T.C.
ERZİNCAN BİNALİ YILDIRIM ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS

ELİPTİK EĞRİLERİN ŞİFRELEMEDE KULLANIMI

Bülent IŞIKLI

Danışman: Dr. Öğr. Üyesi İsrafil OKUMUŞ

Matematik
ANABİLİM DALI

ERZİNCAN
2022

ÖZET

Yüksek Lisans Tezi

ELİPTİK EĞRİLERİN ŞİFRELEMEDE KULLANIMI

Bülent IŞIKLI

Erzincan Binali Yıldırım Üniversitesi
Fen Bilimleri Enstitüsü
Matematik Anabilim Dalı

Danışman: Dr. Öğr. Üyesi İsrafil OKUMUŞ

Eliptik eğri şifreleme algoritması, 1984 yılında Taher ElGammal tarafından ileri sürülen ElGammal şifreleme algoritmasına benzer bir yöntem ile 1985 yılında birbirlerinden bağımsız olarak Miller ve Koblitz tarafından eliptik eğriler üzerinde tanımlanan nokta toplama işlemi kullanılarak asimetrik şifreleme algoritması olarak ileri sürülmüştür. Algoritma, 1978 yılında Rivest, Shamir ve Adleman tarafından ileri sürülen ilk asimetrik şifreleme algoritması olan RSA'ya göre daha kısa anahtar ile eşdeğer güvenlik düzeyi sunduğu için günümüzde yaygın olarak kripto para sistemlerinde kullanıcıların hesap adreslerini oluşturmada da kullanılmaktadır. Bu çalışmada ilk olarak eliptik eğriler ve bu eğriler üzerinde oluşturulan şifreleme algoritmasının cebirsel temeline yer verilmiş, daha sonra eliptik eğri şifreleme algoritması ve eliptik eğri çarpanlara ayırma algoritması anlatılmıştır.

2022, 67 Sayfa

Anahtar Kelimeler: Eliptik eğriler, Eliptik eğri şifreleme, Kriptoloji

ABSTRACT

MSc Thesis

THE USE OF ELLIPTIC CURVES IN ENCRYPTION

Bülent IŞIKLI

Erzincan Binali Yıldırım University
Graduate School of Natural and Applied Sciences
Department of Mathematics

Supervisor: Dr. Öğr. Üyesi İsrafil OKUMUŞ

The elliptic curve encryption algorithm was proposed as an asymmetric encryption algorithm using the point addition process defined on elliptic curves by Miller and Koblitz independently in 1985, with a method similar to the ElGammal encryption algorithm proposed by Taher ElGammal in 1984. Since the algorithm offers the equivalent security level with a shorter key than RSA, which is the first asymmetric encryption algorithm proposed by Rivest, Shamir and Adleman in 1978, it is widely used today in creating the account addresses of users in crypto money systems. In this study, firstly, elliptic curves and the algebraic basis of the encryption algorithm created on these curves are given, then the elliptic curve encryption algorithm and elliptic curve factorization algorithm are explained.

2022, 67 Pages

Keywords: Elliptic curves, Elliptic curve encryption, Cryptology.

TEŞEKKÜR

Yüksek Lisans eğitimim boyunca ve bu tezin hazırlanmasının her sürecinde desteğini hiçbir zaman esirgemeyen, bilgi ve tecrübelerinden faydalandığım danışmanım Sayın Dr. Öğr. Üyesi İsrafil OKUMUŞ hocama teşekkürlerimi sunarım.

Çalışmalarım boyunca benden güvenini, desteğini ve sevgisini esirgemeyen aileme en içten dileklerimle teşekkürlerimi sunarım.

Bülent IŞIKLI
Ocak, 2022

İÇİNDEKİLER

Sayfa

ŞEKİLLER LİSTESİ

Sayfa

TABLOLAR LİSTESİ

Sayfa

SİMGELER ve KISALTMALAR

Simgeler

Z	Tam sayılar kümesi
Q	Rasyonel sayılar kümesi
R	Reel sayılar kümesi
nZ	$nk, k \in Z$
Z_n	$a \in Z: 0 < a < n$

Kısaltmalar

AES	Advanced Encypto System
ALP	Ayrık Logaritma Problemi
DES	Data Encrypto System
ECC	Elliptic Curve Cryptography
GCHQ	Birleşik Krallık Haber Alma Teşkilatı
NSA	National Security Agency
RSA	Rivest Shamir Adelman
YÖK	Yüksek Öğretim Kurumu

1. GİRİŞ

Gizli haberleşme ve güvenli iletişim tarihten günümüze kadar çok önemli olmuştur ve günümüzde elektronik haberleşme, elektronik imza, dijital para, kripto para ve bankacılık işlemleri gibi birçok alanda kullanılmaktadır. Elektronik ortamdaki veriler haberleşme ağı üzerinden gönderilirken, verilerin gönderici tarafından şifrelenmesi verinin tehditlere karşı korunması için gereklidir. Bilginin saklanması, korunması veya güvenli bir şekilde iletilmesi gereksinimden dolayı şifreleme anlamına gelen kriptoloji bilim dalı ortaya çıkmıştır.

Gizlilik bilimi anlamına gelen kriptoloji kelimesi Yunanca "gizli" anlamına gelen "kript" ve "bilim" anlamına gelen "loji" kelimelerinden üretilmiştir. Kriptoloji temel olarak Kriptografi ve Kriptanaliz olmak üzere iki bölüme ayrılır. Kriptografi şifreleme algoritmalarının geliştirildiği, Kriptanaliz ise şifreleme sistemlerinin açıklarının araştırıldığı ve bu sistemlerini kırılmasında kullanılan algoritmaların geliştirildiği bilim dallarıdır.

Sanayi devrimine kadar ilkel yöntemlerle oluşturulan şifreleme teknikleri kullanılırken, sanayi devriminden sonra kırılamayacak modern şifreleme sistemlerinin geliştirmesi çabalarıyla devam etmiştir. 20.yy içinde I.ve II. Dünya savaşlarında diplomasi ve askeri haberleşmede kullanılan gizli haberleşme bu savaşların kaderinde büyük rol oynamıştır.

Modern şifreleme yöntemlerinde güvenlik anahtar olarak adlandırılan sayılarla sağlanmaktadır. Bu algoritmalar kullandıkları anahtar biçimine göre simetrik şifreleme (tek anahtarlı) ve asimetrik şifreleme (çift anahtarlı) olmak üzere iki farklı biçimde ele alınır.

Verileri gizlemek için yapılan şifrelemelerin ilki M.Ö 1500 yılında Mezopotamyalı ustaların çömlek tariflerini gizlemek amaçlı ürettikleri metinlerde görülür. Gizli mesajı iletmek için yapılan ilk şifreleme çalışmalarından biri M.Ö 5-7 yüzyıllarda Spartalılar tarafından kullanılan Scytale adı verilen silindir görünümlü araçtır. Kripto tarihçisi David Kahn'a göre ilk kriptografik belge M.Ö 1900'lere dayanan bir lordun hayatını anlatan bir hiyegroliftir. En basit ve en bilinen şifreleme tekniklerinden biri olan Sezar şifreleme Roma imparatoru Julius Ceasar tarafından oluşturulan alfabetik harf kaydırma tekniğine dayananır. Harf kaydırmayı belirlenen bir anahtarın harflerine göre Sezar şifrelemeye

dayalı olarak yapan Vigenere şifrelemesi ise şimetrik şifrelemenin ilk örneği olarak düşünülebilir.

Simetrik anahtarlı şifreleme algoritmalarında verinin şifrelenmesi ve çözümlenmesinde gizli anahtar olarak adlandırılan tek bir anahtar kullanılır ve genellikle verilerin şifrelenmesinde tercih edilir. Bu sistemin haberleşmede kullanılmasında gönderici ve alıcı gizli anahtarları paylaşmalıdır yani anahtarın farklı bir şekilde alıcıya ulaştırılması gerekir bu nedenle anahtar dağıtım problemi vardır. İlk pratik algoritma 1974 yılında IBM tarafından sunulan LUCİFER algoritmasıdır. 1977 yılında bu algoritma üzerinde NSA tarafından yapılan bazı değişiklikler ile DES algoritması geliştirilmiştir. Sonraki yıllarda sırası ile 1987'de Rivest tarafından RC2, 1993'de NSA tarafından AES ve yine 1998'de Rivest tarafından RC6 algoritmaları geliştirilmiştir.

1976 yılında Diffie ve Hellman simetrik şifreleme sistemleri için güvenli bir anahtar değişim algoritması geliştirmişlerdir. Bu yöntem Diffie-Helman anahtar değişim yöntemi olarak adlandırılır.

Asimetrik anahtarlı şifreleme algoritmalarında ise şifreleme ve şifre çözümleme için kullanılan anahtarlar birbirinden farklıdır. Şifreleme işleminde genel anahtar, şifre açma işleminde özel anahtar kullanılarak hedeflenen gizlilik sağlanır.

1978 yılında Rivers, Shamir ve Adleman tarafından yazarların baş harfleri kullanılarak RSA olarak adlandırılan güvenliği tam sayıların çarpanlara ayrılması zorluğuna dayanan ilk pratik asimetrik şifreleme ve elektronik imza algoritması yayınlanmıştır. Büyük sayıların çarpanlarına ayrılmasının zorluğuna karşılık henüz etkin bir yöntem bulunmuş değildir. 1998 yılında Birleşik Krallık haber alma teşkilatı GCHQ'da çalışan İngiliz matematikçi Clifford Cocks'un 1973'te kurum içi bir dokümanda RSA'a eşdeğer bir sistem önerdiği ortaya çıkmıştır. (Riverst vd., 1978)

1984 yılında Lenstra eliptik eğrileri kullanarak tam sayıların çarpanlarını bulmak için Eliptik Eğri Çarpanlara Ayırma Algoritmasını geliştirmiştir (Lenstra, 1987).

1985 yılında Taher ElGammal güvenliği ayrık logaritma problemine dayanan diğer bir pratik asimetrik kripto sistemini geliştirmiştir (ElGammal, 1985).

1985 yılında Neal Koblitz ve Victor S. Miller birbirlerinden bağımsız olarak Ayrık Logaritma Problemini (ALP) sonlu cisimler üzerinde tanımlı eliptik eğrilerde kullanarak Eliptik Eğri şifreleme algoritmasını önermişlerdir (Koblitz vd., 1994).

Yüksek Öğretim Kurumunun (YÖK) Ulusal Tez Merkezi veri tabanında 28.01.2022 tarihli yapılan taramalar neticesinde, tez konusuyla ilgili olarak taratılan anahtar kelimelerle şu sonuçlara ulaşılmıştır. Aşağıdaki tablo 1.1'den de görüleceği üzere şifreleme bilimi Matematiğin yanı sıra Bilgisayar ve Elektronik alanlarında da önemli düzeyde uygulama alanı bulmuştur.

Tablo 1.1. Tez konusu ile ilgili yapılmış lisansüstü çalışmalar

	Matematik		**Bilgisayar Bilimleri**		**Elektrik-Elektronik Mühendisliği**	
Anahtar Kelime	**Yüksek Lisans**	**Doktora**	**Yüksek Lisans**	**Doktora**	**Yüksek Lisans**	**Doktora**
"RSA"	2	1	12	2	8	-
"Eliptik Eğri"(Elliptic Curve)	16	4	8	-	4	-
Kriptoloji-Şifreleme	32	3	97	17	47	5
Elektronik İmza(Digital Signature)	-	1	7	-	1	4
Dijital Para	-	-	6	-	-	
Toplam	**50**	**9**	**130**	**19**	**60**	**9**

Bu çalışmada eliptik eğri şifreleme algoritması ve algoritmada kullanılan matematiksel tanım ve teoremler konusunda bilgi verilmesi amaçlanmaktadır. Çalışma beş bölümden oluşmaktadır. Giriş bölümünden sonra sırası ile Kuramsal Temeller bölümünde temel tanımlar ve düzlemde eğriler, Materyal ve Yöntem bölümünde RSA ve ElGammal asimetrik şifreleme algoritmaları, Dördüncü bölümde ise eliptik eğrilerin cebirsel yapısı,

araştırma konusu olan eliptik eğri şifreleme algoritması ve eliptik eğri çarpanlara ayırma algoritmasına yer verilmiştir.

2. KURAMSAL TEMELLER

2.1.Temel Kavramlar

Tanım 2.1: Birinci bileşeni a ve ikinci bileşeni b olan a ve b elemanlarının sıralı ikilisi (a, b) şeklinde gösterilir.

$$(a, b) = \{\{a\}, \{a, b\}\}$$

olarak tanımlanır (Taşcı, 2007).

Tanım 2.2: A ve B boş olmayan iki küme olmak üzere bu kümelerin Kartezyen çarpımı;

$$A \times B = \{(a, b): a \in A \; ve \; b \in B\}$$

olarak tanımlanır (Taşcı 2007).

Tanım 2.3: $A \neq \emptyset$ ve $B \neq \emptyset$ olmak üzere $A \times B$ nin her alt kümesine A'dan B'ye bir bağıntı denir (Taşcı, 2007).

Tanım 2.4: A ve B boş olmayan iki küme olsun. Aşağıdaki şartları sağlayan $f \subseteq A \times B$ bağıntısına A dan B ye bir dönüşüm denir.

- $\forall a \in A$ için $f(a) = b$ olacak şekilde $\exists b \in B$ vardır,
- $\forall a_1, a_2 \in A$ için $a_1 = a_2 \Rightarrow f(a_1) = f(a_2)$ dir.

Eğer $f: A \to B$ dönüşümünde $B = R$ ya da $B = C$ ise o zaman f ye bir fonksiyon denir (Taşcı, 2007).

Tanım 2.5: a ve b tamsayılar olsun. Eğer $b = a.c$ olacak şekilde bir c tamsayısı varsa a, b'yi böler denir ve $a|b$ seklinde gösterilir (Taşcı, 2007).

Tanım 2.6: a ve b sıfırdan farklı tam sayılar olmak üzere $c|a$ ve $c|b$ olacak şekilde bir $c > 0$ tamsayısı varsa c ye a ve b nin ortak böleni denir (Altındiş, 2010).

Tanım 2.7: Aşağıdaki özellikleri sağlayan pozitif d tamsayısına a ve b'nin en büyük ortak böleni denir ve $d = ebob(a, b) = (a, b)$ ile gösterilir (Taşcı, 2007).

(i) $d|a$ ve $d|b$ dir.

(ii) Her $c|a$ ve $c|b$ için herhangi $c|d$ dir.

Tanım 2.8: 1 ve kendisinden başka pozitif böleni olmayan 1'den büyük tam sayılara Asal sayı denir (Altındiş 2010).

Tanım 2.9: a, b iki tamsayı olmak üzere $(a, b) = 1$ ise a ve b ye aralarında asaldır denir (Altındiş, 2010).

Teorem 2.10: (Öklid Algoritması) a, b tam sayılar ve $a > 0$ olsun. Bölme algoritması art arda uygulanarak aşağıdaki eşitlikler elde edilir.

$$b = q_0 a + r_0,\ 0 \leq r_0 < a$$

$$a = q_1 r_0 + r_1,\ 0 \leq r_1 < r_0$$

$$r_0 = q_2 r_1 + r_2,\ 0 \leq r_2 < r_1$$

$$r_1 = q_3 r_2 + r_3,\ 0 \leq r_3 < r_2$$

$$\vdots$$

$$r_{n-1} = q_{n+1} r_n + r_{n+1},\ 0 \leq r_{n+1} < r_n$$

$r_{n+1} = 0$ olduğu için r_n değeri a ve b tamsayılarının en büyük ortak böleni olur yani $obeb(a, b) = r_n$ dir. Bu algoritmadaki işlemler sonsuza kadar gitmez, çünkü 0 ile a tamsayısı arasında sonlu sayıda tamsayı vardır (Asar vd ., 2009).

Tanım 2.11: (**Euler Ø Fonksiyonu)** $n \in N$ olmak üzere n den küçük ve n ile aralarında asal olan pozitif tam sayıların sayısına Eulerin Ø fonksiyonu denir ve $Ø(n)$ ile gösterilir (Taşcı, 2007).

Teorem 2.12: $a, b \in$Z olmak üzere $obeb(a, b) = 1$ ise $Ø(a.b) = Ø(a).Ø(b)$ dir (Taşcı, 2007).

Tanım 2.13: a ve b tamsayılar ve $m > 0$ olsun. Eğer $m|a - b$ ise a tamsayısı b tamsayısına m modülüne göre kongrüenttir (denktir) denir ve $a \equiv b(mod\ m)$ şeklinde gösterilir (Asar vd., 2009).

Tanım 2.14: $a, b, m \in Z, m > 0$ olmak üzere

$$ax + c \equiv 0 \ (mod\ m) \tag{2.1}$$

Biçimindeki kongrüansa lineer veya birinci dereceden kongrüans denir ve $-c = b$ yazılırsa (2.1) denkleminin $ax \equiv b \ (mod\ m)$ şekline dönüşeceği açıktır (Nasibov, 2010).

Teorem 2.15: $a, b, m \in Z, m > 0$ ve $(a, m) = d$ olsun. Eğer $d \nmid m$ ise

$$ax \equiv b \ (mod\ m)$$

kongrüansı çözümsüzdür. Eğer $d|b$ ise bu kongrüans d farklı çözüme sahiptir (Asar vd 2009).

Teorem 2.16: $a, b, m \in$ Z, $m > 0$ ve $(a, m) = 1$ ise

$$ax \equiv b \ (mod\ m)$$

Kongrüansının tek çözümü vardır (Asar vd., 2009)**.**

Tanım 2.17: $a.b \equiv 1 \ (mod\ n)$ denkliğini sağlayan b sayısına a'nın n modülüne göre aritmetik tersi denir (Taşcı, 2010).

Tanım 2.18: m modülüne göre kalan sınıfların kümesi Z_m ile gösterilir. $\{0,1,2,3, \dots, m-1\}$ tam sayılarına m modülüne göre en küçük kalanlar sistemi adı verilir (Altındiş, 2005).

Tanım 2.19: $S = \{c_1, c_2, \dots, c_m\}$ birbirinden farklı m tane tam sayı olsun, Bu m tane tam sayıdan herhangi iki tanesi m modülüne göre birbirine kongruent değil yani $\forall i \neq j$ için $c_i \not\equiv c_j$ (mod m) ise S'ye m modülüne göre bir tam/komple kalan sistemi denir (Asar vd., 2009).

Tanım 2.20: Komple kalanlar içinde m yi geçmeyen ve m ile aralarında asal olan kalanlara indirgenmiş kalanlar denir ve indirgenmiş kalanların sayısı $\phi(m)$ tanedir (Altındiş, 2005).

Teorem 2.21: $a_1, a_2, \dots, a_{\phi(m)}$ sayıları m modülüne göre indirgenmiş kalanlar ve $(k, m) = 1$ ise $ka_1, ka_2, \dots ka_{\phi(m)}$ de indirgenmiş kalanlardır (Altındiş, 2005).

Teorem 2.22: (Euler Teoremi): $n > 1$ ve $obeb(a, n) = 1$ ise

$$a^{\emptyset(n)} \equiv 1 \ (\ mod\ n\ )$$

dir (Altındiş, 2005).

Teorem 2.23: (Fermat Teoremi): p asal ve $p \nmid a$ olmak üzere

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

dir (Altındiş, 2005).

Tanım 2.24: $(a, m) = 1$ olsun. Eğer $x^2 \equiv a\ (\ mod\ m)$ kongrüansının çözümü varsa a'ya m modülüne göre bir karesel kalan (Kuadraik Rezidü), eğer çözüm yoksa a'ya m modülüne göre karesel kalan değil (kuadratik non-rezidü) denir (Asar, 2012).

Teorem 2.25: p bir tek asal sayı, $a \in Z$ ve $(a, p) = 1$ olmak üzere;

1) $a^{\frac{p-1}{2}} \equiv 1\ (mod\ p)$ ise a, p modülüne göre bir kuadratik rezidü
2) $a^{\frac{p-1}{2}} \equiv p - 1\ (mod\ p)$ ise a, p modülüne göre bir kuadratik non-rezidüdür (Asar, 2012).

Tanım 2.26: A boştan farklı bir küme olmak üzere

$$*: A \times A \to A$$

dönüşümüne A da bir ikili işlem denir (Taşçı, 2007).

Tanım 2.27: Eğer $*$, A üzerinde bir ikili işlem ise $(A,*)$ ifadesine A'da bir cebirsel yapı denir (Taşçı, 2007).

Tanım 2.28: G boş olmayan bir küme ve bu küme üzerinde bir ikili işlem $*$ olsun. Buna göre eğer aşağıdaki şartlar sağlanırsa $(G,*)$ cebirsel yapısına bir grup denir (Taşçı, 2007).

- Her $a, b, c \in G$ için $a * (b * c) = (a * b) * c$
- Her $a \in G$ için $a * e = e * a = a$ olacak şekilde $e \in G$ vardır.
- Her $a \in G$ için $a * a' = a' * a = e$ olacak şekilde $a' \in G$ vardır.

Tanım 2.29: G bir grup olmak üzere $\forall a, b \in G$ için

$$a * b = b * a$$

oluyorsa o zaman bu gruba değişmeli (abelyan) grup denir (Taşçı, 2007).

Tanım2.30: $(G.*)$ bir grup olsun. Eğer G kümesi sonlu sayıda elemanlı sonlu grup, sonlu değilse sonsuz grup denir. Sonlu grubun eleman sayısına grubun mertebesi denir. $o(G)$ ya da $|G|$ ile gösterilir (Taşçı, 2007).

Tanım 2.31: $(G,*)$ bir grup, $a \in G$ ve e G nin birim(etkisiz) elemanı ve m,$n \in Z^+ \cup \{0\}$ için $a^n = \underbrace{a * a * ... * a}_{n\ tane}$ şeklinde tanımlanır. Şayet "*" işlemi bilinen çarpma işlemi ise $a^n = \underbrace{a.a.....a}_{n\ tane}$ olup ve $(G,.)$ ye çarpımsal grup denir (Taşçı, 2007).

Tanım 2.32: $(G,*)$ bir grup ve H, G'nın boş olmayan bir alt kümesi olsun. Eğer H, G grubundaki işleme göre bir grup teşkil ederse $(H,*)'$ a $(G,*)$ grubunun bir *alt grubu* denir ve "$H \leq G$" şeklinde gösterilir (Taşçı, 2007).

Teorem 2.33:(Lagrage) G sonlu bir grup ve $H \leq G$ ise o taktirde H' ın mertebesi G' nin mertebesini böler. $o(H)|o(G)$ şeklinde gösterilir (Taşçı, 2007).

Tanım 2.34: G bir grup, $a \in G$ olmak üzere $< a >= \{a^n : n \in Z\}$ alt grubuna G'nin a elemanı tarafından üretilen devirli alt grubu, a elemanına G'nin üreteci denir ve $< a > = G$ şeklinde gösterilir (Taşçı 2007).

Tanım 2.35: G sonlu bir grup ve $g \in G$ olmak üzere $g^n = e$ olacak şekilde $n \in Z^+$ tam sayısı varsa a elemanına sonlu mertebedendir denir. $g \in G$ sonlu mertebeden olmak üzere $g^n = e$ olacak şekildeki en küçük pozitif n tam sayısına g nın mertebesi denir. $o(g)$ ya da $|g|$ ile gösterilir (Taşçı, 2007).

Teorem 2.36: Sonlu bir grupta elemanın mertebesi grubun mertebesini böler (Taşcı, 2007).

Tanım 2.37: Boştan farklı bir R kümesi üzerinde toplama $(+)$ ve çarpma $(\cdot)$ denilen iki ikili işlem tanımlanmış olsun. Eğer aşağıdaki şartlar sağlanırsa o zaman $(R, +, \cdot)$ cebirsel yapısına bir halka denir. Halkalar *Ring* (Halka) kelimesinin baş harfi olan "R" ile sembolize edilirler.

i. $(R, +)$ değişmeli bir grup,
ii. $\forall\, a, b \in R$ için $ab \in R$,

iii. $\forall\, a,b,c \in R$ için $(ab)c = a(bc)$,

iv. $\forall\, a,b,c \in R$ için $a(b+c) = ab + ac$, $(b+c)a = ba + ca$

Bir R halkasının toplamsal birimi 0_R ile gösterilir ve buna halkanın sıfırı denir (Asar vd., 2009).

Tanım 2.38: Her $a \in R$ için $a.1 = 1.a = a$ olacak şekilde $1 \in R$ varsa bu elemana halkanın birim elemanı (birimi) denir, bu eleman 1_R ile gösterilir ve halkaya da birimli halka denir (Asar vd., 2009).

Tanım 2.39: R halkası çarpma işlemine değişmeli ise yani her $a, b \in R$ için $ab = ba$ oluyorsa halkaya değişmeli halka denir (Asar vd., 2009).

Tanım 2.40: R bir halka olmak üzere her $r \in R$ için $n.r = 0_R$ olacak şekilde bir n pozitif tamsayısı varsa bu sayıların en küçüğüne halkanın karakteristiği denir. Eğer böyle bir pozitif tamsayı yoksa yani her $r \in R$ için $n.r = 0$ olması $n = 0$ olmasını gerektiriyorsa o zaman R halkasının karakteristiği 0 olarak tanımlanır. R nin karakteristiği kısaca $char\ (R)$ veya $kar\ (R)$ ile gösterilir (Asar vd., 2009).

Örnek: m pozitif tam sayı ise $kar(Z_m) = m$ dir.

Tanım 2.41: R birimli bir halka ve $0_R \neq a \in R$ olsun. Eğer $ab = ba = 1_R$ olacak şekilde $b \in R$ varsa b ye a nın tersi ve a'ya birimsel (tersinir) eleman denir (Asar vd., 2009).

Tanım 2.42: Sıfırdan farklı her elemanı tersinir olan birimli ve değişmeli halkaya cisim (*Field)* denir (Asar vd., 2009).

Tanım 2.43: Sonlu sayıda elemana sahip cisimlere sonlu cisim denir (Asar, 2009).

Örnek: p asal sayı olmak üzere Z_p cisimdir ve $kar(Z_p) = p$ dir.

Tanım 2.44: R bir halka ve $a, b \in R$ olsun. Eğer $a, b \neq 0_R$ iken $ab = 0_R$ ise a ya sol sıfır böleni ve b ye sağ *sıfır böleni* denir (Asar vd., 2009) .

Tanım 2.45: Birimli ve değişmeli ve sıfır bölensiz bir halkaya *Tamlık Bölgesi* (*Domain)* denir (Taşçı, 2007).

Tanım 2.46: R birimli ve değişmeli halka ve x bir bilinmeyen olsun. Buna göre $n \geq 0$ olacak şekilde bir tamsayı ve $a_0, a_1, a_2, \dots, a_n \in R$ olmak üzere

$$a_0x^0 + a_1x^1 + a_2x^2 + \cdots + a_nx^n$$

şeklinde ki bir ifadeye katsayıları R'de olan x bilinmeyenine bağlı bir polinom denir. Burada a_ix^i lere polinomun terimleri ve a_ix^i terimlerindeki a_i'ye x^i nin katsayısı denir.

R halkası üzerindeki x'e bağlı bütün polinomların kümesini $R[x]$ ile gösterilir. Polinomlar genel olarak $f(x)$ sembolü ile gösterilirken buradaki $f(x)$ bir fonksiyon ya da fonksiyon değeri belirtmez. Ayrıca

$$f(x) = a_0x^0 + a_1x^1 + a_2x^2 + \cdots + a_nx^n$$

polinomu kısaca

$$f(x) = \sum_{i=0}^{n} a_ix^i$$

şeklinde de gösterilir (Taşcı, 2007).

Tanım 2.47: $f(x) \in R[x]$ katsayıları R reel sayılar cismi üzerinde olan

$$f(x) = \sum_{i=0}^{n} a_ix^i$$

polinomunda $a_m \neq 0_R$ olsun. a_n ye baş katsayı ve $a_m = 1_R$ ise $f(x)$ e monik polinom denir (Asar, 2009).

Tanım 2.48: D bir tamlık bölgesi $f(x) \in D[x]$ ve $c \in D$ olsun. Eğer $f(c) = 0_D$ ise c ye $f(x)$ polinomunun bir kökü ya da sıfırı ya da $f(x) = 0_D$ cebirsel denkleminin bir kökü ya da bir çözümü denir (Asar vd., 2009).

Teorem 2.49: $f(x) \in F[x]$, n pozitif tamsayı olmak üzere $der\big(f(x)\big) = n$ ve başkatsayısı a olan herhangi bir polinom olsun. Buna göre $x_1, x_2, \dots, x_n$ $f(x)$'in F 'deki n tane farklı kökü ise o zaman $f(x) = a(x - x_1)(x - x_2) \dots (x - x_n)$ dir (Taşçı, 2007).

Örnek: $f(x) = a_3x^3 + a_2x^2 + a_1x + a_0$ $Q[x]$ da bir polinom olsun. $f(x) = 0$ denkleminin kökleri x_1, x_2, x_3 olmak üzere;

$$f(x) = a_3(x - x_1)(x - x_2)(x - x_3) \tag{2.2}$$

olarak yazılabilir, gerekli işlemler yapıldığında

$$f(x) = a_3[x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_1x_3 + x_2x_3)x - x_1x_2x_3] \tag{2.3}$$

elde edilir. (2.3) den katsayılar ve kökler arasındaki ilişkiler

$$x_1 + x_2 + x_3 = -\frac{a_2}{a_3} \tag{2.4}$$

$$x_1x_2 + x_1x_3 + x_2x_3 = \frac{a_1}{a_3} \tag{2.5}$$

$$x_1x_2x_3 = -\frac{a_0}{a_3} \tag{2.6}$$

olarak yazılır.

Tanım 2.50: $f(x) \in F(x)$ n. Dereceden monik bir polinom ve $f(x) = 0$ denkleminin $F(x)$ üzerindeki kökleri x_i olsun, yani

$$f(x) = \prod_{i=1}^{n}(x - x_i)$$

Olsun. Bu durumda f polinomunun diskriminantı

$$\Delta(\boldsymbol{f}) = \prod_{\boldsymbol{i<j}}\left(\boldsymbol{x_i} - \boldsymbol{x_j}\right)^{\boldsymbol{2}}$$

Şeklinde tanımlanır (Fraleigh, 2002).

Örnek: $f(x) = ax^2 + \mathrm{b}x + \mathrm{c}\ Q[x]$ da bir polinom olsun. $f(x) = 0$ denkleminin kökleri x_1 ve x_2 olmak üzere bu denklemin diskriminantı;

$$\Delta = (x_1 - x_2)^2$$

olarak tanımlanır. Kökler ile diskriminant arasında aşağıdaki özellikler geçerlidir.

i. $x_1 \neq x_2 \in \mathrm{R}$ ise $\Delta > 0$
ii. $x_1 = x_2 \in \mathrm{R}$ ise $\Delta = 0$
iii. $x_1 = \overline{x_2} \in \mathrm{C}$ ise $\Delta < 0$

Örnek: $f(x) = a_3x^3 + a_2x^2 + a_1x + a_0\ Q[x]$ da bir polinom olsun. $f(x) = 0$ denkleminin kökleri x_1, x_2, x_3 olmak üzere bu denklemin diskriminantı

$$\Delta = (x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2 \tag{2.7}$$

olarak tanımlanır ve aşağıdaki özellikler geçerlidir.

- $\Delta = 0$ ise kübik polinomun katlı kökü vardır.
- $\Delta \neq 0$ ise kübik polinomun katlı kökü yoktur.

Tanım 2.51: $a, b \in Q$ olmak üzere $x^3 + ax + b = 0$ denkleminin kökleri x_1, x_2, x_3 olsun.

$$x^3 + ax + b = (x - x_1)(x - x_2)(x - x_3) = 0 \tag{2.8}$$

olarak yazılır.

(2.4), (2.5) ve (2.6) den

$$x_1 + x_2 + x_3 = 0 \tag{2.9}$$

$$x_1x_2 + x_1x_3 + x_2x_3 = a \tag{2.10}$$

$$x_1x_2x_3 = -b \tag{2.11}$$

yazabiliriz.

(2.9), (2.10) ve (2.11) eşitlikleri (2.7) de kullanılırsa (2.8) eşitliğinin diskriminantı

$$\Delta = -16(4a^3 + 27b^2)$$

olarak elde edilir (Rotman 2006).

Tanım 2.52: (Limit): $A \subset \mathrm{R}$, $f: A \to R$ bir fonksiyon, a da A kümesinin bir yığılma noktası olsun. Her $\varepsilon > 0$ için, eğer $0 < |x - a| < \delta$ olduğunda $|f(x) - L| < \varepsilon$ kalacak şekilde bir $\delta > 0$ sayısı bulunabiliyorsa x, a noktasına yaklaştığında f fonksiyonunun limiti L dir denir (Bayraktar, 2010).

Tanım 2.53: (Türev): $f: (a, b) \subseteq R \to R$ bir fonksiyon ve $x_0 \in (a, b)$ verilmiş olsun. Eğer

$$\lim_{x \to x_0} \frac{f(x) - f(x_0)}{x - x_0}$$

limiti mevcutsa, f fonksiyonu x_0 noktasında diferansiyellenebilir (türevlenebilir) denir. Bu limitin değeri $f'(x_0)$ veya $\frac{df}{dx}(x_0)$ ile gösterilir ve buna $f(x)$ fonksiyonunun x_0 noktasındaki türevi adı verilir.

$$f'(x_0) = \lim_{x \to x_0} \frac{f(x) - f(x_0)}{x - x_0}$$

ifadesinde $x = x_0 + h$ alınırsa

$$f'(x_0) = \lim_{h \to 0} \frac{f(x_0 + h) - f(x_0)}{h}$$

olarak elde edilir ve h yerine Δx alınırsa

$$f'(x_0) = \lim_{\Delta x \to 0} \frac{f(x_0 + \Delta x) - f(x_0)}{\Delta x}$$

yazılır (Bayraktar, 2010).

Tanım 2.54: (Kısmi Türev): $f: A \subset R^2 \to R$ $f(x, y)$ fonksiyonu $(x_0, y_0) \in A$ noktasında tanımlı olsun. Bu takdirde f nin (x_0, y_0) noktasındaki x e göre kısmi türevi

$$f_x(x_0, y_0) = \lim_{\Delta x \to 0} \frac{f(x_0 + \Delta x, y_0) - f(x_0, y_0)}{\Delta x}$$

ve y' ye göre kısmi türevi

$$f_y(x_0, y_0) = \lim_{\Delta y \to 0} \frac{f(x_0, y_0 + \Delta y) - f(x_0, y_0)}{\Delta y}$$

dir. Bu kısmi türevler genel olarak sırası ile $\frac{\partial f}{\partial x}\Big|_{(x_0, y_0)}$ ve $\frac{\partial f}{\partial y}\Big|_{(x_0, y_0)}$ şeklinde gösterilir.

$y = f(x)$ fonksiyonunun üzerindeki $P(x_0, y_0)$ noktasından çizilen teğetin denklemi bu doğrunun eğimi bulunarak elde edilir.

$P(x_0, y_0)$ için $Q(x_0, +\Delta x, y_0 + \Delta y)$ olsun. P ve Q noktasından geçen doğrunun eğimini

$$m_{PQ=} \frac{\Delta y}{\Delta x} = \frac{f(x_0 + \Delta x) - f(x_0)}{\Delta x}$$

olur. $\Delta x \to 0$ olması halinde P ve Q noktasından geçen doğrunun eğimi ile teğetin eğimi çakışır.

Bu durumda teğetin eğimi m_T ,

$$m_T = \lim_{\Delta x \to 0} \frac{\Delta \gamma}{\Delta x} = \lim_{\Delta x \to 0} \frac{f(x_0 + \Delta x) - f(x_0)}{\Delta x} = f'(x_0)$$

olur.

Bu durumda $y = f(x)$ fonksiyonun $x = x_0$ noktasındaki $f'(x_0)$ türevi, fonksiyonun belirttiği eğriye üzerindeki $(x_0, f(x_0))$ noktasından çizilen teğetin eğimini verir.

O halde $y = f(x)$ fonksiyonu ile verilen eğriye üzerindeki (x_0, y_0) noktasından çizilen teğetin denklemi

$$y - y_0 = f'(x_0)(x - x_0)$$

olarak yazılır (Bayraktar, 2010).

2.2. Vektör Uzayları ve Afin Uzay

Tanım 2.55: Başlangıç noktası A, bitim noktası B olan yönlü doğru parçası $\overrightarrow{AB}$ ile gösterilir. $\overrightarrow{AB}$ yönlü doğru parçasının boyu $[AB]$ doğru parçasının boyudur. Bu sayı $\left|\overrightarrow{AB}\right|$ ile gösterilir.

$\overrightarrow{AB}$ ile $\overrightarrow{CD}$ iki yönlü doğru parçası olsun. Eğer

- $\left|\overrightarrow{AB}\right| = \left|\overrightarrow{CD}\right|$
- $\overrightarrow{AB} \parallel \overrightarrow{CD}$
- $\overrightarrow{AB}$ ile $\overrightarrow{CD}$ aynı yönlü

ise $\overrightarrow{AB}$ ile $\overrightarrow{CD}$ eştir denir, $\overrightarrow{AB} \equiv \overrightarrow{CD}$ biçiminde gösterilir.

($\equiv$) bağıntısı, yönlü doğru parçalarını denklik sınıflarına ayırır. Bu denklik sınıflarının her birine düzlemde bir vektör adı verilir.

$u = (u_1, u_2, \dots, u_n)$ olmak üzere $u_1, u_2, \dots$ sayılarına u vektörünün bileşenleri denir (Balcı, 2012).

Tanım 2.56: $f: R^n \to R^m$ fonksiyonu verilmiş olsun. $m > 1$ ise f ye vektör değerli fonksiyon, $m = 1$ ise f ye skaler değerli fonksiyon denir.

Özel olarak f_i ler birer vektör olmak üzere

$$F: [a, b] \subset \mathrm{R} \to \mathrm{R}^n$$

$$F(t) = (f_1(t), f_2(t) \dots, f_n(t))$$

fonksiyonuna R^n de bir vektör değerli fonksiyon denir. f_i fonksiyonlarına ise F nin koordinat (bileşen) fonksiyonları denir (Bayraktar, 2010).

Tanım 2.57: (Vektör Değerli Fonksiyon için Türev): $F: [a, b] \to R^n$ vektör değerli bir fonksiyon ve $t_0 \epsilon [a, b]$ olsun. Her bir f_i bileşen fonksiyonu t_0 da türevlenebilir ise bu durumda F fonksiyonu da t_0 da türevlenebilirdir denir ve bu noktadaki türevi

$$F'(t_0) = (f_,'(t_0), f_2'(t_0), \dots, f_n'(t_0))$$

olur (Bayraktar, 2010).

Tanım 2.58: V bir vektör kümesi, F bir cisim, $u, v \in V$ vektörleri ve $\alpha \epsilon F$ skaler olmak üzere; $u = (u_1, u_2, \dots, u_n)$, $v = (v_1, v_2, \dots, v_n)$ için

$$(+): V \times V \to V$$

$$u + v = (u_1 + v_1, u_2 + v_2 \dots, u_n + v_n)$$

$$(.): F \times V \to V$$

$$\alpha . u = (\alpha . u_1, \alpha . u_2, \dots, \alpha . u_n)$$

biçiminde tanımlanır (Taşçı, 2007).

Tanım 2.59: V bir vektör kümesi, F bir cisim:

- $(V, +)$ değişmeli gruptur.
- $v \in V$ ve $\alpha \epsilon F$ için $\alpha v \epsilon V$
- Her $u, v \in V$ ve her $\alpha \epsilon F$ için $\alpha(u + v) = \alpha u + \alpha v$
- Her $v \in V$ ve her $\alpha, \beta \epsilon F$ için $(\alpha + \beta)v = \alpha v + \beta v$
- Her $v \in V$ ve her $\alpha, \beta \epsilon F$ için $(\alpha(\beta))v = \alpha \beta v$
- Her $v \in V$ için $1 . v = v$ olacak şekilde $1 \in V$ vardır.

şartları sağlanırsa V ye F cismi üzerinde bir vektör uzayı denir. $F = R$ cismi üzerindeki V vektör uzayını kısaca V ile gösterilir (Taşçı, 2007).

Tanım 2.60: A boş olmayan bir küme V de K cismi üzerinde $n -$ boyutlu bir vektör uzayı olsun. Aşağıdaki önermeleri doğrulayan bir

$$f: A \times A \to V$$

fonksiyonu varsa (A, V, f) sistemine (A *ya* V *birleştirilmiş*) bir afin uzay denir.

i. $\forall P, Q, R \in A$ için $f(P,Q) + f(Q,R) = f(P,R)$
ii. $\forall P \in A \ ve \ \in \vec{v} \in V$ için $f(P,Q) = \vec{v}$

olacak şekilde bir tek $Q \in A$ noktası vardır (Balcı, 2012).

Örnek: R^2, R cismi üzerinde bir vektör uzayı ve düzlemin noktalarının $A \times A$ kümesi olarak alalım.

$$f: A \times A \to R^2$$

$$(P,Q) \to f(P,Q) = (a,b)$$

şeklinde tanımlanan f fonksiyonu Tanım 2.60'daki (i) ve (ii) önermeleri sağladığından düzlem R^2 ile birleştirilmiş bir afin uzaydır.

Tanım 2.61: Bir reel afin uzayı A ve A ile birleşen vektör uzayıda $V = R^n$ olsun.

$$\begin{cases} x = (x_1, x_{2,\dots,} x_n) \\ y = (y_1, y_2, .., y_n) \end{cases}$$

olmak üzere V de bir iç çarpım işlemi olarak;

$$<,>: V \times V \to R$$

$$(x,y) \to \langle x, y \rangle = \sum_{i=1}^{n} x_i y_i$$

öklid iç çarpımı tanımlanır ve bu afin uzaya $n-$*boyutlu öklid uzay* denir. Genel olarak E^n olarak gösterilir. Öklid uzayındaki uzaklık ve metrik gibi kavramlar tanımlanabilir (Balcı,2012).

Örnek: R^2 öklid uzaydır. Reel düzlem olarak şimdiye kadar duyduğumuz düzlemi alalım. Bu düzlem 2-boyutlu reel standart vektör uzayı ile birleştirilmiş R^2 afin uzayıdır.

Ayrıca bu vektör uzayındaki öklid iç çarpımı da

$$\langle , \rangle : R^2 \times R^2 \to R$$

$$(x, y) \to \langle x, y \rangle = \sum_{i=1}^{2} x_i y_i$$

şeklinde tanımlandığından R^2 afin uzayı 2-boyutlu öklid uzayı olur ve E^2olarak gösterilen bu uzaya öklid düzlemi de denir.

2.3.Düzlemde Hareket

2.3.1. Eşmetrel dönüşümler

Eşmetrel dönüşümler, aralarındaki uzaklık aynı kalacak şekilde herhangi iki noktayı farklı iki noktaya gönderen dönüşümlerdir.

$$f : R^2 \to R^2$$

$$(x, y) \to (a_1 x + b_1 y + c_1, a_2 x + b_2 y + c_2)$$

Şeklinde tanımlanan dönüşüm uzaklığı koruyorsa bu dönüşüme eşmetrel dönüşüm denir (Mahir, 1999).

2.3.2. Düzlemde öteleme

Tanım 2.62: (Öteleme): XOY dik koordinat sisteminde, başlangıç noktası $\mathrm{O}'(h, k)$ ve eksenleri X ve Y eksenlerine paralel olan yeni bir $\mathrm{X}'\mathrm{O}'\mathrm{Y}'$ dik koordinat sistemi oluşturalım. XOY sistemindeki $P(x, y)$ noktasının $\mathrm{X}'\mathrm{O}'\mathrm{Y}'$ sistemindeki koordinatları $P'(x', y')$ olsun bu durumda P ile P' noktalarının koordinatları arasında

$$x = x' + h$$

$$y = y' + k$$

veya bunlara eşdeğer olan

$$x' = x - h$$

$$y' = y - k$$

bağıntıları vardır. Böylece öteleme,

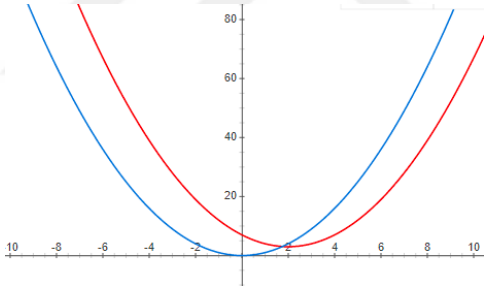
$$T_{(h,k)}: R^2 \to R^2$$

$$(x, y) \to (x', y') = (x - h, y - k)$$

Şeklinde bir eşmetrel dönüşümdür (Mahir, 1999).

- **Teorem 2.63:** Bir öteleme fonksiyonunda aşağıdaki özellikler invaryant (korunur/değişmez, sabit) kalır (Mahir, 1999).
- Uzunluklar
- Açılar
- Alanlar

Örnek: Düzlemde $y = (x - 2)^2 + 3$ parabolü için eksenler $h = 2$ birim sağa k=3 birim yukarı kaydırılırsa $y' = (x')^2$ elde edilir. Yani eksenler parabolün tepe noktasına kaydırılmış olur (Bkz.Şekil 2.1).



Şekil 2.1. Parabol ötelemesi

2.3.3. Düzlemde dönme

Tanım 2.64: (Dönme): XOY dik koordinat sisteminde X ve Y eksenleri O noktası etrafında pozitif yönde θ radyanlık açı yapacak şekilde döndürülürse aynı başlangıç noktasına sahip yeni bir $X'O'Y'$ dik koordinat sistemi elde edilir.

XOY sistemindeki $P(x, y)$ noktasının $X'O'Y'$ sistemindeki koordinatları $P'(x',y')$ olsun bu durumda P noktasının koordinatları ile P' noktasının koordinatları arasında

$$x = \quad x' \cos\theta - y' \sin\theta$$

$$y = \quad x' \sin\theta + y' \cos\theta$$

veya buna eşdeğer olan

$$x' = \quad x \cos\theta + y \sin\theta$$

$$y' = \quad -x \sin\theta + y \cos\theta$$

bağıntıları vardır. Bu bağıntılar matris formunda

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} cos\theta & sin\theta \\ -sin\theta & cos\theta \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix}$$

biçiminde yazılabilir (Mahir, 1999).

Teorem 2.65: Bir dönme işleminde aşağıdaki özellikler invaryant(değişmez) kalır.

- Doğrusallık
- Uzunluklar (Mahir, 1999).

Örnek: $xy = 1$ hiperbolünün bulunduğu düzlemde eksenler pozitif yönde $\theta = \frac{\pi}{4}$ döndürülürse eğrinin yeni koordinat sistemindeki denklemini bulalım

$$x = \quad x' \frac{1}{\sqrt{2}} - y' \frac{1}{\sqrt{2}}$$

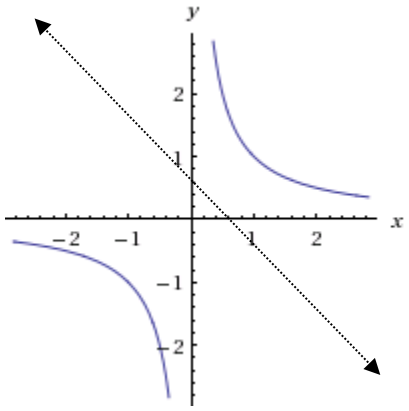
$$y = \quad x' \frac{1}{\sqrt{2}} + y' \frac{1}{\sqrt{2}}$$

Eşitlikleri verilen eğri denkleminde yazılırsa

$$\left(x' \frac{1}{\sqrt{2}} - y' \frac{1}{\sqrt{2}}\right)\left(x' \frac{1}{\sqrt{2}} + y' \frac{1}{\sqrt{2}}\right) = 1$$

$$(x')^2 - (y')^2 = 2$$

elde edilir. Yani hiperbol sabit tutularak eksenler döndürülmüş olur (Bkz.Şekil 2.2).



Şekil 2.2. $xy = 1$ hiperbolünün grafiği

2.3.4. Afin dönüşümler

Genel olarak bir noktayı bir noktaya dönüştüren dönüşümlere afin dönüşüm adı verilir. Düzlemde afin dönüşümler

$$T: R^2 \to R^2$$

$$T(x', y') = (a_1x + b_1y + c_1, a_2x + b_2y + c_2)$$

olarak tanımlanır. Bu dönüşüm matris formunda,

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} a_1 & b_1 \\ a_2 & b_2 \end{bmatrix} . \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} c_1 \\ c_2 \end{bmatrix}$$

şeklinde yazılabilir. Bu dönüşümün bir noktayı tek bir noktaya dönüştürmesi için

$$\Delta = \begin{bmatrix} a_1 & b_1 \\ a_2 & b_2 \end{bmatrix} \neq 0$$

Olmalıdır.

Afin dönüşümler bazı özel durumlar hariç, genel olarak, uzunlukları, alanları ve açıları invaryant bırakmazlar (Mahir, 1999).

2.4. Düzlemde Homojen Koordinatlar

Düzlemde bir dik koordinat sistemi belirlendiğinde düzlem ile R^2 birebir eşlenebilir. Düzlemin bir P noktasına karşılık gelen (x, y) ikilisini vermek bu P noktasını

göstermenin bir yoludur. Ayrıca düzlemin noktalarını reel sayı üçlüleriyle gösterecek biçimde bir eşleme de şu şekilde kurulabilir.

$$u = (u_1, u_2, u_3) \text{ ve } v = (v_1, v_2, v_3)$$

R^3 uzayında iki nokta olmak üzere;

$$u\beta v \Leftrightarrow u = kv, \qquad 0 \neq k \in R$$

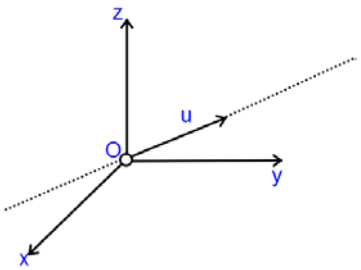
biçiminde tanımlanmış β bağıntısını göz önüne alalım. Bu bağıntının bir denklik bağıntısıdır. u'nun denklik sınıfı

$$[u]_\beta = \{u, v \in R^3 : v\beta u\} = \{u, v \in R^3 : 0 \neq k \in R \; v = ku\}$$

dır. Geometrik olarak;

i. $u = 0$ ise $[u]_\beta = \{0\}$ dır.

$u \neq 0$ ise $[u]_\beta$ kümesi başlangıçtan geçen ve $\vec{u}$ vektörüne paralel olan doğrudan başlangıç noktası çıkarılarak elde edilen kümedir(Bkz. Şekil 2.3).



Şekil 2.3. $[\boldsymbol{u}]_{\boldsymbol{\beta}}$ kümesinin görüntüsü.

β bağıntısına göre elde edilen denklik sınıflarının kümesi $R^3_{/\beta}$ olsun, bu durumda

$$\varphi : R^2 \to R^3_{/\beta}$$

Fonksiyonunu

$$\varphi(x, y) = [(x, y, 1)]_\beta = \{(X, Y, Z) = (xk, yk, k) : 0 \neq k \in R\}$$

Şeklinde tanımlansın.

- φ dönüşümü bire-birdir.

$$\varphi\,(x', y')\; =\; \varphi\,(x, y)\;\Rightarrow\;(x', y') = (x, y)$$

- φ dönüşümü örten değildir.

$Z = 0$ ise $[(X, Y, 0)]_\beta$'nin φ dönüşümünde ters görüntüsü yoktur.

$Z \neq 0$ ise $[(X, Y, Z)]_\beta$'nin φ dönüşümünde ters görüntüsü vardır.

$(\frac{X}{Z}, \frac{Y}{Z}) \in R^2$ ve $\left(\frac{X}{Z}, \frac{Y}{Z}, 1\right) \approx (X, Y, Z)$ olduğundan $\varphi\left(\frac{X}{Z}, \frac{Y}{Z}\right) = \left[\left(\frac{X}{Z}, \frac{Y}{Z}, 1\right)\right]_\beta = [(X, Y, Z)]_\beta$ dır.

Ayrıca düzlemin her $A(x, y)$ noktasının φ dönüşümündeki görüntüsü üçüncü bileşeni sıfır olmayan bir üçlünün denklik sınıfındadır. Sonuç olarak düzlem ile $R^3_{/\beta}$ kümesinin $Z \neq 0$ olacak biçimdeki $H(X, Y, Z)$ elemanlarının kümesi birebir eşlenir (Sabuncuoğlu, 2012).

Tanım 2.66: $R^3_{/\beta}$ kümesinde, $Z \neq 0$ olacak biçimdeki (X, Y, Z) elemanlarının kümesini P ile gösterelim. Düzlemdeki (x, y) noktasına P kümesinde karşılık gelen $[(X, Y, Z)]_\beta$ denklik sınıfındaki her bir (X, Y, Z) üçlüsü için X, Y ve Z sayılarına (x, y) noktasının **homojen koordinatları** denir.

Bu tanıma göre $H(X, Y, Z)$ sayıları $A(x, y)$ noktasının homojen koordinatları ise

$$(X, Y, Z) \approx (x, y, 1)$$

dır. Buna göre, $0 \neq k \in R$ için $(X, Y, Z) = k(x, y, 1)$ dır. Daha açık olarak

$$X\; = kx\;\;, Y\; = ky\;\;, Z = k\;\text{ veya}\;\frac{X}{Z} = x, \frac{Y}{Z} = y$$

dir.

$(X, Y, Z) \approx (x, y, 1)$ olacak biçimdeki her (X, Y, Z) üçlüsü, (x, y) noktasının homojen koordinatlarının üçlüsü olduğundan (x, y) noktasının homojen koordinatları tek değildir.

$Z = 0$ ise $(X, Y, Z) \approx (x, y, 1)$ olamayacağından düzlemdeki her noktanın Z homojen koordinatı sıfırdan farklı olmak zorundadır (Sabuncuoğlu, 2012).

Örnek: R^2 deki $A(5,3)$ noktasının $R^3_{/\beta}$ kümesindeki noktası

$$\varphi(5,3) = [(5,3,1)]_\beta$$

Olup $k \neq 0$ olmak üzere;

$$[(5,3,1)]_\beta = (5k, 3k, k)$$

dır. Bu durumda A noktasının homojen koordinatı

$$A(5,3) = H(5k, 3k, k), \qquad k \neq 0$$

şeklinde yazılabilir.

Örnek: Homojen koordinatları $H(10,6,2)$ olan noktanın Afin koordinatı

$$\frac{10}{2} = 5, \qquad \frac{6}{2} = 3$$

olduğundan $H(10,6,2) = A(5,3)$ noktasıdır.

Özet olarak;

- $A(x, y)$ noktasının homojen koordinatı $H(xk, yk, k), k \neq 0$ dır.
- $A(0,0)$ noktasının homojen koordinatı $Z \neq 0$ olmak üzere, $H(0,0, Z)$ dir.
- $Z \neq 0$ için $H(X, Y, Z)$ noktasının Afin koordinatı $A(\frac{X}{Z}, \frac{Y}{Z})$ dir.
- $Z \to 0$ için $H(X, Y, Z)$ noktasının Afin koordinatı $A(\infty, \infty)$ dir.

2.4.1. Doğruların sonsuzdaki noktası

$(a, b) \neq (0,0)$ olmak üzere Düzlemdeki her bir doğrunun denklemi

$$ax + by + c = 0 \tag{2.12}$$

biçiminde olup bu denkleminde (x, y) yerine homojen koordinatları yazılırsa

$$a\frac{X}{Z} + b\frac{Y}{Z} + c = 0$$

denklemi bulunur.

$Z \neq 0$ için bu denklem

$$aX + bY + cZ = 0 \tag{2.13}$$

denklemine denk olup $ax + by + c = 0$ doğrusu $(b, -a)$ vektörüne paralel bir doğrudur.

$ax + by = 0$ doğrusunu göz önüne alalım. Bu doğru üzerinde bir $(x, y) = (b, -a, Z)$ noktasının, Z homojen koordinatını sıfıra yaklaştıralım. Bu durumda (x, y) noktası bu doğru üstünde kalarak gittikçe uzaklaşır ve bu nokta Z ne olursa olsun $ax + by = 0$ doğrusunun üstündedir. $Z \to 0$ için $(b, -a, Z)$ noktası $ax + by = 0$ doğrusunun üstünde kalarak uzaklaşır. Bundan dolayı $Z \to 0$ için homojen koordinatları $(b, -a, 0)$ olan bir noktanın varlığını benimseyip bu noktaya $ax + by = 0$ doğrusunun "sonsuz noktası" denir.

Homojen koordinatları $(b, -a, Z)$ olan nokta (2.12) doğrusunun da üstünde midir?

(2.12) doğrusunun homojen koordinatlardaki denklemi (2.13) dir. $(b, -a, 0)$ noktasının bu denklemi sağlar. Bundan dolayı $(b, -a, 0)$ ideal noktasının da (2.13) doğrusunun üstünde kaldığını söyleyebiliriz. Sonuç olarak düzlemde , $(b, -a)$ vektörüne paralel olan doğruların tümü ideal nokta adı verilen $(b, -a, 0)$ noktasında kesişirler. $(b, -a, 0)$ noktası (2.13) ve $Z = 0$ önermesini sağlayan biricik noktadır. Buna göre (2.13) doğrusunun sonsuz da bir ve yalnız bir noktası vardır. (Sabuncuoğlu, 2012)

Düzlemdeki her doğrunun ideal noktasını düzleme katarak elde edilen kümeye "*genişletilmiş düzlem***"** adı verilir. Genişletilmiş düzlemde homojen koordinatları (0,0,0) olan bir nokta yoktur. (Sabuncuoğlu, 2002)

2.5. Düzlemde Eğriler

Eğri, R^2 uzayında bir eğri R'nin bir I alt aralığından R^2'ye tanımlı bir fonksiyonun görüntü kümesidir. Bu görüntü kümesinin elemanları düzlemde gösterildiğinde eğrinin grafiği çizilmiş olur. (Balcı 2012)

Tanım 2.67: $I \subseteq \mathbb{R}$ olmak üzere diferansiyellenebilir

$$\alpha: I \to R^n$$

$$t \to \alpha(t) = \left(\alpha_1(\mathrm{t}), \dots, \alpha_\mathrm{n}(\mathrm{t})\right)$$

Fonksiyonu verilmiş olsun. (I, α) koordinat komşuluğu ile tanımlanan $\alpha(I) \subset E^n$ fonksiyonuna E^n de bir *eğri* denir. t'ye de eğrinin parametresi denir (Hacısalioğlu,1982).

Tanım 2.68: E^n de bir M eğrisi (I, α) koordinat komşuluğu ile verilsin. $\alpha: I \to E^n$ fonksiyonunun öklidiyen koordinat fonksiyonu $\alpha_1(\mathrm{t}), \alpha_2(\mathrm{t}), \dots, \alpha_\mathrm{n}(\mathrm{t})$ olmak üzere

$$\alpha'(\mathrm{t}) = \left(\frac{\mathrm{d}\alpha_1(\mathrm{t})}{\mathrm{dt}}, \frac{\mathrm{d}\alpha_2(\mathrm{t})}{\mathrm{dt}}, \dots, \frac{\mathrm{d}\alpha_\mathrm{n}(\mathrm{t})}{\mathrm{dt}}\right)$$

tanjant vektörüne M eğrisinin $t \in I$ parametre değerine karşılık gelen $\alpha(t)$ noktasında (I, α) komşuluğuna göre bir *hız vektörü* denir (Hacısalioğlu,1998).

Tanım 2.69: Bir eğrinin hız vektörü sıfır olan noktalarına eğrinin *Singüler noktaları denir* (Hacısalioğlu,1998).

Tanım 2.70: En az bir noktasında hız vektörü sıfır olan eğrilere de *singüler eğri* denir (Hacısalioğlu,1998).

Tanım 2.71: Her noktasındaki hız vektörü sıfırdan farklı olan $(\forall t \in I \ için\ \alpha'(\mathrm{t}) \neq 0)$ yani singüler olmayan eğrilere *regüler eğri* denir (Hacısalioğlu,1998).

2.5.1. Düzlemde parametrik denklemli eğriler

f ve g birer sürekli fonksiyon ve t bir aralığı taramak üzere eğri üzerindeki noktanın koordinatları

$$x = f(t)$$
$$y = g(t)$$

Biçiminde ifade edilir. Bu denklemlere eğrinin parametrik denklemleri adı verilir. Eğer t nin taradığı aralık $[a, b]$, yani $a \leq t \leq b$ ise $(f(a), g(a))$ noktasına eğrinin başlangıç noktası, $(f(b), g(b))$ noktasına eğrinin bitim noktası denir. Böylece eğri üzerinde bir yön tanımlanmış olur (Balcı,2012).

Tanım 2.72: Düzlemde,

$$\alpha: I \subseteq R \to R^2$$

$$\alpha(t) = \big(x(t), y(t)\big)$$

dönüşümü için,

i. $x: I \subseteq R \to R$
$y:\ I \subseteq R \to R$
fonksiyonları ikinci mertebeden sürekli türevlenebilirdir.

ii. $\forall\ t \in I$ için $\frac{dx}{dy}, \frac{dy}{dt}$
türevlerinden en az biri sıfırdan farklıdır.

iii. $\forall\ s, t \in I$ için $\alpha(t) = \alpha(s) \Leftrightarrow s = t$ dir.

Yukarıdaki özellikler sağlanıyorsa $\alpha'ya$ *uygun parametrik eğri yayı* denir (Karlıağa,2002).

Tanım 2.73: I'nın $t_i \le t \le t_{i+1}$ için
$\alpha: (t_i, t_{i+1}) \to R^2$
şeklinde ifade edildiğinde α uygun parametrik eğri yayı olacak şekilde bir parçalanışı varsa

$$\alpha: I \subseteq R \to R^2$$

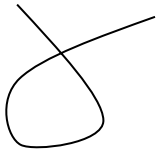
Dönüşümüne *uygun parametrik eğri* denir (Karlıağa,2002).

2.5.1.1.Düzlemde parametrik denklemli eğrilerin özel noktaları

Tanım 2.74: Bir eğrinin uygun parametrik eğri yayı bir alanı kapatıyorsa, bu yaya bu eğrinin bir *ilmiği* denir. Buna göre; bir eğrinin tanım kümesinde

i. $\alpha: (t_0, t_1\ ) \to R^2$ uygun parametrik yayı
ii. $\alpha(t_0) = \alpha(t_1)$

olacak şekilde $t_0 \le t \le t_1$ aralığı varsa bu eğri yayı bir ilmiktir (Bkz.Şekil 2.4).



Şekil 2.4. İlmik

Bu eğri yayı bir ilmik iken $\alpha(t_0) = \alpha(t_1)$ noktasına ilmik noktası denir. Bir ilmiğin kendi kendisini kesmeyen eğri yayı olduğu tanımdan açıktır (Karlıağa,2002).

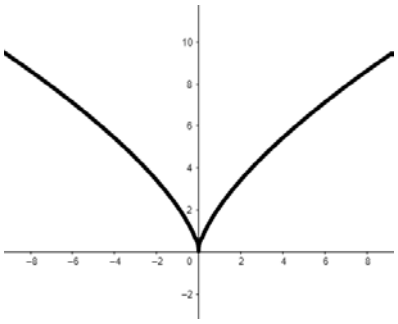
Tanım 2.75: Bir eğrinin tanım kümesindeki bir birinden farklı t_i, $1 \leq i \leq k$ parametre değerlerinin hepsi aynı P noktasını veriyorsa yani; $p = \alpha(t_i),\ 1 \leq i \leq k$ oluyorsa P noktasına bu eğrinin *k-katlı noktası* denir. Her bir singüler nokta ve ilmik noktası iki katlı noktadır (Karlıağa,2002).

Tanım 2.76: Bir eğrinin P noktası iki katlı nokta iken, P den geçen ve bu noktada farklı teğetlere sahip olan iki eğri yayı varsa, Şekil 2.5'deki P noktasına bu eğrinin *düğüm noktası* denir (Karlıağa,2002).

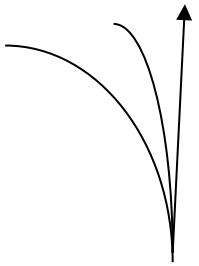
Şekil 2.5. Düğüm Noktası

Tanım 2.77: Bir eğrinin bir P noktası iki katlı nokta iken, P den geçen ve bu noktada çakışık teğete sahip olan iki eğri yayı varsa, P noktasına bu eğrinin bir *cusp* ya da *sivri* noktası denir (Karlıağa,2002).

Tanım 2.78: Bir eğrinin bir P noktası sivri nokta iken, P den geçen ve bu noktada çakışık teğete sahip olan iki eğri yayı teğetin farklı tarafında iseler; Şekil 2.6'daki P noktasına bu eğrinin birinci çeşit cusp ya da birinci çeşit sivri noktası denir. Eğer eğrinin kolları teğetin her iki yanına doğru açılıyorsa Şekil 2.7'daki bu noktaya eğrinin ikinci cins sivri noktası denir(Karlıağa,2002).



Şekil 2.6. Birinci cins sivri nokta



Şekil 2.7. İkinci cins sivri nokta

Tanım 2.79: $\alpha: I \subseteq R \to R^2$ olmak üzere düzlemde parametrik denklemi $\alpha(t) = \big(x(t), y(t)\big)$ olan eğriler için

$$\frac{dx}{dt} = 0$$
$$\frac{dy}{dt} = 0$$

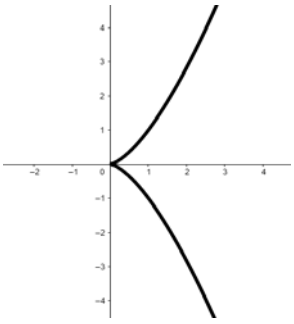
denklem sisteminin çözümüne bu parametrik denklemli eğrinin *singüler* ya da *tekil* noktası denir (Karlıağa,2002).

Örnek: Düzlemde $(x, y) = (t^3, t^2)$ parametrik denklemi ile verilen eğri için

$$\frac{dx}{dt} = 3t^2 = 0$$

$$\frac{dy}{dt} = 2t = 0$$

olup, bu denklem sistemini çözümünden $t = 0$ yani $(x, y) = (0,0)$ noktası bu eğrinin singüler noktasıdır (Bkz.Şekil 2.8).



Şekil 2.8. $(\boldsymbol{x, y}) = (\boldsymbol{t^3, t^2})$

2.5.2. Düzlemde açık denklemli eğriler

Tanım 2.80: Bir eğrinin her herhangi koordinat sistemindeki $f(x,y)=0$ denklemi koordinatlardan birine göre çözülebiliyorsa yani x bağımsız değişken ve y bağımlı değişken olmak üzere $y=f(x)$ formunda yazılabilen denkleme eğrinin açık denklemi denir (Karlıağa, 2002).

2.5.3. Düzlemde kapalı denklemli eğriler

Tanım 2.81: Düzlemde her herhangi koordinat sistemindeki $f(x,y)=0$ denklemi ile verilen bir eğri koordinatlardan birine göre çözülemiyorsa bu denkleme eğrinin kapalı denklemi denir (Karlıağa, 2002).

2.5.3.1.Düzlemde kapalı denklemli eğrilerin özel noktaları

Tanım 2.82: Düzlemde $f(x,y)=0$ denklemi ile verilen eğrinin

$$\begin{cases} f(x,y)=0 \\ f_x(x,y)=0 \\ f_y(x,y)=0 \end{cases}$$

denklem sistemini sağlayan her bir noktasına eğrinin *tekil* ya da *singüler* noktası denir (Karlıağa, 2002).

2.5.3.2. Düzlemde kapalı denklemli eğrilerin teğet denklemi:

Tekil olmayan bir $P(x_0,y_0)$ noktasındaki teğet doğrusunun eğimi

$$m=-\left.\frac{F_x}{F_y}\right|_{(x_0,y_0)}$$

olup, teğet doğrusunun denklemi

$$y-y_0=m(x-x_0)$$

olur (Karlıağa, 2002).

Teorem 2.83: Tekil bir noktadaki teğet doğrusu tek değildir.

Eğer

$$\left(F_{xx}, F_{xy}, F_{yy}\right) \neq (0,0,0)$$

ise, eğrinin en çok iki farklı teğet doğrusu vardır. Bu teğet doğruların eğimleri,

$$F_{xx} + 2F_{xy}y' + F_{yy}(y')^2=0$$

denkleminden y' çözülerek bulunur. Buna göre;

$$\Delta= \left(2F_{xy}\right)^2 - 4F_{xx}F_{yy}$$

olmak üzere

i. $\Delta> 0$ ise eğrinin iki farklı teğeti vardır. Bu durumda bu noktaya *düğüm noktası* denir.

ii. $\Delta= 0$ ise eğrinin çakışık tek teğeti vardır. Eğer eğrinin kolları teğetin tek bir yanında kalıyorsa bu noktaya *eğrinin birinci cins sivri noktası* denir. Eğer eğrinin kolları teğetin her iki yanına doğru açılıyorsa bu noktaya *eğrinin ikinci cins sivri noktası* denir.

iii. $\Delta< 0$ ise eğrinin kolları sanaldır. Bu özellikteki noktalara yalnız noktalar denir.

Eğer

$$\left(F_{xx}, F_{xy}, F_{yy}\right) = (0,0,0)$$

ve

$$\left(F_{xxx}, F_{xxy}, F_{xyy}, F_{yyy}\right) \neq (0,0,0,0)$$

ise eğrinin en çok üç farklı teğet doğrusu vardır. Bu teğetlerin eğimleri

$$F_{xxx} + 3F_{xxy}y' + 3F_{xyy}(y')^2 + F_{yyy}(y')^3 = 0$$

denkleminden y' çözülerek bulunur.

Eğer

$$\left(F_{xx}, F_{xy}, F_{yy}\right) = (0,0,0)$$

ve

$$\left(F_{xxx}, F_{xxy}, F_{xyy}, F_{yyy}\right) = (0,0,0,0)$$

ise eğrinin en çok dört farklı teğet doğrusu vardır. Bu yönteme devam edilerek bir tekil noktadaki tüm teğet doğruları bulunabilir (Karlıağa, 2002).

2.5.4. Cebirsel eğriler

Tanım 2.84: $f(x,y) = 0$ şeklinde verilen eğri için $f(x,y)$ fonksiyonu x ve y değişkenlerinin bir polinomu ise eğriye *cebirsel eğri* denir (Karlıağa 2002).

Örnek: $y^2 - x^3 - x = 0$ Düzlemde bir cebirsel eğri denklemidir.

Tanım 2.85 (Singüler eğri): En az bir noktasında hız vektörü sıfır olan eğrilere singüler (tekil) eğri denir. Bir singüler eğride hız vektörü sıfır olan noktalara da eğrinin singüler (tekil) noktaları denir (Hacısalihoğlu, 1998) .

Teorem 2.86: C cebirsel eğrisi $f(x,y) = 0$ denklemiyle tanımlansın. Bu durumda $P(x,y) \in C$ noktasının C eğrisinin bir singüler(tekil) noktası olması için gerek ve yeter şart

$$\left.\frac{\partial f}{\partial x}\right|_P = \left.\frac{\partial f}{\partial y}\right|_P = 0$$

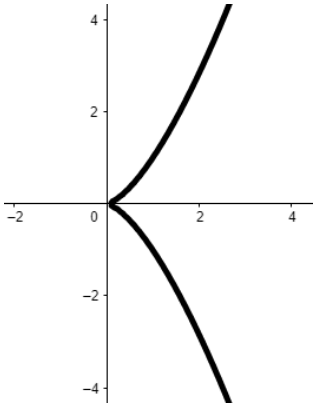
olmasıdır. Bu P noktasında C en az iki farklı teğete sahipse bu noktaya düğüm (node) noktası, birden fazla çakışık teğete sahipse çıkıntı (cusp) noktası denir (Hacısalihoğlu, 1998).

Örnek: $y^2 - x^3 = 0$ eğrisi için;

$$\frac{\partial f}{\partial x} = 0 \Rightarrow x = 0$$

$$\frac{\partial f}{\partial y} = 0 \Rightarrow y = 0$$

olarak elde edilir. Hem $P(0,0) \in C$ olduğundan P noktası C eğrisinin bir singüler noktasıdır ve C singüler bir eğridir. Burada (0,0) noktası bir cusp (doruk) noktasıdır (Bkz. Şekil 2.9).



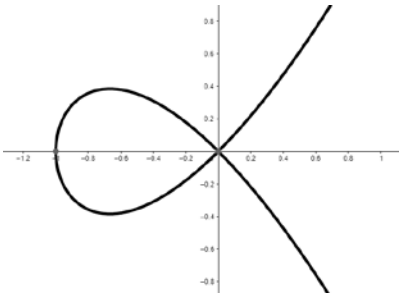
Şekil 2.9. $y^2 = x^3$ eğrisi.

Örnek: $y^2 - x^3 - x^2 = 0$ eğrisi için;

$$\frac{\partial f}{\partial x} = 0 \Rightarrow x_1 = 0, x_2 = \frac{2}{3}$$

$$\frac{\partial f}{\partial y} = 0 \Rightarrow y = 0$$

olarak elde edilir. Hem $P_1(0,0) \in C$ olduğundan C eğrisi süngülerdir ve P_1 noktası düğüm noktasıdır (Bkz.Şekil 2.10).



Şekil 2.10. $y^2 = x^3 + x^2$ eğrisinin grafiği

Tanım 2.87: Singüler olmayan, yani her noktasındaki hız vektörü sıfırdan farklı olan eğrilere regüler (tekil olmayan veya non-singüler) eğri denir. (Hacısalihoğlu, 1998)

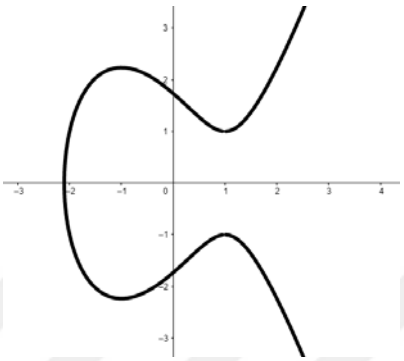
Örnek: $y^2 - x^3 + 3x - 3 = 0$ eğrisi için;

$$\frac{\partial f}{\partial x} = 0 \Rightarrow x = \mp 1$$

ve

$$\frac{\partial f}{\partial y} = 0 \Rightarrow y = 0$$

olarak elde edilir. Hem $P_1(1,0) \notin C$ hemde $P_2(-1,0) \notin C$ olduğundan C eğrisi regülerdir (Bkz.Şekil 2.11).



Şekil 2.11. $y^2 = x^3 - 3x + 3$ eğrisi.

3. MATERYAL ve YÖNTEM

3.1. Şifreleme Algoritmaları

20. yüzyılın ortalarından itibaren geliştirilen şifreleme algoritmalarının güvenliği anahtar olarak adlandırılan sayılarla sağlanmaktadır ve bu algoritmalar anahtar kullanma biçimine göre iki bölüme ayrılırlar;

1. Simetrik (tek anahtarlı) şifreleme algoritmaları
2. Asimetrik (çift anahtarlı) şifreleme algoritmaları

3.1.1. Simetrik şifreleme algoritmaları

Simetrik şifreleme algoritmalarında mesajı şifrelemek ve şifreli mesajın şifresini çözmek için aynı anahtar kullanılır. Bu algoritmalar ile bir mesajı şifrelemek için önce bir anahtar belirlenir. Bu anahtarla düz metin şifrelenir. Şifreli mesaj çözülmek istediğinde aynı anahtar kullanılarak şifre çözülerek ilk metni elde edilir. Bu algoritmaların güçlü yanı hızlı olmalarıdır fakat tek anahtar kullanıldığından şifreli metinlerin alıcı tarafından çözümlenmesinde anahtarın da farklı bir yoldan alıcıya ulaştırılması gerekir. Bu nedenle anahtar dağıtım problemi ortaya çıkar. Bu dezavantajlarından ötürü bu algoritmalar elektronik imza için kullanılamazlar. Bu kategoride yaygın olarak kullanılan algoritmalardan bazıları şunlardır:

- 1974: LUCİFER - IBM,
- 1977: DES - NSA,
- 1982: RC2 - R. Rivest,
- 1993: AES – NSA
- 1998: RC6 – R. Rivest.

3.1.2. Diffie – Hellman anahtar değişim algoritması

Simetrik şifreleme algoritmalarında var olan anahtar dağıtım problemini çözmek için tarafların kullanacakları gizli anahtarı güvenli bir şekilde üretebilecekleri ilk pratik çözüm

1976 yılında Diffie ve Hellman tarafından güvenli anahtar paylaşım algoritması ileri sürülmüştür (Diffie vd., 1976). Algoritmanın adımları aşağıda verilmiştir.

p yeteri kadar büyük bir asal sayı ve g'de Z_p^* ın bir ilkel kökü olsun.

A, aşağıdaki işlemleri yapar

- $0 \leq a \leq p-2$ eşitsizliğini sağlayan rastgele bir a sayısı belirler.
- $c_1 \coloneqq g^a \ (mod\ p)$ değerini hesaplar ve c_1 değerini B'ye gönderir.

B, aşağıdaki işlemleri yapar.

- $0 \leq b \leq p-2$ eşitsizliğini sağlayan rastgele bir b sayısı belirler.
- $c_2 \coloneqq g^b \ (mod\ p)$ değerini hesaplar ve c_2 değerini A'ya gönderir.

A, şu şekilde ortak anahtar olacak k'yı hesaplar:

$$k \coloneqq {c_2}^a (mod\ p)$$

B, şu şekilde ortak anahtar olacak k'yı hesaplar:

$$k \coloneqq {c_1}^b (mod\ p)$$

Böylece ortak bir anahtar olan k için A ve B aralarında anlaşmış olurlar.

Algoritmanın ispatı:

$$k \equiv {c_2}^a \equiv (g^b)^a \equiv g^{ba} \equiv (g^a)^b \equiv {c_1}^b (mod\ p)$$

3.2. Asimetrik Şifreleme Algoritmaları

Asimetrik şifreleme algoritmalarında mesajı şifrelemek ve şifreli mesajın şifresini çözmek için farklı anahtarlar kullanılır. Açık (çift) anahtarlı şifreleme algoritmaları olarak da adlandırılan bu şifreleme sistemlerinde bir metni şifrelemek için Genel (Açık) anahtar adı verilen bir şifreleme anahtarı ile bu anahtarla arasında matematiksel bir ilişki bulunan ve şifreli mesajı çözümlemek içi bir Özel (Gizli) anahtar üretilir. Ayrıca hem şifreleme hem de şifre çözme işlemlerinde kullanılan sayılar da Ortak anahtar denilir. Bu

algoritmalar anahtar dağıtım problemine sahip değildirler fakat simetrik algoritmalara nazaran fazla işlem gücü gerektirdiğinden daha yavaş çalışmaktadırlar.

Günümüzde yaygın olarak kullanılan bazı Asimetrik algoritmalar şunlardır:

- 1978, RSA - Rivest-Shamir-Adleman.
- 1985, El-Gamal - Taher ElGamal.
- 1986, Eliptik Eğri - Miller-Koblitz.

Asimetrik algoritmalar 3 aşamadan oluşur;

1. Anahtar oluşturma (Key Generation)
2. Şifreleme (Encryption)
3. Şifre çözme (Decryption)

3.2.1. RSA şifreleme algoritması

1978'de Rivest, Shamir ve Adleman tarafından hem şifreleme hem de elektronik imza için kullanılabilen, yazarların isimlerinin baş harfleri RSA olarak adlandırılan, ilk asimetrik şifreleme algoritmasını yayınlamışlardır (Rivest vd., 1978). Algoritmanın adımları aşağıda verilmiştir.

Anahtarları oluşturma:

Şifreli bilgiyi almak isteyen A kişisi aşağıdaki işlemleri yapar;

- İki adet yeteri kadar büyük p ve q asal sayıları üretir.
- $n = p.q$ değerini hesaplar, n (her iki tarafın kullandığı) (ortak anahtardır).
- $\emptyset = (p-1).(q-1)$ değerlerini hesaplar.
- $(e, \emptyset) = 1$ ve $1 < e < \emptyset$ şartlarını sağlayan bir e sayısı (Açık anahtar) seçer.
- $e.d \equiv 1\ (mod\ \emptyset)$ olan d sayısı (Gizli anahtar) hesaplar.
- A, ortak anahtar n ile açık anahtarlar e sayılarını B'ye gönderir

Mesajın şifrelenmesi:

RSA'da şifreleme işlemi modüler aritmetik üs alma işlemine dayanır.

- B, şifrelemek istediği mesajı $M \in Z_n$ olan bir tamsayıya dönüştürür ve $C :\equiv M^e (mod\ n)$ değerini hesaplayarak şifreli metin C'yi elde eder ve A'ya gönderir.

Şifreli mesajın çözümlenmesi:

- A, kendi gizli anahtarını kullanılarak $M :\equiv C^d (mod\ n)$ değerini hesaplayarak düz metin M'yi elde eder.

Örnek:

Anahtarları Oluşturma

- $p = 89,\ q = 97$
- $n = 89.97 = 8633$
- $\emptyset(n) = (p-1).(q-1) = (89-1).(97-1) = 8448$
- $1 < e < 8448$ ve 8448 ile aralarında asal olacak şekilde $e = 13$
- $13d = 1(mod\ 8448)$ den $d = 4549$

Mesajın Şifrelenmesi

- $M = 85$
- $C :\equiv 85^{13} (mod\ 8448) = 2743$

Şifreli mesajın çözümlenmesi

- $M :\equiv 2743^{4549} (\text{mod } 8448) = 85$

Algoritmanın ispatı:

- $e.d \equiv 1\ \left(mod\left(\emptyset(n)\right)\right)$ den $e.d = k.\emptyset(n) + 1$ dir. $(k \in Z)$ (Mod teoremi)

- $M^{\emptyset(n)} \equiv 1\ (mod\ n)$ dir. (Euler Teoremi)

$$C^d \equiv (M^e)^d \equiv M^{e.d} \equiv M^{k.\emptyset(n)+1} \equiv \left(M^{\emptyset(n)}\right)^k . M \equiv 1^k . M \equiv M(mod\ n)$$

Algoritmanın güvenilirliği

RSA'nın güvenliği Çarpanlara Ayırma (Integer Factorization) probleminin algoritmik zorluğuna dayanmaktadır. p ve q yeterince büyük asal sayılar olduğunda $n = p.q$ için n sayısı bilindiğinde p ve q sayılarını bulmak için henüz çok kısa sürede sonuç veren bir algoritma geliştirilememiştir. Geçmişte Fermat ($\sim$1960), Euler(~ 1750), Legendre (~ 1790), Gauss($\sim$1800) gibi ünlü matematikçiler tamsayıların çarpanlarına ayrılması ile ilgili çeşitli çalışmalar yapmışlardır.

Çarpanlara ayırma algoritmaları Genel amaçlı (General Purpose) ve Özel amaçlı (Special Purpose) olmak üzere iki guruba ayrılır.

Genel amaçlı çarpanlara ayırma algoritmaların çalışma zamanı verilen n yarı asal sayısının büyüklüğüne bağlıdır. Genel amaçlı çarpanlara ayırma algoritması olarak;

1981 yılında Pomerence, Karesel eleme (Quadratic Sieve) algoritmasını, 1990 yılında Lenstra vd., Genel Sayı Cisim Elemesi (General Number Field Sieve) algoritmasını geliştirmişlerdir ve bu algoritma günümüzde kullanılan en hızlı genel amaçlı çarpanlara ayırma algoritmasıdır (Aybak 2010).

Özel amaçlı çarpanlara ayırma algoritmalarının çalışma zamanı ise verilen n sayısını oluşturan çarpanların belirli özelliklerine veya n sayısının bazı özelliklerine bağlıdır. Bu nedenle RSA'da asal sayılar seçilirken ve n sayısı oluşturulurken özel amaçlı çarpanlara ayırma algoritmalarının da göz önünde bulundurulması bir zorunluluktur. Özel amaçlı çarpanlara ayırma algoritması olarak;

1974 yılında J. M. Pollard, $p-1$ olarak adlandırılan algoritmayı (Bütün 2018), 1982 yılında H. C. Williams, $p+1$ olarak adlandırılan bir diğer algoritmayı (Polat 2018), 1987 yılında H. W. Jr. Lenstra, Eliptik Eğri Çarpanlara Ayırma olarak adlandırılan algoritmayı(Lenstra 1987), 1988 ise yılında J. M. Pollard, Özel Sayı Cismi Elemesi olarak adlandırılan algoritmayı ileri sürmüşlerdir.

3.2.2. ElGammal şifrelme algoritması

Taher El-Gamal, Ayrık Logaritma Problemine dayanan diğer bir pratik asimetrik şifreleme algoritmasını ileri sürmüştür. Algoritmanın adımları aşağıda verilmiştir.

Anahtarları oluşturma:

Şifreli bilgiyi almak isteyen A tarafı aşağıdaki işlemleri yaparak kendi anahtarlarını oluşturur;

- Yeterince büyük rastgele bir p asalı ve Z_p^* çarpımsal grubun üreteci olan bir a sayısı (ortak anahtarlar) seçer.
- $1 \leq d \leq p-2$ eşitsizliğine uygun bir d sayısı (Gizli anahtar) seçer.
- $e :\equiv a^d (mod\ p)$ değerini (Açık anahtar) hesaplar.
- A, ortak anahtarlar p ve a ile açık anahtar e sayılarını B'ye gönderir

Mesajın şifrelenmesi:

- B, şifrelemek istediği mesajı $m \in Z_p$ olacak şekilde bir tamsayıya dönüştürür.
- $1 \leq t \leq p-2$ şartına uygun rastgele bir t tam sayısı seçer.
- $r :\equiv a^t\ (mod\ p)$ ve $s :\equiv m.e^t\ (mod\ p)$ değerlerini hesaplayarak r ve s şifreli metin parçalarını hesaplar.
- B, şifreli metnin parçaları olan r ve s değerlerini A'ya gönderir.

Şifreli mesajın çözümlenmesi:

- A, kendi özel anahtarı olan d'yi kullanılarak $r^{-d}.s\ (mod\ p) = m$ değerini hesaplar ve düz metin m'yi elde eder.

Algoritmanın ispatı:

$$r^{-d}.s \equiv (a^t)^{-d}.m.(a^d)^t \equiv m\ mod\ p$$

Örnek:

Şifreli bilgiyi almak isteyen A kişisi aşağıdaki işlemleri yaparak kendi anahtarlarını oluşturur;

Anahtarları oluşturma:

- $p = 13$, Z_{13}^{*} ın üreteçlerinden $a = 3$ olsun.
- $1 \leq d \leq 11$ olacak şekilde $d := 5$
- $e :\equiv 3^{5}(mod\ 13) = 9$

Mesajın şifrelenmesi:

- $m = 10$ olsun.
- $1 \leq t \leq 11$ için $t = 7$
- $r :\equiv 3^{7}(mod\ 13) = 3$
- $s :\equiv 10.9^{7}(mod\ 13) = 12$

Şifreli Mesajın Çözümlenmesi:

- $m :\equiv 3^{-11}.13(mod\ 13) = 10$

Algoritmanın güvenilirliği:

ElGamal şifreleme algoritmasının güvenliği Ayrık Logaritma Probleminin (DLP) algoritmik zorluğuna dayanmaktadır.

$$a^{x} \equiv b(mod\ p)$$

Kongrüansında a, b, p değerleri bilindiğinde x değerine bulmak için henüz kullanışlı bir algoritma geliştirilememiştir.

4. ARAŞTIRMA KONUSU

Eliptik Eğriler hem şifrelemede hem de tam sayıların çarpanlara ayrılmasında kullanılmaktadır. Bu bölümde eliptik eğrilerin cebirsel yapıları, eliptik eğri şifreleme algoritması ve eliptik eğri çarpanlara ayırma algoritması incelenecektir.

4.1.Eliptik Eğriler

F bir cisim, $a_1, a_2, a_3, a_4, a_6 \in F$ olmak üzere F cismi üzerinde E eliptik eğrisinin genel denklemi

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (4.1)$$

Şeklinde tanımlanır ve "Weierstrassform" olarak adlandırılır. (4.1) formundaki bu denkleme Afin dönüşümler uygulanırsa;

$Kar(F) = 3$ için:

$a_1^2 \neq -a_2$ durumu: (4.1) eşitliğine aşağıdaki dönüşümler uygulanırsa

$$x = x' + \frac{d_4}{d_2}$$

$$y = y' + a_1x' + a_1\frac{d_4}{d_2} + a_3$$

$$d_2 = a_1^2 + a_2$$

$$d_4 = a_4 - a_1a_3$$

Aşağıdaki eşitlik elde edilir.

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

$a_1^2 = -a_2$ durumu: (4.1) eşitliğine aşağıdaki dönüşümler uygulanırsa

$$x = x'$$

$$y = y' + a_1x' + a_3$$

Aşağıdaki eşitlik elde edilir.

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

$Kar(F) = 2$ için:

$a_1 \neq 0$ durumu: (4.1) eşitliğine aşağıdaki dönüşümler uygulanırsa

$$x = {a_1}^2.x' + \frac{a_3}{a_1}$$

$$y = {a_1}^3.y' + \frac{{a_1}^2.a_4 + {a_3}^2}{{a_1}^3}$$

(4.1) denklemi aşağıdaki eşitliğe dönüşür, gerekli işlemler yapılırsa;

$$y'^2 + x'y' = x'^3 + \left(\frac{{a_1}^3.a_2 + {a_1}^4.a_2}{{a_1}^6}\right).x'^2 + \frac{{a_1}^4.{a_4}^2 + {a_3}^4}{{a_1}^{12}} + \frac{{a_3}^3}{{a_1}^9} + \frac{a_2.{a_3}^2}{{a_1}^8} + \frac{a_3.a_4}{{a_1}^7} + \frac{a_6}{{a_1}^6}$$

$$\frac{{a_1}^3.a_2 + {a_1}^4.a_2}{{a_1}^6} = a$$

$$\frac{{a_1}^4.{a_4}^2 + {a_3}^4}{{a_1}^{12}} + \frac{{a_3}^3}{{a_1}^9} + \frac{a_2.{a_3}^2}{{a_1}^8} + \frac{a_3.a_4}{{a_1}^7} + \frac{a_6}{{a_1}^6} = b$$

Aşağıdaki eşitlik elde edilir.

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

$a_1 = 0$ durumu: (4.1) eşitliğine aşağıdaki dönüşümler uygulanırsa

$$x = x' + a_2$$

$$y = y'$$

(4.1) denklemi aşağıdaki eşitliğe dönüşür, gerekli işlemler yapılırsa;

$$y'^2 + (a_1.a_2 + a_1.x' + a_3).y' = x'^3 + ({a_2}^2 + a_4).x' + {a_2}^3 + a_2.a_4 + a_6$$

buradan

$$a_1.a_2 + a_1.x' + a_3 = c$$

$${a_2}^2 + a_4 = a$$

$${a_2}^3 + a_2.a_4 + a_6 = b$$

denilirse aşağıdaki eşitlik elde edilir.

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

$kar(F) \neq 2$ için: (4.1) eşitliğine aşağıdaki dönüşümler uygulanırsa

$$y = \frac{1}{2}(y' - a_1 x' - a_3)$$

dönüşümleri uygulanırsa;

$$y'^2 = 4x'^3 + ({a_1}^2 + 4a_2)x'^2 + 2(2a_4 + a_1.a_3)x' + {a_3}^2 + 4a_6$$

Buradan

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

$$2a_4 + a_1.a_3 = b_4$$

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

denilirse

$$y'^2 = 4x'^3 + b_2 x'^2 + 2b_4 x' + b_6 \qquad (4.2)$$

Denklemine dönüşür. Ayrıca (4.2) eşitliğinde $kar(F) \neq 3$ durumu için;

$$x = \frac{1}{36}(x' - 3b_2)$$

$$y = \frac{1}{108}y'$$

Dönüşümleri uygulanırsa bu durumda $kar(F) \neq 2{,}3$ için

$$y^2 = x'^3 - 27\left({b_2}^2 - 4b_4\right)x' - 54\left(-{b_2}^3 + 36.b_2.b_4 - 216b_6\right)$$

$$-27\left({b_2}^2 - 4b_4\right) = a$$

$$-54\left(-{b_2}^3 + 36.b_2.b_4 - 216b_6\right) = b$$

denilirse

$$E: y^2 = x^3 + ax + b \tag{4.3}$$

Elde edilir. Bu sonuç aynı zamanda (4.1) eşitliğine direkt aşağıdaki dönüşümler uygulanarak ta elde edilebilir.

$$x = \frac{x' - 3{a_1}^2 - 12a_2}{36}$$

$$y = \frac{y' - 3a_1x'}{216} - \frac{a_1^3 + 4a_1a_2 - 12a_3}{24}$$

4.1.1. Eliptik eğrilerin özel noktaları

(4.3) eşitliğindeki $f(x) = x^3 + ax + b$ için $f(x) = 0$ denkleminin kökleri x_1, x_2 ve x_3 olsun. Bu $f(x)$ fonksiyonun disktriminantı;

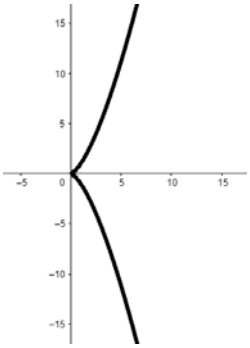
$$\Delta(f) = (x_1 - x_2)^2(x_2 - x_3)^2(x_1 - x_3)^2 = -16(4a^3 + 27b^2)$$

Olduğundan;

i. $\Delta(f) = 0$ ise $f(x)$ kübik polinomunun katlı kökü vardır ve $y^2 = f(x)$ eliptik eğrisi singüler (tekil) noktaya sahiptir. Bu durumda eğri tekil yani singüler olup üzerindeki bazı noktalar için teğet doğrusu tanımlı olmaz, eğri üzerinde bu noktalarda toplama işlemi tanımsız olur ve eliptik eğri üzerinde bir grup yapısı oluşturulamaz (Link2,2021)

Örnek: $y^2 = x^3$ eğrisi singüler eliptik eğridir.

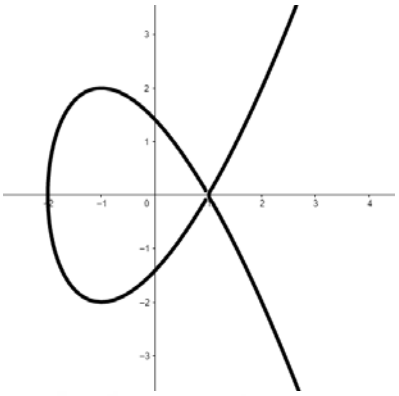
$f(x) = x^3$ polinomunda $\Delta = 0$ olup $x = 0$ bir katlı köktür (Bkz.Şekil 4.1).



Şekil 4.1. $\boldsymbol{y^2 = x^3}$ eğrisi

Örnek: $y^2 = x^3 - 3x + 2$ eğrisi singüler eliptik eğridir.

$f(x) = x^3 - 3x + 2$ polinomunda $\Delta = 0$ olup $x = 0$ bir katlı köktür (Bkz.Şekil 4.2).

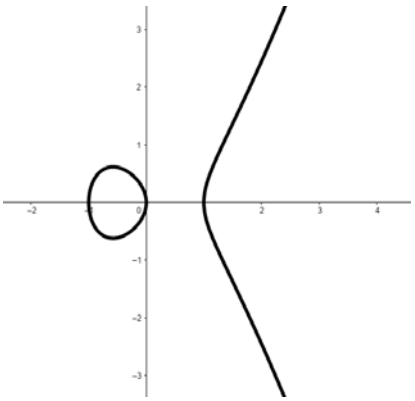


Şekil 4.2. $\boldsymbol{y^2 = x^3 - 3x + 2}$ eğrisi

ii. $\Delta(f) \neq 0$ ise $f(x)$ kübik polinomunun katlı kökü yoktur ve $y^2 = f(x)$ eliptik eğrisinin (tekil) singüler noktası yoktur, bu tür eliptik eğrilere tekil olmayan yani regüler (non-singular) eliptik eğri denir. Bu durumda eliptik eğri üzerindeki tüm noktalarda toplama işlemi tanımlanabilir ve eğri üzerinde grup yapısı oluşturulabilir (Link2, 2021)

Örnek: $y^2 = x^3 - x$ eğrisi regüler eliptik eğridir.

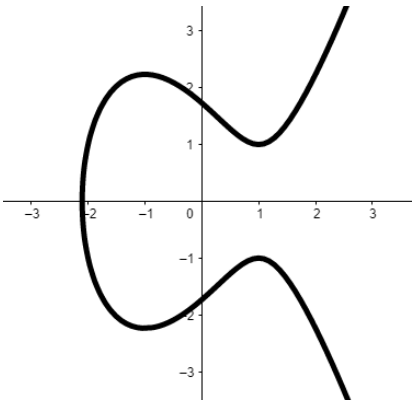
$f(x) = x^3 - x$ polinomunda $\Delta = -4$ tür (Bkz.Şekil 4.3).



Şekil 4.3. $\boldsymbol{y^2 = x^3 - x}$ eğrisi

Örnek: $y^2 = x^3 - 3x + 3$ eğrisi regüler bir eliptik eğridir.

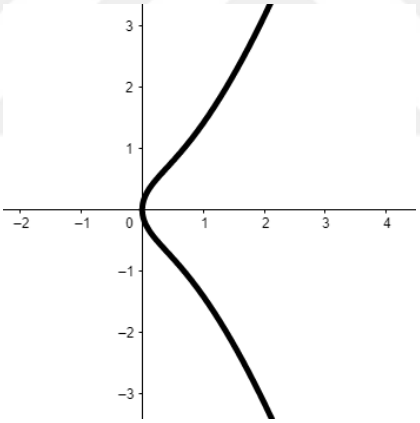
$f(x) = x^3 - 3x + 3$ polinomunda $\Delta = -135$ tir (Bkz.Şekil 4.4).



Şekil 4.4. $\boldsymbol{y^2 = x^3 - 3x + 3}$ eğrisi

Örnek: $y^2 = x^3 + x$ eğrisi regüler bir eliptik eğridir.

$f(x) = x^3 + x$ polinomunda $\Delta = -4$ tür (Bkz.Şekil 4.5).



Şekil 4.5. $\boldsymbol{y^2 = x^3 + x}$ eğrisi

4.1.1.1. Eliptik eğrinin homojen koordinatlardaki sonsuzdaki noktası

$A(x, y)$ noktasının homojen koordinatlardaki karşılığı $H(X, Y, Z)$ olsun. Bu durumda $x = \frac{X}{Z}$ ve $y = \frac{Y}{Z}$ olup bu değerler

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

denkleminde yazılırsa

$$\frac{Y^2}{Z^2} = \frac{X^3}{Z^3} + a\frac{X}{Z} + b$$

elde edilir. Eşitlik Z^3 ile genişletilirse

$$Y^2Z = X^3 + aXZ^2 + bZ^3 \tag{4.4}$$

elde edilir. (4.4) eşitliğinde $Z = 0$ yazılırsa $0 = X^3$ den $X = 0$ elde edilir. Bu durumda $(0, Y, 0)$ noktası (4.4) denkleminin sonsuzdaki noktası olarak adlandırılır ve $(0, Y, 0) \approx (0,1,0)$ olduğu kolayca görülebilir.

4.1.2. Eliptik eğrilerin cebirsel yapısı

Tanım 2.88: F bir cisim ve E, (4.3) formunda bir eliptik eğri olsun. Bu durumda F cismi üzerindeki eliptik eğri

$$E(F) = \{(x, y) \in F \times F : y^2 = x^3 + ax + b, a, b \in F\} \tag{4.5}$$

şeklinde tanımlanır ve (4.5) kümesinde özel olarak $F = Q$ alınırsa E'nin Q üzerindeki rasyonel noktalarının kümesi

$$E(Q) = \{(x, y) \in Q \times Q : y^2 = x^3 + ax + b, a, b \in Q\} \tag{4.6}$$

Olup, (4.6) kümesine sonsuzdaki nokta eklenerek elde edilen

$$E(Q) = \{\infty\} \cup \{(x, y) \in Q \times Q : y^2 = x^3 + ax + b, a, b \in Q\} \tag{4.7}$$

(4.7) kümesine Q cismi üzerinde tanımlı eliptik eğri adı verilir.

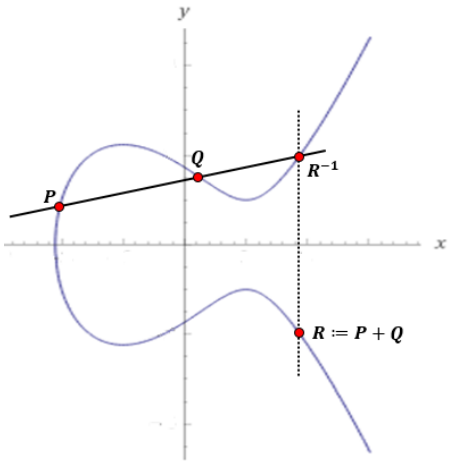
4.1.2.1. Eliptik eğriler üzerinde nokta toplama

E (4.7) formunda ve regüler bir eliptik eğri olsun. $P(x_1, y_1)$ ve $Q(x_2, y_2)$ E eğrisi üzerinde iki nokta olmak üzere Afin koordinatlarda $R := P + Q$ nokta toplamı şu şekilde tanımlanır.

AT1) $P \neq Q$ için;

AT1.1) $x_1 \neq x_2$ durumu: P ve Q noktalarından geçen doğru eliptik eğriyi üçüncü bir R^{-1} noktasında keser. Bu R^{-1} noktasının x eksenine göre simetriği alınarak P ve Q noktalarını

toplamı olan R noktası elde edilir. (Bkz. Şekil 4.6)



Şekil 4.6. $x_1 \neq x_2$ olma durumu.

Örnek:

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

olsun. E eliptik eğrisi üzerindeki $P(-1,0)$ ve $Q(2,3)$ noktalarının toplamını bulalım.

Çözüm: P ve Q noktalarından geçen doğru denklemi

$$d: y = x + 1$$

dir. d doğrusu ile E eğrinin kesişiminden

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

Kübik denklemi elde edilir. Bu denklemin kökleri

$$x_1 = -1,\ x_2 = 2 \text{ ve } x_3 = 0$$

dir. $x_3 = 0$ değeri d doğrusunda yazılırsa $y_3 = 1$ olarak bulunur. Sonuç olarak

$R^{-1}(0,1)$ olup bu noktanın x eksenine göre simetriği alınırsa

$$R(0,-1)$$

olarak hesaplanır.

$P + Q$ toplamını veren formüllerin bulunması:

P ve Q noktalarından geçen d_1 doğrusunun eğimi

$$m = (y_2 - y_1)(x_2 - x_1)^{-1} \tag{4.8}$$

Olup d_1 doğrusunun denklemini

$$d_1 : y = m(x - x_1) + y_1 \tag{4.9}$$

Olarak yazılır ve (4.9) ve (4.3) eşitlikleri ile ortak çözüm yapılırsa;

$$(m(x - x_1) + y_1)^2 = x^3 + ax + b$$

yazılır, buradan

$$x^3 - m^2x^2 + (-2m^2x_1 - 2my_1 + a)x + (-x_1^2m^2 + 2mx_1y_1 - y_1^2 + b) = 0$$

$$x^3 - m^2x^2 + b_1x + c_1 = 0 \tag{4.10}$$

kübik denklemi elde edilir.

(4.10) denklemin kökleri d_1 ile E'nin kesişim noktalarıdır. (4.10) denklemin kökler toplamından

$$x_1 + x_2 + x_3 = m^2$$

Yazılır. Buradan;

$$x_3 = m^2 - x_1 - x_2 \tag{4.11}$$

Elde edilir. Köklerden x_1 ve x_2 eğri üzerinde olup (4.3) denklemini sağlar, bu durumda (4.11) eşitliği R^{-1} noktasının apsisidir. Bu durumda (4.9) denkleminde x yerine x_3 yazılırsa R^{-1} noktasının ordinatı

$$y_3{}' = m(x_3 - x_1) + y_1$$

Şeklinde elde edilmiş olur.

Son olarak $R^{-1}(x_3, y_3')$ noktasının x eksenine göre simetrisi alınırsa

$$y_3 = m(x_1 - x_3) - y_1 \tag{4.12}$$

R noktasının koordinatları (4.11) ve (4.12) olarak elde edilir.

Örnek:

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

olsun. E eğrisi üzerindeki $P(-1,0)$ ve $Q(2,3)$ noktalarının toplamını formül yardımı ile hesaplayalım.

Çözüm: P ve Q için

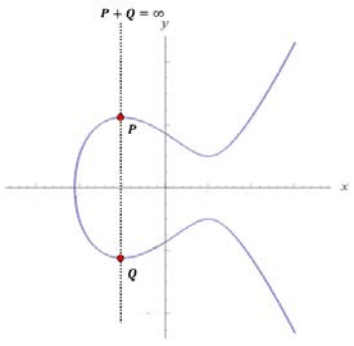
$$m = 1$$

$$x_3 = m^2 - x_1 - x_2 = 1 + 1 - 2 = 0$$

$$y_3 = m(x_1 - x_3) - y_1 = 1(-1 - 0) - 0 = -1$$

olarak bulunur.

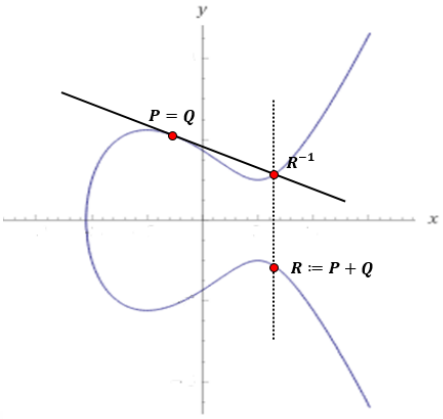
AT1.2) $x_1 = x_2$ durumu: $y_1 \neq y_2$ olduğundan (4.8) ile verilen m tanımsız olup P ve Q noktalarından geçen doğru x eksenine diktir. Bu durumda $P + Q = \infty$ olarak tanımlanır. (Bkz. Şekil 4.7)



Şekil 4.7. $\boldsymbol{x_1 = x_2}$ ve $\boldsymbol{y_1 \neq y_2}$ olma durumu.

AT2) $P = Q$ için;

AT2.1) $y_1 = y_2 \neq 0$ durumu: E eğrisine $P = Q$ noktasında teğet olan doğru eliptik eğriyi ikinci bir R^{-1} noktasında keser. Bu R^{-1} noktasının x eksenine göre simetriği alınarak P ve Q noktalarının toplamı olan R noktası elde edilir. (Bkz. Şekil 4.8)



Şekil 4.8. $\boldsymbol{x_1 = x_2}$ ve $\boldsymbol{y_1 = y_2 \neq 0}$ olma durumu.

Örnek:

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

eğrisi üzerinde $P(1,2)$ noktasının kendisi ile toplamını olan $2P$ noktasını bulalım.

Çözüm: $2yy' = 3x^2 \Rightarrow m = y'_{(1,2)} = \frac{3}{4}$ ve böylece P noktasından geçen teğet doğrunun denklemi

$$d: 4y = 3x + 5$$

biçimindedir.

d ile E ortak çözülürse

$$16x^3 - 9x^2 - 30x + 23 = 0$$

elde edilir. Bu eşitliğin kökler toplamı

$$x_1 + x_2 + x_3 = \frac{9}{16}$$

olup iki kökü $x_1 = x_2 = 1$ olduğundan

$$1 + 1 + x_3 = \frac{9}{16} \Rightarrow$$

$$x_3 = \frac{-23}{16}$$

ve bu değer d doğrusunda yazılırsa

böylece

$$y_3 = \frac{11}{64}$$

olarak bulunur. Sonuç olarak $(-\frac{23}{16}, \frac{11}{64})$ ve bu noktanın x eksenine göre simetriği alınarak

$$2P(-\frac{23}{16}, -\frac{11}{64})$$

Olarak bulunur.

$\boldsymbol{P + P = 2P}$ toplamını veren formüllerin bulunması:

$P = Q$ noktasında eğriye teğet olan doğrunun eğimi (4.3) denkleminin türevi alınarak şu şekilde elde edilir.

$$2y\frac{dy}{dx} = 3x^2 + a$$

$$m = (3x_1^2 + a)(2y_1)^{-1} \tag{4.13}$$

Eğriye P noktasında teğet olan doğrunun denklemi

$$d_2: y = m(x - x_1) + y_1 \tag{4.14}$$

(4.14) ve (4.3) denklemleri ortak çözülürse bir önceki formülün bulunmasında yapıldığı gibi (4.10) eşitliği elde edilir. d_2 doğrusu E eğrisine P noktasında teğet olduğundan x_1 çift katlı kök olup x_3 eliptik eğri ve d_2 doğrusunun 2. kesişime noktasının apsisidir. Bu durumda

$$x_3 = m^2 - 2x_1 \tag{4.15}$$

yazabiliriz ve (4.15) i (4.14) de kullanırsak;

$$y_3{}' = m(x_3 - x_1) + y_1$$

Elde ederiz. Son olarak bu $(x_3, y_3{}')$ noktasının x eksenine göre simetriği alınırsa

$$y_3 = m(x_1 - x_3) - y_1 \tag{4.16}$$

$P + P = 2P$ noktasının koordinatları (4.15) ve (4.16) olarak elde edilir.

Örnek:

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

eğrisi üzerinde $P(1,2)$ noktasının kendisi ile toplamını olan $2P$ noktasını formül kullanarak bulalım.

Çözüm:

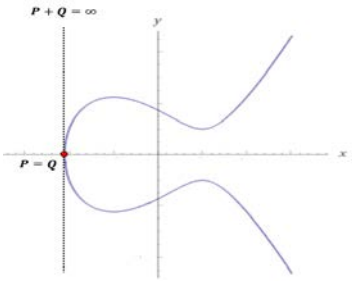
$$2yy' = 3x^2 \Rightarrow m = y'_{(1,2)} = \frac{3}{4}$$

$$x_3 = m^2 - 2x_1 = \left(\frac{3}{4}\right)^2 - 2.1 = -\frac{23}{16}$$

$$y_3 = m(x_1 - x_3) - y_1 = \frac{3}{4}\left(1 + \frac{23}{16}\right) - 2 = -\frac{11}{64}$$

olarak bulunur.

AT2.1) $y_1 = y_2 = 0$ durumu: bu durumda (4.13) ile verilen m tanımsız olup teğet doğrusu x eksenine diktir. Bu durumda $P + Q = \infty$ olarak tanımlanır. (Bkz. Şekil 4.9)



Şekil 4.9. $x_1 = x_2$ ve $y_1 = y_2 = 0$ olma durumu.

4.1.2.2. Eliptik eğrilerin grup yapısı

Teorem 2.89: E eliptik eğrisi üzerindeki toplama işlemi aşağıdaki özellikleri sağlar.

G1) Kapalılık: $P, Q \in E$ olmak üzere $P + Q \in E$ dir.

G2) Birleşme: $P, Q, R \in E$ olmak üzere $(P + Q) + R = P + (Q + R)$ dir.

G3) Birim Eleman: Her $P \in E$ için $P + \infty = P$ dir.

G4) Ters Eleman: $P \in E$ ise $P + P' = \infty$ olacak biçimde $P' \in E$ vardır. Bu P' noktası – P olarak gösterilecektir ve bu noktanın koordinatı $(x, -y)$ dir.

Yukarıdaki özellikler sağlandığından E eğrisi üzerindeki noktalar toplama işlemine bir grup oluşturur. Burada ∞ grubun birim elemanıdır. Ayrıca $P + Q = Q + P$ olup grup değişmelidir.

4.1.2.3. Homojen koordinatlarda toplama

Afin koordinatlarda nokta toplama işleminde yer alan modüler bölme işlemine nazaran homojen koordinatlarda nokta toplama işlemi daha az maliyetlidir (Link1, 2021).

Afin koordinatı $P_A(x_1, y_1)$ ve $Q_A(x_2, y_2)$ olan noktaların homojen koordinatı sırasıyla $P_H(X_1, Y_1, Z_1)$ ve $Q_H(X_2, Y_2, Z_2)$ olsun. Bu durumda

$$x_1 = \frac{X_1}{Z_1} \tag{4.17}$$

$$y_1 = \frac{Y_1}{Z_1} \tag{4.18}$$

$$x_2 = \frac{X_2}{Z_2} \tag{4.19}$$

$$y_2 = \frac{Y_2}{Z_2} \tag{4.20}$$

yazabiliriz.

HT1) $P_A \neq Q_A$ ve $x_1 \neq x_2$ için $P_A + Q_A$ toplamının bulunması:

(4.17)-(4.20) değerleri (4.8) de yazılırsa:

$$m = \frac{Y_1 Z_2 - Y_2 Z_1}{X_1 Z_2 - X_2 Z_1} \tag{4.21}$$

olup (4.21) eşitliğinde sırasıyla

$$T_1 = Y_1 Z_2,$$

$$T_2 = Y_2 Z_1,$$

$$T = T_1 - T_2$$

$$U_1 = X_1 Z_2,$$

$$U_2 = X_2 Z_1,$$

$$U = U_1 - U_2$$

alınırsa

$$m = \frac{T}{U} \tag{4.22}$$

elde edilir. Ayrıca (4.17), (4.19) ve (4.22) değerleri (4.11) de yazılırsa:

$$x_3 = \left(\frac{T}{U}\right)^2 - \frac{X_1}{Z_1} - \frac{X_2}{Z_2} = \frac{T^2 Z_1 Z_2 - U^2(U_1 + U_2)}{U^2 Z_1 Z_2} \tag{4.23}$$

olup (4.23) de sırasıyla

$$V = Z_1 Z_2$$

$$W = T^2 V - U^2(U_1 + U_2)$$

alınırsa

$$x_3 = \frac{W}{U^2 V} \tag{4.24}$$

elde edilir. Şimdi (4.17), (4.18), (4.22) ve (4.24) değerleri (4.12) de yazılırsa:

$$y_3 = \frac{T}{U}\left[\frac{X_1}{Z_1} - \frac{W}{U^2 V}\right] - \frac{Y_1}{Z_1} = \frac{T(U_1 U^2 - W) - T_1 U^3}{U^3 V} \tag{4.25}$$

elde edilir. (4.25) eşitliğinde

$$Z_3 = U^3V$$

$$Y_3 = T(U_1U^2 - W) - T_1U^3$$

alalım. Son olarak (4.24) eşitliği U ile genişletilirse

$$x_3 = \frac{UW}{U^3V} \tag{4.26}$$

ede edilir. (4.26) eşitliğinde

$$X_3 = UW$$

alınırsa R_H noktasının koordinatları (X_3, Y_3, Z_3) şeklinde bulunmuş olur.

Örnek:

$$E\colon\ y^2 = x^3 + 1$$

E eğrisi üzerindeki $P_H(-1,0,1) + Q_H(2,3,1)$ toplamını bulalım.

Çözüm:

$$T_1 = Y_1Z_2 = 0$$

$$T_2 = Y_2Z_1 = 3$$

$$T = T_1 - T_2 = -3$$

$$U_1 = X_1Z_2 = -1$$

$$U_2 = X_2Z_1 = 2$$

$$U = U_1 - U_2 = -3$$

$$V = Z_1Z_2 = 1$$

$$W = T^2V - U^2(U_1 + U_2) = 0$$

$$Z_3 = U^3V = -27$$

$$X_3 = UW = 0$$

$$Y_3 = T(U_1U^2 - W) - T_1U^3 = 27$$

$$R_H(0{,}27, -27) = R_A(0, -1)$$

Örnek:

$$E\colon\ y^2 = x^3 + 3$$

E eğrisi üzerindeki $P_H(1{,}2{,}1) + Q_H(1, -2{,}1)$ toplamını bulalım.

Çözüm:

$$T_1 = 2, T_2 = -2, T = 4, U_1 = 1, U_2 = 1, U = 0$$

$$V = 1, W = 16, Z_3 = 0, X_3 = 0, Y_3 = -64$$

$$R_H(0, -64{,}0) \approx (0{,}1{,}0)$$

HT2) $P_A = Q_A$ ve $y_1 \neq 0$ için $P_A + P_A$ toplamın bulunması:

i. (4.17) ve (4.18) değerleri (4.13) eşitliğinde yazılırsa

$$m = \frac{3\left(\frac{X_1}{Z_1}\right)^2 + a}{2\left(\frac{Y_1}{Z_1}\right)} = \frac{3{X_1}^2 + a{Z_1}^2}{2Y_1Z_1} \qquad (4.27)$$

olup (4.27) eşitliğinde sırasıyla

$$T = 3{X_1}^2 + a{Z_1}^2$$

$$U = 2Y_1Z_1$$

alınırsa

$$m = \frac{T}{U} \qquad (4.28)$$

elde edilir.

ii. (4.17) ve (4.28) değerleri (4.15) da yazılırsa

$$x_3 = \left(\frac{T}{U}\right)^2 - 2\frac{X_1}{Z_1} = \frac{T^2}{U^2} - \frac{2X_1}{Z_1}.\frac{4{Y_1}^2.Z_1}{4{Y_1}^2Z_1} = \frac{T^2}{U^2} - \frac{4UX_1Y_1}{U^2} = \frac{T^2-4UX_1Y_1}{U^2} \qquad (4.29)$$

olup (4.29) eşitliğinde sırasıyla

$$V = 2UX_1Y_1$$

$$W = T^2 - 2V$$

alınırsa

$$x_3 = \frac{W}{U^2} = \frac{W}{U^2}.\frac{U}{U} = \frac{UW}{U^3} \qquad (4.30)$$

elde edilir.

iii. (4.17), (4.18), (4.28) ve (4.30) değerleri (4.16) da yazılırsa

$$y_2 = \frac{T}{U}\left(\frac{X_1}{Z_1} - \frac{W}{U^2}\right) - \frac{Y_1}{Z_1} = \frac{T}{U}\left(\frac{X_1}{Z_1}.\frac{4{Y_1}^2Z_1}{4{Y_1}^2Z_1} - \frac{W}{U^2}\right) - \frac{Y_1}{Z_1}$$

$$= \frac{T}{U}\left(\frac{V}{U^2} - \frac{W}{U^2}\right) - \frac{Y_1}{Z_1} = \frac{T}{U}\left(\frac{V-W}{U^2}\right) - \frac{Y_1}{Z_1} = \frac{T(V-W)}{U^3} - \frac{Y_1}{Z_1}$$

$$= \frac{T(V-W)}{U^3} - \frac{Y_1}{Z_1}.\frac{8{Y_1}^3{Z_1}^2}{8{Y_1}^3{Z_1}^2} = \frac{T(V-W) - 2U^2{Y_1}^2}{U^3}$$

$$= \frac{T(V-W)-2(UY)^2}{U^3} \qquad (4.31)$$

elde edilir. Son olarak

$$Z_3 = U^3$$

alınırsa (4.30) ve (4.31) eşitliklerinden $R_H(X_3, Y_3, Z_3)$ noktasının koordinatları

$$X_3 = UW$$

$$Y_3 = T(V-W) - 2(UY_1)^2$$

şeklinde elde edilir.

Örnek:

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

eğrisi üzerinde $P_H(1,2,1)$ noktasının kendisi ile toplamını olan $2P_H$ noktasını bulalım.

$$T = 3{X_1}^2 + a{Z_1}^2 = 3$$

$$U = 2Y_1Z_1 = 4$$

$$V = 2UX_1Y_1 = 16$$

$$W = T^2 - 2V = -23$$

$$Z_3 = U^3 = 64$$

$$X_3 = UW = -92$$

$$Y_3 = T(V - W) - 2(UY_1)^2 = -11$$

$$2P_H(-92, -11,64) = 2P_A\left(-\frac{23}{16}, -\frac{11}{64}\right)$$

4.1.2.4. Eliptik eğri skaler nokta çarpma işlemi

Eliptik eğri üzerindeki en temel işlem bir noktanın k skaler sayısı ile çarpımıdır. Eliptik eğri üzerindeki P noktasın bir k tamsayı ile skaler nokta çarpımı aşağıdaki gibi tanımlanır;

$$k.P = \underbrace{P + P + \cdots + P}_{k\ tane}$$

Çok büyük k değeri için $k.P$ değeri işlem maliyetini azalmak için ikile-ve-topla algoritması kullanarak hesaplanır:

Öncelikle $k = (k_{m-1}, k_{m-2}, \dots, k_1, k_0)_2$ formunda yazılır. $i = m-1, m-2, \dots, 1,0$ olmak üzere önce sırasıyla her k_i değeri için $k_i = 1$ ise $2 \times P$ ve $k_i = 0$ için $P + Q$ işlemleri uygulanır.

Örnek olarak $20.P$ değerini bulmak için önce $P, 2.P, 4.P, 8.P$ ve $16.P$ değerleri hesaplanır ve son olarak toplama işlemi ile $4.P + 16.P = 20.P$ istenilen sonuç elde edilir (Yavuz,2008).

E Eğrisi üzerinde verilen $P \neq \infty$ noktasının verilen bir $k \geq 0$ tamsayısı için $k.P$ değeri aşağıdaki algoritma ile hesaplanır.

Adım 1. $Q := \infty$ olarak al.

Adım 2. $k = 0$ ise Q'yu yaz ve bitir.

Adım 3. $k\ (mod\ 2) = 1$ ise $Q := Q + P\ ve\ k := k - 1$ al ve Adım 2'ye git.

Adım 4. $Q := 2 \times P\ ve\ k := k/2$ al ve Adım 2'ye git.

4.1.3. Sonlu cisimler üzerinde eliptik eğriler

$p > 3$ asal, $r \in Z^+$ ve $q = p^r$ olacak şekilde F_q bir sonlu cisim ve $a, b \in F_q$ için

$$y^2 = x^3 + ax + b\ (mod\ p)$$

Kogrüansının $(x, y) \in F_q \times F_q$ çözümleri ve sonsuzdaki noktanın oluşturduğu kümeye F_q üzerinde eliptik eğri denir ve $E(F_q)$ ile gösterilir. $q = p$ için F_p üzerindeki nokta toplama ve skalerle çarpma için algoritmalarını verelim.

4.1.3.1.Sonlu cisimler üzerinde toplama

$E(Z_p)$ eğrisi üzerinde verilen P ve Q noktalarının toplamı aşağıdaki algoritma ile hesaplanır.

Nokta Toplama Algoritması

AT1: $x_1 \neq x_2$ ise: (bkz. Şekil 4.6)

$$m \equiv \frac{y_2 - y_1}{x_2 - x_1}\ (mod\ p)$$

$$x_3 \equiv m^2 - x_1 - x_2 (mod\ p)$$

$$y_3 \equiv m(x_1 - x_3) - y_1 (mod\ p)$$

AT2: $x_1 = x_2$ ise:

AT2.1: $y_1 \neq y_2$ ise: (Bkz. Şekil 4.7)

$$P + Q = \infty$$

AT2.2: $y_1 = y_2$ ise:

AT2.2.1: $y_1 \neq 0$ ise: (Bkz. Şekil 4.9)

$$m \equiv \frac{3(x_1)^2 + a}{2y_1}\ (mod\ p)$$

$$x_3 \equiv m^2 - 2x_1 (mod\ p)$$

$$y_3 \equiv m(x_1 - x_3) - y_1 (mod\ p)$$

AT2.2.2: $y_1 = 0$ ise: (Bkz. Şekil 4.8)

$$P + Q = \infty$$

4.1.3.2.Sonlu cisimler üzerinde nokta sayısı

E eğrisi üzerindeki $(x, y) \in F_q \times F_q$ noktalarının sayısı ile ilgili teoremi vermeden önce aşağıdaki örnekle $y^2 = x^3 + 2$ F_7 üzerindeki noktalarını hesaplayalım.

F_7 üzerindeki $y^2 = x^3 + 2$ eğrisinin noktaları $y^2 \equiv x^3 + 2\ (mod\ 7)$ kongrüansının çözümleri ile hesaplanabilir.

$x = 0$ için $y^2 \equiv 2 (mod\ 7)$ kongrüansının çözümleri 3 ve 4 olup eğri üzerindeki noktalar $(0,3)$ ve $(0,4)$ dir.

$x = 1$ için $y^2 \equiv 3\ (mod\ 7)$ kongrüansının çözümü yoktur.

$x = 2$ için $y^2 \equiv 3\ (mod\ 7)$ kongrüansının çözümü yoktur.

$x = 3$ için $y^2 \equiv 5\ (mod\ 7)$ kongrüansının çözümleri 1 ve 6 olup eğri üzerindeki noktalar $(3,1)$ ve $(3,6)$ dir.

$x = 4$ için $y^2 \equiv 3\ (mod\ 7)$ kongrüansının çözümü yoktur.

$x = 5$ için $y^2 \equiv 1\ (mod\ 7)$ kongrüansının çözümleri 1 ve 6 olup eğri üzerindeki noktalar $(3,1)$ ve $(3,6)$ dir.

$x = 6$ için $y^2 \equiv 1\ (mod\ 7)$ kongrüansının çözümleri 1 ve 6 olup eğri üzerindeki noktalar $(3,1)$ ve $(3,6)$ dir.

Yani toplam 8 tane nokta vardır.

Şayet a ve b değerleri farklı seçildiğinde bu noktalar ve sayılarının değişeceği açıktır. Bu grubun mertebesi eliptik eğrilerin kriptografik uygulamaları açısından son derece önemlidir. Şimdi bu kısımla ilgili Hasse teoremini verelim.

Teorem 2.90: (Hasse teoremi): E, F_q üzerinde bir eliptik eğri olsun. $E(F_q)$ grubunuın mertebesi

$$|q + 1 - \#E(F_q)| \leq 2\sqrt{q}$$

Eşitsizliğini sağlar. Burada $\#E(F_q)$, F_q üzerindeki noktaların sayısı yani $E(F_q)$ grubunuın mertebesidir. Bu durumda $x, y \in F_q$ olan sonlu sayıda (x, y) nokta çifti vardır ve $E(F_q)$ grubu sonludur.

Örnek: $q = 7$ için $8 - 2\sqrt{7} \leq \#E(F_7) \leq 8 + 2\sqrt{7}$ olup $E(F_7)$ grubunun mertebesi eğri denklemindeki a ve b sayılarının farklı seçimlerine bağlı olarak $3, 4, 5, \ldots, 12, 13$ değerlerini alabilir.

Teorem 2.91: $a, b \in Z$ olmak üzere Q üzerindeki E eliptik eğrisi

$$E = \{(x, y) \in Q: y^2 = x^3 + ax + b, a, b \in Z\}$$

olsun. Bu durumda E sonlu tane tamsayı bileşenli noktaya sahiptir (Yücelen, 2011).

4.1.3.3. Sonlu cisimler üzerinde karekök bulma

p bir tek asal sayı, $(a, p) = 1$ olacak şekilde bir a tamsayısı için a, p modülüne göre bir kuadratik rezidü ise $x^2 \equiv a\ (mod\ p)$ kongrüansının çözümü olan x değeri aşağıdaki şekilde hesaplanır:

i. $p = 8k + 3$ ise $x := a^{k+1}\ (mod\ p)$

ii. $p = 8k + 7$ ise $x := a^{k+1}\ (mod\ p)$

iii. $p = 8k + 5$ ve $a^{2k+1} \equiv 1\ (mod\ p)$ ise $x := a^{k+1}\ (mod\ p)$

iv. $p = 8k + 5$ ve $a^{2k+1} \equiv -1\ (mod\ p)$ ise $x := a^{k+1}(2^{3k+1} + 2^k)\ (mod\ p)$

v. $p = 8k + 1$ ise aşağıdaki adımları uygula;

Adım 1: $Q := a$ al.

Adım 2: $0 < P < p$ olacak şekilde rasgele bir P sayısı üret.

Adım 3: $U := U_{2k+1}(mod\ p\ )$ ve $V := V_{2k+1}(mod\ p)$ değerlerini hesapla.

Adım 4: Eğer $U := 0$ ise $x := V/2(mod\ p)$ bitir.

Adım 5: Eğer $V := 0$ ise karekök yok, bitir.

Adım 6: Adım 2'ye git.

4.2. ElGammal Tabanlı Eliptik Eğri Şifreleme Algoritması

Bu şifreleme yönteminde şifreleme, ElGammal şifreleme algoritmasının aritmetik işlemlerinin eliptik eğrilerin F_p sonlu cismi üzerindeki nokta toplama işlemleriyle yapılması esas alınmıştır.

Anahtarları oluşturma:

- E eliptik eğrisi ve bir p asalı belirler.
- $P \in E(F_p)$ olacak şekilde bir P noktası (ortak anahtar) seçer.
- P'nin mertebesi n için $1 < e < n - 1$ aralığında rastgele bir e tamsayısı (Gizli anahtar) seçer.
- $D := e.P\ (mod\ p)$ noktasını (Açık anahtar) hesaplar.
- A, otak anahtar P ve Açık anahtar D'yi B'ye gönderir.

Mesajın şifrelenmesi:

- Şifrelemek istediği mesajı M noktası olsun.
- B, $1 < t < n - 1$ aralığında rastgele bir t tamsayısını seçer.
- $R :\equiv t.P\ (mod\ p)$ ve $S :\equiv t.D + M(mod\ p)$ noktalarını hesaplar ve R ve S'yi A'ya gönderir.

Şifreli mesajın çözümlenmesi:

- A, kendi özel anahtarı olan e sayısını kullanarak $M :\equiv S - e.R\ (mod\ p)$ değerini hesaplar ve açık M'yi elde eder.

Örnek:

Anahtar oluşturma:

- $E: y^2 = x^3 + x + 1$ non-singüler eğri. $(\Delta = 4.1^3 + 27.1^2 = 31 \neq 0)$
- $p = 113$
- $P = (3,12) \in E(F_{113})$
- $25P = \infty$ olup, $1 < e < 24$ için rastgele e sayısı $e = 13$

- $D := 13(3,12) \equiv (71,15)\ (mod\ 113)$

Şifreleme:

- $m = (98,1)$ olsun.
- $t = 9$
- $R := 9(3,12) \equiv (83,54)\ (mod\ 113)$
- $S := 9(71,15) + (98,1) \equiv (71,15)\ (mod\ 113)$

Şifre çözme:

- $M := (71,15) - 13(83,54) \equiv (98,1)\ (mod\ 113)$

4.2.1. Metin şifreleme

Metinler $E(F_q)$ Eliptik Eğrisi üzerinde şifrelerken öncelikle $m \in [0, M]$ olacak şekilde kodlanmış bir m tam sayısına karşılık eliptik eğri üzerinde bir P_m noktasının elde edilmesi gerekir. Öncelikle $M.k < q$ olacak şekilde bir k tam sayısı belirlenir. Burada algoritmanın başarısızlık olasılığı $2^{\frac{1}{k}}$ dır. Daha sonra sırasıyla her bir $j = 1,2, \dots, k-1$ değeri için $x_j = mk + j$ tamsayıları $y^2 = x^3 + ax + b$ denkleminde x yerine yazılarak $y^2 \equiv f(x_j)(mod\ p)$ kongrüansının çözümleri aranır, çözüm bulunduğunda m noktasına karşılık gelen $P_m(x_j, y)$ noktası hesaplanmış olur. Tersine tam değer fonksiyonu kullanılarak $\left\lfloor \frac{x_j}{k} \right\rfloor = m$ ile $P_m(x_j, y)$ noktasından m açık mesajı kolayca hesaplanabilir (Link2, 2021).

Örnek:

Öncelikle metni oluşturan karakterlerin her biri için birer doğal sayı gelecek şekilde birer bir eşleme tablosu oluşturulur.

$$A = 1, B = 2, C = 3, Ç = 4, \dots, Z = 29$$

Eliptik eğri üzerindeki nokta sayısı en az 29 olacak şekilde bir p asalı belirleyelim.

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

Eğrisi için $p = 113$ alınırsa Hasse teoreminden $114 - 2\sqrt{113} \leq \#E(F_q) \leq 114 + 2\sqrt{113}$ olup (F_q) grubunun mertebesi [93,135] olup bu aralık tabloda verilen değerleri şifrelemek için yeterli bir aralıktır.

Şifrelenecek mesaj "M" olarak seçelim. Bu harfin tablodaki karşılığı 16 olup öncelikle 16 sayısına karşılık eliptik eğri üzerinde bir nokta belirleyelim. $16.k < 113$ eşitsizliğine uyun en büyük tam sayı $k = 6$ olarak seçelim. $j = 1,2, \ldots ,5$ için

$$x_j = 16.6 + j = 97,98,99,100,101$$

Tam sayıları sırasıyla $y^2 = x^3 + x + 1\ (mod\ 113)$ denkleminde yazılırsa $j = 2$ için

$$1^2 \equiv (98^3 + 98 + 1)\ (mod\ 113)$$

Olup $P(98,1)$ noktası eğri üzerindedir. Bir önceki örnekte bu noktanın eğri üzerindeki şifreleme ve şifre çözme adımları mevcut olup bu noktadan açık metin olan 16=M mesajı Tersine $\left\lfloor \frac{98}{6} \right\rfloor = 16$ şeklinde kolaya hesaplanabilir.

4.3. Eliptik Eğri Çarpanlara Ayırma Algoritması

Tam Sayılarının çarpanlara ayrılması problemi özellikle RSA şifreleme yönteminde önemli olup Eliptik Eğriler şifrelemenin yanı sıra Tam Sayıların çarpanlarının bulunması içinde kullanılmaktadır.

P eliptik eğri üzerinde bir nokta olsun. Sonlu Cisimler üzerinde Eliptik Eğri Skaler Nokta Çarpımı olan $k.P$ değeri hesaplanırken (4.8) ile hesaplanan m değeri Modül n'de tanımsız olduğunda $x_1 - x_2$ Modül n'ye göre terslenemezdir. Teorem (2.17) göz önüne alınırsa $ebob(x_1 - x_2, n) = d > 1$ dir. Eğer $d \neq n$ ise $d|n$ dir. Benzer olarak (4.13) ile verilen m değeri Modül n'de tanımsız olduğunda, $y_1 = 0\ (mod\ n)$ olup yani y_2 Modül n'ye göre terslenemezdir. Teorem (2.17) göz önüne alınırsa $ebob(y_1, n) = d > 1$ dir. Eğer $d \neq n$ ise $d|n$ dir. Sonuç olarak, E eliptik eğrisi üzerinde bir Π noktası ve büyük bir k tamsayısı için $k.P$ skaler çarpımı hesaplarken $P + Q$ veya $2P$ toplamı tanımsız olduğunda ν sayısının bir bölenini bulunmuş olur.

5. SONUÇ

Tezde eliptik eğrilerin şifrelemede kullanımı konusu ele alınmıştır. İlk olarak düzlemde eğrilerin cebirsel özelliklerine yer verilmiştir. Daha sonra simetrik ve asimetrik şifreleme algoritmaları ve bu sınıfta yer alan RSA ve ElGammal asimetrik şifreleme algoritmaları anlatılmıştır.

Tez konusu olan Eliptik Eğri Şifreleme algoritmasının tam olarak anlaşılması bakımında eliptik eğrilerin cebirsel yapısı, eliptik eğriler üzerinde nokta toplama işlemi, eliptik eğrilerin grup yapısı ve sonlu cisimler üzerinde eliptik eğriler incelenip örneklerle desteklenmiştir. Son olarak ElGammal tabanlı eliptik eğri şifreleme algoritması ile metin şifreleme ve eliptik eğrilerin Kriptanalizde kullanımı olarak Eliptik Eğri Çarpanlara Ayırma algoritmaların incelenip örnekler verilmiştir.

KAYNAKLAR

Altındiş , H., (2005) "Sayılar teorisi ve uygulamaları" , 2. Baskı, ***Erciyes Üniversitesi Fen Fakültesi Matematik Bölümü***, Kayseri, 1-141.

Altındiş, H. (2010) Sayılar teorisi ve uygulamaları 3. Baskı, ***Erciyes Üniversitesi Fen Fakültesi Matematik Bölümü***, Ankara.

Arjen, K, Lenstra and H. W. Lenstra, Jr (eds). (1993) " The development of the number field sieve". Lecture Notes in Math. 1554. Springer-Verlang.

Asar, O., Arıkan,. A., ve Arıkan, A., (2009) "Cebir", ***Eflatun yayınevi*** , Ankara.

Asar, O., ve Arıkan, A.., (2012) "Sayılar Teorisi", ***Gazikitavevi***, Ankara

Atay S., "Eliptik Eğri Kriptosistem Yazılım Uygulamalarında Hız Problemi", ***Ege Üniversitesi fen Bilimleri Enstitüsü***, Doktora Tezi, İzmir, (2006).

Aybak , L. (2010) "Sayı Cismi Çarpanlara Ayırma Yöntemi", ***Yüksek Lisans Tezi***, Ankara Üniversitesi Fen Bilimleri Enstitüsü,Ankara.

Balcı, M. (1997) "Analiz", Cilt 2, ***Balcı yayınları***, Ankara.

Balcı, M. (1999) "Analiz", Cilt 1, ***Balcı yayınları***, Ankara.

Balcı, M. (2012) "Analitik Geometri", ***Sürat Üniversite yayınları***, İstanbul.

Bayraktar, M. (2010) "Analiz", ***Nobel yayın dağıtım***, Ankara.

Bayraktar. (2010) Soyut Cebir ve Sayılar Teorisi, ***Gazi Kitapevi***, Ankara

Bütün, N. (2018) "RSA Kriptosistemleri ve $p-1$ Çarpanlara Ayırma Algoritması", ***Yüksek Lisans Tezi***, Erzincan.

Çallıalp, F. (2009) "Soyut Cebir", ***Birsen Yayınevi***, İstanbul.

Diffie, W., Hellman, M, (1976) "New directions in crytography", ***IEEE Transaction on Informations Theory***,IT-22,644-654.

ElGamal, T. (1985) "A public-key cryptosystem and a signature scheme based on discrete logaritms", ***IEEE Transactions on Information Theory***, 31(4), 469-472.

Fraleigh, J. B., (2002) "A First Course in Abstract Algabra", Historical Notes by Victor ***Katz, Univesty of District of Columbia.*** **7th. Ed.**

Hacısalihoğlu, H. (1982) "Diferansiyel Geometri", ***Ankara Üniversitesi Fen Fakültesi,*** Ankara.

Hacısalihoğlu, H.H. (1998) "Diferensiyel Geometri", ***Fen Fakültesi Yayınları, Ankara Üniversitesi, Cilt I***

K. Lenstra, H.W. Lenstra, Jr., M. S. Manasse, J.M. Pollard, (1990) The number Md sieve, in preparation. Extended abstract: Proc. 22nd Ann. ACM Symp. ***On Theory of Computing*** (STOC), 564-572.

Karlıağa, B. (2002) ”Düzlemde Analitik Geometri”, ***Gazi Üniversitesi***, Ankara, 129-165.

Keyman, E., Yıldırım, M. (2004) “Kriptoloji Giriş Ders Notları”,***Uygulamalı Matematik Enstitüsü,Kriptoloji Bölümü ODTÜ***

Koblitz, N. (1987) “Elliptic Curve Cryptosystems”, ***Math. Comp. Vol: 48, 203-209.***

Koblitz, N. (1994) “A course in Number Theory and Cryptography”, ***Springer Verlag.***

Koblitz, N., (1984) “Introduction to Elliptic Curves and Modular Form, Graduate Text in Mathematics”, ***Vol. 97, Springer Verlag, New York***.

Lentra, H. W. Jr. (1987) “Factoring integers with elliptic curves”, Annals ***Mathematics***,126,679-673.

Link1:https://www.nayuki.io/page/elliptic-curve-point-addition-in-projective-coordinates Son Erişim Tarihi:09.10.2021

Mahir, N. (1999) “ Analitik Geometri”,***Anadolu Üniversitesi Yayınlar,no:1077***

Menezes, A. J., Oorschot, P. C. V. and Vanstone, S. A. (1996) “***Handbook of Applied Cryptography***”, CRC Press.

Miller, V. (1986) “Uses of Elliptic Curves in Cryoptagtsphy, in Advances in Cryptography, Crypto 85”, ***Springre Verlag, Vol 218 pp. 417-426.***

Nasibov, F., Hacısalihoğlu,H., ve Kılıçoğlu, Ş. (2010) ”***Sayılar Teorisi***”, Seçkin yayıcılık, Ankara.

Okumuş, İ. (2012) “RSA Kriptosisteminin Hızını Etkileyen Faktörler”, ***Doktora Tezi***, Atatürk Üniversitesi Fen Bilimleri Enstitüsü, Erzurum.

Polard, J. M. (1974) “Theorems of factorization and primality testing”,***Proceedings of the Cambridge Philosophical Society***, 76(3),521-528.

Polat, K, M. (2018) “Lucas Sayı Dizisinin Bir Uygulaması Olarak $p+1$ Algoritması”, ***Yüksek Lisans Tezi***, Erzincan.

Riverst, R., Shamir, A. and Adleman, L. (1978) “A Method for obtaining digital signatures and public-key cryptosystems” ***Communications of the ACM, v.*** 21(2), 120-126.

Rotman, j. J., “A first Course in Abstract Algebra with Applications” ***Pearson Prentice Hall, Third Edition.*** New Jersey.

Sabuncuoğlu , A., (2004) “Diferensiyel Geometri” 2.Baskı, ***Nobel Yayın Dağıtım***,Ankara, 556s.

Sabuncuoğlu, A. (2011) ”Çözümlü Analitik Geometri Alıştırmaları”, ***Nobel yayın dağıtım***, Ankara.

Sabuncuoğlu, A. (2012) ”Analitik Geometri”, ***Nobel yayın dağıtım***, Ankara.

Schneider B. (1996) “ Applied Crytoraphy Second Edition”, ***John Wiley and Sons, Inc.,*** New York.

Silverman H. J, (1986) “The aritmetic of elliptic curves”, Graduate Text in mathematics”, ***vol. 106, Springer Verlag, New York.***

Silverman J. S., (1985) “ The Aritmetic of Eliptic Curves”, ***Springer***, New York, 41-66.

Şahin, M. “ Ankara Üniversitesi Açık Ders Notları”, Link2:https://acikders.ankara.edu.tr/course/view.php?id=26 Son erişim tarihi:15.11.2021.

Taşçı D., (2011) “Lineer Cebir”, ***Öziş Matbaacılık***, 4. Baskı, Ankara.

Taşçı, D. (2007) Soyut Cebir, ***Alp Yayınevi***, Ankara.

Taşçı, D. (2010)“Soyut Cebir”, ***Öziş Matbaacılık***, 2. Baskı, Ankara.

Williams, H. C. (1982) “A $p+1$ method of factoring”, ***Mathematics of Computation 39 (159): 225-234.***

Yavuz, İ. (2008) “Eliptik Eğri Kriptosisteminin FPGA Üzerinde Gerçekleşmesi”, ***Yüksek Lisans Tezi***, İstanbul Teknik Üniversitesi Fen Bilimleri Ensitüsü, İstanbul.

Yücelen , A., M. (2017) “Krıptolojide Eliptik Eğri Algoritmasının Uygulanması”, ***Mühendislik dergisi***, 8(3), 504-511.

Yücelen, A. M. (2011) “Kriptolojide Eliptik Eğri Algoritması”, ***Yüksek Lisans Tezi***, Dicle Üniversitesi Fen Bilimleri Enstitüsü, Diyarbakır.

EKLER

Ek-1. Tez Çalışması Süresince Yapılan Akademik Çalışmalar

Okumuş, İ., **Işıklı, B.,** (2021) “On the Infinity Point of the Elliptic Curves”, 5 th International Conference On Computational Mathematics and Engineering Sciences, 2021 Van Turkey.