T.C.
ULUDAĞ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SONLU CİSİMLER ÜZERİNDE BACHET ELİPTİK EĞRİLERİ

Gökhan SOYDAN

DOKTORA TEZİ
MATEMATİK ANABİLİM DALI

BURSA 2006

ÖZET

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

Birinci bölümde, çalışmanın ikinci ve üçüncü bölümlerine temel oluşturacak kavramlar verilmiştir. İkinci bölümde $y^2 = x^3 + a^3$ Bachet eliptik eğrilerinin nokta sayıları ile ilgili bazı sonuçlar verilmiştir. Üçüncü bölümde bu eğrilerin $p \equiv 5 \pmod 6$ bir asal iken devirli grup yapısına sahip olduğu; $p \equiv 1 \pmod 6$ bir asal ve $m, n \in \mathbb{N}^+$ iken de ya $C_n \times C_{nm}$ ya da $p = n^2 \pm n + 1$ olmak üzere $C_n \times C_n$ şeklinde bir grup yapısına sahip olduğu gösterilmiştir. Bu eğrilerin grup yapısı incelenirken nokta sayısına da bakılmıştır. Ayrıca a'nın Q_p'de bulunup bulunmayışına göre grubun üçüncü mertebeden elemana sahip olup olmayacağı gösterilmiştir.

Anahtar Kelimeler: Sonlu cisimler üzerinde eliptik eğriler, rasyonel noktalar, Bachet eliptik eğrileri, Weierstrass eliptik eğrileri.

ABSTRACT

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

In the first chapter, the fundamental notions necessary in the second and third chapters are recalled. In the second chapter, some results concerning the number of rational points on Bachet elliptic curves $y^2 = x^3 + a^3$ are given. In the third chapter, it is shown that the group structure of the rational points on these curves is cyclic when $p \equiv 5 \pmod 6$ is prime; and while $p \equiv 1 \pmod 6$ is prime, it is isomorphic to the direct product of two cyclic groups $C_n \times C_{nm}$ where $m, n \in \mathbb{N}^+$ or to the direct product $C_n \times C_n$ with $p = n^2 \pm n + 1$. While studying the group structure of these curves, the number of points is also discussed. Furthermore, whether the group has a point of order three or not according to a belongs to Q_p or not is shown.

Key Words: Elliptic curves over finite fields, rational points, Bachet elliptic curves, Weierstrass elliptic curves.

İÇİNDEKİLER

SİMGELER DİZİNİ

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

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

ŞEKİLLER DİZİNİ **Sayfa**

ÇİZELGELER DİZİNİ **Sayfa**

GİRİŞ

Bu çalışmanın amacı, p asal iken $\mathbb{F}_p$ sonlu cisimlerinde basitleştirilmiş Weierstrass denkleminin özel bir hali olan Bachet eliptik eğrilerinin nokta sayılarını ve grup yapısını incelemektir.

Bilindiği gibi Diophant denklemleri teorisi, tam sayılardaki polinom denklemlerin çözümü ile ilgilenen bir sayılar teorisi dalıdır. Bu konu adını eski Yunan cebircisi Diophantus Alexandra'dan alır. Diophantus bu denklemlerin çözümlerini formülize etmiştir.

Bu denklemleri temel alan bir başka popüler problem Fermat'ın son teoremidir. 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.

Diğer bir örnek de bir tam sayıyı, kare ile kübün farkı olarak yazma problemidir. Bir başka ifadeyle sabit bir $c \in \mathbb{Z}$ tam sayısı için

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

Diophant denkleminin çözümlerini araştıralım. Bu denklem *"Bachet denklemi"* olarak adlandırılır. Ayrıca *"Mordell denklemi"* olarak da bilinir. 20. yüzyılın ünlü matematikçisi L. J. Mordell bu ve benzeri birçok Diophant denkleminin çözümüne temel oluşturacak katkılarda bulunmuştur.

Bu denklemin $x, y \in \mathbb{Q}$ rasyonel sayı çözümleriyle ilgilenmediğimizi varsayalım. Denklemi ilginç kılan özellik *"ikiye katlama formülü (duplication formula)"*nün varlığıdır. Bu formül 1621'de Bachet tarafından keşfedilmiştir. $x, y \in \mathbb{Q}$ iken (x, y) bu denklem için bir çözüm ise aynı denklem için

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

ifadesinin de bir çözüm olduğunu göstermek kolaydır. Bundan başka, orijinal çözüm $xy \neq 0$ ve $c \neq 1, -432$ ise bu durumda ikiye katlama formülünün sonsuz çoklukta farklı çözüme götürdüğünü ispatlamak mümkündür. (Bachet bunu ispatlayamamıştır.)

Böylece bir tam sayı küp ve kare farkı olarak ifade edilebiliyorsa, bu sonsuz çoklukta yolla ifade edilebilir. Örneğin,

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

denklemine $(3,5)$ çözümüyle başlarsak ve Bachet ikiye katlama formülünü uygularsak

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

çözümlerinin bir dizisini elde ederiz.

Sonra aynı denklemin $x, y \in \mathbb{Z}$ çözümlerini arayalım. 1650'lerde Fermat İngiliz matematik topluluğuna $y^2 - x^3 = -2$ denkleminin tam sayılarda sadece iki çözümü $(3, \pm 5)$ olduğunu iddia etmiştir. Bu, biraz önce görmüş olduğumuz rasyonel sayılardaki çözümlerin sonsuz çoklukta oluşuyla çelişen bir iddiadır. Fakat dönemindeki matematikçilerin hiçbiri bu problemi çözemedi. 1730'larda Euler tarafından yanlış bir şekilde çözüldü. 150 yıl sonra ispatın doğrusu verildi. 1908'de Axel Thue konuyla ilgili olağanüstü bir gelişme kaydetti. c sıfırdan farklı bir tam sayı iken $y^2 - x^3 = c$ denkleminin sonlu sayıda x, y tam sayı çözümü olabileceğini gösterdi. Bu, Fermat'ın iddiasının bir genellemesidir. Rasyonel sayılarda sonsuz çoklukta çözümü olmasına rağmen tam sayı çözümleri sonlu tanedir.

Şimdi tam sayılar ve rasyonel sayılar üzerindeki üçüncü dereceden polinomları gözden geçirelim. Böyle polinomlar için bir örnek,

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

ile verilen Bachet denklemidir. Bundan başka

$$y^2 = x^3 + ax^2 + bx + c \text{ ve } ax^3 + by^3 = c$$

eğrileri örnek olarak verilebilir. Böyle denklemlerin reel çözümleri kübik eğriler veya eliptik eğriler olarak adlandırılır.

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

İkinci olarak kübik denklemin sonsuz çoklukta da olabilecek rasyonel çözümlerinin tümü, çözümlerin sonlu bir kümesi ile başlanarak ve Bachet'in ikiye katlama formülüne benzer geometrik bir işlemin tekrarlı uygulamasıyla bulunabilir. Böyle üretilmiş sonlu kümelerin var olduğu 1901'de Poincaré tarafından ortaya atıldı.

1922'de L.J. Mordell $\mathbb{Q}$ sayı cisminde tanımlı eliptik eğriler üzerindeki rasyonel noktaların grubunun daima sonlu üreteçli olduğunu ispatladı. 1928'de de Weil bu teoremi tezinde sayı cisimlerine ve yüksek cinse sahip eğrilere karşılık gelen durumlara genelleştirmiştir. Mordell teoreminin ispatı rasyonel çözümlerin kümesi için sonlu bir üreteç kümesi bulmaya imkan sağlayan bir yöntem verir. Fakat Mordell'in metodunun bir üreteç kümesi verdiği henüz ispatlanamamıştır. O halde $y^2 - x^3 = c$ veya $ax^3 + by^3 = c$ gibi özel tipteki kübik denklemler için bile rasyonel çözümlerinin varlığı veya sayısı hakkında net bir cevap bulunamamıştır. Ayrıca $\mathbb{Q}$ cisminde tanımlı eliptik eğriler üzerindeki sonlu mertebeli rasyonel noktaların ya devirli grup ya da iki devirli grubun direkt çarpımına izomorf olduğu 1974'te Barry Mazur tarafından ispatlanmıştır.

Son yirmi otuz yıldır eliptik eğriler hem sayılar teorisinde hem de buna bağlı olan kriptografi gibi teorilerde giderek artan bir önem kazanmaya başlamıştır. Örneğin 1980'lerden itibaren eliptik eğriler kriptografide, çarpanlara ayırma ve asallık testlerinde kullanılmaya başlamıştır. Benzer şekilde 1980'li ve 1990'lı yıllarda Fermat'ın son teoreminin ispatında da eliptik eğriler kullanılan en önemli kavram olmuştur.

Çalışmanın birinci bölümünde, diğer bölümlere temel teşkil edecek bazı tanım ve sonuçlar verilmiştir. İlk olarak, eliptik eğriler üzerindeki rasyonel nokta sayısını veren formülleri ifade etmede kullanılacak olan ikinci ve üçüncü dereceden kalan kavramlarının tanımları verilmiştir. Devamında *"uzun Weierstrass normal formundaki eğriler"* verilmiş, bu eğriler üzerinde bulundukları $\mathbb{F}$ cisimlerinin karakteristiklerine göre sınıflandırılmış ve diskriminantı sıfırdan farklı olanlar ise $\mathbb{F}$ üzerinde bir "*eliptik eğri"* şeklinde tanımlanmıştır. Bununla birlikte çalışmamızda kullandığımız uzun Weierstrass normal formundaki eliptik eğriler, karakteristiğin 2 ve 3'ten farklı olması durumunda "*basitleştirilmiş Weierstrass normal formundaki eliptik eğriler"* olarak ifade edilmiştir. İkinci olarak eliptik eğriler üzerindeki rasyonel noktalar için tanımlanan toplama işlemi verilmiş ve bu noktaların toplama işlemine göre değişmeli grup oluşturduğu gösterilmiştir. Ayrıca eliptik eğrilerin grup yapıları ile ilgili olan Nagel-Lutz teoremi, Mordell teoremi, Mazur teoremi, Siegel teoremi gibi çok önemli teoremler ifade edilmiştir. Üçüncü olarak eliptik eğrilerin nokta sayılarının hesaplanmasında önemli bir yeri olan *"Frobenius endomorfizmi"* ve buna bağlı olarak *"Frobenius endomorfizminin izi"* tanımlanmış olup, üçüncü bölümde de Frobenius endomorfizminin izi ile ilgili bir sınıflandırma yapılmıştır. Sonrasında süpersingüler

eğriler tanımlanmış, ikinci bölümde; çalıştığımız eğrilerden hangilerinin süpersingüler oldukları belirtilmiştir.

Rasyonel nokta sayısı hesaplamaları ile ilgili ilk formül olan Hasse teoremi ifade edilmiş, ikinci bölümde bu teoremden yararlanarak yeni formüller elde edilmiştir. Son olarak bir eliptik eğrinin *"eşleniği"* kavramı ifade edilmiş, üçüncü bölümde de eğrilerin kendisi ve eşlenikleri ile ilgili bazı sonuçlar verilmiştir.

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

$$E_a : y^2 = x^3 + a^3$$

Bachet eliptik eğrileri ele alınmıştır. Bu eğrilerin $p \equiv 1 \pmod 6$ bir asal olmak üzere $\mathbb{F}_p$ sonlu cisimleri üzerindeki nokta sayıları ve bu noktaların mertebeleri incelenmiştir. Nokta sayısı ve noktaların mertebeleri ile ilgili hesaplamalarda Maple ve Visual basic programları kullanılmıştır. E_a eğrisi üzerindeki rasyonel noktaların sayısının, sonsuzdaki nokta ile beraber

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

olduğu gösterilmiştir. Ayrıca Hasse teoremi yardımıyla verilen $y^2 = x^3 + a^3$ eğrisi üzerindeki nokta sayısı formülü üçüncü dereceden kalanlar yardımıyla yeniden düzenlenerek, $t = y^2 - a^3$ olmak üzere

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

iken

$$\#E_a(\mathbb{F}_p) = N_{p,a} = 1 + \sum f(t)$$

şeklinde ifade edilmiştir. Bundan başka eğri üzerindeki rasyonel noktaların apsisleri toplamının

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

formülü ile ifade edilebileceği gösterilmiştir.

Üçüncü bölümde $y^2 = x^3 + a^3$ Bachet eliptik eğrisinin $\mathbb{F}_p$ sonlu cismi üzerindeki grup yapısı incelenmiştir. $p \equiv 5 \pmod 6$ bir asal olmak üzere E_a eğrisi üzerindeki rasyonel noktaların grup yapısının $E_a(\mathbb{F}_p) \cong C_{p+1}$ olduğu bilinmektedir. $p \equiv 1 \pmod 6$ bir asal iken bu grubun C_n ve C_{mn} devirli gruplarının direkt çarpımına izomorf olduğu gösterilmiştir. Yani $m, n \in \mathbb{N}^+$ için

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

dir. t, frobenius endomorfizminin izini göstermek üzere E_a eğrisi üzerindeki rasyonel noktaların sayısı

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

iken $a \in Q_p$ oluyorsa $t > 0$, diğer durumda ise $t < 0$ olduğu ifade edilmiştir. Ayrıca p asal sayısının 12 modundaki sınıflandırmasına göre t'ler sınıflandırılmıştır. Son olarak $p \equiv 1 \pmod 6$ bir asal iken a'nın Q_p'de bulunup bulunmayışına göre nokta sayısının bir sınıflandırması ve buna bağlı olarak da bu eğride üçüncü mertebeden elemanların ne zaman bulunacağı gösterilmiştir.

1. BÖLÜM

ÖN BİLGİLER

Bu bölümde çalışmamızda kullanacağımız bazı temel kavramları tanımlayacağız ve bazı temel teoremleri vereceğiz. Bu teoremlerin ispatları sayılar teorisi kitaplarında bulunabilir.

1.1. İkinci ve Üçüncü Dereceden Kalanlar

1.1.1 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.

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

1.1.3. 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.

1.1.4. 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.

1.1.5. 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*" denilir ve bu şekildeki ikinci derece kalanların kümesi Q_n ile gösterilir.

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

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

Şimdi, verilen bir $\bar{a}\in U_n$ biriminin bir ikinci dereceden kalan olup olmadığını belirleyeceğiz. Modun asal olması durumunda işlem kolaydır. $n=2$ ise $Q_2=\{\bar{1}\}$ dir ve $\bar{1}$ ikinci dereceden bir kalandır. O halde $n=p$ nin tek asal olması durumuyla başlayalım.

1.1.8. 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.

1.1.9. 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.

1.1.10. 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.

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

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

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

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

1.1.14. 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. 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:

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

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

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

1.1.18. 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. (Namlı 2001)

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

1.1.20. Teorem. $p \equiv 1 \pmod 3$ asal ise p modundaki farklı üçüncü dereceden kalanların sayısı $\frac{p+2}{3}$ tür. (Namlı 2001)

1.2. Normal Formlar

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

1.2.1. 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.

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

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

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (1)$$

şeklindeki bir denklem "*uzun Weierstrass normal formu"* olarak adlandırılır. Burada sonsuzdaki nokta olarak adlandırılan "o" noktamız var. Bu noktanın afin temsili $o = (\infty, \infty)$ dur.

1.2.4. 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. (Schmitt ve Zimmer 2003)

1.2.5. 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. Bu sabitler aşağıdaki bağıntıları sağlar:

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

1.2.6. Tanım. C düzlemsel cebirsel eğrisi $f(x,y) = 0$ polinom denklemiyle tanımlansın. Bu durumda $P = (x_0, y_0) \in C$ nin 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.

1.2.7. 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. (Silverman 1986)

1.2.4.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:

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

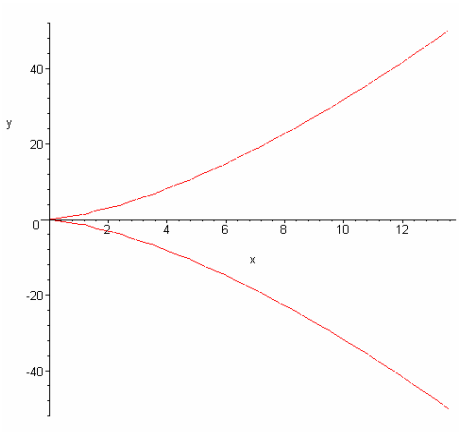
eğrisinin kısmi türevleri

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

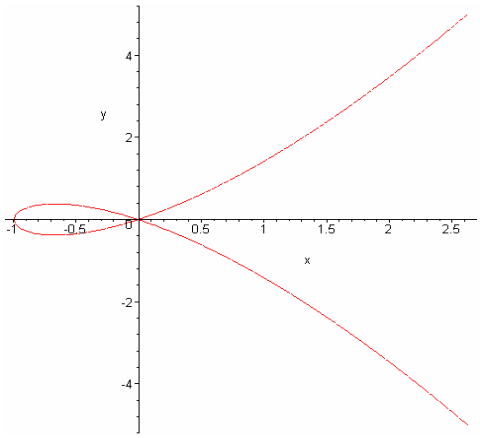
dir. Karakteristik ne olursa olsun bu üç denklemin

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

bir tek çözümü vardır. Bu da $x = y = 0$ dır. (Schmitt ve Zimmer 2003)



$y^2 = x^3$ (Çıkıntı)



$y^2 = x^3 + x^2$ (Düğüm)

Şekil 1.2.1

1.2.8. 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.

1.2.9. Tanım. E ve E' eliptik eğrileri

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

ve

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

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

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

şeklindedir. Böyle dönüşümlere "*birasyonel*" denilmektedir. Bu durumda

$$\begin{aligned}
&ua' = a_1 + 2s,\\
&u^2a_2' = a_2 - sa_1 + 3r - s^2,\\
&u^3a_3' = a_3 + ra_1 + 2t,\\
&u^4a_4' = a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st,\\
&u^6a_6' = a_6ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1,\\
&u^2b_2' = b_2 + 12r,\\
&u^4b_4' = b_4 + rb_2 + 6r^2,\\
&u^6b_6' = b_6\,2rb_4 + r^2b_2 + 4r^3,\\
&u^8b_8' = b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4,\\
&u^4c_4' = c_4,\\
&u^6c_6' = c_6,\\
&u^{12}\Delta' = \Delta,\\
&j' = j.
\end{aligned}$$

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

1.2.10. 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.

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

$$y^2 = x^3 + a_4 x + a_6 \tag{2}$$

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

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.

İspat. a) Eğer $Kar(\mathbb{F}) \neq 2$ ise (1) tipindeki Weierstrass denklemini kareye tamamlayarak basitleştirebiliriz. Denklemde $y + \frac{1}{2}(a_1 x + a_3)$ yerine $\frac{1}{2}y$ yazarsak sonuç

$$y^2 = 4x^3 + b_2 x^2 + 2b_4 x + b_6 \tag{3}$$

olur.

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

$$y^2 = x^3 - 27c_4 x - 54c_6 \tag{4}$$

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

b) (1) tipindeki Weierstrass denklemini alalım ve denklemin sol tarafını kareye tamamlayalım. Bu bize $\Delta = {a_2}^2 {a_4}^2 - {a_2}^3 a_6 - {a_4}^3$ ve $j = \frac{{a_2}^6}{\Delta}$ değişmezleri ile

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

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

c) Tekrar (1) tipindeki Weierstrass denklemini alarak ispata başlayalım. Karakteristik 2 iken

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

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

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

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

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

ifadeleri denklemde yerine konursa istenilen denklem elde edilir.□

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

$$E' : y^2 = x^3 + Ax + B \qquad (A, B \in \mathbb{F}) \tag{5}$$

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

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

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

halini alacaktır.

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

Sadece birasyonel dönüşümler basitleştirilmiş Weierstrass normal formunu

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

dönüşümleri altında değişmez bırakır. Bu durumda

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

dönüşümlerini elde ederiz.

1.2.12. 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.

İspat. Basitleştirilmiş Weierstrass normal formundaki eğrileri

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

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

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

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

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

Eğer $A = 0$ ise $B \neq 0$'dır. Böylece $A' = 0$ ve $B' \neq 0$'dır. Bu durumda $u = (\frac{B}{B'})^{\frac{1}{6}}$ alabiliriz. Eğer $B = 0$ ise $A \neq 0$'dır. Böylece $B' = 0$ ve $A' \neq 0$'dır. Bu durumda $u = (\frac{A}{A'})^{\frac{1}{4}}$ alabiliriz. Eğer $AB \neq 0$ ise $A'B' \neq 0$ dır. Gerçekten $A'B' = 0$ ise $A' = 0$ ve $B' = 0$ dır. Böylece $\Delta' = 0$ dır. Bu ise istisnadır.

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

elde ederiz. Bu durumda

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

alabiliriz. □

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

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

Çizelge 1.2.1

(Schmitt ve Zimmer 2003)

1.3. Toplama Kuralı

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

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

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

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

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

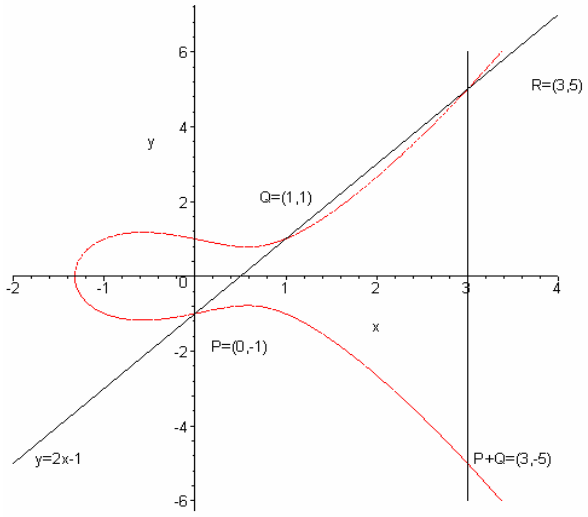
1.3.4. Tanım. $E \setminus \mathbb{F}$ eliptik eğri $P_1, P_2 \in E(\mathbb{F})$ farklı olması gerekli olmayan iki nokta olsunlar. P_1 ve P_2'den geçen doğru (örneğin kesen) eliptik eğriyi üçüncü bir P_3' noktasında keser. P_3' ve o'dan geçen doğruyu göz önüne alalım. Bu doğru eğriyi üçüncü nokta P_3'de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

1.3.5. Örnek. $\mathbb{Q}$ cismi üzerinde $y^2 = x^3 - x + 1$ eliptik eğrisini ve bu eğri üzerinde $P = (0, -1)$ ve $Q = (1, 1)$ noktalarını ele alalım. Aşağıda verilen şekle göre P

ve Q noktalarını $y = 2x - 1$ doğrusu birleştirmektedir. O halde doğrunun eğri ile üçüncü kesişim noktası ortak çözümlenerek bulunabilir. $x = 0$ ve $x = 1$, P ve Q nun apsisleri olduğuna göre üçüncü nokta $R = (3,5)$'dir. P'nin Q ile toplamı R'nin x-eksenine göre yansımasıdır. Yani $-R = P + Q = (3,-5)$'dir. (Mollin 2001)

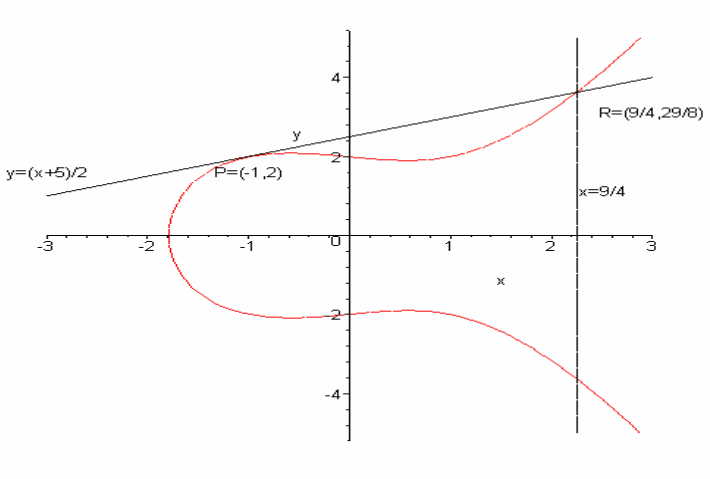


Şekil.1.3.1

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

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

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



Şekil.1.3.2

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

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

İspat. Toplamanın aşağıdaki özelliklerini elde etmek kolaydır:

i) $P_1, P_2 \in E(\mathbb{F})$ için $P_1 + P_2 \in E(\mathbb{F})$ dir. 1.3.6. Teoremde uzun olan Weierstrass normal formundaki eliptik eğriler için toplama formülü vereceğiz.

ii) Birim eleman: o (Şekil.1.3.3)

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.1.3.4)

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

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

olduğunu göstermeliyiz. Bunun için aşağıdaki doğruları (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

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

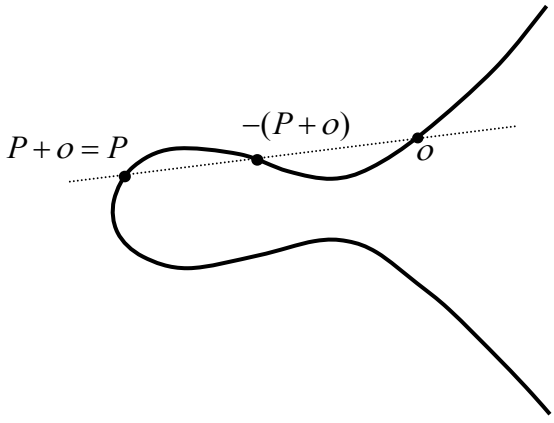
C' eğrisi C ve E eğrisinin ortak noktalarının ilk sekizinde kesişirler. Diğer taraftan C' nün E 'de 9 ortak noktası vardır:

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

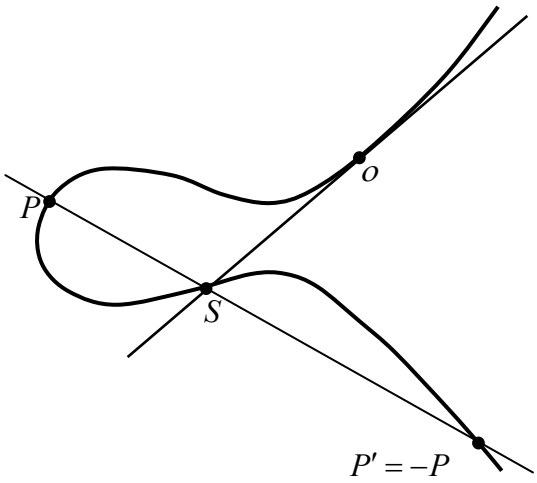
Böylece

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

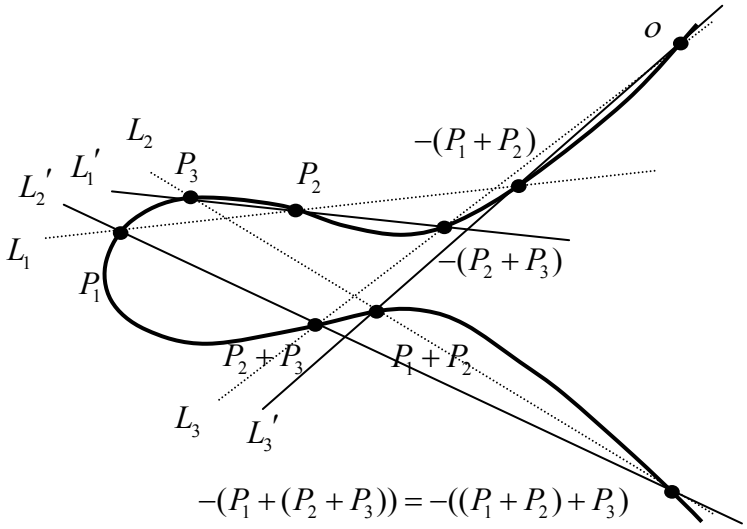
olur (Şekil.1.3.5).□



Şekil.1.3.3 (Birim eleman)



Şekil.1.3.4 (Ters eleman)



Şekil.1.3.5 (Birleşme özelliği)

1.3.8. Toplama Teoremi. $E \setminus \mathbb{F}$, $\mathbb{F}$ cismi üzerinde (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) $-P_1 = (x_1, -y_1 - a_1 x_1 - a_3)$

ii) $x_1 = x_2$ ve $y_2 + y_1 + a_1 x_1 + a_3 = 0$ 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

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

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

şeklinde ve eğer $x_1 = x_2$ ise

$$\lambda = \frac{3x_1^{\,2} + 2a_2 x_1 + a_4 - a_1 y_1}{2y_1 + a_1 x_1 + a_3},$$

$$\nu = \frac{-x_1^{\,3} + a_4 x_1 + 2a_6 - a_3 y_1}{2y_1 + a_1 x_1 + a_3} = y_1 - \lambda x_1,$$

şeklinde olur. Bu durumda

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

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

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

şeklinde verilir. (Schmitt ve Zimmer 2003)

Bilindiği gibi eliptik eğriler üzerindeki noktaların en genel temsili uzun Weierstrass normal formundaki afin temsildir. 1.3.8 Teoremde bu temsil için bir toplam formülü tanımladık. Bu temsil keyfi bir karakteristikteki herhangi bir cisim için kullanılır. Şimdi (5) tipindeki Weierstrass eğrileri için toplam formülünü vereceğiz.

1.3.9. Tanım. $E \setminus \mathbb{F}$, (5) tipinde bir eliptik eğri ve $P_1 \neq -P_2$ olacak şekilde $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2) \in E$ olsun. 1.3.8.Teorem gereği $P_1 + P_2 = (x_3, y_3)$

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

ve

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

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

ile verilir.

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

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

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

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

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

1.3.12. Tanım (Bachet'in İkiye Katlama Formülü). $y^2 = x^3 + a_2x^2 + a_4x + a_6$ kübik eğrisini ele alalım. Bu eğri üzerindeki bir P noktasının koordinatlarını kullanarak $2P$ için açık bir dönüşüm elde etmek istiyoruz. Bu kübik eğri için 1.3.8 Teoremde

verdiğimiz $x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$ formülünü kullanırsak $a_1 = 0$ ve $x_1 = x_2$ olduğundan λ yerine de $\lambda = \frac{f'(x)}{2y}$ 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.

1.3.13. 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.

1.3.14. 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. 1.3.12 Tanım gereği

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

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

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

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

eliptik 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. (Mollin 2001)

1.3.16. Örnek. $\mathbb{Q}$ üzerinde

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

eliptik eğrisini ele alalım.

$P=(-1,3)$, $Q=(0,0)\in E(\mathbb{Q})$ dur. $P+Q=(10,30)$ olur. Q'nun mertebesi 2'dir: $2Q=o$. P noktası sonsuz mertebelidir. $2P=(\frac{121}{36},\frac{451}{216}), 3P=(\frac{-57121}{24649},\frac{-12675843}{3869893})$, $4P=(\frac{761815201}{29289744},\frac{-20870873704079}{158516094528})\ldots$. (Schmitt ve Zimmer 2003)

Yukarıda görüldüğü gibi her toplamada bileşenler giderek karmaşıklaşır.

1.3.17. Nagel-Lutz Teoremi. E, $\mathbb{Q}$ üzerinde (5) tipinde bir eliptik eğri ve $P=(x_1,y_1)\in E(\mathbb{Q})_t$ ise bu durumda $x_1,y_1\in\mathbb{Z}$ 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. (Mollin 2001)

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

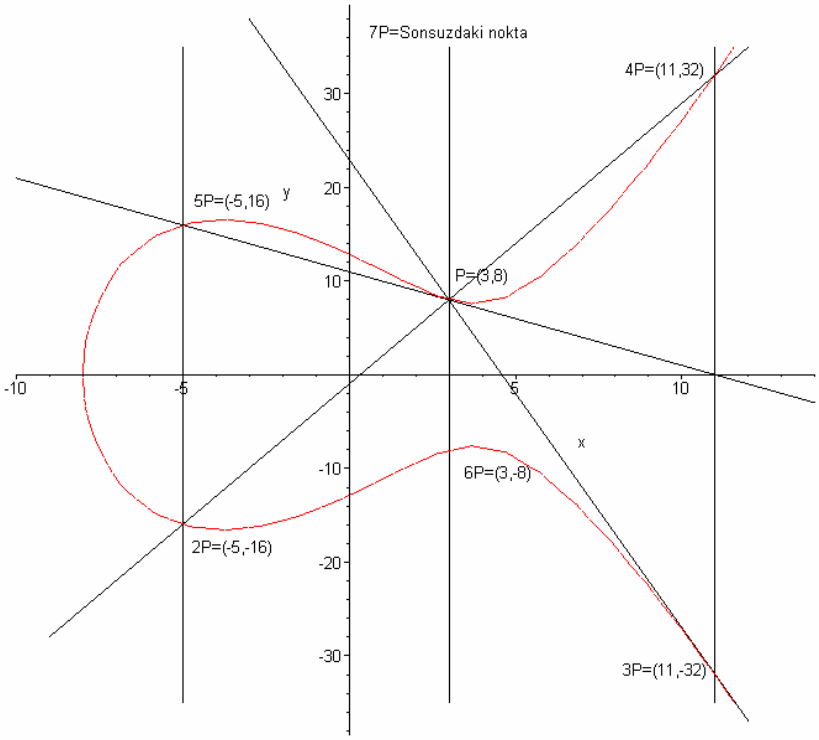
1.3.19. Örnek. $\mathbb{Q}$ cismi üzerinde $E: y=x^3+4$ eliptik eğrisi verilsin. Bu durumda $4A^3+27B^2=432$ olur. $P(x,y)$, $E(\mathbb{Q})$'da sonlu mertebeli bir nokta olsun. $0=x^3+4$ denkleminin rasyonel çözümleri olmadığından $y\neq 0$ dır. Bu yüzden $y^2\mid 432$ olur. Böylece $y=\pm1,\pm2,\pm3,\pm4,\pm12$ dir. Sadece $y=\pm2$ x'in rasyonel değerini verir. Böylece mümkün olan sonlu mertebeli noktalar $(0,2),(0,-2)$ dir. Kolay bir hesaplama ile $3(0,\pm2)=o$ olduğunu buluruz. $E(\mathbb{Q})$ nun büküm alt grubu 3 mertebeli devirli bir gruptur. (Washington 2003)

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

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

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

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



Şekil.1.3.6

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

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

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

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

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

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

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

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

$\mathbb{F}$'nin karakteristiği 2 ise

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

dir. (Washington 2003)

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

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

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

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

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

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

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

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

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

1.3.27. Mazur Teoremi. $E \setminus \mathbb{Q}$ 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. (Mollin 2001)

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

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

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

dir. (Kato ve ark. 2000)

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

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

dir. (Kato ve ark. 2000)

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

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

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

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

$$E_k: y^2 = x^3 + k \tag{6}$$

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

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

şeklinde ifade edilir.(Schmitt ve Zimmer 2003)

Şimdi de (5) tipindeki denklemlerin tam sayı çözümlerini arayalım.

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

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

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

1.4. Sonlu Cisimler Üzerinde Eliptik Eğriler

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

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

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

Çizelge 1.4.1

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

1.4.2. Örnek. $\mathbb{F}_7$ üzerinde $E: y^2 = x^3 + 2$ eliptik eğrisi olsun. Bu durumda $E(\mathbb{F}_7) = \{o, (0,3), (0,4), (3,1), (3,6), (5,1), (5,6), (6,1), (6,6)\}$ olur. Kolay bir hesaplamayla bu P noktalarının tümünün $3P = o$ şartını sağladığını görebiliriz. Bundan dolayı bu grup $\mathbb{Z}_3 \times \mathbb{Z}_3$'e izomorftur. (Washington 2003)

1.4.3. Teorem. E, $\mathbb{F}_q$ sonlu cismi üzerinde bir eliptik eğri olsun. Bu durumda 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

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

olur.

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

1.5. Frobenius Endomorfizmi ve Süpersingüler Eğriler

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

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

olacak şekilde verilir.

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

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

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

olur.

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

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

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. (Schmitt ve Zimmer 2003)

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

1.5.4. Yardımcı Teorem. 1.3.31 Teoremde tanımladığımız $\mathbb{F}_p$ üzerindeki $E_k : y^2 = x^3 + k$ Mordell eğrisini ele alalım. Ayrıca p asal $p \nmid 6k$ ve $p \equiv 2 \pmod 3$ olsun. Bu durumda $E_k \setminus \mathbb{F}_p$ süpersingülerdir ve $\# E_k(\mathbb{F}_p) = p + 1$ 'dir. (Schmitt ve Zimmer 2003)

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

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

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

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

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

ile verilen E eliptik eğrisi süpersingülerdir. (Washington 2003)

1.6. Rasyonel Noktaların Sayısını Hesaplama

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

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

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

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

olur.(Washington 2003)

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

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

şeklindedir.

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

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

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

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

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

olur.

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

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

Sonuç Hasse teoreminden görülür.□

1.6.4. Örnek. $\mathbb{F}_5$ üzerinde $E : y^2 = x^3 + x + 1$ eliptik eğrisi verilsin. 5 modunda ikinci dereceden 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. (Washington 2003)

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

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

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

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

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

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

$$Z\left(T;E\setminus\mathbb{F}_q\right)=\frac{1-tT+qT^2}{(1-T)(1-qT)} \qquad (7)$$

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

$$N = q + 1 - t$$

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

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

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

şeklindedir. (Koblitz 1994)

1.7. Grup Mertebeleri Verilen Eliptik Eğrilerin Yapısı

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

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

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

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

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

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

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

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

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

İspat. a) Bu kısmı hesaplamak oldukça kolaydır.

b) $Kar(\mathbb{F}_q) > 3$ olsun. $\mathbb{F}_q$'nun bir elemanının ikinci dereceden bir kalan olması için gerek ve yeter koşul p asal ve $q = p^k$ olmak üzere bu elemanın $\mathbb{F}_p$'de bir ikinci dereceden kalan olmasıdır. $x \in \mathbb{F}_q$ olan q tane eleman vardır. Eğer $x^3 + a_4 x + a_6$ denklemi tam kare ise $(x, \pm y) \in E(\mathbb{F}_q)$ olan iki nokta vardır. Ayrıca bu durumda, $c \in \mathbb{F}_q^*$ ikinci dereceden bir kalan olmadığı için

$$\left(\frac{(cx)^3 + a_4 c^2 (cx) + a_6 c^3}{p} \right) = \left(\frac{c}{p} \right) \left(\frac{x^3 + a_4 x + a_6}{p} \right) = -1$$

öyle ki $E'(\mathbb{F}_q)$'da apsisi cx olan hiçbir nokta yoktur. Eğer $x^3 + a_4 x + a_6$ denklemi $\mathbb{F}_q$'da bir tam kare değil ise, $E(\mathbb{F}_q)$'da apsisi x olan hiçbir nokta yoktur. Fakat

$$\left(\frac{(cx)^3 + a_4 c^2 (cx) + a_6 c^3}{p} \right) = \left(\frac{c}{p} \right) \left(\frac{x^3 + a_4 x + a_6}{p} \right) = 1$$

dir. Bu yüzden $E'(\mathbb{F}_q)$' da apsisi cx olan $(cx, \pm y)$ biçiminde iki nokta vardır.

$E(\mathbb{F}_q)$'daki her $x \in \mathbb{F}_q$ apsisi, biri E'de diğeri E''de bulunan iki nokta verir. Bu iki noktanın toplamı sonsuzdaki noktadır.□

1.7.3. Önerme. E, $\mathbb{F}_q$'da (5) tipinde bir eliptik eğri ve belli bir n tamsayısı için

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

olsun. O zaman

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

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

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

dir.(Washington 2003)

İspat. Hasse teoremine göre $|t| \leq 2q$ iken $n^2 = q + 1 - t$ dir. Bu önermeyi ispatlamak için aşağıdaki yardımcı teoremi kullanacağız. Bu yardımcı teorem t ile ilgili kesin bir sınırlama verir.

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

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

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

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

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

dur. Son eşitsizlikte her iki tarafın karesini alırsak

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

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

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

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

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

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

1.7.6. Örnek. $p = 17$ için $y^2 \equiv x^3 + 4^3 \pmod{17}$ eğrisi üzerindeki noktalar: $E(\mathbb{F}_{17}) = \{(0,8),(0,9),(2,2),(2,15),(4,3),(4,14),(5,6),(5,11),(6,5),(6,12),(7,4),(7,13),(8,7),(8,10),(11,1),(11,16),(13,0),o\}$ şeklindedir. Yani $\#E(\mathbb{F}_{17}) = 18$'dir. Bu eğrinin grup yapısı da $E(\mathbb{F}_{17}) \cong C_{18}$ olur.

2. BÖLÜM

F_p SONLU CİSİMLERİNDEKİ $y^2=x^3+a^3$ BACHET ELİPTİK EĞRİLERİ ÜZERİNDEKİ RASYONEL NOKTALAR

2.1. Bachet Eliptik Eğrileri

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

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

eğrisini ele alalım. $A = 0$ durumunda elde ettiğimiz eliptik eğri

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

"*Bachet eliptik eğrisi*" (ya da Mordell eğrisi) olarak adlandırılır. Çalışmamızda $\mathbb{F}_p$ sonlu cisminde $B = a^3$ durumundaki

$$y^2 = x^3 + a^3 \qquad (a \in \mathbb{F}_p^{\,*}) \tag{8}$$

Bachet eliptik eğrilerini inceleyeceğiz. Bu bölümde verdiğimiz örneklerde nokta sayısı hesaplamalarında Maple ve Visual Basic programları kullanılmıştır. Burada ilk olarak şu iki önemli sonucu verebiliriz.

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

2.1.2. Sonuç. $p \equiv 5 \pmod 6$ asal iken $y^2 \equiv x^3 + a^3 \pmod{p}$ Bachet eliptik eğrisi "süpersingülerdir". $p \equiv 1 \pmod 6$ iken ise "süpersingüler değildir".

Bu bölümde Bachet eliptik eğrilerinin üzerindeki nokta sayıları ve bu noktaların apsisleri toplamı ile ilgili bazı sonuçlar elde etmeye çalışacağız. Ayrıca üçüncü dereceden kalanlar yardımıyla bu eğrilerin nokta sayısını formülize edeceğiz.

2.2. Bachet Eliptik Eğrilerinin Nokta Sayılarının Yeniden Hesaplanması

Şimdi (8) eğrisini ele alalım ve bunu E_a ile gösterelim. E_a eğrisindeki $\mathbb{F}_p$-rasyonel noktalarının kümesini $E_a(\mathbb{F}_p)$, bu noktaların sayısını yani $\#E_a(\mathbb{F}_p)$ sayısını $N_{p,a}$ ile gösterelim. $y^2 \equiv u \pmod{p}$ denklemini sağlayan noktaların sayısının $1+\chi(u)$ olduğu bilinmektedir ve dolayısıyla $y^2 \equiv x^3 + a^3 \pmod{p}$ denklemini sağlayan noktaların sayısı sonsuzdaki noktayla beraber Hasse teoreminden

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

şeklinde ifade edilir. (8) 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 (8) denklemini sağlar. Bunun sebebi her bir $x \in \mathbb{F}_p$ için en çok iki tane $y \in \mathbb{F}_p$ vardır ve bunlar (8) denklemini sağlar.

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

O halde $\mathbb{F}_p$ cisminde E_a eğrisi üzerindeki nokta sayısının daha kesin formülü

$$N_{p,a} = p + 1 + \sum_{x \in \mathbb{F}_p} \chi(x^3 + a^3) \tag{9}$$

şeklindedir.

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

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

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

toplamına eşittir ve burada

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

şeklinde ifade edilir. Formüldeki dört noktadan üçü $y=0$ durumundaki (x,y)'ler; dördüncü nokta ise sonsuzdaki noktadır. Aynı zamanda böyle y değerlerinin toplamı da p'ye eşittir.

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

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

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

toplamına eşittir ve burada

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

şeklinde tanımlanır. Formüldeki 1 sayısı sonsuzdaki noktayı ifade etmektedir. Ayrıca $y^2\equiv x^3+a^3 \pmod p$ Bachet eliptik eğrisinde $\mathrm{p}\equiv 5 \pmod 6$ asal olması durumunda $p+1$ tane rasyonel nokta vardır. Şimdi bu iki duruma birer örnek verelim.

2.2.2.Örnek. $y^2\equiv x^3+2^3 \pmod{13}$ Bachet eliptik eğrisi üzerindeki dört nokta $(7,0),(8,0),(11,0)$ ve o dur. Diğer noktaları formülden şöyle hesaplayabiliriz:

$Q_{13}=\{1,3,4,9,10,12\}$ olduğundan

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

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

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

2.2.3. Örnek. $y^2\equiv x^3+2^3 \pmod{11}$ Bachet eliptik eğrisi üzerindeki noktalardan biri sonsuzdaki nokta olduğuna göre diğer noktaları şöyle hesaplayabiliriz:

$Q_{11}=\{1,3,4,5,9\}$ olduğundan

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

dır. O halde bu eğri üzerinde sonsuzdaki nokta ile beraber toplam 12 tane nokta bulunur.

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

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

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

şeklinde bir fonksiyon tanımlayalım. Bu takdirde $y^2\equiv x^3+a^3 \pmod p$ eğrisi üzerindeki nokta sayısı

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

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

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

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

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

dır. O halde bu eğri üzerinde 16 nokta bulunur.

Şimdi (8) eğrisi üzerindeki noktalardan y ekseni üzerinde olanları ele alalım.

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

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

2.2.7. Örnek. $x \equiv 0 \pmod{13}$ için $4 \in Q_{13}$ olduğundan $y^2 \equiv x^3 + 4^3 \pmod{13}$ eğrisi üzerinde $(0,5),(0,8)$ noktaları vardır. Fakat $5 \notin Q_{13}$ olduğundan $y^2 \equiv x^3 + 5^3 \pmod{13}$ eğrisi üzerinde $x \equiv 0 \pmod{13}$ için y değerleri mevcut değildir.

Bundan başka $a = 0,1,2,...,p-1 \pmod p$ ve $p \equiv 1 \pmod 6$ bir asal iken $y^2 \equiv x^3 + a^3 \pmod p$ eğri ailesinin noktalarının toplam sayısını ele alalım. $(a,p)=1$ iken $y^2 \equiv x^3 + a^3 \pmod p$ eğrisi üzerinde uygun bir k tam sayısı için $p+1-2k$ ya da $p+1+2k$ tane nokta olduğunu biliyoruz.

Şimdi de E_a eğri ailesinin nokta sayılarının toplamı ile ilgili şu sonucu verelim:

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

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

dir.

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

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

olur. (8)'e göre

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

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

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

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

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

ifadesini elde ederiz. Sonuç olarak biliyoruz ki

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

dır. Buradan da

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

olur.□

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

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

Yukarıdaki sonucu ve 1.6.6 Weil Teoremini kullanarak:

2.2.11. Örnek. $\mathbb{F}_7$ cisminde tanımlı $y^2 = x^3 + 4^3$ Bachet eliptik eğrisi üzerindeki noktaları bulalım. Burada $N_1 = 12$ tane nokta vardır. Bunlar $(0,1), (0,6), (1,3), (4,4)$, $(2,3), (2,4), (3,0), (4,3), (5,0), (6,0)$ ve sonsuzdaki noktadır. $N_{p,a} = p + 1 - t$ formülünden $N_{p,a} = N_1$ olduğundan $t = -4$ bulunur.

Şimdi $r = 2$ için $\mathbb{F}_{49}$ cismi üzerindeki nokta sayısını hesaplayalım. İlk olarak 1.6.6 Weil teoremi ve 1.6.7. Uyarıya göre

$$1 + 4T + 7T^2 = 0$$

ikinci derece denkleminden $\alpha = -2 - \sqrt{3}i$ ve $\beta = -2 + \sqrt{3}i$ bulunur. Sonuç olarak da $\mathbb{F}_{49}$ cismi üzerindeki nokta sayısı

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

formülünden $N_2 = 48$ bulunur. Benzer olarak $\mathbb{F}_{343}$ cismi üzerindeki nokta sayısı $N_3 = 324$ hesaplanabilir.

2.2.12. Örnek. $\mathbb{F}_5$ cisminde tanımlı $y^2 = x^3 + 8$ Bachet eliptik eğrisi üzerindeki noktaları bulalım. Burada $N_1 = 6$ tane nokta vardır. Bunlar $(1,2),(1,3),(2,1),(2,4),(3,0)$ ve sonsuzdaki noktadır.

Şimdi *r = 2* için $\mathbb{F}_{25}$ cismi üzerindeki nokta sayısını hesaplayalım.Yani

$$N_2 = 25 + 1 - \alpha^2 - \beta^2$$

bulmaya çalışalım. Eşlenik kökler olan α ve β'yı bulmak için $N = q + 1 - t$ formülünü alalım. Böylece $6 = 5 + 1 - t$ eşitliğinden $t = 0$ bulunur. Bu durumda $1 + 5T^2 = 0$ denkleminin kökleri $\frac{\pm i}{\sqrt{5}}$'dir. Yani $\alpha = \sqrt{5}i$ ve $\beta = -\sqrt{5}i$ olur. Sonuç olarak nokta sayısı

$$N_r = \begin{cases} 5^r + 1 & , \ r \ tek \ ise \\ 5^r + 1 - 2.(-5)^{\frac{r}{2}} & , \ r \ çift \ ise \end{cases}$$

şeklinde ifade edilebilir. Bu durumda $N_2 = 5^2 + 1 - 2(-5)^{\frac{2}{2}} = 36$ olur. Benzer olarak $N_3 = 5^3 + 1 = 126$ ve $N_4 = 576$ bulunur.

2.3. Bachet Eliptik Eğrilerinin Rasyonel Noktalarının Apsisleri Toplamı

Şimdi (8) eğrisi üzerindeki rasyonel noktaların apsislerinin toplamını formülleştireceğiz ve apsisler toplamı ile ilgili bazı sonuçları elde edeceğiz.

2.3.1. Teorem. $p \equiv 1 \pmod 6$ bir asal olsun. $y^2 \equiv x^3 + a^3 \pmod p$ eğrisi üzerindeki rasyonel noktaların apsisleri toplamı

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

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 $x^3+a^3\equiv 0 \pmod p$ dir ve $p\mid 0$ iken $\chi_p(x^3+a^3)=0$ dır. Eğri üzerindeki her bir $(x,0)$ noktası için $(1+0).x=x$ toplama eklenir.

$x^3+a^3=t$ 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. □

Yukarıdaki formülün $\mathrm{p}\equiv 5 \pmod 6$ için de geçerli olduğu gösterilebilir.

2.3.2. Örnek. $y^2\equiv x^3+2^3 \pmod 7$ Bachet eliptik eğrisi üzerindeki rasyonel noktaların apsisleri toplamını bulalım: $Q_7=\{1,2,4\}$ olduğundan

$$\begin{aligned}\sum_{x\in\mathbb{F}_p}(1+\chi_p(x^3+2^3)).x &= (1+\chi_7(1)).0+(1+\chi_7(2)).1+(1+\chi_7(2)).2+(1+\chi_7(0)).3\\ &\quad +(1+\chi_7(2)).4+(1+\chi_7(0)).5+(1+\chi_7(0)).6\\ &=0+2+4+3+8+5+6\\ &=28\end{aligned}$$

dir.

Aşağıdaki sonuçtan da görebileceğimiz gibi yukarıda verilen toplam daima p modunda sıfıra denktir.

2.3.3. Teorem. $\mathrm{p}\equiv 1 \pmod 6$ bir asal olsun. Bu takdirde $x^3\equiv t \pmod p$ kongrüansının x tam sayı çözümlerinin toplamı p modunda sıfıra denktir.

İspat. $x^3 \equiv 1 \pmod{p}$ kongrüansının 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. □

Şimdi aşağıdaki sonucu ispatlayabiliriz.

2.3.4. Teorem. $\mathrm{p} \equiv 1 \pmod{6}$ bir asal olsun. $0 \le x \le p-1$ olacak şekilde bir x tam sayısı alalım. O zaman herhangi bir $1 \le a \le p-1$ için

$$r(p) = \sum_{x=0}^{p-1} (1 + \chi(x^3 + a^3)).x$$

$p \mid r(p)$ dir. Özellikle

$$s(p) = \sum_{x=0}^{p-1} \chi(x^3 + a^3).x$$

toplamı p ile bölünür.

İspat. Her y değeri için $t = y^2 - a^3$ olsun. O zaman $x^3 \equiv t \pmod{p}$ kongrüansının çözümlerinin toplamı, 2.3.3 Teorem gereği sıfıra denktir.

Tüm y değerleri için bu geçerlidir. Böylece tüm apsislerin toplamı sıfıra denktir.□

$\mathrm{p} \equiv 1 \pmod{6}$ hipotezi bu teoremde gerekli. Yani buna ters örnek $a = 1, p = 11$ aldığımızda $r(11) = 56$ ve $s(11) = 1$ olduğu kolayca görülür. Yani bunların hiçbiri 11 ile bölünemez.

2.3.5. Örnek. $y^2 \equiv x^3 + 8^3 \pmod{13}$ eğrisini ele alalım.

$$r(p) = \sum_{x=0}^{p-1} (1 + \chi(x^3 + a^3).x)$$

formülünden $r(13) = \sum_{x=0}^{12} (1 + \chi(x^3 + 8^3).x) = 78$ olur. Bu da 13 modunda sıfıra denktir.

Şimdi ordinatı aynı olan noktaları inceleyelim.

2.3.6. Teorem. $p \equiv 1 \pmod{6}$ bir asal olsun. $y^2 \equiv x^3 + a^3 \pmod{p}$ eğrisi üzerinde ordinatı aynı olan (x, y) rasyonel noktalarının apsisleri toplamı p modunda sıfıra denktir.

İspat. y verilsin. Bu takdirde

$$x^3 \equiv y^2 - a^3 \pmod{p}$$

kongrüansı $t = y^2 - a^3$ değişikliğinden sonra

$$x^3 \equiv t \pmod{p}$$

haline gelir. Sonuç 2.3.3 Teoremden elde edilir.□

$p \equiv 5 \pmod{6}$ bir asal iken de $y^2 \equiv x^3 + a^3 \pmod{p}$ eliptik eğrisi üzerinde ordinatı aynı olan iki nokta yoktur.

2.3.7. Örnek. $y^2 \equiv x^3 + 2^3 \pmod{13}$ eğrisini ele alalım. Bu eğri üzerinde ordinatı aynı olan noktalara örnek olarak $(2,4),(5,4),(6,4)$ ya da $(7,0),(8,0),(11,0)$ verilebilir. Bu noktaların apsisleri toplamı da 13 modunda sıfıra denktir.

3. BÖLÜM

F_p SONLU CİSİMLERİNDEKİ $y^2=x^3+a^3$ BACHET ELİPTİK EĞRİLERİNİN GRUP YAPISI

3.1. Giriş

p asal olsun. $a \in \mathbb{F}_p^* = \mathbb{F}_p - \{0\}$ iken E_a Bachet eliptik eğrilerinin grup yapısını inceleyeceğiz. Eğer $p \equiv 5 \pmod 6$ ise 1.7.5 Yardımcı Teorem gereği $E_a(\mathbb{F}_p) \cong C_{p+1}$, $p+1$ mertebeli devirli gruptur. Fakat $p \equiv 1 \pmod 6$ ise $E_a(\mathbb{F}_p)$'nin grup yapısını veren bilinen bir sonuç yoktur. Bu bölümde, $p \equiv 1 \pmod 6$ iken $E_a(\mathbb{F}_p)$'nin grup yapısını inceleyeceğiz. Bu grubun, C_n ve C_{nm} devirli gruplarının bir direkt çarpımına izomorf olduğunu göstereceğiz. Yani $m,n \in \mathbb{N}$ için

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

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

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

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

3.1.1. Teorem. E_a eliptik eğrileri için

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

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

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

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

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

eğrisi $y^2 \equiv x^3 + a^3$ eğrisinin eşleniği olarak tanımlanır. Burada $a \in Q_p$ ise $ga \in Q_p'$ ve $a \in Q_p'$ ise $ga \in Q_p$ şeklindedir. (8) tipindeki herhangi bir eğri ile eşleniğinin t'lerinin işaretlerinin farklı olduğunu göstermek kolaydır. O halde aşağıdaki teoremi verebiliriz:

3.2.1. Teorem. $p \equiv 1 \pmod 6$ bir asal olsun. (8) tipindeki eğri $n^2 m = p + 1 - t$ mertebeli $C_n \times C_{nm}$ grubuna izomorf ise bunun eşleniği $r^2 s = p + 1 - t$ mertebeli $C_r \times C_{rs}$ grubuna izomorftur. (Yıldız ve ark. 2005)

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

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

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

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

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

ve benzer olarak

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

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

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

3.2.5. Örnek. $p = 139 \equiv 7 \pmod{12}$ bir asal iken $y^2 \equiv x^3 + 3^3 \pmod{139}$ eliptik eğrisini ele alalım. $N_{139,3} = 124$ ve $t = 16 \equiv 4 \pmod{12}$ dir. Ayrıca $124 \equiv 4 \pmod{12}$ dir. $y^2 \equiv x^3 + 25^3 \pmod{139}$ eğrisi için ise $N_{139,25} = 156$ ve $t = -16 \equiv 8 \pmod{12}$ dir. Ayrıca $156 \equiv 0 \pmod{12}$ dir.

3.2.6. Teorem. $p \equiv 1 \pmod{6}$ bir asal olsun. Bu durumda t, 6 ile bölünemez.

İspat. Tersine t'nin 6 ile bölündüğünü varsayalım. Bu durumda $k \in \mathbb{Z}$ için $t = 6k$ ve $n \in \mathbb{N}$ için $p = 1+6n$ koyarsak

$$N = 6n+1+1-6k$$

elde ederiz. Bu da $N \equiv 2 \pmod{6}$ oluşunu gerektirir. Fakat N, 6 modunda 2'ye denk olamaz. Gerçekten de N'nin çift olduğunu bildiğimizden $N \equiv 0, 2$ veya $4 \pmod{6}$ olur. Eğer $N \equiv 0 \pmod{6}$ ise $r \in \mathbb{Z}$ için $N = 6r$ dir. Buradan

$$t = p+1-N = 6n+2-6r$$

olur. Bu da $t \equiv 2 \pmod 6$ oluşunu gerektirir. O halde varsayımımızla çelişiriz. İkinci olarak $N \equiv 4 \pmod 6$ ise, bu durumda $c \in \mathbb{Z}$ için

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

olur. Bu da varsayımımızla çelişir. Bu yüzden t, 6 ile bölünemez.□

3.2.7. Örnek. $p = 751 \equiv 1 \pmod 6$ bir asal iken $y^2 \equiv x^3 + 42^3 \pmod{751}$ eliptik eğrisini ele alalım. $N_{751,42} = 804$ dir. $N = p + 1 - t$ formülünden $t = -52$ bulunur. $6 \nmid -52$ dir. Ayrıca $y^2 \equiv x^3 + 22^3 \pmod{751}$ eğrisini de incelersek $N_{751,22} = 700$ dür. Nokta sayısı formülünden $t = 52$ bulunur. Yine $6 \nmid 52$ dir.

3.2.8. Sonuç. $p \equiv 1 \pmod 6$ asal olsun. Bu durumda $N \equiv 0$ veya $N \equiv 4 \pmod 6$ olur. (Yıldız ve ark. 2005)

3.2.9. Örnek. $y^2 \equiv x^3 + 212^3 \pmod{379}$ eliptik eğrisini ele alalım. Nokta sayısı $N_{379,212} = 388$ dir. O halde $N \equiv 0 \pmod 6$ dir. $y^2 \equiv x^3 + 4^3 \pmod{379}$ eğrisi için ise $N_{379,4} = 372$ dir. O halde $N \equiv 4 \pmod 6$ dir.

3.2.3. Teorem ile 3.2.8. Sonuç birleştirilerek aşağıdaki sonucu elde edilir:

3.2.10. Teorem. $p \equiv 1 \pmod{12}$ bir asal ise $t \equiv \mp 2 \pmod{12}$ ve $p \equiv 7 \pmod{12}$ bir asal ise $t \equiv \mp 4 \pmod{12}$ olur.(Yıldız ve ark. 2005)

Şimdi de $b = |t|$ olacak şekilde bir b tam sayısı tanımlayalım. Yani $b = |p + 1 - N|$ olsun. Bundan sonraki hesaplamalarımızda b ve t ile ilgili sonuçlar elde edeceğiz. (8) tipindeki eğri için $t = b$ ise eşleniği için $t = -b$ dir. İlk olarak (8) tipindeki Bachet eliptik eğrisi ve eşleniği üzerindeki rasyonel noktaların sayısı hakkında aşağıdaki sonucu verebiliriz.

3.2.11. Teorem. $p \equiv 1 \pmod 6$ asal olsun. Bu durumda

a) $b \equiv 2 \pmod 6$ ise (8) tipindeki eğri için $t = b$ ve $N \equiv 0 \pmod 6$ ve bu eğrinin eşleniği için $t = -b$ ve $N \equiv 4 \pmod 6$ olur.

b) $b \equiv 4 \pmod 6$ ise (8) tipindeki eğri için $t = b$ ve $N \equiv 4 \pmod 6$ ve bu eğrinin eşleniği için $t = -b$ ve $N \equiv 0 \pmod 6$ olur.

İspat. $p \equiv 1 \pmod 6$ asal olsun. $n \in \mathbb{Z}$ için $p = 1 + 6n$ yazalım. $b \equiv 2 \pmod 6$ olsun. Eğer $t = b$ ise $t \equiv 2 \pmod 6$ olur. Şimdi $m \in \mathbb{Z}$ için $t = 2 + 6m$ yazalım. O halde

$$\begin{aligned} N &= p + 1 - t = 6n + 1 + 1 - 2 - 6m \\ &= 6(n - m) \end{aligned}$$

olur. Bu da $N \equiv 0 \pmod 6$ oluşunu gerektirir. Diğer kısımlar benzer şekilde ispatlanabilir.

3.2.12. Örnek. $p = 313 \equiv 1 \pmod 6$ bir asal iken $y^2 \equiv x^3 + 2^3 \pmod{313}$ eliptik eğrisini ele alalım. $N = N_{313,2} = 336$ ve $t = -22$ olur. $t = b$ olduğundan $b = -22 \equiv 2 \pmod 6$ dir. O halde $N \equiv 0 \pmod 6$ dir. Bu eğrinin bir eşleniği olan $y^2 \equiv x^3 + 222^3 \pmod{313}$ eğrisi üzerindeki nokta sayısının $N_{313,222} = 292$ olduğunu buluruz. Nokta sayısı formülünden $t = 22$ bulunur. $t = -b$ olduğundan $b = -22 \equiv 2 \pmod 6$ bulunur. O halde $N \equiv 4 \pmod 6$ dır.

3.3. Bachet Eliptik Eğrileri Üzerindeki 3.Mertebeden Elemanlar

Bu bölümde E_a Bachet eliptik eğrilerinde 3.mertebeden eleman bulunma koşulları belirlenecek ve bunlarla ilgili bazı sonuçlar elde edilecektir. İlk olarak aşağıdaki sonucu verelim:

3.3.1. Sonuç a) $p \equiv 1 \pmod{12}$ bir asal olsun. Eğer $b \equiv 2 \pmod{12}$ ise (8) tipindeki eğri için $t = b$ ve $N \equiv 0 \pmod{12}$ olur. Ayrıca $E_a(\mathbb{F}_p)$'nin 3.mertebeden elemanı vardır. Bu eğrinin eşleniği için $t = -b$ ve $N \equiv 4 \pmod{12}$ olur. Bu da 3.mertebeden eleman bulundurmamayı gerektirir.

Eğer $b \equiv 10 \pmod{12}$ ise (8) eğrisi için $t = b$ ve $N \equiv 4 \pmod{12}$ ve $E_a(\mathbb{F}_p)$'nin 3. mertebeden elemanı yoktur. Bu eğrinin eşleniği için $t = -b$ ve $N \equiv 0 \pmod{12}$ olur. Bu da grubun 3.mertebeden eleman bulundurmasını gerektirir.

b) $p \equiv 7 \pmod{12}$ bir asal olsun. Eğer $b \equiv 4 \pmod{12}$ ise (8) tipindeki eğri için $t = b$ ve $N \equiv 4 \pmod{12}$ olur. Bu yüzden de $E_a(\mathbb{F}_p)$'nin 3.mertebeden elemanı yoktur. Bu eğrinin eşleniği için $t = -b$ ve $N \equiv 0 \pmod{12}$ olur. Ayrıca $E_a(\mathbb{F}_p)$ 3.mertebeden eleman bulundurur.

Eğer $b \equiv 8 \pmod{12}$ ise (8) tipindeki bir eğri için $t = b$ ve $N \equiv 0 \pmod{12}$ olur. Ayrıca $E_a(\mathbb{F}_p)$'nin 3.mertebeden elemanı vardır. Bu eğrinin eşleniği için $t = -b$ ve $N \equiv 4 \pmod{12}$ olur. Bu yüzden de grubun 3.mertebeden elemanı yoktur. (Yıldız ve ark. 2005)

3.3.2. Örnek. $p = 673 \equiv 1 \pmod{12}$ bir asal iken $y^2 \equiv x^3 + 2^3 \pmod{673}$ eliptik eğrisini ele alalım. $N_{673,2} = 624$, $t = 50$ ve $b = 50 \equiv 2 \pmod{12}$ dir. O halde $N \equiv 0 \pmod{12}$ olur. Bu eğri 3.mertebeden 2 eleman bulundurur. Bu elemanlar $(0,107), (0,566)$ dır. Bu eğrinin bir eşleniği olan $y^2 \equiv x^3 + 22^3 \pmod{673}$ eliptik eğrisini alırsak $N_{673,22} = 724$, $t = -50$ ve $b = 50 \equiv 2 \pmod{12}$ olur. O halde $N \equiv 4 \pmod{12}$ tür. Bu eğride 3.mertebeden eleman bulunmaz.

Eliptik eğrilerin p modunda sınıflandırılmasında 3.mertebeden elemanlar önemlidir. Şimdi 3.mertebeden eleman sayısının 2 ya da 8 olduğunu gösterelim.

3.3.3. Teorem. $p \equiv 1 \pmod{6}$ bir asal olsun. Eğer E_a eğrisi üzerindeki nokta sayısı $N \equiv 0 \pmod{6}$ ise eğri üzerinde 3.mertebeden 2 ya da 8 tane nokta vardır.

İspat. 1.3.25 Sonuç gereği E_a eğrisi üzerinde sonsuzdaki nokta ile birlikte en çok 9 nokta vardır. Bu noktalar bir alt grup oluştururlar. Bu alt grup ya aşikâr grup, ya 3 mertebeli bir devirli grup ya da 3 mertebeli iki devirli grubun çarpımına izomorftur.

Üçüncü mertebeden elemanların sayısını ifade etmek istediğimizden bu grup aşikar grup olamaz. O halde grup yapısı C_3 ya da $C_3 \times C_3$ tür. Bu grupların da sırasıyla 3.mertebeden 2 ya da 8 eleman bulundurduğu iyi bilinir. □

Gerçekten de $E_a(\mathbb{F}_p) \cong C_n \times C_{nm}$ alırsak $3 \mid n$ iken $E_a(\mathbb{F}_p)$'de 3.mertebeden 8 nokta, aksi halde 3.mertebeden 2 nokta vardır.

3.3.4. Örnek. $y^2 \equiv x^3 + 4^3 \pmod{19}$ eliptik eğrisini ele alalım. Nokta sayısı $N_{19,4} = 12 \equiv 0 \pmod 6$ olur. Bu eğri üzerinde 3.mertebeden 2 eleman vardır: $(0,8),(0,11)$. $y^2 \equiv x^3 + 10^3 \pmod{31}$ eliptik eğrisi için ise $N_{31,10} = 36 \equiv 0 \pmod 6$ dır. Bu eğri üzerinde 3.mertebeden 8 eleman vardır: $(0,15),(0,16),(6,10),(6,21),(26,10)$ $(30,10),(30,21)$.

İleride 3.3.9 Teoremde ana sonuçlardan birini vereceğiz. Bunun için ilk olarak aşağıdaki sonuçlara gereksinimimiz var:

3.3.5.Teorem. p bir asal olsun. O halde $\mathbb{F}_p$'deki tüm x'lerden sadece 0 için $x^3 + 1$, 1 değerini alır.

İspat. $x = 0$ durumunda şartın sağlandığı açıktır. x'in diğer değerlerinden hiçbirinin $x^3 + 1 = 1$ şartını sağlamaması p'nin asal oluşundan çıkar.□

3.3.6. Teorem. p bir asal olsun. x'in 1 ile p arasında $x^3 + 1 \equiv 0 \pmod p$ şartını sağlayan 3 değeri vardır.

İspat. Her $a \neq 0$ değeri için $x^3 \equiv a \pmod p$'nin üç tane çözümü olduğu açıkça görülür. Burada $a = -1$ için ispat elde edilebilir.□

3.3.7. Teorem. $p \equiv 1 \pmod 6$ asal olsun. Bu durumda

$$\sum_{x \in \mathbb{F}_p} \chi(x^3 + 1) \equiv 4 \pmod 6$$

olur.

İspat. Her bir $x \in \mathbb{F}_p$ için x^3+1'in p tane değeri hesaplanır. 3.3.5 Teorem gereği göre bu değerlerden biri 1'dir. 3.3.6 Teoreme göre bu değerlerden üçü 0'dır. x^3+1'in kalan $p-4$ değeri $\frac{p-4}{3}$ tane üçlü şeklinde gruplandırılır. $p \equiv 1 \pmod 6$ iken $\frac{p-4}{3}$ tektir. Gerçekten $k \in \mathbb{Z}$ için $p = 1+6k$ yazarsak $\frac{p-4}{3} = 2k-1$ olur. Varsayalım ki bu üçlülerden s tanesi Q_p'de $2k-1-s$ tane Q_p' nde olsun. Bir üçlü Q_p'de ise $\sum_{x \in \mathbb{F}_p} \chi(x^3+1)$ toplamına 3 eklenir. Eğer Q_p' nde ise toplama (-3) eklenir. Bu yüzden

$$\begin{aligned}\sum_{x \in \mathbb{F}_p} \chi(x^3+1) &= 1+3.0+s.(+3)+(2k-1-s).(-3) \\ &= 6(s-k)+4\end{aligned}$$

ifadesi sonucu gerektirir.

3.3.8. Örnek. $p = 13$ olsun. Bu durumda,

$$\begin{aligned}\sum_{x \in \mathbb{F}_{13}} \chi(x^3+1) &= \chi(1)+\chi(2)+\chi(9)+\chi(2)+\chi(0)+\chi(9)+\chi(9) \\ &\quad +\chi(6)+\chi(6)+\chi(2)+\chi(0)+\chi(5)+\chi(0) \\ &= 1-1+1-1+0+1+1-1-1-1+0-1+0 \\ &= -2 \equiv 4 \pmod 6\end{aligned}$$

3.3.9. Teorem. $p \equiv 1 \pmod 6$ bir asal olsun. E_a eğrisinde $a \in Q_p$ olması için gerek ve yeter şart $N \equiv 0 \pmod 6$ dır.

İspat.

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

ifadesi iyi bilinir. $n \in \mathbb{Z}$ için $p = 1+6n$ koyarsak $N_{p,a} = 6n+2+\sum_{x \in \mathbb{F}_p} \chi(x^3+a^3)$ elde ederiz. Şimdi $\chi(a) = 1$ iken ve x^3'ün değerleri kümesi ile a^3x^3'ün değerlerinin kümesi aynı olduğundan

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

yazılabilir. 3.3.7 Teoreme göre bu toplam da 6 modunda 4'e denktir. Böylece $r\in\mathbb{Z}$ için $\sum_{x\in\mathbb{F}_p}\chi(x^3+a^3)=4+6r$ değerini yerine koyarak $N_{p,a}=N=6n+2+4+6r$ elde edilir.

Bu da $N\equiv 0 \pmod 6$ oluşunu gerektirir.□

3.3.10. Örnek. $y^2\equiv x^3+122^3 \pmod{181}$ eğrisini ele alalım. $122\in Q_{181}$ olduğundan eğri üzerindeki nokta sayısı $N=156\equiv 0 \pmod{12}$ olur.

3.3.11. Sonuç. $p\equiv 1 \pmod 6$ asal olsun. Eğer $N\equiv 0 \pmod 6$ ise $t\equiv 2 \pmod 6$ dır.

İspat. $N=p+1-t=p+1+\sum_{x\in\mathbb{F}_p}\chi(x^3+a^3)$ iken $t=-\sum_{x\in\mathbb{F}_p}\chi(x^3+a^3)$ olduğu bilinir. 3.3.7 Teoremden sonuç görülür.□

3.3.12. Örnek. 3.3.10. Örnekteki eğriyi ele aldığımızda $N=156\equiv 0 \pmod{12}$ olduğu görülür. Bu durumda $N=p+1-t$ formülünden $156=181+1-t$, $t=26$ ve $t\equiv 2 \pmod 6$ olur.

Benzer olarak şunu elde ederiz.

3.3.13. Teorem. $p\equiv 1 \pmod 6$ bir asal olsun. E_a eğrisini ele alalım. Bu durumda $a\in Q_p'$ olması için gerek ve yeter şart $N\equiv 4 \pmod 6$'dır. (Yıldız ve ark. 2005)

3.3.14. Örnek. $y^2 \equiv x^3 + 22^3 \pmod{181}$ eliptik eğrisini ele alalım. $22 \notin Q_{181}$ olduğundan eğri üzerindeki nokta sayısı $N = 208 \equiv 4 \pmod{12}$ dır.

3.3.15. Sonuç. $p \equiv 1 \pmod 6$ bir asal olsun. E_a eğrisini ele alalım. Bu durumda

a) $a \in Q_p$ olması için gerek ve yeter şart $E_a(\mathbb{F}_p)$'de 3.mertebeden 2 ya da 8 eleman vardır.

b) $a \in Q_p'$ olması için gerek ve yeter şart $E_a(\mathbb{F}_p)$'de 3.mertebeden eleman bulunmamasıdır.

İspat. Bu, 3.3.1. Sonuç ve 3.3.9. Teoremden açıkça görülür.□

3.3.16. Örnek. $y^2 \equiv x^3 + 4^3 \pmod{19}$ eğrisinde $4 \in Q_{19}$ olduğundan 3.mertebeden 2 eleman vardır. $y^2 \equiv x^3 + 10^3 \pmod{31}$ eğrisinde ise $10 \in Q_{31}$ olduğundan 3.mertebeden 8 eleman vardır. $y^2 \equiv x^3 + 3^3 \pmod{31}$ eğrisinde $3 \notin Q_{31}$ olduğundan 3.mertebeden eleman yoktur.

3.4. $C_n \times C_n$ Grup Yapısındaki Bachet Eliptik Eğrileri

Şimdi bazı n değerleri için grup yapısı $C_n \times C_n$'e izomorf olan Bachet eliptik eğrilerinin durumunu inceleyeceğiz. Bunun sadece $p \equiv 1 \pmod 6$ iken mümkün olduğunu göstereceğiz. Diğer durumda ise yani $p \equiv 5 \pmod 6$ iken $E(\mathbb{F}_p)$'nin grup yapısı C_{p+1}'e izomorftur.

Bu kez 1.7.3 Önermede ifade edilen Washington'un sonucundan yararlanarak Bachet eliptik eğrilerinin grup yapısı ile ilgili yeni bir sonuç elde edeceğiz.

3.4.1.Teorem. E_a eğrisini ele alalım. Varsayalım ki

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

olsun. Bu durumda $p = n^2 \mp n + 1$'dir.

İspat. 1.7.3. Önerme gereği p için üç ihtimal vardır. $p = n^2 + 1,\ p = n^2 \mp n + 1$ ya da $p = (n \mp 1)^2$ 'dir. Bunlardan sonuncusu p asal olup bir tam kare olamayacağından hemen elenir. O halde sadece p 'nin $n^2 + 1$'e eşit olamayacağını göstermemiz gerekir. Eğer $p = n^2 + 1$ ise $n^2 = p - 1$'dir ve böylece $p - 1$ elemanı Q_p'dedir. Fakat sadece $p \equiv 5 \pmod 6$ asal iken $p - 1$ 'in Q_p'de olduğu bilinir. Sonuç buradan görülür.

3.4.2. Örnek. $y^2 \equiv x^3 + 24^3 \pmod{1723}$ eliptik eğrisini ele alalım. Bu eğri üzerindeki nokta sayısı $N = 1764$ 'tür. $p = n^2 - n + 1$ formülünden $1723 = 42^2 - 42 + 1$ olduğundan bu eğrinin grup yapısı $C_{42} \times C_{42}$ dir.

EKLER

># y^2=x^3+a^3 (mod p) EĞRİSİ ÜZERİNDEKİ RASYONEL NOKTA SAYISINI HESAPLAMA#

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

ÖRNEK

```
> #y^2=x^3+24^3 (mod 1723) Eğrisi Üzerindeki Rasyonel Nokta Sayısını Hesaplama#
> restart;
> p:=prime;a:=int;n:=posint;l:int;
> hesapla:=proc(p,a);
>  n:=p+1;
>    for x from 0 to p-1 do
>      with(numtheory):
>       l:=legendre(x^3+a^3,p);
>       n:=n+l;
>    end do;
>  end proc;
Warning, `n` is implicitly declared local to procedure `hesapla`
Warning, `x` is implicitly declared local to procedure `hesapla`
Warning, `l` is implicitly declared local to procedure `hesapla`
```

```
hesapla := proc(p, a)
local n, x, l;
    n := p + 1;
    for x from 0 to p − 1 do
        with(numtheory); l := legendre(x^3 + a^3, p); n := n + l
    end do
end proc
```

```
> hesapla(1723,24);
```

Warning, the protected name order has been redefined and unprotected

1764

```
> # P MODUNDA İKİNCİ DERECEDEN KALANLARI HESAPLAMA#
> restart;
>  p:=prime;x:=int;s:=int;
>  hesapla:=proc(p);
>    for x from 1 to p-1 do
>      with(numtheory):
>      s:=mroot(x,2,p);
>      if s<>FAIL then
>         print(x);
>      end if;
>    end do;
> end proc;
> hesapla(p);
```

ÖRNEK

```
>#Q31 'i Hesaplama#
> restart;
>  p:=prime;x:=int;s:=int;
>  hesapla:=proc(p);
>    for x from 1 to p-1 do
```

```
>     with(numtheory):
>     s:=mroot(x,2,p);
>     if s<>FAIL then
>       print(x);
>     end if;
>   end do;
> end proc;
>hesapla(31);
```

p := *prime*

x := *int*

s := *int*

Warning, `x` is implicitly declared local to procedure `hesapla`

Warning, `s` is implicitly declared local to procedure `hesapla`

hesapla := **proc**(*p*)
local *x*, *s*;
    for *x* **to** *p* − 1 **do**
        with(*numtheory*); *s* := mroot(*x*, 2, *p*); **if** *s* ≠ *FAIL* **then** print(*x*) **end if**
    end do
end proc

Warning, the protected name order has been redefined and unprotected

1
2
4
5
7
8
9
10
14
16
18
19

```
 20
 25
 28
```

> # p=1 (mod 6) ASALLARI LİSTELER #

```
>restart;
>asallistele:=proc(n);
>x:=int;a:=prime;i:=int;
>  for i from 1 while ithprime(i)< n do
>   with(numtheory):
>   a:=ithprime(i);
>   x:=a mod 6;
>     if x = 1 then
>      lprint(a);
>     end if;
>  end do;
>end proc;
>asallistele(n);
```

> # p=5 (mod 6) ASALLARI LİSTELER #

```
>restart;
>asallistele:=proc(n);
>x:=int;a:=prime;i:=int;
>  for i from 1 while ithprime(i)< n do
>   with(numtheory):
>   a:=ithprime(i);
>   x:=a mod 6;
>     if x = 5 then
>      lprint(a);
>     end if;
>  end do;
>end proc;
```

```
>asallistele(n);
```

> #y^2=x^3+a^3 (mod p) EĞRİSİNDEKİ NOKTALARIN MERTEBELERİNİ BULMA#

```
> restart;
> mertebe:=proc(x1,y1,p);
>x:=int;y:=int;x2:=int;y2:=int;
> n:=2;
> if y1<>0 then
>    n:=n+1;
>    m:=((3*x1^2)/(2*y1)) mod p;
>    x:=(m^2-x1-x1) mod p;
>    y:=(m*(x1-x)-y1) mod p;
>    #print([x,y],"mertebe:",n);
>    x2:=x;y2:=y;
>    while x<>x1 or y<>p-y1 do
>         n:=n+1;
>        m:=((y-y1)/(x-x1)) mod p;
>        x:=(m^2-x-x1) mod p;
>        y:=(m*(x2-x)-y2) mod p;
>       #print([x,y],"mertebe:",n);
>       x2:=x;y2:=y;
>    end do;
> print("mertebe:",n);
> else  print("mertebe:",n);
> end if;
>end proc;
> hesapla:=proc(p,a);
>   xgec:=int;ygec:=int;l:=int;
>   for xgec from 0 to p-1 do
>     with(numtheory);
>     l:=xgec^3+a^3;
```

```
>     ygec:=msqrt(l,p);
>     if   ygec<>FAIL  then
>      if ygec<>0 then
>        print([xgec,ygec],[xgec,-ygec]);
>      else
>        print([xgec,ygec]);
>      end if;
>     mertebe(xgec,ygec,p);
>     end if;
>   end do;
> end proc;
> hesapla(p,a);
```

ÖRNEK

> #y^2=x^3+4^3 (mod 19) EĞRİSİNDEKİ NOKTALARIN MERTEBELERİNİ BULMA#

```
> restart;
> mertebe:=proc(x1,y1,p);
>x:=int;y:=int;x2:=int;y2:=int;
> n:=2;
> if y1<>0 then
>    n:=n+1;
>    m:=((3*x1^2)/(2*y1)) mod p;
>    x:=(m^2-x1-x1) mod p;
>    y:=(m*(x1-x)-y1) mod p;
>    #print([x,y],"mertebe:",n);
>    x2:=x;y2:=y;
>    while x<>x1 or y<>p-y1 do
>          n:=n+1;
>         m:=((y-y1)/(x-x1)) mod p;
>         x:=(m^2-x-x1) mod p;
```

```
>         y:=(m*(x2-x)-y2) mod p;
>        #print([x,y],"mertebe:",n);
        x2:=x;y2:=y;
>     end do;
> print("mertebe:",n);
>else  print("mertebe:",n);
> end if;
>end proc;
`Warning, \`x\` is implicitly declared local to procedure \`mertebe\`\n`
`Warning, \`y\` is implicitly declared local to procedure \`mertebe\`\n`
`Warning, \`x2\` is implicitly declared local to procedure \`mertebe\`\n`
`Warning, \`y2\` is implicitly declared local to procedure \`mertebe\`\n`
`Warning, \`n\` is implicitly declared local to procedure \`mertebe\`\n`
`Warning, \`m\` is implicitly declared local to procedure \`mertebe\`\n`
mertebe := proc(x1, y1, p)
local x, y, x2, y2, n, m;
    x := int;
    y := int;
    x2 := int;
    y2 := int;
    n := 2;
    if y1 ≠ 0 then
        n := n + 1;
        m := (3/2×x1^2/y1) mod p;
        x := (m^2 – 2×x1) mod p;
        y := (m×(x1 – x) – y1) mod p;
        x2 := x;
        y2 := y;
        while x ≠ x1 or y ≠ p – y1 do
            n := n + 1;
            m := (y – y1)/(x – x1) mod p;
            x := (m^2 – x – x1) mod p;
            y := (m×(x2 – x) – y2) mod p;
            x2 := x;
```

```
                y2 := y
            end do ;
            print( "mertebe:", n )
        else print( "mertebe:", n )
        end if
    end proc
> hesapla:=proc(p,a);
>xgec:=int;ygec:=int;l:=int;
> for xgec from 0 to p-1 do
> with(numtheory);
> l:=xgec^3+a^3;
> ygec:=msqrt(l,p);
> if   ygec<>FAIL  then
>if ygec<>0 then
 >print([xgec,ygec],[xgec,-ygec]);
 >else
 >print([xgec,ygec]);
>end if;
>mertebe(xgec,ygec,p);
> end if;
> end do;
> end proc;
Warning, `xgec` is implicitly declared local to procedure `hesapla`
Warning, `ygec` is implicitly declared local to procedure `hesapla`
Warning, `l` is implicitly declared local to procedure `hesapla`
hesapla := proc(p, a)
local xgec, ygec, l;
    xgec := int;
    ygec := int;
    l := int;
    for xgec from 0 to p - 1 do
        with( numtheory );
        l := xgec^3 + a^3;
        ygec := msqrt( l, p );
        if ygec ≠ FAIL then
```

```
            if ygec ≠ 0 then print( [ xgec, ygec ], [ xgec, –ygec ] )
            else print( [ xgec, ygec ] )
            end if ;
            mertebe( xgec, ygec, p )
        end if
    end do
end proc
```

```
> hesapla(19,4);
```

Warning, the protected name order has been redefined and unprotected

```
                    [ 0, 8 ], [ 0, -8 ]
                    "mertebe:", 3
                    [ 8, 5 ], [ 8, -5 ]
                    "mertebe:", 6
                        [ 10, 0 ]
                    "mertebe:", 2
                   [ 12, 5 ], [ 12, -5 ]
                    "mertebe:", 6
                        [ 13, 0 ]
                    "mertebe:", 2
                        [ 15, 0 ]
                    "mertebe:", 2
                   [ 18, 5 ], [ 18, -5 ]
                    "mertebe:", 6
```

 # Eliptik Eğri Üzerindeki Noktaların Mertebelerini Hesaplar # Visual Basic

```
Sub Makro1()
    j = 2
    Do While Sheets(1).Cells(j, 1) <> "son"
      i = 2
      x1 = Sheets(1).Cells(j, 1)
      y1 = Sheets(1).Cells(j, 2)
      k = Sheets(1).Cells(j, 3)
```

```
a = Sheets(1).Cells(j, 4)
If y1 <> 0 Then
   i = i + 1
   m1 = (3 * x1 * x1 + a)
   m2 = (2 * y1)
   Sheets(2).Cells(1, 1) = m1
   Sheets(2).Cells(1, 2) = m2
   Sheets(2).Cells(2, 1) = "=MOD(R[-1]C,R[-1]C[1])"
   Do While Sheets(2).Cells(2, 1) <> 0
      m1 = m1 + k
      Sheets(2).Cells(1, 1) = m1
      Sheets(2).Cells(1, 2) = m2
     Sheets(2).Cells(2, 1) = "=MOD(R[-1]C,R[-1]C[1])"
   Loop
   m = m1 / m2
   Sheets(3).Cells(1, 1) = m
   Sheets(3).Cells(2, 1) = "=MOD(R[-1]C,'1'!RC[2])"
   m = Sheets(3).Cells(2, 1)
   x = m * m - x1 - x1
   y = m * (x1 - x) - y1
   Sheets(3).Cells(1, 2) = x
   Sheets(3).Cells(2, 2) = "=MOD(R[-1]C,'1'!RC[1])"
   Sheets(3).Cells(1, 3) = y
   Sheets(3).Cells(2, 3) = "=MOD(R[-1]C,'1'!RC[0])"
   x = Sheets(3).Cells(2, 2)
   y = Sheets(3).Cells(2, 3)
   x2 = x
   y2 = y

   Do While x <> x1 Or y <> (k - y1)
      i = i + 1
      m1 = y - y1
```

```
            m2 = x - x1
            Sheets(2).Cells(1, 1) = m1
            Sheets(2).Cells(1, 2) = m2
            Sheets(2).Cells(2, 1) = "=MOD(R[-1]C,R[-1]C[1])"
            Do While Sheets(2).Cells(2, 1) <> 0
               m1 = m1 + k
               Sheets(2).Cells(1, 1) = m1
               Sheets(2).Cells(1, 2) = m2
               Sheets(2).Cells(2, 1) = "=MOD(R[-1]C,R[-1]C[1])"
            Loop
            m = m1 / m2
            Sheets(3).Cells(1, 1) = m
            Sheets(3).Cells(2, 1) = "=MOD(R[-1]C,'1'!RC[2])"
            m = Sheets(3).Cells(2, 1)
            x = m * m - x - x1
            y = m * (x2 - x) - y2
            Sheets(3).Cells(1, 2) = x
            Sheets(3).Cells(2, 2) = "=MOD(R[-1]C,'1'!RC[1])"
            Sheets(3).Cells(1, 3) = y
            Sheets(3).Cells(2, 3) = "=MOD(R[-1]C,'1'!RC[0])"
            x = Sheets(3).Cells(2, 2)
            y = Sheets(3).Cells(2, 3)
            x2 = x
            y2 = y

         Loop
         Sheets(1).Cells(j, 5) = i
      End If
      j = j + 1
      Loop

End Sub
```

```
Sub xolus()
    ' xolus Makro
    'Sheets("nokta belirle").Columns("A:A").Select
    'Selection.ClearContents
    Sheets("nokta belirle").Cells(1, 1) = "x"
    Sheets("grafik veri").Cells(1, 1) = "x"
    Sheets("grafik veri").Cells(1, 2) = "y"
    td = Sheets("nokta belirle").Cells(2, 2)
    gg = 1
    sat = 2
    j = 2
    For md = 0 To td - 1
      Sheets("nokta belirle").Cells(md + 2, 2) = td
      Sheets("nokta belirle").Cells(md + 2, 1) = md
      Sheets("nokta belirle").Cells(md + 2, 5) = md ^ 3 + a * md +
    Sheets("nokta belirle").Cells(2, 4)
      Sheets("nokta belirle").Cells(md + 2, 6) = "=MOD(R[0]C[-1],RC[-4])"
      ag = Sheets("nokta belirle").Cells(md + 2, 6)
        For yf = 0 To td - 1
          For ch = 0 To td - 1
            If ((yf * yf) - ch * td) = ag Then
              gg = gg + 1
              Sheets(1).Cells(gg, 1) = Sheets("nokta belirle").Cells(2 +
    md, 1)
              Sheets(1).Cells(gg, 2) = yf
              Sheets(1).Cells(gg, 3) = Sheets("nokta belirle").Cells(2, 2)
              Sheets(1).Cells(gg, 4) = Sheets("nokta belirle").Cells(2, 3)
              i = 2
              x1 = Sheets(1).Cells(gg, 1)
              y1 = Sheets(1).Cells(gg, 2)
              k = Sheets(1).Cells(gg, 3)
              a = Sheets(1).Cells(gg, 4)
```

```
Sheets(1).Cells(2, 2 * gg + 3) = x1
Sheets(1).Cells(2, 2 * gg + 4) = y1
Sheets("grafik veri").Cells(sat, 1) = x1
Sheets("grafik veri").Cells(sat, 2) = y1
sat = sat + 1
Sheets(1).Cells(1, 2 * gg + 3) = "x"
Sheets(1).Cells(1, 2 * gg + 4) = "y"
Sheets(1).Cells(i, 6) = 1
If y1 <> 0 Then
   i = i + 1
   m1 = (3 * x1 * x1 + a)
   m2 = (2 * y1)
   Sheets(2).Cells(1, 1) = m1
   Sheets(2).Cells(1, 2) = m2
   Sheets(2).Cells(2, 1) = "=MOD(R[-1]C,R[-1]C[1])"
   Do While Sheets(2).Cells(2, 1) <> 0
   m1 = m1 + k
      Sheets(2).Cells(1, 1) = m1
      Sheets(2).Cells(1, 2) = m2
      Sheets(2).Cells(2, 1) = "=MOD(R[-1]C,R[-1]C[1])"
   Loop
   m = m1 / m2
   Sheets(3).Cells(1, 1) = m
   Sheets(3).Cells(2, 1) = "=MOD(R[-1]C,'1'!RC[2])"
   m = Sheets(3).Cells(2, 1)
   x = m * m - x1 - x1
   y = m * (x1 - x) - y1
   Sheets(3).Cells(1, 2) = x
   Sheets(3).Cells(2, 2) = "=MOD(R[-1]C,'1'!RC[1])"
   Sheets(3).Cells(1, 3) = y
   Sheets(3).Cells(2, 3) = "=MOD(R[-1]C,'1'!RC[0])"
   x = Sheets(3).Cells(2, 2)
```

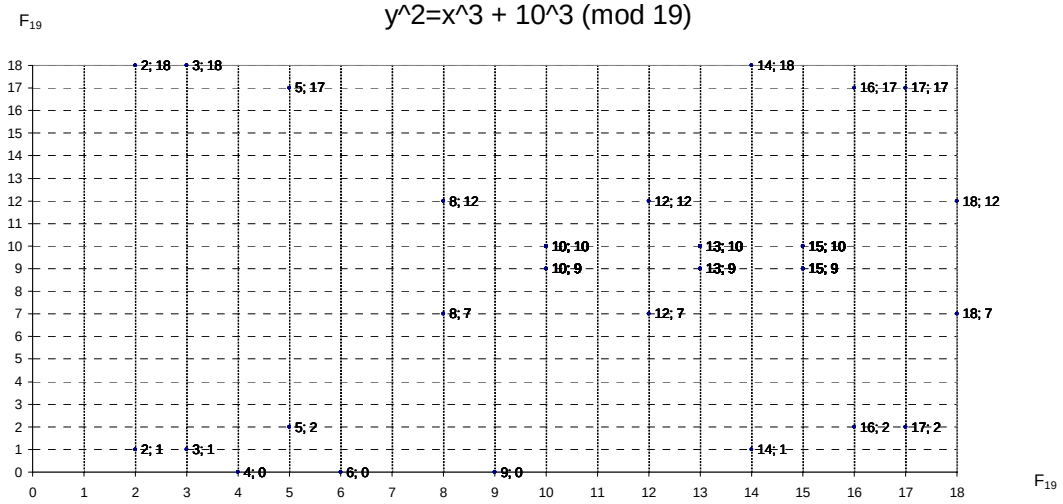
```
y = Sheets(3).Cells(2, 3)
Sheets(1).Cells(i, 2 * gg + 3) = x
Sheets(1).Cells(i, 2 * gg + 4) = y
Sheets(1).Cells(i, 6) = i - 1
Sheets("grafik veri").Cells(sat, 1) = x
Sheets("grafik veri").Cells(sat, 2) = y
sat = sat + 1
x2 = x
y2 = y
Do While x <> x1 Or y <> (k - y1)
   i = i + 1
   m1 = y - y1
   m2 = x - x1
   Sheets(2).Cells(1, 1) = m1
   Sheets(2).Cells(1, 2) = m2
   Sheets(2).Cells(2, 1) = "=MOD(R[-1]C,R[-1]C[1])"
   Do While Sheets(2).Cells(2, 1) <> 0
      m1 = m1 + k
      Sheets(2).Cells(1, 1) = m1
      Sheets(2).Cells(1, 2) = m2
      Sheets(2).Cells(2, 1) = "=MOD(R[-1]C,R[-1]C[1])"
   Loop
   m = m1 / m2
   Sheets(3).Cells(1, 1) = m
   Sheets(3).Cells(2, 1) = "=MOD(R[-1]C,'1'!RC[2])"
   m = Sheets(3).Cells(2, 1)
   x = m * m - x - x1
   y = m * (x2 - x) - y2
   Sheets(3).Cells(1, 2) = x
   Sheets(3).Cells(2, 2) = "=MOD(R[-1]C,'1'!RC[1])"
   Sheets(3).Cells(1, 3) = y
   Sheets(3).Cells(2, 3) = "=MOD(R[-1]C,'1'!RC[0])"
```

```
                x = Sheets(3).Cells(2, 2)
                y = Sheets(3).Cells(2, 3)
                x2 = x
                y2 = y
            Sheets(1).Cells(i, 6) = i - 1
            Sheets(1).Cells(i, 2 * gg + 3) = x
            Sheets(1).Cells(i, 2 * gg + 4) = y
            Sheets("grafik veri").Cells(sat, 1) = x
            Sheets("grafik veri").Cells(sat, 2) = y
            sat = sat + 1
            Loop
            Sheets(1).Cells(j, 5) = i
          Else
            Sheets(1).Cells(j, 5) = 2
          End If
        j = j + 1
      End If
    Next
  Next
Next
End Sub
```

ÖRNEK

$y^2 \equiv x^3 + 10^3 \pmod{19}$ eliptik eğrisi üzerindeki noktaları, bu noktaların kuvvetlerini ve mertebelerini bulunuz.

x	y	MOD	a	MERTEBE	KUVVET	x	y	x	y	x	y	x	y	x	y	x	y	x	y	x	y	x	y	x	y	x	y	x	y	x	y	x	y	x	y	x	y	x	y
2	1	19	10	14	1	2	1	2	18	3	1	3	18	4	0	5	2	5	17	6	0	8	7	8	12	9	0	10	9	10	10	12	7	12	12	13	9	13	10	14	1	14	18	15	9
2	18	19	10	14	2	13	9	13	10	10	9	10	10			15	10	15	9			10	9	10	10			15	9	15	10	15	9	15	10	10	9	10	10	15	9	15	10	13	9
3	1	19	10	14	3	5	2	5	17	17	2	17	17			8	7	8	12			2	18	2	1			13	10	13	9	3	18	3	1	15	10	15	9	16	2	16	17	10	10
3	18	19	10	14	4	10	9	10	10	15	9	15	10			13	10	13	9			15	9	15	10							13	9	13	10			13	9	13	10		
4	0	19	10	2	5	8	12	8	7	12	12	12	7			2	1	2	18			5	2	5	17							17	2	17	17			18	12	18	7		
5	2	19	10	14	6	15	10	15	9	13	10	13	9			10	9	10	10			13	10	13	9							10	10	10	9			10	10	10	9		
5	17	19	10	14	7	9	0	9	0	4	0	4	0			9	0	9	0			9	0	9	0							4	0	4	0			6	0	6	0		
6	0	19	10	2	8	15	9	15	10	13	9	13	10			10	10	10	9			13	9	13	10							10	9	10	10			10	9	10	10		
8	7	19	10	14	9	8	7	8	12	12	7	12	12			2	18	2	1			5	17	5	2							17	17	17	2			18	7	18	12		
8	12	19	10	14	10	10	10	10	9	15	10	15	9			13	9	13	10			15	10	15	9							13	10	13	9			13	10	13	9		
9	0	19	10	2	11	5	17	5	2	17	17	17	2			8	12	8	7			2	1	2	18							3	1	3	18			16	17	16	2		
10	9	19	10	4	12	13	10	13	9	10	10	10	9			15	9	15	10			10	10	10	9							15	10	15	9			15	10	15	9		
10	10	19	10	4	13	2	18	2	1	3	18	3	1			5	17	5	2			8	12	8	7							12	12	12	7			14	18	14	1		
12	7	19	10	14																																					
12	12	19	10	14																																					
13	9	19	10	4																																					
13	10	19	10	4																																					
14	1	19	10	14																																					
14	18	19	10	14																																					
15	9	19	10	4																																					
15	10	19	10	4																																					
16	2	19	10	14																																					
16	17	19	10	14																																					
17	2	19	10	14																																					
17	17	19	10	14																																					
18	7	19	10	14																																					
18	12	19	10	14																																					



KAYNAKLAR

Çelik, B. 2004. Maple ve Maple ile Matematik. Nobel Yayın Dağıtım Adakale sok. No:15/2 Yenişehir. Ankara.561 s.

Demirci, M., G.Soydan, İ.N.Cangül. 2005. Rational points on the elliptic curves $y^2 \equiv x^3 + a^3 \pmod{p}$ in F_p where $p \equiv 1 \pmod{6}$ is prime. Rocky J. of Maths, (basımda).

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

Knapp, A.W. 1992. Elliptic Curves. Princeton University Press. New Jersey.427 p.

Koblitz, N. 1994. A Course in Number Theory and Cryptography. Springer-Verlag New york Inc.235 p.

Mollin, R. A. 2001. An Introduction to Cryptography. Chapman&Hall/CRC. United States of America.373 p.

Namlı, D. 2001. Kübik Rezidüler. Doktora Tezi. Balıkesir Üniversitesi (yayımlanmamış), Balıkesir.74 s.

Paillier, Pascal. 2000. Trapdooring Discrete Logarithms on Elliptic Curves over Rings. Advances in Cryptology, vol.1976, p.573-584

Schmitt, S. ve H.G.Zimmer. 2003. Elliptic Curves A Computational Approach. Walter de Gruyter. Berlin. 367 p.

Silverman, J. H. 1986. The Arithmetic of Elliptic Curves, Springer-Verlag New York Inc. 400 p.

Silverman, J. H. ve J.Tate. 1992. Rational Points on Elliptic Curves, Springer-Verlag New York Inc.281 p.

Washington, L. C. 2003 Elliptic Curves. Number Theory and Cryptography. Chapman&Hall/CRC. United States of America. 428 p.

Yıldız İkikardeş, N., M.Demirci, G.Soydan, I.N.Cangül, 2005. The Group Structure of Bachet Elliptic Curves Over Finite F_p, (sunuldu).

İNDEKS

ÖZGEÇMİŞ

22.11.1974'te İzmir'de doğan Gökhan SOYDAN; ilk okul öğrenimini İzmir'de, ortaokul öğrenimini Konya'da, lise öğrenimini Adana'da tamamladı. 1992 yılında Hacettepe Üniversitesi Eğitim Fakültesi Matematik Öğretmenliği Bölümü'nde lisans öğrenimine başladı. 1996 yılından itibaren yüksek öğrenimine Kara Kuvvetleri Komutanlığı nam ve hesabına devam etti. 1997 yılında teğmen rütbesi ile mezun oldu. Aynı yıl Balıkesir Çok Programlı Astsubay Hazırlama Okul Komutanlığı'nda matematik öğretmeni olarak göreve başladı. 1999-2001 yılları arasında Balıkesir Üniversitesi Fen Edebiyat Fakültesi Matematik Bölümü'nde yüksek lisans öğrenimini tamamladı. 2001 yılında Uludağ Üniversitesi Fen Edebiyat Fakültesi Matematik Bölümü'nde doktora öğrenimine başladı. 2002 yılı atamalarında Bursa Işıklar Askeri Lisesi Komutanlığı'na matematik öğretmeni olarak atandı. Halen bu görevine devam etmektedir.

TEŞEKKÜR

F-2003/63 ve F-2004/40 nolu projeler kapsamında yürüttüğümüz çalışmalarım esnasında karşılaştığım zorluklarda yardım ve desteğini esirgemeyen, pozitif yaklaşımları ile beni her zaman motive eden, tecrübe ve bilgisi ile yönlendiren Danışman Hocam Sayın Prof. Dr. İsmail Naci CANGÜL'e içtenlikle teşekkür ederim.

Akademik çalımalarım esnasında tüm imkanlarını seferber eden Işıklar Askeri Lisesi Komutanlığı'ndaki sıralı amirlerime ve mesai arkadaşlarıma teşekkürlerimi sunarım.

Çalışmalarımızı beraber yürüttüğümüz kıymetli arkadaşlarım Arş. Gör. Musa DEMİRCİ ve Arş. Gör. Nazlı YILDIZ İKİKARDEŞ, size de teşekkürler...

Bu aşamaya gelene kadar maddi manevi desteklerini eksik etmeyen anneme, babama ve kardeşime de teşekkürü borç bilirim.

Bu uzun ve yorucu çalışma döneminde her türlü desteğini, sabrını ve sevgisini hiçbir zaman eksik etmeyen kıymetli eşim Filiz'e ve tez çalışmalarım esnasında dünyaya gelen, çalışmalarımdan dolayı çok ihmal ettiğim kızım Begüm'e sonsuz teşekkürler...