T.C.
ERZİNCAN BİNALİ YILDIRIM ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

LUCAS SAYI DİZİSİNİN BİR UYGULAMASI OLARAK $P+1$ ALGORİTMASI

Mehtap Kübra POLAT

Danışman: Dr. Öğr. Üyesi İsrafil OKUMUŞ

MATEMATİK ANABİLİM DALI

ERZİNCAN
2018
Her Hakkı Saklıdır.

Kabul ve Onay Sayfası

Dr. Öğr. Üyesi İsrafil OKUMUŞ danışmanlığında, Mehtap Kübra POLAT tarafından hazırlanan bu çalışma 27/11/2018 tarihinde aşağıdaki jüri tarafından Matematik Anabilim Dalı'nda Yüksek Lisans Tezi olarak oybirliği/~~oy çokluğu~~ (3./.3) ile kabul edilmiştir.

Başkan	: Prof. Dr. Ekrem KADIOĞLU	İmza:
Üye	: Dr. Öğr. Üyesi İsrafil OKUMUŞ	İmza:
Üye	: Dr. Öğr. Üyesi Tufan ÖZDİN	İmza:

Yukarıdaki sonuç Enstitü Yönetim Kurulunun 20 / 12 / 2018 tarih ve 46./.11..... sayılı kararı ile onaylanmıştır.

Prof. Dr. Mustafa Fatih ERTUGAY
Enstitü Müdürü

Not: Bu tezde kullanılan özgün ve başka kaynaklardan yapılan bildirişlerin, şekil ve tabloların kaynak olarak kullanımı, 5846 sayılı Fikir ve Sanat Eserleri Kanunundaki hükümlere tabidir.

Bilimsel Etiğe Uygunluk Sayfası

"Lucas Sayı Dizisinin Bir Uygulaması Olarak $p+1$ Algoritması" isimli "Yüksek Lisans" tezim tarafımca intihal tespit programı ile incelenmiştir. Buna göre tezimde bilimsel etik ihlali ve intihal olarak nitelendirilebilecek herhangi bir durum olmadığını taahhüt ederim.

Bu çalışmadaki tüm bilgilerin, akademik ve etik kurallara uygun bir biçimde elde edildiğini; aynı zamanda bu kural ve davranışların gerektirdiği gibi, bu çalışmanın özünde olmayan tüm materyal ve sonuçları tam olarak aktardığımı ve referans gösterdiğimi beyan ederim. 27/11/2018

Mehtap Kübra POLAT

ÖZET

Yüksek Lisans Tezi

LUCAS SAYI DİZİSİNİN BİR UYGULAMASI OLARAK $P+1$ ALGORİTMASI

Mehtap Kübra POLAT

Erzincan Binali Yıldırım Üniversitesi
Fen Bilimleri Enstitüsü
Matematik Anabilim Dalı

Danışman: Dr. Öğr. Üyesi İsrafil OKUMUŞ

Rivest, Shamir ve Adleman tarafından 1978 yılında ilk açık anahtarlı kripto sistem olan ve günümüzde yaygın olarak şifreleme ve elektronik imza algoritması olarak kullanılan RSA algoritması geliştirildi. Williams 1982 yılında Lucas sayı dizilerinin n. teriminin hesaplanması için hızlı bir algoritma oluşturarak ve Lehmer'in 1930 yılında Lucas sayı dizisi ile ilgili verdiği teoremi kullanarak RSA kripto sistemine karşı kullanılan bir çarpanlara ayırma algoritması önerdi.

Bu tezde sırası ile; RSA kripto sistemi ve bu kripto sistem için geliştirilen özel amaçlı çarpanlara ayırma algoritmalarının kısa özetleri verilmiş, bunlardan önemli bir tanesi olan $p+1$ algoritması teorik altyapısı ile birlikte detaylı olarak ele alınmıştır.

2018, 55 Sayfa

Anahtar Kelimeler: Çarpanlara ayırma algoritmaları, Lucas sayı dizisi, $p+1$ algoritması, RSA, Şifreleme

ABSTRACT

Master Thesis

$P+1$ ALGORITHM AS AN APPLICATION OF LUCAS NUMBER SEQUENCE

Mehtap Kübra POLAT

Erzincan Binali Yıldırım University
Institute of Natural and Applied Sciences
Department of Mathematics

Supervisor: Asist. Prof. Dr. İsrafil OKUMUŞ

RSA algorithm which is the first public key cryptosystem and which is widely used as enciphering and electronic signature algorithm nowadays was developed by Rivest, Shamir Adleman in 1978. Williams proposed a factoring algorithm which was used against RSA algorithm cryptosystem by creating a fast algorithm to calculate n. term of Lucas number system in 1982 and using the theorem which was given about Lucas number system by Lehmer in 1930.

In this thesis, RSA cryptosystem and brief summary of purpose made factoring algorithms which were developed for this cryptosystem were given respectively. An important one of these, $p+1$ algorithm were reviewed with its theoretical substructure in detail.

2018, 55 Pages

Keywords: Encryption, Integer factorization algorithms, Lucas number sequence, $p+1$ Algorithm, RSA

TEŞEKKÜR

Yüksek Lisans eğitimim boyunca desteğini hiçbir zaman esirgemeyen, bilgi ve tecrübelerinden faydalandığım danışmanım Sayın Dr. Öğr. Üyesi İsrafil OKUMUŞ hocama teşekkürlerimi sunuyorum.

Savunma sürecinde kıymetli görüşlerini ve tecrübelerini paylaşan Sayın Prof. Dr. Ekrem KADIOĞLU ve Sayın Dr. Öğr. Üyesi Tufan ÖZDİN hocalarıma ayrıca teşekkür ederim.

Bu günlere gelmemde büyük pay sahibi olan annem Hatice Polat'a teşekkür ederim.

Mehtap Kübra POLAT
Kasım, 2018

İÇİNDEKİLER

Sayfa

ŞEKİLLER LİSTESİ

Sayfa

TABLOLAR LİSTESİ

Sayfa

SİMGELER ve KISALTMALAR

Simgeler

$a\|b$	a böler b'yi
(a,b)	a ile b nin en büyük ortak böleni
C	Şifreli Metin
d	RSA'da Özel Anahtar
e	RSA'da Genel Anahtar
F_n	Fibonacci sayı dizisi
L_n	Lucas sayı dizisi
M	Açık Metin
$\mathbb{N}$	$\{1,2 \dots\}$ kümesi
$\mathbb{N}_0$	$\{0,1,2, \dots\}$ kümesi
$n\mathbb{Z}$	$\{0, \pm n, \pm 2n, \dots\}$ kümesi
$U_n(P,Q)$, U_n	(P,Q)-Genelleştirilmiş Fibonacci dizisi
$V_n(P,Q)$, V_n	(P,Q)-Genelleştirilmiş Lucas dizisi
$\mathbb{Z}$	Tam sayılar kümesi
$\mathbb{Z}_n$	$\{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$ kümesi
$\equiv$	Denk
Δ	Diskriminant
$\boldsymbol{\Delta}$	İleri fark operatörü
ε	Legendre Değeri
$\phi(n)$	Euler Phi Fonksiyonu

Kısaltmalar

RSA	Rivest, Shamir, Adleman

1. GİRİŞ

Gizli haberleşme yaklaşık 4000 yıl önce kullanılmaya başlanmış; askeri ve diplomasi alanlarında önemli bir yere sahip olmuş, II. Dünya Savaşı gibi modern savaşların seyrini değiştirmiştir.

Günümüzde internet üzerindeki haberleşmelerin güvenliği, elektronik imza ve dijital paraların dijital cüzdanlar arasında güvenli transferi gibi birçok alanda kullanılmaktadır.

Kriptoloji, Yunanca "kript"→gizli ve "loji"→bilim kelimelerinden türetilmiş olup şifreleme bilimi olarak değerlendirilir. Kriptoloji, Kriptografi ve Kriptanaliz olmak üzere iki alt bölüme ayrılır. Kriptografi şifreleme algoritmalarının oluşturulması veya geliştirilmesi, kriptanaliz ise şifreleme algoritmalarının kırılmasında ve açıklarının tespit edilmesinde kullanılan tekniklerin güvenliği üzerine çalışılan alt bilim dalıdır.

20. yüzyılın ortalarından itibaren geliştirilen modern şifreleme algoritmalarının güvenliği anahtar olarak adlandırılan sayılarla sağlanmaktadır. Şifrelenmek istenen metnin her bir harfi sayısallaştırıldıktan sonra anahtar adı verilen sayı/sayılar kullanılarak şifreleme ve şifre çözme işlemleri gerçekleştirilir. Kriptografik algoritmalar kullandıkları anahtar biçimine göre iki kısımdan oluşmaktadır;

- Simetrik Kriptografik Algoritmalar (Tek anahtarlı)
- Asimetrik Kriptografik Algoritmalar (Çift anahtarlı)

Simetrik kriptografik algoritmalar olarak adlandırılan şifreleme algoritmalarında mesajı şifrelemek ve şifrelenmiş mesajın şifresini çözmek için kullanılan anahtar aynıdır. Bu şifreleme algoritmalarında mesajı şifrelemek isteyen kişi öncelikle bir anahtar üretir ve bu anahtar hem şifreleme hem de şifre çözme işlemleri için kullanılır. Bu algoritmaların güçlü yanı hızlı olmalarıdır. Bunun yanında tek anahtar kullanıldığından şifreli metinlerin alıcı tarafından çözümlenmesinde anahtarın da farklı bir yoldan alıcıya ulaştırılması nedeniyle anahtar dağıtım problemine sahiptir. Bu dezavantajlarından ötürü bu algoritmalar elektronik imza için kullanılamazlar.

Asimetrik kriptografik algoritmalar olarak adlandırılan şifreleme algoritmalarında ise mesajı şifrelemek ve şifrelenmiş mesajın şifresini çözmek için kullanılan anahtarlar

farklıdır. Bu şifreleme algoritmalarında aralarında matematiksel bir ilişki bulunan bir genel anahtar ve bir özel anahtar üretilir. Herhangi bir düz metni şifrelemek için genel anahtar, şifreli mesajı çözmek için ise özel anahtar kullanılır. Bu algoritmalara açık anahtarlı algoritmalar da denilmektedir. Bu algoritmalar anahtar dağıtım problemine sahip değildirler fakat simetrik algoritmalara nazaran fazla işlem gücü gerektirdiğinden daha yavaş çalışmaktadırlar. Günümüzde kullanılan bazı asimetrik algoritmalar şunlardır:

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

Diffie ve Hellman'ın 1976 yılında "*New Directions in Cryptography*" adlı makalelerinin yayınlanması kriptografi tarihinin en önemli gelişmesi olmuştur. Bu makalede simetrik kriptografik algoritmalarda kullanılan güvenli anahtar değişimi için bir matematiksel teknik vermişlerdir.

1978 yılında Ron Rivest**,** Adi Shamir ve Leonard Adleman "*A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*" adlı makalelerinde iletilecek mesajı şifreleme ve elektronik imza amacıyla kullanılan ilk asimetrik şifreleme algoritması olan RSA algoritmasını vermişlerdir. Algoritmanın güvenliği büyük tam sayıları çarpanlarına ayırmanın algoritmik zorluğuna dayanır. Verilen herhangi iki asal sayıyı çarpmak kolay olmasına rağmen, verilen bir tam sayının çarpanlarını bulmak kolay değildir.

Taher El-Gamal 1985'te, "*A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms*" adlı makalesinde güvenliği Discrete Logaritma probleminin zorluğuna dayanan diğer bir pratik asimetrik şifreleme ve elektronik imza algoritmasını sunmuştur.

RSA algoritmasının kırılması RSA'da kullanılan anahtarın bir parçası olan ve genellikle iki büyük asal sayının çarpımından oluşan sayının çarpanlarına ayrılmasıyla mümkündür.

Büyük sayıları çarpanlarına ayırmanın zorluğuna karşılık henüz etkili bir yöntem bulunmuş değildir. Çarpanlara ayırma algoritmaları genel amaçlı ve özel amaçlı olarak iki gruba ayrılmaktadır. Genel amaçlı çarpanlara ayırma algoritmalarının çalışma süreleri çarpanlarına ayrılacak sayının büyüklüğüne, özel amaçlı çarpanlara ayırma algoritmalarının çalışma süreleri ise çarpanlarına ayrılacak sayıyı oluşturan çarpanların bazı özelliklerine bağlıdır. Bu algoritmaların çalışma süreleri ile ilgili detaylı bilgi üçüncü bölümde verilmiştir.

Fermat (~ 1640), Euler (~ 1750), Legendre (~ 1790), Gauss (~ 1800) gibi ünlü matematikçilerin tam sayıları çarpanlara ayırma ile ilgili çeşitli çalışmaları olmuştur.

Genel amaçlı çarpanlara ayırma algoritması olarak, Pomerance (1981)'de "Quadratic Sieve" algoritmasını, Lenstra vd. (1990) günümüzde en hızlı genel amaçlı çarpanlara ayırma algoritması olarak bilinen "General Number Field Sieve" algoritmasını geliştirmiştir.

Özel amaçlı çarpanlara ayırma algoritması olarak Pollard (1974) $p-1$ algoritmasını, Lenstra (1987) Eliptik Eğri Çarpanlara Ayırma algoritmasını, Pollard (1988) Özel Sayı Cismi Elemesi olarak adlandırılan algoritmayı geliştirmişlerdir.

Fibonacci sayıları 13. yüzyılda yaşamış ünlü İtalyan matematikçi Leonardo Fibonacci tarafından tanımlanmıştır. İlk ve en iyi bilinen kitabı Liber Abaci'yi 1202 yılında yazmıştır. Binet (1843) Fibonacci sayı dizisinin terimlerini veren ve kendi ismiyle anılan formülü verdi.

Lucas (1878), Lucas sayı dizilerini ve bu dizilere ait bazı özellikleri ortaya koydu. Lehmer (1930) Lucas fonksiyoları ile ilgili bazı teoremler ortaya koydu. Williams (1982) Lucas fonksiyonlarının özelliklerini kullanarak $p+1$ algoritmasını geliştirdi.

Ülkemizde, Fibonacci, Lucas, Pell, Jacobsthal vb. sayı dizileri ve bu sayı dizilerinin özellikleri ile ilgili lisansüstü çalışmalar yapılmıştır. Ayrıca asal sayılar, çarpanlara ayırma algoritmaları, kriptoloji ve RSA üzerine farklı ana bilim/bilim dallarında lisansüstü çalışmalar yapılmıştır.

Pamukçu (2006) "Kriptografi için Faktorizasyon Metodları" isimli yüksek lisans tezi hazırlamıştır. Aybak (2010) "Sayı Cismi Çarpanlara Ayırma Yöntemi" isimli yüksek

lisans tezi hazırlamıştır. Nuriyeva (2010) “Çarpanlara Ayırma Algoritmaları” isimli yüksek lisans tezi hazırlamıştır.

YÖK Ulusal Tez Merkezi veri tabanında “tez adı” ile ilgili olarak taratılan anahtar kelimelerle ile yapılan taramalar sonucunda, kriptoloji alanı ile ilişkili istatistiksel bilgiler aşağıdaki Tablo 1.1’de verilmiştir.

Tablo 1.1. Şifreleme konusu ile ilgili YÖK Ulusal Tez Merkezi veri tabanından elde edilen sayısal veriler

Bilim Dalları	**Matematik**		**Bilgisayar Mühendisliği Bilimleri**		**Elektrik-Elektronik Mühendisliği Bilimleri**		**Fizik ve Fizik Mühendisliği**	**İstatistik**
Taratılan Anahtar Kelimeler	Yüksek Lisans	Doktora	Yüksek Lisans	Doktora	Yüksek Lisans	Doktora	Yüksek Lisans	Yüksek Lisans
Asal Sayılar	4	1	-	-	-	-	-	-
Çarpanlara Ayırma	5	2	-	-	-	-	-	-
Eliptik Eğri	4	1	9	2	11	-	-	-
Kriptanaliz-Kriptoanaliz	3	-	9	2	3	-	-	-
Kriptografi	14	4	28	4	7	5	1	1
Kriptoloji	6	-	5	-	1	1	-	-
RSA	1	1	10	1	6	-	-	-
Şifreleme	15	1	63	14	35	4	1	-
Toplam	**52**	**10**	**124**	**23**	**63**	**10**	**2**	**1**

(İlgili veriler Ulusal Tez Merkezi veri tabanından, 04.11.2018 tarihli tarama sonucunda elde edilmiştir.)

Tablo 1.1'deki verilerden anlaşılacağı gibi kriptoloji bilimi, matematik alanının yanında özellikle Elektrik – Elektronik Mühendisliği ve Bilgisayar Mühendisliği alanlarının da çalışma konusudur. Bu çalışmada matematik dışındaki araştırmacıları da göz önüne alarak çalışma konusunun matematiksel temelleri elementer seviyede ve ayrıntılı olarak verilmeye çalışılmıştır.

Bu çalışma beş bölümden oluşmaktadır. Giriş bölümünden sonra Kuramsal Temeller adı verilen ikinci bölümde çalışmada kullandığımız temel tanım, teorem ve kavramlar ile birlikte Lucas sayı dizileri hakkında bazı temel bilgiler verilmiştir.

Materyal ve Yöntem adı verilen üçüncü bölümde, RSA kripto sistemi ile bu kripto sistemin kriptanalizi için geliştirilen özel amaçlı bazı algoritmalar hakkında özet niteliğinde bilgiler verilmiştir.

Araştırma Konusu adı verilen dördüncü bölümde, RSA kripto sisteminin kriptanalizi için Lucas sayı dizilerinin bazı özellikleri kullanılarak geliştirilen $p+1$ özel amaçlı çarpanlara ayırma algoritması verilmiştir.

Son bölüm olan Sonuç bölümünde, özel amaçlı çarpanlara ayırma algoritmalarından biri olan $p+1$ algoritmasına karşı dayanıklı asal sayı üreten Gordon Algoritması hakkında özet niteliğinde bilgi verilmiştir.

2. KURAMSAL TEMELLER

Şifreleme bilimi üzerine lisansüstü düzeyde matematik ve mühendislik alanlarında disiplinler arası çalışmalar yapıldığından, mühendislik alanlarında çalışmalar yapan araştırmacılar için bu bölümde verilen temel tanım ve teoremlerin daha kolay anlaşılması için temel düzeyde örnekler verilmeye çalışılmıştır.

Bu bölümde araştırma konumuz olan özel amaçlı çarpanlara ayırma algoritmalarında kullanılan bazı temel tanım ve teoremler verilmiştir.

2.1. Sayılar Kuramı

Tanım 2.1: $a, b \in \mathbb{Z}$ ve $a \neq 0$ olsun. Eğer $b = at$ olacak biçimde bir $t \in \mathbb{Z}$ varsa a, b yi böler, denir ve $a|b$ ile gösterilir. Eğer a, b yi bölmez ise bu durum $a \nmid b$ ile gösterilir. (Altındiş, 2011).

Teorem 2.2: $a, b, c \in \mathbb{Z}$ olsun. Aşağıdaki özellikler sağlanır:

i. $a|b$ ve $b|c$ ise $a|c$ dir.
ii. $a|b$ ve $a|c$ ise her $x, y \in \mathbb{Z}$ için $a|(bx + cy)$ dir. (Asar vd., 2012).

Teorem 2.3 (Bölme Algoritması): $a, b \in \mathbb{Z}$ ve $a > 0$ olsun. Öyle $q, r \in \mathbb{Z}$ vardır ki

$$b = qa + r \text{ ve } 0 \leq r < a$$

dır. Ayrıca q ve r tek türlü belirlidir. (Asar vd., 2012).

Tanım 2.4: $p > 1$ tam sayısına kendisinden ve 1 den başka pozitif böleni yoksa asaldır denir. 1 den büyük herhangi bir tam sayı asal değilse bileşik sayı adını alır. (Altındiş, 2011).

Teorem 2.5: Eğer n bileşik sayı ise n nin $\sqrt{n}$ yi geçmeyen bir asal böleni vardır. (Altındiş, 2011).

Örnek: $\sqrt{101} \leq 11$ olup, $2 \nmid 101$, $3 \nmid 101$, $5 \nmid 101$ ve $7 \nmid 101$ olduğundan 101 asaldır.

Tanım 2.6: a ve b tam sayılar olmak üzere $d|a$ ve $d|b$ şartlarını sağlayan $d > 0$ tam sayısına bu iki tam sayının ortak böleni denir. a ve b tam sayılarının ortak bölenlerinin en büyüğüne bu sayıların en büyük ortak böleni denir ve (a, b) ile gösterilir. $(a, b) = 1$ ise a ve b sayılarına aralarında asal denir. (Taşçı, 2007).

Teorem 2.7: a ve b tam sayılarının ikisi birden sıfır olmamak üzere $(a, b) = d$ ise d sayısı, $ax + by$ şeklindeki bütün pozitif tam sayılar kümesinin en küçük elemanıdır. (Altındiş, 2011).

Teorem 2.8: $(a, b) = d$ olması için gerek ve yeter şart $d > 0$ ve ayrıca,

i. $d|a$ ve $d|b$,
ii. Her $c|a$ ve $c|b$ şartlarını sağlayan c tam sayısı için $c|d$

olmasıdır. (Altındiş, 2011).

Teorem 2.9 : (Euclid Algoritması) a, b tam sayılar ve $a > 0$ olsun. Bölüm algoritması art arda uygulanarak aşağıdaki eşitlikler elde edilir.

$$\begin{aligned}
b &= q_0 a + r_0, & 0 \le r_0 < a \\
a &= q_1 r_0 + r_1, & 0 \le r_1 < r_0 \\
r_0 &= q_2 r_1 + r_2, & 0 \le r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3, & 0 \le r_3 < r_2 \\
&\vdots & \vdots \\
r_{s-2} &= q_s r_{s-1} + r_s, & 0 \le r_s < r_{s-1} \\
r_{s-1} &= q_{s+1} r_s + 0 & r_{s+1} = 0
\end{aligned}$$

Burada öyle bir en küçük $s \ge 0$ vardır ki $r_{s+1} = 0$ dır. Bu durumda $(a, b) = r_s$ dır. Ayrıca Teorem 2.7 gereğince $d = ax + by$ olacak şekildeki x, y tam sayıları bulunabilir. Yukarıdaki eşitliklerden sırasıyla $r_{s-1}, r_{s-2}, \dots, r_0$ değerleri bir önceki eşitliklerde yerine yazılarak $r_s = ax + by$ eşitliğini sağlayan x, y tam sayıları bulunur. (Asar vd., 2012).

Örnek: 288, 51 tam sayı çiftinin ebobunu hesaplayalım.

$$288 = 5.51 + 33$$

$$51 = 1.33 + 18$$

$$33 = 1.18 + 15$$

$$18 = 1.15 + 3$$

$$15 = 5.3 + 0$$

buradan $(288{,}51) = 3$ olduğu görülür.

Ayrıca $3 = 288.x_0 + 51.y_0$ eşitliğini sağlayan x_0 ve y_0 değerlerini bulmak için öncelikle son satır hariç yukarıdaki eşitliklerde kalanlar yalnız bırakılır.

$$33 = 288 - 5.51$$

$$18 = 51 - 1.33$$

$$15 = 33 - 1.18$$

$$3 = 18 - 1.15$$

Daha sonra sondan başa doğru sırasıyla tüm eşitlikler kullanılarak aşağıdaki işlemler yapılır.

Son eşitlikte 15 yerine bir önceki eşitlikteki $33 - 1.18$ değeri yazılır,

$$\begin{aligned} 3 &= 18 - 1.15 \\ &= 18 - 1.(33 - 1.18) \\ &= -1.33 + 2.18 \end{aligned}$$

burada 18 yerine $51 - 1.33$ değeri yazılır,

$$\begin{aligned} 3 &= -1.33 + 2.18 \\ &= -1.33 + 2.(51 - 1.33) \\ &= 2.51 - 3.33 \end{aligned}$$

son olarak 33 yerine $288 - 5.51$ değeri yazılır,

$$\begin{aligned} 3 &= 2.51 - 3.33 \\ &= -2.51 - 3.(288 - 5.51) \end{aligned}$$

$$= -3.288 + 17.51$$

Buradan $x_0 = -3$ ve $y_0 = 17$ değerleri elde edilir.

Tanım 2.10: $m > 0$ tam sayı ve $a, b \in \mathbb{Z}$ olsun.

$$a \equiv b \pmod{m} \Leftrightarrow m|(a-b)$$

ile tanımlanan denklik bağıntısına kısaca kongrüans denir. Ayrıca a ve b, m modülüne göre birbirine kongrüenttir denir. (Asar vd., 2012).

Teorem 2.11: $1 \leq k \leq \frac{n-1}{2}$ herhangi bir tam sayı olmak üzere;

$$\binom{n-1}{2k} \equiv 1 \pmod{n}$$

denkliği vardır. (Lucas, 1878).

Tanım 2.12 : $n > 0$, a, b, n tam sayılar ve $a \not\equiv 0 \pmod{n}$ olmak üzere,

$$ax \equiv b \pmod{n}$$

şeklindeki bir kongrüansa bir bilinmeyenli lineer kongrüans adı verilir. (Asar vd., 2012).

Teorem 2.13: $n > 0$**,** a, b, n tam sayılar ve $(n, a) = d$ olsun.

$$ax \equiv b \pmod{n}$$

kongrüansının çözülebilir olması için gerek ve yeter şart $d|b$ olmasıdır. Eğer bu kongrüans çözülebilirse birbirlerine kongrüent olmayan d tane çözüm vardır. (Altındiş, 2011).

Sonuç 2.14: a ve $n > 0$ tam sayılar olmak üzere**,**

$$ax \equiv 1 \pmod{n}$$

denkleminin tam sayılı çözümü olması için gerek ve yeter şart $(a, n) = 1$ olmasıdır. x sayısına a nın n modülüne göre aritmetik tersi denir. (Taşçı, 2007; Altındiş 2011).

Örnek: $17x \equiv 1 \pmod{3120}$ kongrüansını çözelim.

Önce göre $(3210, 17)$ değerini Euclid algoritması yardımıyla hesaplayalım.

$$3120 = 183.17 + 9$$

$$17 = 1.9 + 8$$

$$9 = 1.8 + 1$$

$$8 = 8.1 + 0$$

olup $(17,3120) = 1$ dir. Kalanlar yalnız bırakılırsa,

$$9 = 3120 - 183.17$$

$$8 = 17 - 1.9$$

$$1 = 9 - 1.8$$

elde edilir. Buradan,

$$1 = 9 - 1.(17 - 1.9) = 2.9 - 17$$

$$1 = 2.(3120 - 183.17) - 17$$

$$1 = 2.3120 - 367.17$$

olup $x = -367 \equiv 2753 \pmod{3120}$ olarak bulunur.

Tanım 2.15 (**Euler ϕ Fonksiyonu) :** $n \geq 1$ olmak üzere n den küçük ve n ile aralarında asal olan pozitif tam sayıların sayısını veren fonksiyona Euler ϕ fonksiyonu denir ve $\phi(n)$ ile gösterilir. (Altındiş, 2011).

Teorem 2.16: $n > 1$ bir tam sayı olsun. $p_1, p_2, \dots, p_t$ birbirinden farklı asal sayılar ve $e_1, e_2, \dots, e_t$ pozitif tam sayılar olmak üzere

$$n = {p_1}^{e_1} {p_2}^{e_2} \dots {p_t}^{e_t}$$

olsun. O zaman

$$\phi(n) = \prod_{i=1}^{t} {p_i}^{e_i - 1} (p_i - 1) = n \prod_{i=1}^{t} \left(1 - \frac{1}{p_i}\right)$$

dir. (Asar ve Arıkan, 2012).

Örnek: $n = 60$ için $\phi(n)$ yi bulalım. $n = 2^2.3.5$

$$\phi(60) = 60.\left(1-\frac{1}{2}\right).\left(1-\frac{1}{3}\right).\left(1-\frac{1}{5}\right)$$

$$= 16$$

Teorem 2.17 : p asal sayı ise $\phi(p) = p-1$ dir. (Altındiş, 2011).

Teorem 2.18 : a ile $b \in \mathbb{Z}$ olmak üzere $(a,b) = 1$ ise $\phi(a.b) = \phi(a).\phi(b)$ dir. Bu durumda p ile q asal sayılar ise $\phi(p.q) = \phi(p).\phi(q) = (p-1).(q-1)$ olur. (Altındiş, 2011).

Tanım 2.19: $a \in \mathbb{Z}$ olsun. n modülüne göre a nın denklik sınıfı

$$\bar{a} = \{a + kn : k \in \mathbb{Z}\}$$

dir. $\bar{a}$ ya a nın n modülüne göre kalan sınıfı denir. Bölüm algoritmasından dolayı $a = qn + r$ ve $0 \leq r < n$ olacak biçimde $q, r \in \mathbb{Z}$ vardır. Buradan $a - r = qn$ olduğundan $r \in \bar{a}$ dır. Dolayısıyla $\bar{a} = \bar{r}$ dir. Böylece bütün kalan sınıfları

$$\bar{0}, \bar{1}, \ldots, \overline{n-1}$$

dir. $\mathbb{Z}$ nin n modülüne göre bütün kalan sınıflarının kümesi $\mathbb{Z}_n$ ile gösterilir. Böylece

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$$

dir. Örnek olarak

$$\mathbb{Z}_{10} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}\}$$

kümesi yazılabilir. (Asar vd., 2012).

Tanım 2.20: $\bar{a} \in \mathbb{Z}_n$ ve $(a,n) = 1$ ise $\bar{a}$ sınıfına bir asal kalan sınıfı denir. $\mathbb{Z}_n$ nin bütün asal (indirgenmiş) kalan sınıfları $\mathbb{Z}_n^*$ ile gösterilir ve

$$\mathbb{Z}_n^* = \{a : (a,n) = 1\}$$

dır. (Çallıalp, 2009).

Asal kalan sisteminin eleman sayısı $\phi(n)$ tanedir. Örnek olarak

$$\mathbb{Z}_{10}^* = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\}$$

kümesini yazabiliriz. Bu örnekte görüldüğü gibi $\mathbb{Z}_{10}^{*}$ kümesinin eleman sayısı $\phi(10) = 4$ tanedir.

Teorem 2.21: $(k,n) = d$ olmak üzere $ak \equiv bk\ (\mathrm{mod}\, n)$ ise $a \equiv b\ (\mathrm{mod}\ \frac{n}{d})$ dir. (Altındiş, 2011).

Sonuç 2.22: $(k,n) = 1$ ise $ak \equiv bk(\mathrm{mod}\, n) \Rightarrow a \equiv b(\mathrm{mod}\, n)$ dir. (Altındiş, 2011).

Teorem 2.23: $a_1, a_2, \dots, a_{\phi(n)}$ sayıları n modülüne göre indirgenmiş kalanlar ve $(k,n) = 1$ ise $ka_1, ka_2, \dots, ka_{\phi(n)}$ de indirgenmiş kalanlardır. (Altındiş, 2011).

Teorem 2.24: (Euler Teoremi) $n > 1$ ve $(a,n) = 1$ ise

$$a^{\phi(n)} \equiv 1\ (\mathrm{mod}\, n)$$

dir. (Altındiş, 2011).

İspat: $a_1, a_2, \dots, a_{\phi(n)}$ tam sayıları, n modülüne göre bir asal kalan sistemi ve $(a,n) = 1$ olsun. Bu takdirde Teorem 2.23 e göre $aa_1, aa_2, \dots, aa_{\phi(n)}$ tam sayıları da n modülüne göre bir asal kalan sistemi oluşturur. Şu halde,

$$aa_1 . aa_2 \dots aa_{\phi(n)} \equiv a_1 . a_2 \dots a_{\phi(n)} (\mathrm{mod}\, n)$$

$$a^{\phi(n)} (a_1 . a_2 \dots a_{\phi(n)}) \equiv a_1 . a_2 \dots a_{\phi(n)} (\mathrm{mod}\, n)$$

$$a^{\phi(n)} \prod_{j=1}^{\phi(n)} a_j \equiv \prod_{j=1}^{\phi(n)} a_j \ (\mathrm{mod}\, n)$$

olur, diğer yandan

$$(a_j, n) = 1, \qquad j = 1,2, \dots, \phi(n) \Rightarrow \left(\prod_{j=1}^{\phi(n)} a_j , n \right) = 1$$

olduğundan Sonuç 2.22 ye göre

$$a^{\phi(n)} \equiv 1 (\mathrm{mod}\, n)$$

elde ederiz.

Teorem 2.25: (Fermat Teoremi) p asal ve $p \nmid a$ olmak üzere

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

dir. (Altındiş, 2011).

İspat: p bir asal sayı ve $p \nmid a$ olduğundan, $(p, a) = 1$ dir. Ayrıca $\phi(p) = p - 1$ olduğundan, Teorem 2.24 ten dolayı

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

dir.

Teorem 2.26: (Wilson Teoremi): p bir asal sayı olsun. O zaman

$$(p-1)! \equiv -1 \ (\text{mod } p)$$

dir. (Asar vd., 2012).

İspat: $p = 2$ için $(2-1)! = 1! = 1 \equiv -1 \ (\text{mod } 2)$ dir. Şimdi ise p bir asal tek sayı olsun. $1 \leq i < p - 1$ tam sayısını alalım. $(i, p) = 1$ olduğundan $ij + pk = 1$ olacak biçimde j, k tam sayıları vardır. Buradan $ij \equiv 1 \ (\text{mod } p)$ elde edilir. Aynı zamanda $1 \leq j \leq p - 1$ alınabilir. Böylece 1 ile $p - 1$ arasındaki her i sayısı bu aralıkta bir j sayısı ile eşlenir. Mümkünse $i^2 \equiv 1 \ (\text{mod } p)$ olsun. O zaman $p | i^2 - 1$ olacağından $p | \, i - 1$ ya da $p | \, i + 1$ dir. $1 \leq i < p$ olduğundan ilk halde $i = 1$ ve ikinci halde $i + 1 = p$ yani $i = p - 1$ olur. O halde $2, 3, \ldots, p - 2$ sayılarından her biri bu sayılardan başka biriyle eşlenir. Buradan

$$2.3 \ldots . (p-2) \equiv 1(\text{mod } p)$$

elde edilir. Bu ifadenin iki yanı $1.(p-1)$ ile çarpılırsa

$$1.2.3 \ldots (p-2).(p-1) \equiv 1.(p-1) \equiv -1 \ (\text{mod } p)$$

olur. Dolayısıyla

$$(p-1)! \equiv -1 \ (\text{mod } p)$$

dir.

Tanım 2.27: a bir tam sayı ve $(a, n) = 1$ olsun. $x^2 \equiv a(\text{mod } n)$ kongrüansının çözümü varsa a ya n modülüne göre bir kuadratik rezidü (kuadratik kalan) ve eğer $x^2 \equiv$

$a(\text{mod}\, n)$ kongrüansının çözümü yoksa a ya n modülüne göre bir kuadratik non-rezidü denir. Kısaca kuadratik rezidü yerine KR, kuadratik non- rezidü yerine KNR yazacağız. (Erdoğan ve Yılmaz, 2008).

Örnek: $n = 5$ modülüne göre kuadratik ve kuadratik non-rezidüleri bulalım.

$1^2 \equiv 1(\text{mod } 5),\ 2^2 \equiv 4(\text{mod } 5),\ 3^2 \equiv 4(\text{mod } 5),\ 4^2 \equiv 1(\text{mod } 5)$

olduğundan 1 ve 4 sayıları 5 modülüne göre kuadratik rezidüdür (KR), 2 ve 3 sayıları ise kuadratik non-rezidüdür (KNR).

Tanım 2.28: n bir tek asal sayı ve $(a, n) = 1$ olsun.

$$\left(\frac{a}{n}\right) = \begin{cases} 1 & a, KR \text{ ise} \\ -1 & a, KNR \text{ ise} \end{cases}$$

şeklinde tanımlı $\left(\frac{a}{n}\right)$ sembolüne Legendre sembolü adı verilir. (Altındiş, 2011).

Örnek: $x^2 \equiv 4\ (\text{mod } 5)$ kongrüansı çözülebilir olduğundan 4 sayısı 5 modülüne göre KR dir ve bundan dolayı $\left(\frac{4}{5}\right) = 1$ dir.

$x^2 \equiv 3\ (\text{mod } 5)$ kongrüansının çözümü olmadığından 3 sayısı 5 modülüne göre KNR olup $\left(\frac{3}{5}\right) = -1$ bulunur.

Teorem 2.29: (Euler Kriteri) $p > 2$ ve a da $(p, a) = 1$ olan bir tam sayı ise

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (\text{mod } p)$$

dir. (Altındiş, 2011).

İspat: İlk olarak $\left(\frac{a}{p}\right) = 1$ olduğunu kabul edersek $x^2 \equiv a\ (\text{mod}\ p)$ kongrüansı çözülebilir demektir. $x = x_0$ bir çözüm olsun. Fermat teoremi gereği

$$a^{(p-1)/2} = (x_0^2)^{(p-1)/2} = x_0^{p-1} \equiv 1\ (\text{mod } p)$$

olur, o halde $\left(\frac{a}{p}\right) = 1$ alındığından

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} (\text{mod } p)$$

yazılır.

$\left(\frac{a}{p}\right) = -1$ olması halinde, $x^2 \equiv a(\text{mod } p)$ kongrüansı çözülemez demektir. Teorem 2.13 gereği $1 \leq i \leq p-1$ olan her bir i için $ij \equiv a \,(\text{mod } p)$ olacak şekilde $1 \leq i \leq p-1$ olan bir tek j tamsayısı vardır. Ayrıca $x^2 \equiv a \,(\text{mod } p)$ kongrüansı çözülemez olduğundan $i \neq j$ dir, dolayısıyla $1,2,\ldots,p-1$ sayılarını $ij \equiv a(\text{mod } p)$ olacak şekilde $(p-1)/2$ parçaya ayırabiliriz. Bu parçalar taraf tarafa çarpılırsa

$$(p-1)! \equiv a^{\frac{p-1}{2}} (\text{mod } p)$$

bulunur. Wilson teoremine göre

$$-1 \equiv a^{\frac{p-1}{2}} (\text{mod } p)$$

elde edilir ki yine $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2}$ olduğu gösterilmiş olur.

2.2. Fonksiyonlar

Tanım 2.30: X ve Y boş olmayan herhangi iki küme olmak üzere her bir $x \in X$ elemanına belli bir $y \in Y$ elemanını karşılık getiren f bağıntısına X ten Y ye bir dönüşüm denir ve $f: X \to Y$ şeklinde gösterilir. X e dönüşümün tanım kümesi, Y ye ise değer kümesi denir. (Taşçı, 2007).

Tanım 2.31: F cisim, X ve Y aynı F cisim üzerindeki vektör uzayları olmak üzere;

- $f: A \subseteq F \to F$ dönüşümüne fonksiyon denir. Örnek olarak A ve B sayı kümeleri olduğunda $f: A \to B$ dönüşümüne fonksiyon denir. (Taşçı, 2007).
- $f: X \to Y$ dönüşümüne operatör denir. Örnek olarak X ve Y fonksiyon kümeleri olduğunda $f: X \to Y$ dönüşümüne operatör denir. (Bayraktar, 2006; Hacısalihoğlu vd.; 2000).
- $f: X \to F$ operatörüne fonksiyonel adı verilir. Örnek olarak değer kümesi sayı kümesi olan $f: X \to R$ operatörlere fonksiyonel denir. (Bayraktar, 2006; Hacısalihoğlu vd., 2000).

Tanım 2.32: Bir f fonksiyonunun tanım kümesi ve değer kümesi $\mathbb{R}$ reel sayılar kümesinin birer alt kümesi ise f ye reel değişkenli ve reel değerli fonksiyon denir. (Cengiz vd., 2010).

Tanım 2.33: $c_1, c_2, \dots, c_m$ sabit katsayılar, $f_1(x), f_2(x), \dots, f_m(x)$ reel değerli fonksiyonlar olmak üzere;

$$c_1 f_1(x) + c_2 f_2(x) + \cdots + c_m f_m(x)$$

şeklinde elde edilen fonksiyona bu fonksiyonların lineer birleşimi denir. (Aydın vd., 2016).

Tanım 2.34: $c_1, c_2, \dots, c_m$ sabit katsayılar ve $f_1(x), f_2(x), \dots, f_m(x)$ reel değerli fonksiyonlar olmak üzere;

$$c_1 f_1(x) + c_2 f_2(x) + \cdots + c_m f_m(x) = 0 \qquad (2.1)$$

denklemini sağlayan hepsi birden sıfır olmayan $c_1, c_2, \dots, c_m$ sabitleri var ise bu durumda $f_1(x), f_2(x), \dots, f_m(x)$ fonksiyonlarına *lineer bağımlıdır* denir. Eğer (2.1) eşitliği sadece ve sadece $c_1 = c_2 = \cdots = c_m = 0$ durumunda sağlanıyorsa $f_1(x), f_2(x), \dots, f_m(x)$ fonksiyonlarına *lineer bağımsız fonksiyonlar* denir. (Kutay, 2010).

Teorem 2.35: S kümesi $S = \{f_1(x), f_2(x), \dots, f_m(x)\}$ şeklinde elemanları fonksiyon olan bir küme olsun. Bu takdirde S nin lineer bağımlı olması için gerek ve yeter şart, S kümesinde bulunan herhangi bir fonksiyonun bu kümedeki bir ya da daha fazla fonksiyonun lineer birleşimi olarak ifade edilebilmesidir. (Kolman, 2000).

Örnek: $S = \{x^2, 2x + 1, 3x^2 + 4x + 2, x^3\}$ kümesini göz önüne alalım.

$$3x^2 + 4x + 2 = 3(x^2) + 2(2x + 1)$$

şeklinde yazılabildiğinden S kümesindeki fonksiyonlar lineer bağımlıdır.

Tanım 2.36: n bağımsız değişken olmak üzere tanım kümesi $\mathbb{Z}$ tam sayılar kümesi olan fonksiyonlara tam değer argümanlı fonksiyon denir ve genel olarak $y(n)$ veya y_n şeklinde gösterilir. (Amirali ve Duru, 2002).

Örnek: $y(n) = n2^n$ fonksiyonu kısaca $y_n = n2^n$ olarak ifade edilir ve bu durumda $y_{n+1} = (n+1)2^{n+1}$ olacağı açıktır.

Tanım 2.37: $n_0 \in \mathbb{N}$ ve $c_1, c_2, \dots, c_m$ sabit katsayılar ve $y_1(n), y_2(n), \dots, y_m(n)$ tam değer argümanlı fonksiyonlar olmak üzere her $n \geq n_0$ için

$$c_1 y_1(n) + c_2 y_2(n) + \cdots + c_m y_m(n) = 0 \qquad (2.2)$$

denklemini sağlayan hepsi birden sıfır olmayan $c_1, c_2, \dots, c_m$ sabitleri var ise bu durumda $n \geq n_0$ için $y_1(n), y_2(n), \dots, y_m(n)$ fonksiyonlarına *lineer bağımlıdır* denir. Eğer (2.2) eşitliği her $n \geq n_0$ için sadece ve sadece $c_1 = c_2 = \cdots = c_m = 0$ durumunda sağlanıyorsa $y_1(n), y_2(n), \dots, y_m(n)$ fonksiyonlarına $n \geq n_0$ için *lineer bağımsızdır* denir. (Kutay, 2010).

Örnek: $y_1(n) = 3^n, y_2(n) = n3^n, y_3(n) = n^2 3^n$ fonksiyonları için; c_1, c_2, c_3 sabit katsayılar olmak üzere $\forall\, n \geq 1$ için

$$c_1 3^n + c_2 n3^n + c_3 n^2 3^n = 0$$

eşitliğini göz önüne alalım bu eşitlik 3^n ile bölünürse

$$c_1 + c_2 n + c_3 n^2 = 0, \qquad \forall\, n \geq 1$$

elde edilir, bu ise en fazla iki $n \geq 1$ için doğrudur. Her $n \geq 1$ için eşitliği ancak ve ancak $c_1 = c_2 = c_3 = 0$ durumunda sağlandığından bu fonksiyonlar $n \geq 1$ için lineer bağımsızdırlar.

2.3. Fark Denklemleri

Tanım 2.38: n bağımsız değişken, y_n tam değer argümanlı fonksiyon olmak üzere I özdeşlik (birim) operatörü:

$$Iy_n = y_n$$

E öteleme (kaydırma) operatörü:

$$Ey_n = y_{n+1}$$

ve

$$E^k y_n = y_{n+k}$$

olarak tanımlanır. (Uçar, 2013).

Örnek: $y_n = 3^n$ fonksiyonu için $Ey_n = 3^{n+1}$ dir.

Tanım 2.39: n bağımsız değişken, $y: \mathbb{N}_0 \to \mathbb{R}$ bir fonksiyon ve kısaca $y(n) = y_n$ olmak üzere,

$$\boldsymbol{\Delta} y_n = y_{n+1} - y_n$$

şeklinde tanımlanan $\boldsymbol{\Delta}$ ya ileri fark operatörü veya y_n nin birinci basamaktan (mertebeden) farkı denir. $\boldsymbol{\Delta} = E - I$ olduğu kolayca görülebilir.

y_n nin ikinci basamaktan farkı ($\boldsymbol{\Delta}^2 y_n$)

$$\begin{aligned} \boldsymbol{\Delta}^2 y_n &= \boldsymbol{\Delta}(\boldsymbol{\Delta} y_n) \\ &= \boldsymbol{\Delta}(y_{n+1} - y_n) \\ &= \boldsymbol{\Delta} y_{n+1} - \boldsymbol{\Delta} y_n \\ &= (y_{n+2} - y_{n+1}) - (y_{n+1} - y_n) \\ &= y_{n+2} - 2y_{n+1} + y_n \end{aligned}$$

ve genel olarak y_n nin k ıncı basamaktan farkı ($\boldsymbol{\Delta}^k y$)

$$\begin{aligned} \boldsymbol{\Delta}^k y_n &= (E - I)^k y_n \\ &= \sum_{j=0}^{k} \binom{k}{j} (-I)^j \, y_{n+k-j} \\ &= \sum_{j=0}^{k} \binom{k}{j} (-1)^j \, y_{n+k-j} \end{aligned}$$

şeklinde hesaplanır. (Kutay, 2010).

Tanım 2.40: n bağımsız değişken, y_n de bir $S \subseteq \mathbb{N}_0$ kümesi üzerinde tanımlı bağımlı değişken olmak üzere, n bağımsız değişkeni, y_n bağımlı değişkeni ve bağımlı değişkenin $Ey_n, E^2y_n, \dots, E^m y_n$ gibi farklarını içeren

$$F\{n, y_n, Ey_n, E^2y_n, \dots, E^m y_n\} = 0 \tag{2.3}$$

bağıntısına S kümesi üzerinde tanımlanmış m. mertebeden (basamaktan) *fark denklemi* denir. (2.3) denkleminde y_n bağımlı değişkeni birinci dereceden ise yani $i = 1,2, \dots, m$ için $a_m(n) \neq 0$ olmak üzere $a_i(n)$ ler katsayı fonksiyonları ve $g(n)$, $n \geq n_0$ için tanımlı reel değerli fonksiyon olmak üzere

$$E^m y_n + a_1(n)E^{m-1}y_n + \cdots + a_{m-1}(n)Ey_n + a_m(n)Iy_n = g(n) \tag{2.4}$$

denklemine *lineer fark denklemi* adı verilir.

a) Bütün katsayıları $a_i(n) = c_i$ şeklinde sabit olan

$$E^m y_n + c_1E^{m-1}y_n + \cdots + c_{m-1}Ey_n + c_mIy_n = g(n) \tag{2.5}$$

şeklindeki (2.5) denklemine *sabit katsayılı* lineer fark denklemi denir.

b) $g(n) = 0$ olan

$$E^m y_n + a_1(n)E^{m-1}y_n + \cdots + a_{m-1}(n)Ey_n + a_m(n)Iy_n = 0 \tag{2.6}$$

şeklindeki (2.6) denklemine *homojen lineer fark denklemi* adı verilir.

c) $a_i(n) = c_i$ ve $g(n) = 0$ şartlarının her ikisini de sağlayan

$$E^m y_n + c_1E^{m-1}y_n + \cdots + c_{m-1}Ey_n + c_mIy_n = 0 \tag{2.7}$$

şeklindeki (2.7) denklemine *sabit katsayılı homojen lineer fark denklemi* adı verilir. (Uçar, 2013).

Tanım 2.41: Yukarıdaki (2.4) denklemini sağlayan m tane lineer bağımsız $\lambda_1^n, \lambda_2^n, \dots, \lambda_m^n$ elemandan oluşan kümeye denklemin *temel çözüm kümesi,* temel çözüm kümesindeki lineer bağımsız bütün çözümlerin

$$c_1\lambda_1^n + c_2\lambda_2^n + \cdots + c_m\lambda_m^n$$

şeklindeki lineer birleşiminden oluşan çözüme *genel çözüm* denir. (Karaman, 2010; Kutay, 2010).

$\lambda \epsilon \mathbb{R}\, ve\ \lambda^n \neq 0$ olmak üzere $m.$ mertebeden sabit katsayılı homojen lineer fark denkleminin bir çözümü $y_n = \lambda^n$ olsun. Bu çözüm (2.7) denkleminde yerine yazılırsa

$$E^m\lambda^n + c_1E^{m-1}\lambda^n + \cdots + c_{m-1}E\lambda^n + c_mI\lambda^n = 0$$

elde edilir. Bu eşitlik açık olarak yazılıp

$$\lambda^{n+m} + c_1\lambda^{n+m-1} + \cdots + c_{m-1}\lambda^{n+1} + c_m\lambda^n = 0$$

λ^n parantezine alınırsa

$$(\lambda^m + c_1\lambda^{m-1} + \cdots + c_{m-1}\lambda + c_m)\lambda^n = 0$$

$\lambda^n \neq 0$ olduğundan buradan;

$$\lambda^m + c_1\lambda^{m-1} + \cdots + c_{m-1}\lambda + c_m = 0 \qquad (2.8)$$

elde edilir. Bu $m.$ dereceden (2.8) denklemine (2.7) denkleminin karakteristik polinom denklemi denir.

Teorem 2.42: $c_1, c_2, \dots, c_m$ keyfi sabitler olmak üzere (2.7) ile belirtilen $m.$ mertebeden sabit katsayılı homojen lineer fark denkleminin (2.8) ile belirtilen karakteristik polinomunun kökleri $\lambda_1, \lambda_2, \dots, \lambda_m \in \mathbb{R}$ olsun. Eğer bu kökler birbirinden farklı ise (2.7) homojen denklemi

$$y_n = c_1\lambda_1^n + c_2\lambda_2^n + \cdots + c_m\lambda_m^n$$

biçiminde keyfi sabitlere bağlı genel çözüme sahiptir. (Akın ve Bulgak, 1998; Uçar, 2013).

Örnek: $n \geq 0$ tam sayı olmak üzere

$$y_{n+2} - 5y_{n+1} + 6y_n = 0 \qquad (2.9)$$

ikinci mertebeden sabit katsayılı homojen lineer fark denkleminin genel çözümünü bulalım.

2. mertebeden sabit katsayılı (2.9) homojen lineer fark denkleminin bir çözümü $\lambda \epsilon \mathbb{R}$ ve $\lambda^n \neq 0$ olmak üzere $y_n = \lambda^n$ olsun. Bu çözüm (2.9) denkleminde yerine yazılırsa

$$\lambda^{n+2} - 5\lambda^{n+1} + 6\lambda^n = 0$$

λ^n parantezine alınırsa

$$\lambda^n(\lambda^2 - 5\lambda + 6) = 0$$

$\lambda^n \neq 0$ olduğundan buradan;

$$\lambda^2 - 5\lambda + 6 = 0 \tag{2.10}$$

denklemi elde edilir. (2.10) karakteristik polinom denkleminin kökleri $\lambda_1 = 2,\ \lambda_2 = 3$ olup (2.9) denkleminin temel çözüm kümesi $\{\lambda_1^n = 2^n, \lambda_2^n = 3^n\}$ ve genel çözümü c_1, c_2 keyfi sabitler olmak üzere

$$y_n = c_1 2^n + c_2 3^n$$

şeklinde elde edilir.

Tanım 2.43: $i = 1,2, \dots, m$ için c_i ler reel katsayılar ve $[t_0, t_1]$ aralığında $t_0 \leq j \leq t_1$ olmak üzere

$$y_j = \alpha_1,\quad y_{j+1} = \alpha_2,\quad \dots,\quad y_{j+m-1} = \alpha_m$$

başlangıç şartlarını sağlayan çözüme sahip olan

$$E^m y_n + c_1 E^{m-1} y_n + \cdots + c_{m-1} E y_n + c_m I y_n = 0 \tag{2.11}$$

m. mertebeden sabit katsayılı homojen lineer fark denklemine Cauchy (başlangıç değer) fark denklemi denir. (Uçar, 2013).

Teorem 2.44: Tanım 2.43 te verilen (2.11) Cauchy fark denkleminin $n \geq n_0$ için tanımlı olan y_n çözümü vardır ve tektir. (Uçar, 2013).

Örnek: $y_0 = 0, y_1 = 1$ başlangıç değerleri olmak üzere;

$$y_{n+2} = y_{n+1} + y_n \tag{2.12}$$

2. mertebeden sabit katsayılı homojen lineer fark denkleminin çözümünü bulalım.

$\lambda \epsilon \mathbb{R}$ ve $\lambda^n \neq 0$ olmak üzere (2.12) denkleminin bir çözümü $y_n = \lambda^n$ olsun. Bu çözüm (2.12) denkleminde yerine yazılırsa

$$\lambda^{n+2} - \lambda^{n+1} - \lambda^n = 0$$

elde edilir. Bu durumda

$$\lambda^n(\lambda^2 - \lambda - 1) = 0$$

yazılır. $\lambda^n \neq 0$ olduğundan

$$\lambda^2 - \lambda - 1 = 0 \tag{2.13}$$

denklemi elde edilir. Bu (2.13) denkleminin kökleri

$$\lambda_1 = \frac{1+\sqrt{5}}{2} \text{ ve } \lambda_2 = \frac{1-\sqrt{5}}{2} \tag{2.14}$$

dir.

Bu reel kökler birbirinden farklı olup Teorem 2.42 den dolayı c_1, c_2 keyfi sabitler olmak üzere (2.12) denklemi

$$y_n = c_1\lambda_1^n + c_2\lambda_2^n \tag{2.15}$$

şeklinde genel çözüme sahiptir.

Başlangıç şartları verilen (2.12) denklemi Cauchy fark denklemi olup başlangıç şartları göz önüne alınırsa

$$\begin{aligned} y_0 = \quad & c_1\lambda_1^0 + c_2\lambda_2^0 \quad = 0 \\ y_1 = \quad & c_1\lambda_1 + c_2\lambda_2 \quad = 1 \end{aligned} \tag{2.16}$$

lineer denklem sistemi elde edilir. Bu (2.16) denklem sisteminin çözümü

$$c_1 = \frac{1}{\lambda_1 - \lambda_2} \tag{2.17}$$

$$c_2 = -\frac{1}{\lambda_1 - \lambda_2}$$

olup (2.17) deki değerler (2.15) te yazılırsa (2.12) denkleminin genel çözümü

$$y_n = \frac{\lambda_1^n - \lambda_2^n}{\lambda_1 - \lambda_2}$$

olarak elde edilir.

Örnek: $y_0 = 0, y_1 = 1$ başlangıç değerleri olmak üzere

$$y_{n+2} = Py_{n+1} - Qy_n \tag{2.18}$$

2. mertebeden sabit katsayılı homojen lineer fark denkleminin çözümünü bulalım.

$\lambda \epsilon \mathbb{R}$ ve $\lambda^n \neq 0$ olmak üzere (2.18) denkleminin bir çözümü $y_n = \lambda^n$ olsun. Bu çözüm (2.18) denkleminde yerine yazılırsa

$$\lambda^{n+2} - P\lambda^{n+1} + Q\lambda^n = 0$$

elde edilir. Bu durumda

$$\lambda^n(\lambda^2 - P\lambda + Q) = 0$$

$\lambda^n \neq 0$ olduğundan buradan,

$$\lambda^2 - P\lambda + Q = 0$$

denklemi elde edilir. $\Delta = P^2 - 4Q > 0$ için bu denklemin birbirinden farklı λ_1 ve λ_2 reel kökleri vardır. Bu durumda Teorem 2.42 den dolayı c_1, c_2 keyfi sabitler olmak üzere (2.18) denklemi

$$y_n = c_1\lambda_1^n + c_2\lambda_2^n \tag{2.19}$$

şeklinde genel çözüme sahiptir.

Başlangıç şartları verilen (2.19) denklemi Cauchy fark denklemi olup başlangıç şartlarını göz önüne alırsak

$$\begin{aligned} y_0 &= c_1\lambda_1^0 + c_2\lambda_2^0 = 0 \\ y_1 &= c_1\lambda_1 + c_2\lambda_2 = 1 \end{aligned} \tag{2.20}$$

lineer denklem sistemi elde edilir. (2.20) denklem sisteminin çözümü

$$c_1 = \frac{1}{\lambda_1 - \lambda_2}$$
$$c_2 = -\frac{1}{\lambda_1 - \lambda_2} \tag{2.21}$$

olup (2.21) deki değerler (2.19) da yerine yazılırsa (2.18) denkleminin genel çözümü

$$y_n = \frac{\lambda_1^n - \lambda_2^n}{\lambda_1 - \lambda_2}$$

olarak elde edilir.

Örnek: $y_0 = 2, y_1 = 1$ başlangıç değerleri olmak üzere

$$y_{n+2} = y_{n+1} + y_n \tag{2.22}$$

2. mertebeden sabit katsayılı homojen lineer fark denkleminin çözümü bulalım.

$\lambda \epsilon \mathbb{R}$ ve $\lambda^n \neq 0$ olmak üzere (2.22) denkleminin bir çözümü $y_n = \lambda^n$ olsun. Bu çözüm (2.22) denkleminde yerine yazılırsa

$$\lambda^{n+2} - \lambda^{n+1} - \lambda^n = 0$$

elde edilir. Bu durumda

$$\lambda^n(\lambda^2 - \lambda - 1) = 0$$

yazılır. $\lambda^n \neq 0$ olduğundan buradan

$$\lambda^2 - \lambda - 1 = 0 \tag{2.23}$$

denklemi elde edilir. Bu (2.23) denkleminin kökleri

$$\lambda_1 = \frac{1+\sqrt{5}}{2} \text{ ve } \lambda_2 = \frac{1-\sqrt{5}}{2}$$

dir.

Bu reel kökler birbirinden farklı olup Teorem 2.42 den dolayı c_1, c_2 keyfi sabitler olmak üzere (2.22) denklemi

$$y_n = c_1\lambda_1^n + c_2\lambda_2^n \tag{2.24}$$

şeklinde genel çözüme sahiptir.

Başlangıç şartları verilen (2.22) denklemi Cauchy fark denklemi olup başlangıç şartlarını göz önüne alınırsa

$$\begin{aligned} y_0 = \quad & c_1\lambda_1^0 + c_2\lambda_2^0 \quad = 2 \\ y_1 = \quad & c_1\lambda_1 + c_2\lambda_2 \quad = 1 \end{aligned} \tag{2.25}$$

lineer denklem sistemi elde edilir. (2.25) denklem sisteminin çözümü

$$c_1 = \frac{2\lambda_2 - 1}{\lambda_2 - \lambda_1}$$

$$c_2 = -\frac{2\lambda_1 - 1}{\lambda_2 - \lambda_1} \tag{2.26}$$

olup (2.23) denklemi için (2.26) daki eşitliklerde $\lambda_1 = 1-\lambda_2$ yazılırsa $c_1 = c_2 = 1$ elde edilir. Bu değerler (2.24) te yerine yazılırsa (2.22) denkleminin genel çözümü

$$y_n = {\lambda_1}^n + {\lambda_2}^n \tag{2.27}$$

olarak elde edilir.

Örnek: $y_0 = 2, y_1 = P$ olmak üzere

$$y_{n+2} = Py_{n+1} - Qy_n \tag{2.28}$$

2. mertebeden sabit katsayılı homojen lineer fark denkleminin çözümünü bulalım.

$\lambda\epsilon\mathbb{R}$ ve $\lambda^n \neq 0$ olmak üzere (2.28) denkleminin bir çözümü $y_n = \lambda^n$ olsun. Bu çözüm denklemde yerine yazılırsa

$$\lambda^{n+2} - P\lambda^{n+1} + Q\lambda^n = 0$$

$$\lambda^n(\lambda^2 - P\lambda + Q) = 0$$

$\lambda^n \neq 0$ olduğundan buradan,

$$\lambda^2 - P\lambda + Q = 0$$

denklemi elde edilir. $\Delta = P^2 - 4Q > 0$ için bu denklemin birbirinden farklı λ_1 ve λ_2 reel kökleri vardır. Bu durumda Teorem 2.39 dan dolayı c_1, c_2 keyfi sabitler olmak üzere (2.28) denklemi

$$y_n = c_1\lambda_1^n + c_2\lambda_2^n \tag{2.29}$$

şeklinde genel çözüme sahiptir.

Başlangıç şartları verilen (2.24) denklemi Cauchy fark denklemi olup başlangıç şartları göz önüne alınırsa

$$\begin{aligned} y_0 &= c_1\lambda_1^0 + c_2\lambda_2^0 = 2 \\ y_1 &= c_1\lambda_1 + c_2\lambda_2 = P \end{aligned} \tag{2.30}$$

lineer denklem sistemi elde edilir. (2.30) denklem sisteminin çözümü

$$\begin{aligned} c_1 &= 1 \\ c_2 &= 1 \end{aligned} \tag{2.31}$$

olup (2.31) deki değerler (2.29) da yerine yazılırsa (2.28) denkleminin genel çözümü

$$y_n = {\lambda_1}^n + {\lambda_2}^n$$

olarak elde edilir.

2.4. Fibonacci Sayıları

Tanım 2.45: $n \geq 0$ tam sayı ve $F_0 = 0$ ve $F_1 = 1$ başlangıç değerleri olmak üzere

$$F_{n+2} = F_{n+1} + F_n$$

rekürans (indirgeme) bağıntısı ile tanımlanan $F_n = 0, 1, 1, 2, 3, 5, 8, 13, 21, \ldots$ dizisine Fibonacci dizisi, bu dizinin terimlerine *Fibonacci sayıları* denir. (Vajda, 1989; Robbins, 1993; Koshy, 2001).

Tanım 2.46: $n \geq 0$ tam sayı, $x^2 - x - 1$ polinomunun sıfırları x_1 ve x_2 olmak üzere, Fibonacci dizisinin F_n terimlerini veren binet formülü

$$F_n = \frac{{x_1}^n - {x_2}^n}{x_1 - x_2}$$

şeklindedir. (Vajda, 1989; Koshy; 2001).

Örnek: F_n Fibonacci dizisinin ilk dört terimi Binet formülü ile aşağıdaki gibi bulunur.

$$F_0 = \frac{{x_1}^0 - {x_2}^0}{x_1 - x_2} = 0$$

$$F_1 = \frac{x_1 - x_2}{x_1 - x_2} = 1$$

$$F_2 = \frac{{x_1}^2 - {x_2}^2}{x_1 - x_2} = x_1 + x_2 = 1$$

$$F_3 = \frac{{x_1}^3 - {x_2}^3}{x_1 - x_2} = {x_1}^2 + x_1 x_2 + {x_2}^2 = 2$$

Tanım 2.47: $n \in \mathbb{N}_0$ ve $\Delta = P^2 - 4Q \neq 0$ şartını sağlayan $0 \neq PQ \in \mathbb{Z}$ olmak üzere; $U_0 = 0$ ve $U_1 = 1$ başlangıç değerleri için

$$U_{n+2}(P, Q) = PU_{n+1} - QU_n$$

rekürans ile tanımlanan diziye $U_n(P, Q)$-*Genelleştirilmiş Fibonacci dizisi* denir.
$\mathrm{P} = 3, \mathrm{Q} = 2$ için bu dizinin terimleri $U_n(P, Q) = 0, 1, 3, 7, 15, 31, 63, \ldots$ şeklindedir. (Robbins, 1993).

Tanım 2.48: $n \in \mathbb{Z}^+$ ve $x^2 - Px + Q$ polinomunun sıfırları $x_1,\ x_2$ olmak üzere;

$$U_n(P, Q) = \frac{{x_1}^n - {x_2}^n}{x_1 - x_2}$$

bağıntısına $U_n(P,Q)$ dizisinin terimlerini veren Binet formülü denir. (Vajda, 1989; Koshy; 2001).

Örnek: $U_n(P,Q)$ Genelleştirilmiş Fibonacci dizisinin ilk dört terimi Binet formülü ile aşağıdaki gibi bulunur.

$$U_0(P,Q) = \frac{{x_1}^0 - {x_2}^0}{x_1 - x_2} = 0$$

$$U_1(P,Q) = \frac{x_1 - x_2}{x_1 - x_2} = 1$$

$$U_2(P,Q) = \frac{{x_1}^2 - {x_2}^2}{x_1 - x_2} = x_1 + x_2 = P$$

$$U_3(P,Q) = \frac{{x_1}^3 - {x_2}^3}{x_1 - x_2} = {x_1}^2 + x_1x_2 + {x_2}^2 = 7$$

Böylece $U_n(P,Q)$ Genelleştirilmiş Fibonacci dizisinin ilk dört terimi elde edilmiş olur.

2.5. Lucas Sayıları

Tanım 2.49: $n \in \mathbb{N}_0$, $L_0 = 2$, $L_1 = 1$ başlangıç değerleri olmak üzere

$$L_{n+2} = L_{n+1} + L_n$$

rekürans bağıntısı ile tanımlanan $L_n = 2, 1, 3, 4, 7, 11, 18, \ldots$ dizisine Lucas dizisi, bu dizinin terimlerine *Lucas sayıları* denir. (Vajda, 1989; Robbins, 1993; Koshy, 2001).

Tanım 2.50: $n \in \mathbb{Z}^+$, $x_1 = \frac{1+\sqrt{5}}{2}$ ve $x_2 = \frac{1-\sqrt{5}}{2}$ değerleri $x^2 - x - 1$ polinomunun sıfırları olmak üzere,

$$L_n = {x_1}^n + {x_2}^n$$

bağıntısına L_n dizisinin terimlerini veren Binet formülü denir. (Vajda, 1989; Koshy; 2001).

Örnek: L_n Lucas dizisinin ilk dört terimi Binet formülü ile aşağıdaki gibi bulunur.

$$L_0 = {x_1}^0 + {x_2}^0 = 2$$

$$L_1 = {x_1}^1 + {x_2}^1 = 1$$

$$L_2 = {x_1}^2 + {x_2}^2 = 3$$

$$L_3 = {x_1}^3 + {x_2}^3 = 4$$

Tanım 2.51: $V_0 = 2$ ve $V_1 = P$ başlangıç değerleri için

$$V_{n+2}(P,Q) = PV_{n+1} - QV_n$$

rekürans bağıntısı ile tanımlanan diziye $V_n(P,Q)$-*Genelleştirilmiş Lucas dizisi* denir.

$\mathrm{P} = 3, \mathrm{Q} = 1$ için bu dizinin terimleri $L_n(P,Q) = 2, 3, 7, 18, 47, 123, 322, \ldots$ şeklindedir. (Robbins, 1993).

Tanım 2.52: $n \in \mathbb{Z}^+$, $x^2 - Px + Q$ polinomunun sıfırları x_1 ve x_2 olmak üzere;

$$V_n(P,Q) = {x_1}^n + {x_2}^n$$

bağıntısına $V_n(P,Q)$ dizisinin terimlerini veren Binet formülü denir. (Vajda, 1989; Koshy; 2001).

Örnek: $\mathrm{P} = 3, \mathrm{Q} = 1$ için için $V_n(P,Q)$ Lucas dizisinin ilk dört terimi binet formülü ile aşağıdaki gibi bulunur.

$$L_0 = {x_1}^0 + {x_2}^0 = 2$$

$$L_1 = {x_1}^1 + {x_2}^1 = 3$$

$$L_2 = {x_1}^2 + {x_2}^2 = 7$$

$$L_3 = {x_1}^3 + {x_2}^3 = 18$$

3. MATERYAL ve YÖNTEM

3.1. RSA Şifreleme Algoritması

Günümüzde kullanılan diğer modern Asimetrik algoritmalar gibi RSA şifreleme algoritması da 3 aşamadan oluşur;

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

RSA algoritmasının aşamaları aşağıdaki gibidir.

Anahtar Oluşturma

Şifreli bilgiyi almak isteyen taraf aşağıdaki işlemleri yaparak şifreleme ve şifre çözme anahtarlarını oluşturur.

i. İki adet birbirinden bağımsız yaklaşık olarak aynı büyüklükte p ve q asal sayılarını üretir.
ii. $n = p.q$ ve $\phi(n) = (p-1).(q-1)$ değerlerini hesaplar.
iii. $(e, \phi(n)) = 1$ ve $1 < e < \phi(n)$ şartlarını sağlayan rastgele bir e sayısı seçer.
iv. $1 < d < \phi(n)$ olacak şekilde $e.d \equiv 1 \pmod{(\phi(n))}$ şartlarını sağlayan d sayısını Euclid Algoritmasını kullanarak hesaplar.

Bu işlemler sonucunda üretilen n ve e sayıları açık anahtar, d sayısı ise gizli anahtar olarak adlandırılır.

Şifreli bilgiyi almak isteyen taraf diğer tarafa kendi açık anahtarı olan n ve e sayılarını gönderir.

Şifreleme

Şifreli bilgiyi gönderecek taraf şifrelemek istediği M mesajını $[0, n-1]$ aralığında bir tam sayıya dönüştürür. Aşağıdaki denklem yardımıyla şifreli metin C'yi hesaplar ve karşı tarafa gönderir.

$$M^e \equiv C \pmod{n}$$

Şifre çözme

Şifreli bilgiyi alan taraf kendi özel anahtarını d yi kullanarak aşağıdaki denklem yardımıyla düz metin M yi hesaplayarak düz metni elde eder.

$$C^d \equiv M \pmod{n}$$

Algoritmanın doğrulaması aşağıda görülebilir.

$e.d \equiv 1 (\text{mod } \phi(n))$

$e.d = k.\phi(n) + 1$

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

$M^{\phi(n)} \equiv 1 (\text{mod } n)$ olduğundan

$C^d \equiv \left(M^{\phi(n)}\right)^k . M \equiv M \pmod{n}$

Örnek:

Anahtar Oluşturma

i. $p = 61$ ve $q = 53$ iki asal sayı olsun.

ii. $n = 61.53 = 3233$ ve $\phi(n) = (61-1).(53-1) = 3120$

iii. $\left(e, \phi(n)\right) = 1$ ve $1 < e < \phi(n)$ olacak şekilde $e = 17$ seçilsin.

iv. Tanım 2.12 ye göre ve Teorem 2.8 kullanılarak
$1 < d < \phi(n)$ ve $17.d \equiv 1 \pmod{\phi(n)}$ şartlarını sağlayan d sayısı hesaplanırsa

$$3120 = \quad 183.17 + 9$$

$$17 = 1.9 + 8$$
$$9 = 1.8 + 1$$
$$8 = 8.1 + 0$$

buradan kalanlar yalnız bıraklırsa

$$9 = 3120 - 183.17 \quad (3.1)$$
$$8 = 17 - 1.9 \quad (3.2)$$
$$1 = 9 - 1.8 \quad (3.3)$$

(3.3) teki değer (3.2) eşitliğinde yazılırsa

$$1 = 9 - 1.(17 - 1.9)$$
$$1 = 2.9 - 17 \quad (3.4)$$

Son olarak (3.1) değeri (3.4) eşitliğinde yazılırsa

$$1 = 2.(3120 - 183.17) - 17$$
$$1 = 2.3120 - 367.17$$

Buradan $d = (-367) = 2753$ elde edilmiş olur.

Şifreleme

Şifrelenecek sayımız $M = 123$ olsun bu durumda

$$C \equiv 123^{17} \equiv 855 \pmod{3233}$$

olarak bulunur.

Şifre çözme

$C = 855$ sayısı için

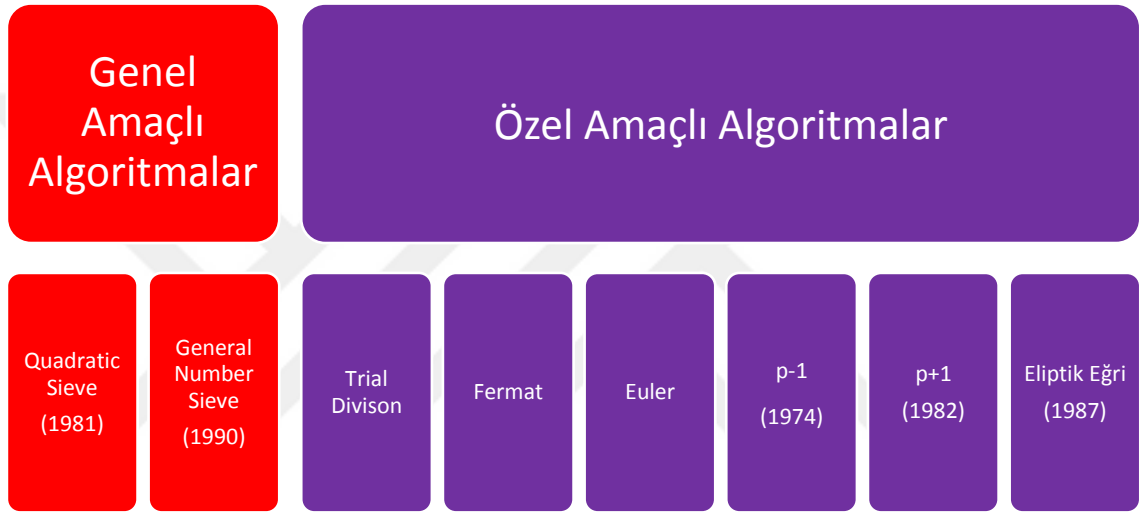
$$M \equiv 855^{2753} \equiv 123 \pmod{3233}$$

olarak elde edilir.

3.2. RSA Kriptanalizi

RSA'da anahtarların bir parçası olan n tam sayısı çarpanlarına ayrılırsa bu çarpanları kullanarak $\phi(n)$ değeri kolayca hesaplanarak genel anahtarın bir diğer parçasını oluşturan e tam sayısı kullanılarak d özel anahtarı bulunabilir.

Çarpanlara ayırma algoritmaları Genel amaçlı (General Purpose Factorization Algoritms) ve Özel amaçlı (Special Purpose Factorization Algorithms) olmak üzere iki gruba ayrılmaktadır.



Şekil 3.1. Çarpanlara Ayırma Algoritmaları

3.2.1. Genel amaçlı çarpanlara ayırma algoritmaları

Genel amaçlı çarpanlara ayırma algoritmalarının çalışma süresi çarpanlarına ayrılacak tam sayının büyüklüğüne bağlıdır. Günümüzde yaygın olarak kullanılan genel amaçlı algoritmalar şunlardır: (Aybak, 2010).

- Quadratic Sieve
- General Number Field sieve

3.2.2. Özel amaçlı çarpanlara ayırma algoritmaları

Bu bölümde RSA anahtarları oluşturulurken göz önünde bulundurulması bir zorunluluk olan bazı önemli özel amaçlı çarpanlara ayırma algoritmaları özet olarak verilmiştir.

Özel amaçlı çarpanlara ayırma algoritmalarının çalışma süreleri ise çarpanlarına ayrılacak sayının belirli özeliklerine veya sayıyı oluşturan çarpanların belirli özelliklerine bağlıdır. Bu nedenle RSA Kripto sisteminde anahtar oluşturulurken asal sayılar bu özel amaçlı algoritmalar göz önünde bulundurularak oluşturulmalıdır. Bu sınıftaki algoritmaların en önemlileri şunlardır:

- Trial division
- Fermat
- Euler
- Pollard $p-1$
- Williams $p+1$
- Eliptic curve

3.2.2.1. Basit bölme algoritması

En basit özel amaçlı çarpanlara ayırma algoritması olan basit bölme (trial division) algoritması, eğer N sayısını oluşturan asal çarpanlardan biri çok küçük ise bu çarpan N'nin 2 den başlanarak sırası ile $2, 3, 5, 7, 11, 13, 17, 19 \ldots$ şeklinde asal sayılara bölünüp bölünmediği kontrol edilerek bulunabilir. (Menezes vd., 1997).

3.2.2.2. Fermat çarpanlara ayırma algoritması

a ve b tamsayılar olmak üzere

$$N = a^2 - b^2$$

denklemini sağlayan a ve b tam sayıları elde edildiğinde, N sayısını veren çarpanlar $(\mathrm{a} + \mathrm{b})(\mathrm{a} - \mathrm{b})$ şeklinde bulunmuş olur. N sayısının çarpanları arasındaki fark çok küçük ise bu algoritma kullanışlıdır. RSA da kullanılacak olan N sayısı oluşturulurken birbirine çok yakın olmayan p ve q asalları seçilmelidir. (Aybak, 2010).

3.2.2.3. Euler çarpanlara ayırma algoritması

Bu algoritmada a, b, c, d tam sayılar olmak üzere N tam sayısı

$$N = a^2 + b^2$$

ve

$$N = c^2 + d^2$$

olarak yazılabiliyorsa N sayısının çarpanları kolayca hesaplanabilir. (McKee, 1996)

3.2.2.4. Pollard $p - 1$ çarpanlara ayırma algoritması

Şayet p asalı için $p - 1$ sayısının en büyük asal çarpanı yeterince küçük bir değere sahipse bu asalla oluşturulan bileşik sayının çarpanı bu algoritma ile makul bir zamanda hesaplanabilmektedir. Bu algoritmanın hesaplama süresi $p - 1$ sayısının en büyük asal çarpanının büyüklüğüne bağlıdır. RSA kripto sisteminde kullanılacak p ve q asalları seçilirken hem $p - 1$ in hem de $q - 1$ in en büyük asal çarpanının yeterince büyük olması bir zorunluluktur. (Menezes vd., 1997).

3.2.2.5. Williams $p + 1$ çarpanlara ayırma algoritması

Şayet p asalı için $p + 1$ sayısının en büyük asal çarpanı yeterince küçük bir değere sahipse bu asalla oluşturulan bileşik sayının çarpanı bu algoritma ile makul bir zamanda hesaplanabilmektedir. Bu algoritmanın hesaplama süresi $p + 1$ sayısının en büyük asal çarpanının büyüklüğüne bağlıdır. RSA kripto sisteminde kullanılacak p ve q asalları seçilirken hem $p + 1$ in hem de $q + 1$ in en büyük asal çarpanının yeterince büyük olması bir zorunluluktur. (Williams, 1982).

3.2.2.6. Eliptik eğri çarpanlara ayırma algoritması

Bu yöntemde N sayısını oluşturan asal çarpanlardan biri yeterince küçük ise eliptik eğriler üzerinde kurulan grup yapısı ile bu çarpan makul bir sürede elde edilebilmektedir. (Menezes vd., 1997).

4. ARAŞTIRMA KONUSU

4.1. P + 1 Çarpanlara Ayırma Algoritması

Bu bölümde araştırma konusu olan $p+1$ algoritmasının temel teoremleri, algoritmada kullanılan Lucas sayı dizisinin n. terimini hızlı olarak hesaplamak için geliştirilen algoritma, algoritmanın teorik altyapısı, algoritmanın kurulması ve daha hızlı sonuca ulaşan iki aşamalı algoritma detaylı olarak ele alınmıştır. (Lucas, 1878; Lehmer 1930; Williams, 1982).

4.1.1. Algoritmanın temel teoremleri

Teorem 4.1: Genelleştirilmiş Lucas dizisinin terimleri arasında aşağıdaki bağıntılar vardır.

$$\begin{aligned} &\textbf{i.} && V_{2n} = V_n^2 - 2Q^n \\ &\textbf{ii.} && V_{2n-1} = V_n V_{n-1} - PQ^{n-1} \\ &\textbf{iii.} && V_{2n+1} = V_{n+1} V_n - PQ^n \end{aligned} \tag{4.1}$$

İspat:

i.
$$\begin{aligned} V_{2n} &= \alpha^{2n} + \beta^{2n} \\ &= (\alpha^n + \beta^n)^2 - 2\alpha^n\beta^n \\ &= V_n^2 - 2Q^n \end{aligned}$$

ii.
$$\begin{aligned} V_{2n-1} &= \alpha^{2n-1} + \beta^{2n-1} \\ &= \alpha^n\alpha^{n-1} + \beta^n\beta^{n-1} + \alpha^n\beta^{n-1} - \alpha^n\beta^{n-1} + \alpha^{n-1}\beta^n - \alpha^{n-1}\beta^n \\ &= \alpha^{n-1}(\alpha^n + \beta^n) + \beta^{n-1}(\alpha^n + \beta^n) - \alpha^n\beta^{n-1} - \alpha^{n-1}\beta^n \\ &= (\alpha^n + \beta^n)(\alpha^{n-1} + \beta^{n-1}) - (\beta^{n-1}\alpha^{n-1})(\alpha + \beta) \end{aligned}$$

$$= V_n V_{n-1} - PQ^{n-1}$$

iii. $V_{2n+1} = \alpha^{2n+1} + \beta^{2n+1}$

$$= \alpha^n \alpha^{n+1} + \beta^n \beta^{n+1} + \alpha^{n+1}\beta^n - \alpha^{n+1}\beta^n + \alpha^n \beta^{n+1} - \alpha^n \beta^{n+1}$$

$$= \alpha^{n+1}(\alpha^n + \beta^n) + \beta^{n+1}(\alpha^n + \beta^n) - \alpha^n \beta^n (\alpha + \beta)$$

$$= (\alpha^n + \beta^n)(\alpha^{n+1} + \beta^{n+1}) - \alpha^n \beta^n (\alpha + \beta)$$

$$= V_{n+1} V_n - PQ^n$$

Özel olarak (4.1) ile verilen eşitliklerde $Q = 1$ yazılırsa

$$\begin{aligned} V_{2n} &= V_n^2 - 2 \\ V_{2n-1} &= V_n V_{n-1} - P \\ V_{2n+1} &= V_{n+1} V_n - P \end{aligned} \tag{4.2}$$

rekürans bağıntıları elde edilir.

Teorem 4.2: $x^2 - Px + Q$ polinomu üzerinde tanımlı $V_n(P, Q)$ dizisinin terimleri arasında

$$V_{nk}(P, Q) = V_n(V_k(P, Q), Q^k)$$

bağıntısı vardır.

İspat: x_1 ve x_2

$$x^2 - Px + Q$$

polinomunun sıfırları olmak üzere Tanım 2.52 den

$$V_k(P, Q) = x_1^k + x_2^k$$

olup

$$x_1^k = \alpha_1$$

$$x_2^k = \alpha_2$$

alalım. Sıfırları α_1 ve α_2 olan polinom

$$\alpha^2 - P'\alpha + Q'$$

olsun. Bu durumda

$$\begin{aligned} P' &= \alpha_1 + \alpha_2 \\ &= x_1^k + x_2^k \\ &= V_k(P,Q) \end{aligned}$$

ve

$$\begin{aligned} Q' &= \alpha_1.\alpha_2 \\ &= x_1^k.x_2^k \\ &= (x_1.x_2)^k \\ &= Q^k \end{aligned}$$

dir. Bu durumda

$$\begin{aligned} V_{nk}(P,Q) &= x_1^{nk} + x_2^{nk} \\ &= (x_1^k)^n + (x_2^k)^n \\ &= \alpha_1^n + \alpha_2^n \\ &= V_n(P',Q') \end{aligned}$$

$$= \quad V_n(V_k(P,Q), Q^k)$$

elde edilir.

Teorem 4.3 (LEHMER): $p > 2$, $p \nmid Q$ ve $\varepsilon = \left(\frac{\Delta}{p}\right) \equiv \Delta^{\frac{p-1}{2}} (\text{mod } p)$ Legendre değeri olmak üzere aşağıdaki denklik vardır.

$$V_{(p-\varepsilon)m}(P,Q) \equiv 2Q^{m(\frac{1-\varepsilon}{2})} \ (\text{mod } p)$$

İspat: n tek asal sayı ve sıfırları x_1, x_2 olan $x^2 - Px + Q$ polinomu için

$$\begin{aligned} x_1 + x_2 &= P \\ x_1 . x_2 &= Q \\ \Delta &= P^2 - 4Q \end{aligned} \tag{4.3}$$

olmak üzere

$$x_1 = \frac{P + \sqrt{\Delta}}{2}$$

$$x_2 = \frac{P - \sqrt{\Delta}}{2}$$

olup buradan

$$\begin{aligned} 2x_1 &= P + \sqrt{\Delta} \\ 2x_2 &= P - \sqrt{\Delta} \end{aligned} \tag{4.4}$$

yazılabilir.

a) $\varepsilon = 1$ için (4.4) eşitliklerinin $n-1$. kuvvetleri alınırsa

$$\begin{aligned} 2^{n-1} {x_1}^{n-1} &= (P + \sqrt{\Delta})^{n-1} \\ &= P^{n-1} + \binom{n-1}{1} P^{n-2}\sqrt{\Delta} + \binom{n-1}{2} P^{n-3}\sqrt{\Delta}^2 + \cdots + \binom{n-1}{n-2} P\sqrt{\Delta}^{n-2} + \binom{n-1}{n-1}\sqrt{\Delta}^{n-1} \end{aligned}$$

ve

$$2^{n-1}{x_2}^{n-1} = (P-\sqrt{\Delta})^{n-1}$$

$$= P^{n-1} - \binom{n-1}{1}P^{n-2}\sqrt{\Delta} + \binom{n-1}{2}P^{n-3}\sqrt{\Delta}^2 - \cdots - \binom{n-1}{n-2}P\sqrt{\Delta}^{n-2} + \binom{n-1}{n-1}\sqrt{\Delta}^{n-1}$$

elde edilir. Bu eşitlikler taraf tarafa toplanırsa

$$2^{n-1}({x_1}^{n-1} + {x_2}^{n-1}) = 2P^{n-1} + 2\binom{n-1}{2}P^{n-3}\sqrt{\Delta}^2 + \cdots + 2\binom{n-1}{n-3}P^2\sqrt{\Delta}^{n-3} + 2\binom{n-1}{n-1}\sqrt{\Delta}^{n-1}$$

$$2^{n-1}V_{n-1} = 2P^{n-1} + 2\binom{n-1}{2}P^{n-3}\sqrt{\Delta}^2 + \cdots + 2\binom{n-1}{n-3}P^2\sqrt{\Delta}^{n-3} + 2\binom{n-1}{n-1}\sqrt{\Delta}^{n-1}$$

bulunur. Bu son eşitlikte $0 < k < n$, $\binom{n}{k} \equiv 1 \pmod{n}$ olduğu göz önüne alınırsa

$$2^{n-1}V_{n-1} \equiv 2P^{n-1} + 2P^{n-3}\sqrt{\Delta}^2 + \cdots + 2\sqrt{\Delta}^{n-1} \pmod{n}$$

$$2^{n-1}V_{n-1} \equiv 2\sqrt{\Delta}^{n-1}\left[\frac{P^{n-1}}{\sqrt{\Delta}^{n-1}} + \frac{P^{n-3}}{\sqrt{\Delta}^{n-3}} + \cdots + \frac{P^2}{\sqrt{\Delta}^2} + 1\right] \pmod{n}$$

$$2^{n-1}V_{n-1} \equiv 2\sqrt{\Delta}^{n-1}\left[\left(\frac{P^2}{\Delta}\right)^{\frac{n-1}{2}} + \left(\frac{P^2}{\Delta}\right)^{\frac{n-3}{2}} + \cdots + \left(\frac{P^2}{\Delta}\right)^{1} + 1\right] \pmod{n}$$

$$2^{n-1}V_{n-1} \equiv 2\sqrt{\Delta}^{n-1}\left[\frac{\left(\frac{P^2}{\Delta}\right)^{\frac{n-1}{2}+1} - 1}{\frac{P^2}{\Delta} - 1}\right] \pmod{n}$$

$$2^{n-1}V_{n-1} \equiv 2\sqrt{\Delta}^{n-1}\left[\frac{P^{n+1} - \Delta^{\frac{n+1}{2}}}{\Delta^{\frac{n+1}{2}}} \cdot \frac{\Delta}{P^2-\Delta}\right] \pmod{n}$$

$$2^{n-1}V_{n-1} \equiv 2\frac{P^{n+1} - \Delta^{\frac{n+1}{2}}}{P^2-\Delta} \pmod{n} \tag{4.5}$$

yazılır. p asal sayı olmak üzere Fermat teoreminden

$$2^{p-1} \equiv 1 \pmod{p}$$

$$P^{p+1} \equiv P^2 \pmod{p}$$

$$\Delta^{\frac{p+1}{2}} \equiv \Delta \pmod{p}$$

eşitlikleri göz önüne alınarak (4.5) eşitliğinde $n = p$ değeri yazılırsa

$$2^{p-1}V_{p-1} \equiv 2\frac{P^2-\Delta}{P^2-\Delta} \pmod{p}$$

$$2^{p-1}V_{p-1} \equiv \ 2 \ (\text{mod}\ p)$$

$$V_{p-1} \equiv \ 2 \ (\text{mod}\ p) \tag{4.6}$$

elde edilir.

b) Benzer olarak $\varepsilon = -1$ için (4.4) eşitliklerinin $n+1$. kuvvetlerini alınırsa

$$2^{n+1}{x_1}^{n+1} = \ (P + \sqrt{\Delta})^{n+1}$$

$$= \ P^{n+1} + \binom{n+1}{1} P^n \sqrt{\Delta} + \binom{n+1}{2} P^{n-1} \sqrt{\Delta}^2 + \cdots + \binom{n+1}{n+1} \sqrt{\Delta}^{n+1}$$

ve

$$2^{n+1}{x_2}^{n+1} = \ (P - \sqrt{\Delta})^{n+1}$$

$$= \ P^{n+1} - \binom{n+1}{1} P^n \sqrt{\Delta} + \binom{n+1}{2} P^{n-1} \sqrt{\Delta}^2 - \cdots + \binom{n+1}{n+1} \sqrt{\Delta}^{n+1}$$

elde edilir.

Bu eşitlikler taraf tarafa toplanırsa

$$2^{n+1}({x_1}^{n+1} + {x_2}^{n+1}) = \ \ 2P^{n+1} + 2\binom{n+1}{2} P^{n-1} \sqrt{\Delta}^2 + \cdots + 2\binom{n+1}{n+1} \sqrt{\Delta}^{n+1}$$

ve gerekli düzenlemeler yapılırsa,

$$2^n V_{n+1} \equiv \ P^{n+1} + \tbinom{n+1}{2} P^{n-1} \sqrt{\Delta}^2 + \cdots + \tbinom{n+1}{n+1} \sqrt{\Delta}^{n+1} \ (\text{mod}\ n)$$

$$2V_{n+1} \equiv \ P^2 + \sqrt{\Delta}^{n+1} \ (\text{mod}\ n)$$

$$2V_{n+1} \equiv \ P^2 + \Delta . \sqrt{\Delta}^{n-1} \ (\text{mod}\ n)$$

$$2V_{n+1} \equiv \ P^2 + \Delta . \Delta^{\frac{n-1}{2}} \ (\text{mod}\ n)$$

olduğu görülür. Burada p asal sayı olmak üzere $n = p$ alındığında Teorem 2.29 gereğince

$$\Delta^{\frac{p-1}{2}} \equiv \ -1 \ (\text{mod}\ p)$$

olup

$$2V_{p+1} \equiv \ P^2 + \Delta.(-1) \ (\text{mod}\ p)$$

veya

$$2V_{p+1} \equiv \ P^2 - \Delta \ (\text{mod}\ p)$$

yazılır. Burada (4.3) eşitliği göz önüne alınırsa

$$2V_{p+1} \equiv \ 4Q \ (\text{mod}\ p)$$

veya

$$V_{p+1} \equiv \ 2Q \ (\text{mod}\ p) \qquad (4.7)$$

elde edilir.

Ayrıca (4.6) ve (4.7) eşitliklerini

$$V_{p-\varepsilon} \equiv 2Q^{f(\varepsilon)} \ (\text{mod}\ p)$$

şeklinde tek bir denklem ile ifade etmek için

$$f(1) = 0,$$

$$f(-1) = 1$$

şartlarını sağlayan

$$f(x) = ax + b$$

fonksiyonunu göz önüne alalım. Bu fonksiyonun katsayıları

$$f(1) = a + b = 0$$

$$f(-1) = -a + b = 1$$

şeklinde elde edilen denklem sisteminin çözümünden

$$a = -\frac{1}{2}$$

ve

$$b = \frac{1}{2}$$

olarak bulunur. Buradan

$$V_{p-\varepsilon}(P,Q) \equiv \quad 2Q^{\left(\frac{1-\varepsilon}{2}\right)} \pmod{p} \tag{4.8}$$

elde edilmiş olur. Son olarak Teorem 4.2 ye göre

$$V_{(p-\varepsilon)m}(P,Q) = V_{(p-\varepsilon)}(V_m(P,Q), Q^m) = 2(Q^m)^{\left(\frac{1-\varepsilon}{2}\right)}$$

olduğu (4.8) denkliğinde göz önüne alındığında

$$V_{(p-\varepsilon)m}(P,Q) \equiv 2Q^{m\left(\frac{1-\varepsilon}{2}\right)} \pmod{p} \tag{4.9}$$

bulunur. Böylece teoremin ispatı tamamlanmış olur.

4.1.2. V_n değerinin hızlı hesaplanması

H. C. Williams (1982) "A $p+1$ Method of Factoring" isimli makalesinde Teorem 4.1 de verilen rekürans bağıntıları yardımıyla Lucas sayı dizisinin terimlerini hızlı olarak hesaplamak için kullanışlı bir yöntem önermiştir.

V_n değerini bu yöntemle hesaplayabilmek için öncelikle n sayısının ikilik sistemdeki karşılığı bulunur.

V_0 ve V_1 başlangıç değerleri ve (4.2) ile verilen rekürans bağıntıları kullanılarak V_n değeri bulununcaya kadar n sayısının ikilik sistemde soldan sağa doğru basamaklarındaki her sayı değeri için sırasıyla aşağıdaki terimler hesaplanır.

i. her 0 değeri için;
- $V_{2k} = V_k^2 - 2$
- $V_{2(k+1)-1} = V_{k+1}V_k - P$

ii. her 1 değeri için;
- $V_{2k+1} = V_k V_{k+1} - P$

- $V_{2(k+1)} = V_{k+1}^2 - 2$

Aşağıdaki Tablo 4.1 de örnek olarak $V_{25}(P,1)$ değerinin bu yöntemle nasıl hesaplandığı verilmiştir

Tablo 4.1. $\mathbf{25 = (11001)_2}$ sayısı için $\boldsymbol{V_{25}(P,1)}$ değerininin hesaplanması.

Basamağın sayı değeri	Kullanılan Terimler	Hesaplanan Terimler
1	V_0 ve V_1	$V_1 = V_1.V_0 - P$=3
	V_1	$V_2 = {V_1}^2 - 2$=7
1	V_1 ve V_2	$V_3 = V_2.V_1 - P$=18
	V_2	$V_4 = {V_2}^2 - 2$=47
0	V_3	$V_6 = {V_3}^2 - 2$=322
	V_3 ve V_4	$V_7 = V_4.V_3 - P$=843
0	V_6	$V_{12} = {V_6}^2 - 2$=103682
	V_6 ve V_7	$V_{13} = V_7.V_6 - P = 271443$
1	V_{12} ve V_{13}	$V_{25} = V_{13}.V_{12} - P = 28143753123$
	V_{13}	$V_{26} = {V_{13}}^2 - 2 = 73681302247$

$P = 3, Q = 1, V_0 = 2, V_1 = P = 3$

4.1.3. $V_{n!}$ Değerinin hesaplanması

Teorem 4.3 in bir sonucu olarak $V_{n!}(P,1)$ terimi çok hızlı olarak hesaplanabilir.

$$V_{n!}(P,1) = V_n\big(V_{(n-1)!}(P,1),1\big) \tag{4.10}$$

4.1.4. Algoritmanın teorik alt yapısı

p ve q farklı asallar olmak üzere $n = pq$ olsun. Özel olarak $Q = 1$ ve $\varepsilon = -1$ değerlerini sağlayan herhangi bir P tam sayısı ile oluşturulan $V_n(P,1)$ genelleştirilmiş Lucas sayı dizisi için (4.9) eşitliği göz önüne alınırsa,

$$V_{(p+1)m} \equiv 2 \pmod p$$

olup Tanım 2.10 dan

$$p\big|\big(V_{(p+1)m} - 2\big) \tag{4.11}$$

elde edilir. Teorem 2.3 e göre

$$V_{(p+1)m} - 2 = n.t + r \tag{4.12}$$

olacak şekilde t ve r tam sayıları vardır. Buradan,

$$r = \left(V_{(p+1)m} - 2\right) - n.t \tag{4.13}$$

yazılır. (4.13) eşitliğinde (4.11) ve $p|n$ olduğu göz önüne alınırsa, teorem 2.2 (ii) gereğince

$$p|r \tag{4.14}$$

olduğu görülür.

Ayrıca (4.12) den

$$\left(V_{(p+1)m} - 2\right) - r = n.t$$

yazılır. Tanım 2.1 e göre

$$n|\left[\left(V_{(p+1)m} - 2\right) - r\right]$$

olup Tanım 2.7 ye göre de

$$r \equiv V_{(p+1)m} - 2 \pmod{n} \tag{4.15}$$

elde edilir.

Son olarak (4.14) ve (4.15) ifadeleri göz önüne alındığında

$$p|\ [\ \left(V_{(p+1)m} - 2\ \right) \bmod n\ ]$$

veya

$$\left(\left(\left(V_{(p+1)m} - 2\right) \bmod n\right), n\right) = p \tag{4.16}$$

olduğu görülür.

Bu (4.16) eşitliği bize Genelleştirilmiş Lucas sayı dizilerinin herhangi bir tam sayının asal çarpanını bulmak için kullanılabileceğini göstermektedir.

4.1.5. $P + 1$ Algoritmasının kurulması

Şimdi n sayısının çarpanlarından biri olan p asalı için

$$p+1=\prod_{i=1}^{k} p_i^{\alpha_i} = {p_1}^{\alpha_1}.{p_2}^{\alpha_2}\dots{p_k}^{\alpha_k}$$

olduğunu varsayalım.

$${p_k}^{\alpha_k} = B$$

olsun. Bu durumda

$$(p+1)|B!$$

olduğundan

$$V_{B!}(P,Q) \equiv 2 \pmod{p}$$

ve bunun sonucunda

$$p|\,(V_{B!}(P,Q)-2)$$

yazılabilir.

Bu durumda aşağıdaki adımlar uygulanarak algoritma elde edilir.

i. $i = 0, 1,2,3$ ... için $V_{i!} \bmod n$ hesaplanır.

ii. Her adımda $((V_{i!} \bmod n) - 2, n) \neq 1$ olup olmadığı kontrol edilir.

iii. $i = B$ için $((V_{B!} \bmod n) - 2, n) = p$ olup n sayısının p çarpanı elde edilir.

Şayet $p + 1$ sayısının en büyük asal çarpanı olan B yeterince küçük bir değere sahipse bu asalla oluşturulan n bileşik sayısının çarpanı bu şekilde hesaplanabilir.

Algoritmanın genel yapısı Algoritma 4.1'de verilmiştir

Algoritma 4.1. $p+1$ Çarpanlara Ayırma Algoritması

GİRDİ : p ve q asallar olmak üzere $n = pq$ şeklindeki n sayısı
ÇIKTI : p ile q asalları
Adım 1: Başla
Adım 2: n sayısını oku
Adım 3: $P \leftarrow 3, Q \leftarrow 1$
Adım 4: $V_0 \leftarrow 2, V_1 \leftarrow P$
Adım 5: $j \leftarrow 2$ için Döngüyü Başlat
Adım 6: $V \leftarrow V_{j!} \bmod n$
Adım 7: $d \leftarrow (V-2, n)$
Adım 8: Eğer $d \neq 1$ ise $d, \frac{N}{d}$ sayılarını yaz ve Adım 10'a git.
Adım 9: $j \leftarrow j+1$
Adım 10: Adım 5'e git.
Adım 11: Döngüyü sonlandır.
Adım 12: Bitir.

Örnek: Çarpanlara ayrılacak sayı $n = 5682511$ olsun. Sırası ile

$$[V_{0!} \rightarrow V_{1!} \rightarrow V_{2!} \rightarrow V_{3!} \rightarrow \cdots] \bmod 5682511$$

terimleri hesaplanırsa $V_{43!}$ için

$$\left((V_{43!} \bmod 5682511) - 2\ ,5682511\right) = 2837$$

olup $p = 2837$ çarpanı elde edilir.

Burada $p+1 = 2.3.11.43$ olduğundan algoritma $V_{43!}$ değerine ulaştığında verilen n tam sayısının asal çarpanı elde edilmektedir.

4.1.5.1. İki aşamalı algoritma

Algoritmanın daha verimli çalışması için iki aşamalı olarak adlandırılan ve aynı zamanda $p-1$ algoritmasında kullanılan yöntem bu algoritma için aşağıdaki şekilde uygulanmıştır.

Şimdi n sayısının çarpanlarından biri olan p asalı için

$$p+1 = \prod_{i=1}^{k} p_i^{\alpha_i} = {p_1}^{\alpha_1}.{p_2}^{\alpha_2} \ldots {p_k}^{\alpha_k}$$

olduğunu varsayalım.

$$p_k{}^{\alpha_k} = B$$

olsun.

Aşağıdakli adımları uygulayalım;

i. Alt sınır B_1 tek sayısı seçilir ve $V_{B_1!} \pmod n$ değeri hesaplanır.

ii. $i = 0,1,2,3,$ ... için p_i' ler sırası ile B_1 den hemen sonra gelen ardışık asal sayılar olmak üzere $V_{p_i}(V_{B_1!}, 1) \bmod n$ hesaplanır.

iii. Her adımda $\left((V_{p_i}(V_{B_1!}, 1) \bmod n) - 2, n\right) \neq 1$ olup olmadığı kontrol edilir.

iv. $p_i = B$ için $\left((V_B(V_{B_1!}, 1) \bmod n) - 2, n\right) = p$ olup n sayısının p çarpanı elde edilir.

Örnek: Çarpanlara ayrılacak sayı $n = 5682511$ olsun.

$B = 15$ sınır olarak seçelim.

Ilk once $V_{15!}(P, 1)$ değerini $\bmod 5682511$ de hesaplanır.

$V_{17}(V_{15!}(P, 1), 1)$ değerini $\bmod 5682511$'de hesaplanır.

Sonra sırası ile

$$[V_{17}(V_{15!}, 1) \to V_{19}(V_{15!}, 1) \to V_{23}(V_{15!}, 1) \to \cdots] \bmod 5682511$$

terimleri hesaplanırsa $V_{43}(V_{15!}, 1)$ için

$$([V_{43}(V_{15!}, 1) \bmod 5682511] - 2, 5682511) = 2837$$

olup $p = 2837$ çarpanı elde edilir.

5. SONUÇ

Bu çalışmada, RSA kripto sisteminin anahtar üretiminde göz önünde bulundurulması bir zorunluluk olan Özel Amaçlı Çarpanlara Ayırma Algoritmalarının bazıları hakkında özet bilgi verilmiş ve Williams $p+1$ algoritması ve teorik alt yapısı detaylı olarak ele alınmıştır.

Gordon (1984) RSA kripto sistemi için hem Pollard $p-1$ hem de Williams $p+1$ algoritmalarına karşı dayanıklı asal sayılar üreten bir algoritma önerdi. Algoritma bir fazlasının ve bir eksiğinin en büyük asal çarpanları yeterince büyük olan asal sayılar üretmektedir. (Menezes vd., 1997 Sayf. 150)

KAYNAKLAR

Altındiş, H. (2011) Sayılar teorisi ve uygulamaları 3. Baskı, ***Erciyes Üniversitesi Fen Fakültesi Matematik Bölümü***, Ankara.

Akın, Ö., Bulgak, H. (1998) Lineer Fark Denklemleri ve Kararlılık Teorisi, ***Selçuk Üniversitesi Basımevi***, Konya.

Amirali, G., Duru, H. (2002) Nümerik Analiz, Pegem Yayıncılık, Ankara.

Asar, A., Arıkan, A. ve Arıkan, A. (2012) Cebir 2. Baskı, ***Gazi Kitabevi***, Ankara.

Asar, A., Arıkan, A. (2012) Sayılar Teorisi, ***Gazi Kitabevi***, Ankara.

Aydın, M., Kuryel, B., Gündüz, G. ve Oturanç, G. (2016) Diferansiyel Denklemler ve Uygulamaları, ***Barış Yayınları Fakülteler Kitabevi***, İzmir.

Aybak, L. (2010) "Sayı Cismi çarpanlara ayırma yöntemi", Yüksek Lisans Tezi, ***Ankara Üniversitesi Fen Bilimleri Enstitüsü***, Ankara.

Bayraktar, M. (2006) Fonksiyonel Analiz, ***Gazi Kitabevi***, Ankara.

Cengiz, N., Tarakçı, Ö., Aktaş, M., Tosun, M., Kadakal, M., Şengül, S., Kaplan, A., Kır, E., (2010) Genel Matematik 1, Sağel, M. K, Aktaş M., ***Pegem Yayınevi.***

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

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

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

Erdoğan, M., Yılmaz, G. (2008) Çözümlü Problemlerle Soyut Cebir ve Sayılar Teorisi, ***Bilkent Üniversitesi Yayınevi***, İstanbul.

Gordon, J. (1984) "Strong RSA keys", ***Electronics Letters***, 20(12) 514-516.

Hacısalihoğlu, H., Hacıyev, A., Kalantarov, V., Sabuncuoğlu, A., Brown, L. M., İbikli, E., Brown, S. (2000) Matematik Terimleri Sözlüğü, ***Türk Dil Kurumu Yayınları***, Ankara.

Hoggat, V. E. (1969) "Fibonacci and Lucas Numbers", Houghton- Mifflin, Palo Alto, California, 92 p.

Karaman, E. (2010) "Yüksek mertebeden fark denklemlerinin salınımlılık davranışı", ***Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü***, Afyonkarahisar.

Kılıç, E.T. (2010) "İkinci dereceden bazı indirgeme dizileri", Yüksek Lisans Tezi, ***Ankara Üniversitesi Fen Bilimleri Enstitüsü***, Ankara.

Kolman, B. (2000) Lineer Cebir, Kaya, R., Arvasi, Z., Dağ, İ., Eser, D., Kocayusufoğlu, E., Koçak, M., Olgun, Ş., Özer, M. N., ***Bilim Teknik Yayınevi***, İstanbul.

Koshy, T. (2001) Fibonacci and Lucas numbers with applications, ***Pure and Applied Mathematics, Wiley-Interscience***, New York, 641 p.

Kutay, V. (2010) "Fark denklemleri", Yüksek Lisans Tezi, ***Ankara Üniversitesi Fen Bilimleri Enstitüsü***, Ankara.

Lehmer, D. H., (1930) "An extended theory of Lucas' functions", ***The Annals of mathematics***, Second Series, Vol. 31, No. 3, pp. 419-448.

Lenstra, H. W. Jr. (1987) "Factoring integers with elliptic curves", ***Annals Mathematics***, 126, 649-673.

Lucas, E., (1878) "Théorie des fonctions numériques simplement périodiques", ***American Journal of Mathematics***, Vol. 1, No. 2, pp. 184-196.

Lucas, E., (1878) "Théorie des fonctions numériques simplement périodiques. [Continued]", ***American Journal of Mathematics***, Vol. 1, No. 3, pp. 197-240.

Lucas, E., (1878) "Théorie des fonctions numériques simplement périodiques. [Continued]", ***American Journal of Mathematics***, Vol. 1 No. 4, pp. 289-321.

Menezes, A. J., Van Oorschot, P. C. and Vanstone, S. A. (1997) Handbook of Applied Cryptography, ***CRC Press***.

McKee, J., (1996) "Turning Euler's factoring method into a factoring algorithm", ***Bulletin of the London Mathematical Soceity,*** 4(28), 351-355.

Nuriyeva, F. (2010) "Çarpanlara ayırma algoritmaları", Yüksek Lisans Tezi, ***Ege Üniversitesi Fen Bilimleri Enstitüsü***, İzmir.

Okumuş, İ. (2012) "RSA kriptositeminin hızını etkileyen faktörler", Doktora Tezi, ***Atatürk Üniversitesi Fen Bilimleri Enstitüsü***, Erzurum.

Pamukçu, B. (2006) "Factorization methods for cryptography", MS Thesiz, İstanbul.

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

Rivest, 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.

Robbins, N. (1993) Beginning number theory, ***Wm. C. Brown Publishers***, Dubuque, Iowa, 308 p.

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

Uçar, Z. (2013) "Fark denklem sistemlerinin çözümleri ve global davranışları", Yüksek Lisans Tezi, ***Niğde Üniversitesi Fen Bilimleri Enstitüsü***, Niğde.

Vajda, S. (1989) “Fibonacci & Lucas numbers and golden section”, ***John Wiley & Sons, Inc.***, New York, 190 p.

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

Williams, H. C., Dubner, H. (1986) “The primality of R1031”, ***Mathematics of Computation***, Vol.47, No. 176, pp. 703-711.

EKLER

Ek-1. Tez Çalışması Süresince Yapılan Akademik Çalışmalar

Okumuş, İ., **Polat, M. K.,** (2018) "$p+1$ Algoritması (Lucas Sayı Dizileri ve Kriptoloji)", Türk Matematik Derneği, 31. Ulusal Matematik Sempozyumu, ERZİNCAN

ÖZGEÇMİŞ

Mehtap Kübra POLAT, 1991 yılında Erzincan'da doğdu. Lise öğrenimini Erzincan Lisesi'nde tamamladı. 2015 yılında Atatürk Üniversitesi Kazım Karabekir Eğitim Fakültesi Matematik Öğretmenliği bölümünden mezun oldu. 2016 yılında Erzincan Binali Yıldırım Üniversitesi Fen Bilimleri Enstitüsü Matematik Bölümünde yüksek lisans eğitimine başladı.