULMA"

```
> #y^2=x^3-n^2x (mod p) EĞRİSİNDEKİ NOKTALARIN MERTEBELERİNİ
BULMA#
> restart;
> mertebe:=proc(x1,y1,p,k);
x:=int;y:=int;x2:=int;y2:=int;
> n:=2;
> if y1<>0 then
>    n:=n+1;
>    m:=((3*x1^2-k^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;
```

```
mertebe := proc(x1, y1, p, k)
local x, y, x2, y2, n, m;
    x := int;
    y := int;
    x2 := int;
        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;
end proc
```

```
y2 := int;
n := 2;
if y1 ≠ 0 then
    n := n + 1;
    m := (1/2×(3×x1^2 – k^2)/y1) mod p;
        y2 := y
    end do;
    print("mertebe:", n)
else print("mertebe:", n)
end if
```

```
> hesapla:=proc(p,k);
xgec:=int;ygec:=int;l:=int;
> for xgec from 0 to p-1 do
> with(numtheory);
> l:=xgec^3-(k^2)*xgec;
> 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,k);
> end if;
> end do;
> end proc;
```

```
hesapla := proc(p, k)
local xgec, ygec, l;
    xgec := int;
    ygec := int;
    l := int;
        if ygec ≠ 0 then print([xgec, ygec], [xgec, –ygec])
        else print([xgec, ygec])
        end if ;
        mertebe(xgec, ygec, p, k)
    end if
```

```
for xgec from 0 to p – 1 do
    with(numtheory);
    l := xgec^3 – k^2×xgec;
    ygec := msqrt(l, p);
    if ygec ≠ FAIL then
```

```
end do
end proc
```

- **hesapla(5,1);**
-

[0, 0]

"mertebe:", 2

[1, 0]

"mertebe:", 2

[2, 1], [2, -1]

"mertebe:", 4

[3, 2], [3, -2]

"mertebe:", 4

[4, 0]

"mertebe:", 2

EK B : " $y^2 = x^3 - n^2 x \pmod{p}$ EĞRİSİ ÜZERİNDEKİ NOKTALARIN MERTEBELERİNİ 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 And 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()

'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)
```

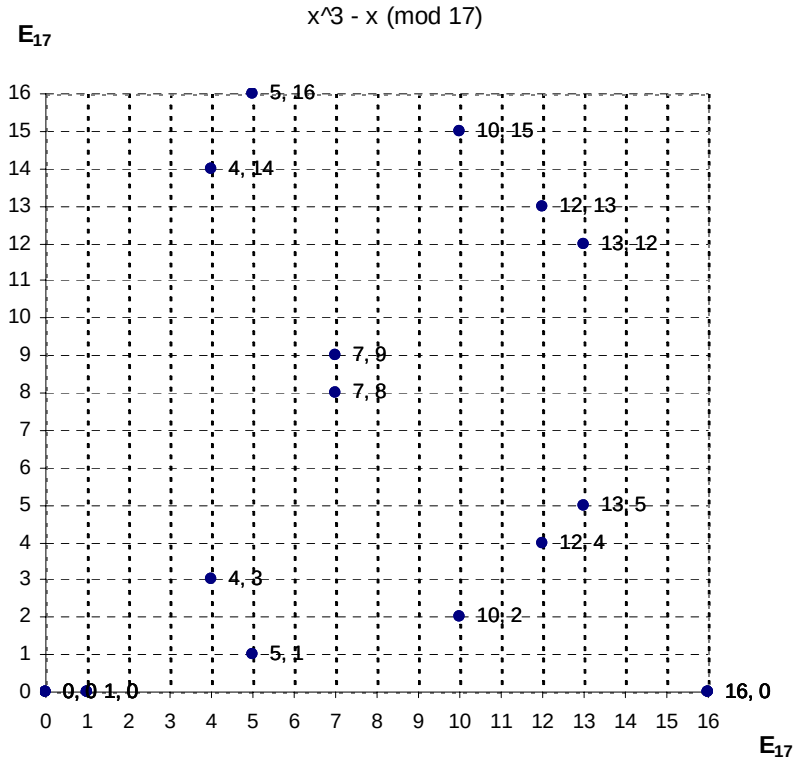
```
Sheets(1).Cells(gg, 2) = yf
Sheets(1).Cells(gg, 3) = Sheets("nokta belirle").Cells(2, 2)
Sheets(1).Cells(gg, 4) = Sheets("nokta belirle").Cells(2, 3)
i = 2
x1 = Sheets(1).Cells(gg, 1)
y1 = Sheets(1).Cells(gg, 2)
k = Sheets(1).Cells(gg, 3)
a = Sheets(1).Cells(gg, 4)
Sheets(1).Cells(2, 2 * gg + 3) = 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 And 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
```

EK C : " $y^2 = x^3 - 1^2 x \pmod{17}$ EĞRİSİ ÜZERİNDEKİ NOKTALAR, BU NOKTALARIN KUVVETLERİ VE MERTEBELERİ**"**

x	y	MOD	n	MERT	KUV	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
0	0	17	-1	2	1	0	0	1	0	4	3	4	14	5	1	5	16	7	8	7	9	10	2	10	15	12	4	12	13	13	5	13	12	16	0
1	0	17	-1	2	2					0	0	0	0	16	0	16	0	1	0	1	0	16	0	16	0	1	0	1	0	0	0	0	0		
4	3	17	-1	4	3					4	14	4	3	5	16	5	1	7	9	7	8	10	15	10	2	12	13	12	4	13	12	13	5		
4	14	17	-1	4																															
5	1	17	-1	4																															
5	16	17	-1	4																															
7	8	17	-1	4																															
7	9	17	-1	4																															
10	2	17	-1	4																															
10	15	17	-1	4																															
12	4	17	-1	4																															
12	13	17	-1	4																															
13	5	17	-1	4																															
13	12	17	-1	4																															
16	0	17	-1	2																															



EK D : "*p*=1 (mod 4) ASALLARIN LİSTESİ"

 # *p*=1 (mod 4) 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 4;
if x = 1 then
>   lprint(a);
>  end if;
> end do;
end proc;
> asallistele(1000);
```

EK E : "*p*=3 (mod 4) ASALLARIN LİSTESİ"

 # *p*=3 (mod 4) 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 4;
if x = 3 then
>   lprint(a);
>  end if;
> end do;
end proc;
> asallistele(1000);
```

EK F : " $y^2 = x^3 - n^2 x \pmod{p}$ EĞRİSİ ÜZERİNDEKİ RASYONEL NOKTA SAYISINI HESAPLAMA"

>\# y^2=x^3-n^2x (mod *p*) EĞRİSİ ÜZERİNDEKİ RASYONEL NOKTA SAYISINI HESAPLAMA#

```
> restart;
> p:=prime;a:=int;n:=posint;l:int;
> hesapla:=proc(p,k);
>  n:=p+1;
>    for x from 0 to p-1 do
>      with(numtheory):
>       l:=legendre(x^3-k^2x,p);
>       n:=n+l;
>    end do;
>  end proc;
> hesapla(p,n);
```

EK G : "*p* MODUNDA İKİNCİ DERECEDEN KALANLARI HESAPLAMA"

> # *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);
```

EK H : "37 MODUNDA İKİNCİ DERECEDEN KALANLARI HESAPLAMA"

```
>#Q37 '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(37);
```

```
p := prime
x := int
s := int

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
```

1

3

4

7

9

10

11

12

16

21

25

26

27

28

30

33

34

36

>

EK I : “*p* MODUNDA ÜÇÜNCÜ DERECEDEN KALANLARI HESAPLAMA”

```
>#  p MODUNDA ÜÇÜNCÜ DERECEDEN KALANLARI HESAPLAMA #
> restart;
 p:=prime;x:=int;s:=int;
 hesapla:=proc(p);
    for x from 0 to p-1 do
      with(numtheory):
      s:=mroot(x,3,p);
      if s<>FAIL then
         print(x);
      end if;
    end do;
 end proc;
 hesapla(p);
```

EK J : "37 MODUNDA ÜÇÜNCÜ DERECEDEN KALANLARI HESAPLAMA"

># K_{37} 'i HESAPLAMA #

```
> restart;
 p:=prime;x:=int;s:=int;
 hesapla:=proc(p);
   for x from 0 to p-1 do
     with(numtheory):
     s:=mroot(x,3,p);
     if s<>FAIL then
       print(x);
     end if;
   end do;
 end proc;
 hesapla(37);
```

$$p := prime$$

$$x := int$$

$$s := int$$

```
hesapla := proc(p)
local x, s;
    for x from 0 to p − 1 do
        with(numtheory); s := mroot(x, 3, p); if s ≠ FAIL then print(x) end if
    end do
                                    end proc
```

0

1

6

8

10

11

14

23

26

27

29

31

36

>

KAYNAKLAR

[1] Jones, G.A., Jones, J.M., Elementary Number Theory, Springer-Verlag New York, Inc., (1998).

[2] LeVeque, W.J., Fundamentals of Number Theory, Dover Publications, New York, (1996).

[3] Gioia, A.A., The Theory of Numbers An Introduction, Dover Publications, New York, (2001).

[4] Andrews, G.E., Number Theory, Dover Publications, New York, (1994).

[5] Mollin, R.A., Algebraic Number Theory, Chapman&Hall/CRC, United States of America, (1999).

[6] Schmitt, S., Zimmer, H.G., Elliptic Curves A Computational Approach, Walter de Gruyter, Berlin, (2003).

[7] Silverman, J. H., Tate, J., Rational Points on Elliptic Curves, Springer-Verlag New York, Inc., (1992).

[8] Mollin, R.A., An Introduction to Cryptography, Chapman&Hall/CRC, United States of America, (2001).

[9] Knapp, A.W., Elliptic Curves, Princeton University Press, New Jersey, (1992).

[10] Washington, L. C., Elliptic Curves Number Theory and Cryptography, Chapman & Hall/CRC, United States of America, (2003).

[11] Kato, K., Kurokawa, N., Saito, T., "Number Theory 1 Fermat's Dream", American Mathematical Society, United States of America, (2000) 154 p.

[12] Silverman, J. H., A Friendly Introduction to Number Theory, Prentice-Hall, Inc., New Jersey, (2001).

[13] Silverman, J. H., "Points of Finite order on Elliptic Curve", The American Mathematical Monthly, Volume 93, No.10 December, (1986) 793-795 p.

[14] Hankerson, D., Menezes, A., Vanstone, S., Guide to Elliptic Curve Cryptography, Springer-Verlag New York, Inc., (2004).

[15] Koblitz, N., A Course in Number Theory and Cryptography, Springer-Verlag New york, Inc., (1994).

[16] Hellegouarch, Y., Invitation to the Mathematics of Fermat-Wiles, Academic Press, 84 Theobald's Road, London WC1X8RR, (2002).

[17] Cassels, J.W.S., Lectures on Elliptic Curves, Cambridge University Press, (1991).

[18] Rosing, M., Implementing Elliptic Curve Cryptography, Manning Publications Co., (1999).

[19] Silverman, J. H., The Arithmetic of Elliptic Curves, Springer-Verlag New York, Inc., (1986).

[20] Blake, I.F., Seroussi, G., Smart, N.P., Elliptic Curves in Cryptography, Cambridge University Press, (1999).

[21] Stinson, D.R., Cryptography Theory and Practice, Chapman & Hall/CRC, United States of America, (2002).

[22] Çelik, B., Maple ve Maple ile Matematik, Nobel Yayın Dağıtım Adakale sok. No:15/2 Yenişehir, Ankara, (2004).

[23] Sury, B., "Elliptic Curves over Finite Fields", Proceedings of the Advanced Instructional Workshop on Algebraic Number Theory, HRI, Allahabad, (2000) Hindustan Book Agency, New Delhi (2003) 33-47 p.

[24] Thomas, A.D., Wood, G.V., Group Tables, Shiva Publishing Limited, 9 Clareville Road, Orpington, Kent BR5 1RU, UK, (1980).

[25] Bremner, A., Cassels, W.S., "On the Equation $Y^2 = X(X^2 + p)$", Mathematics of Computation, Volume 42, Number 165, January, (1984) 257-264 p.

[26] Bremner, A., "An Equation of Mordell", Mathematics of Computation, Volume 29, Number 131, July, (1975) 925-928 p.