SİMETRİK HİPERBOLİK FONKSİYONLAR VE BİR KRİPTOGRAFİK UYGULAMA ÜZERİNE

Özge BOSTANCI

YÜKSEK LİSANS TEZİ
MATEMATİK

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

EKİM 2012
ANKARA

Özge BOSTANCI tarafından hazırlanan "SİMETRİK HİPERBOLİK FONKSİYONLAR VE BİR KRİPTOGRAFİK UYGULAMA" adlı bu tezin Yüksek Lisans tezi olarak uygun olduğunu onaylarım.

Prof. Dr. Dursun TAŞÇI .....
Tez Danışmanı, Matematik Anabilim Dalı

Bu çalışma, jürimiz tarafından oy birliği ile Matematik Anabilim Dalında Yüksek Lisans tezi olarak kabul edilmiştir.

Prof. Dr. Sait HALICIOĞLU .....
Matematik Anabilim Dalı, A.Ü.

Prof. Dr. Dursun TAŞÇI .....
Matematik Anabilim Dalı, G.Ü.

Doç. Dr. Naim TUĞLU .....
Matematik Anabilim Dalı, G.Ü.

Tez Savunma Tarihi: 30/10/2012

Bu tez ile G.Ü. Fen Bilimleri Enstitüsü Yönetim Kurulu Yüksek Lisans derecesini onamıştır.

Prof. Dr. Şeref SAĞIROĞLU .....
Fen Bilimleri Enstitüsü Müdürü

SİMETRİK HİPERBOLİK FONKSİYONLAR VE BİR KRİPTOGRAFİK UYGULAMA ÜZERİNE
(Yüksek Lisans Tezi)

Özge BOSTANCI

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
Ekim 2012

ÖZET

A. Stakhov, B. Rozin Fibonacci ve Lucas sayılarına ilişkin Binet formüllerinin sürekli bölgelerdeki genişletmeleri olan simetrik hiperbolik fonksiyonları tanımladılar. Fibonacci dizisinin karakteristik polinomunu göz önüne alarak $a \in Z^+$ **olmak üzere** $x^2 = ax + 1$ **karakteristik polinomuna ilişkin** $U_{n+2} = aU_{n+1} + U_n,\ n \geq 0;\ U_0 = 0, U_0 = 0$ **ve** $V_{n+2} = aV_{n+1} + V_n, n \geq 0;\ V_0 = 2, V_1 = a$ **indirgeme bağıntılarıyla verilen** U_n **ve** V_n **dizileri elde edilebilir.**

Bu tezde U_n, V_n **dizilerinin özellikleri,** U_n, V_n **dizileri arasındaki ilişkiler ve ayrıca bu dizilerin hiperbolik fonksiyonlarla olan ilişkileri verildi.** U_n, V_n **dizilerinin sürekli halleri olan simetrik hiperbolik fonksiyonlar tanımlandı. Bu fonksiyonlar yardımıyla Genelleştirilmiş Altın Matrisler tanımlandı. Son olarak Genelleştirilmiş Altın Matrislerin kullanıldığı bir Kriptografik uygulama verildi.**

Bilim kodu : 204.1.025
Anahtar Kelimeler : Simetrik hiperbolik fonksiyonlar, kriptoloji
Sayfa adedi : 88
Tez Yöneticisi : Prof. Dr. Dursun TAŞÇI

ON THE SYMMETRICAL HYPERBOLİC FUNCTIONS AND A CRYPTOGRAPHIC APPLICATION

(M. Sc. Thesis)

Özge BOSTANCI

GAZİ UNIVERSITY
INSTUTE OF SCIENCE AND TECHNOLOGY

October 2012

ABSTRACT

A. Stakhov, B. Rozin defined symmetrical hyperbolic functions which are the being extensions of Binet formulas for the Fibonacci and Lucas numbers in continuous domain. By concidering the characteristical polynomial of the Fibonacci sequences, the sequences U_n and V_n for the characteristical polynomial $x^2 = ax + 1$, $a \in Z^+$ can be obtained with following reccurence relations $U_{n+2} = aU_{n+1} + U_n$, $n \geq 0$; $U_0 = 0$, $U_1 = 1$ and $V_{n+2} = aV_{n+1} + V_n$, $n \geq 0$; $V_0 = 2$, $V_1 = a$.

In this thesis, the proporties of U_n and V_n, the relations between U_n and V_n, also the relations between hyperbolic functions and them were given. Furthermore, the symmetrical hyperbolic functions U and V were defined, which are continuous cases of U_n and V_n. By the help of these functions, Generalized Golden Matrices were defined. Finally, a cryptographic application were given, in which the Generalized Golden Matrices are used.

Science Code : 204.1.025
Key Words : Symmetrical Hyperbolic Functions, cryptography
Page number : 88
Adviser : Prof. Dr. Dursun TAŞÇI

TEŞEKKÜR

Çalışmamın her aşamasında yakın ilgi ve önerileri ile beni yönlendiren saygıdeğer Hocam Prof. Dr. Dursun TAŞÇI'ya; yine tecrübelerinden faydalandığım, bu süreçte her türlü yardımını esirgemeyen ve bana destek olan sevgili hocam Doç. Dr. Naim TUĞLU'ya; bu yolda ilerlememe vesile olan ve cesaretlendiren tüm lisans hocalarıma; hayat boyu her türlü sıkıntımda yanımda olan ve bu süreçte bana anlayış gösteren sevgili aile fertlerime ve arkadaşlarıma en içten saygı ve teşekkürlerimi sunmayı bir borç bilirim.

İÇİNDEKİLER

Sayfa

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış bazı simgeler, açıklamaları ile birlikte aşağıda sunulmuştur.

Simgeler	**Açıklama**
U_n	$n.\ U$ sayısı
V_n	$n.\ V$ sayısı
$\det E$	E matrisinin determinantı
$\det M$	M matrisinin determinantı
$\det U^n$	U^n matrisinin determinantı

1. GİRİŞ

Bu çalışmada $n \geq 0$ ve a,b keyfi tamsayılar olmak üzere;

$$U_{n+2} = aU_{n+1} + bU_n \tag{1.1}$$

$$U_0 = 0\,, U_t = 1 \tag{1.2}$$

Eş. 1.2 başlangıç şartlarıyla birlikte verilen Eş. 1.2 reküransının ürettiği dizileri inceleyeceğiz.

Eş. 1.1'de $a = b = 1$ aldığımızda;

$$U_{n+2} = U_{n+1} + U_n\,, n \geq 0 \tag{1.3}$$

$$U_0 = 0\,, U_t = 1 \tag{1.4}$$

Fibonacci indirgeme bağıntısını elde ederiz. Eş. 1.4 başlangıç şartlarıyla birlikte verilen Eş. 1.3 rekürans bağıntısı $\{0,1,1,2,3,5,8,...\}$ Fibonacci sayılarını üretir. Eş. 1.4 başlangıç şartlarını $U_o = 2$, $U_1 = 1$ olarak değiştirirsek Eş. 1.3 rekürans bağıntısı $\{2,1,3,4,7,11,...\}$ Lucas sayılarını üretir.

Eş. 1.1'de $a = 2$, $b = 1$ aldığımızda;

$$U_{n+2} = 2U_{n+1} + U_n \ , \ n \geq 0 \tag{1.5}$$

$$U_0 = 0\,, U_t = 1 \tag{1.6}$$

indirgeme bağıntısını buluruz. Eş. 1.6 başlangıç şartlarıyla birlikte verilen Eş. 1.5 reküransı $\{0,1,2,5,12,29...\}$ Pell sayılarını üretir. Eş. 1.6 başlangıç şartlarını $U_0 = 2$, $U_1 = 2$ olarak değiştirirsek; Eş. 1.5 reküransı $\{2,2,6,14,34,...\}$ Pell Lucas saylarını,

$U_0 = 1$, $U_1 = 1$ olarak değiştirirsek $\{1,1,3,7,17,....\}$ Modife Edilmiş Pell sayılarını üretir$[1-16]$.

2. U_n VE V_n DİZİLERİ İLE U^n MATRİSLERİ

2.1. U_n Dizileri ve Genel Özellikleri

Bu çalışmada, keyfi a pozitif tamsayısı ve $n \geq 0$ olmak üzere;

$$U_{n+2} = aU_{n+1} + U_n \tag{2.1}$$

$$U_1 = 1, U_0 = 0 \tag{2.2}$$

reküransının ürettiği U_n dizisi üzerinde duracağız.

Eş. 2.1 reküransının karakteristik denklemi;

$$x^2 = ax + 1 \tag{2.3}$$

dir. $a \geq 1$ olduğundan Eş. 2.3 karakteristik denkleminin iki reel kökü vardır. Bu kökler $\alpha = \frac{a + \sqrt{a^2 + 4}}{2}$ ve $\beta = \frac{a - \sqrt{a^2 + 4}}{2}$ dir. $a \geq 1$ olduğundan α, Eş. 2.3 denkleminin pozitif kökü, β ise negatif köküdür.

α ve β sayılarını kullanarak Eş. 2.2 başlangıç şartlarıyla birlikte verilen Eş. 2.1 reküransının ürettiği U_n dizisi için genel formül bulalım. $\forall n \in \mathrm{N}$ için c_1, c_2 sabitler olmak üzere;

$$U_n = c_1 a\alpha^n + c_2\beta^n \tag{2.4}$$

$$U_0 = 0, U_1 = 1 \tag{2.5}$$

dir. Eş. 2.5 başlangıç şartlarını kullanarak Eş. 2.4 denklemini çözelim.

$n=0$ için;

$$U_0 = 0 = c_1 a + c_2 \tag{2.6}$$

dir. $n=1$ için;

$$U_1 = 1 = c_1 a\alpha + c_2 \beta \tag{2.7}$$

dir. Eş. 2.6 ve Eş. 2.7 birlikte düşünüldüğünde $c_1 = \frac{1}{a(\alpha-\beta)}$ ve $c_2 = \frac{-1}{\alpha-\beta}$ bulunur. c_1 ve c_2'nin değerleri Eş. 2.4 'te yerine yazılacak olursa;

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \tag{2.8}$$

elde edilir.

$a=1$ için Eş. 2.3; Fibonacci dizisinin karakteristik denklemine, $a=2$ için ise Pell dizisinin karakteristik denklemine dönüşür. Benzer şekilde $a=1$ alındığında α; altın orana, $a=2$ alındığında ise gümüş orana dönüşür. Burada ardışık iki Fibonacci sayısının limit durumunda oranlarının altın orana $\left(\frac{1+\sqrt{5}}{2}\right)$ ve ardışık iki Pell sayısının limit durumunda oranlarının gümüş orana $\left(1+\sqrt{2}\right)$ eşit olduğunu hatırlatalım[1−15]. Yani;

$$\lim_{n\to\infty} \frac{F_{n+1}}{F_n} = \frac{1+\sqrt{5}}{2}$$

$$\lim_{n\to\infty}\frac{P_{n+1}}{P_n}=1+\sqrt{2}$$

eşitlikleri doğrudur.

Aşağıdaki teorem ise U_n dizisinin ardışık iki teriminin limit durumlarında oranlarının Eş. 2.3 karakteristik denkleminin pozitif köküne eşit olacağını gösterir.

2.1. Teorem

$\forall n\in \mathrm{N}$, $a\in \mathrm{Z}^+$ ve U_{n+1} ile U_n; U_n dizisinin ardışık iki terimi olmak üzere;

$$\lim_{n\to\infty}\frac{U_{n+1}}{U_n}=\alpha \tag{2.9}$$

dir. Burada $\alpha=\dfrac{a+\sqrt{a^2+4}}{2}$ dir.

İspat

Eş. 2.9'un her iki tarafını α ile çarparsak, gerekli düzenlemelerden sonra;

$$\begin{aligned}\alpha U_n &= \frac{\alpha^{n+1}-\alpha\beta^n}{\alpha-\beta}\\ &= \frac{\alpha^{n+1}-\alpha\beta\beta^{n-1}+\beta^{n+1}-\beta^{n+1}}{\alpha-\beta}\\ &= U_{n+1}+\frac{\beta^{n-1}\left(1+\beta^2\right)}{\alpha-\beta}\\ &= U_{n+1}+\frac{\beta^{n-1}\left(\beta-\alpha\right)\beta}{\alpha-\beta}\end{aligned}$$

$$\alpha U_n = U_{n+1}-\beta^n \tag{2.10}$$

denklemini elde ederiz. Eş. 2.10'un her iki tarafına 1 eklersek;

$$\alpha U_n + 1 = U_{n+1} + 1 - \beta^n \tag{2.11}$$

olur. $1-\beta^n > 0$ olduğundan;

$$U_{n+1} < \alpha U_n + 1 \tag{2.12}$$

dir. $1-\beta^n < 1$ olduğundan;

$$\alpha U_n + 1 < U_{n+1} + 1 \tag{2.13}$$

dir. Eş. 2.12 ve Eş. 2.13 birlikte düşünüldüğünde;

$$U_{n+1} < \alpha U_n + 1 < U_{n+1} + 1 \tag{2.14}$$

eşitsizlik sistemi elde edilir. Tam değer fonksiyonunun tanımından;

$$U_{n+1} = \left[\alpha U_n + 1\right] \tag{2.15}$$

yazılır. Şimdi,

$$\lim_{n\to\infty} \frac{U_{n+1}}{U_n} = \alpha \tag{2.16}$$

olduğunu gösterelim. Eş. 2.15'deki tam değer fonksiyonun tanımı gereği;

$$U_{n+1} = \alpha U_n + 1 + \theta, 0 \le \theta < 1 \tag{2.17}$$

yazılabilir. Eş. 2.17, Eş. 2.16'da kullanılırsa;

$$\lim_{n\to\infty}\frac{U_{n+1}}{U_n}=\lim_{n\to\infty}\frac{\alpha U_n+1+\theta}{U_n}$$

$$=\lim_{n\to\infty}\alpha+\lim_{n\to\infty}\frac{1+\theta}{U_n}$$

$$=\alpha$$

elde edilir.

2.2. V_n Dizileri ve Genel Özellikleri

Keyfi a pozitif tamsayısı ve $n\geq 0$ olmak üzere;

$$V_{n+2}=aV_{n+1}+V_n \tag{2.18}$$

$$V_0=2,\ V_1=a \tag{2.19}$$

şeklindeki indirgeme bağıntısını göz önüne alalım.

$a=1$ alındığında Eş. 2.18; $\{2,1,3,4,7,11,...\}$ Lucas sayılarını, $a=2$ alındığında ise $\{2,2,6,14,...\}$ Pell-Lucas sayılarını üretir.

Eş. 2.18 reküransının karakteristik denklemi, Eş. 2.1 reküransının karakteristik denklemi olan Eş. 2.3'e eşittir. Bu yüzden Eş. 2.3 karakteristik denkleminin kökleri olan $\alpha=\frac{a+\sqrt{a^2+4}}{2}$ ve $\beta=\frac{a-\sqrt{a^2+4}}{2}$ da Eş. 2.18 reküransının karakteristik denkleminin kökleridir.

α ve β 'yı kullanarak Eş. 2.18 rekürans için genel formül bulalım. d_1, d_2 sabitler ve $n\geq 0$ olmak üzere;

$$V_n=d_1a\alpha^n+d_2\beta^n \tag{2.20}$$

$V_0 = 2, V_1 = a$

olarak alalım. Bu durumda $n = 0$ için;

$$V_0 = 2 = d_1 a + d_2 \tag{2.21}$$

dir. n=1 için;

$$V_1 = a = d_1 a\alpha + d_2 \beta \tag{2.22}$$

dir. Eş. 2.21 ve Eş. 2.22 birlikte düşünüldüğünde;

$$\begin{aligned} d_1 a + d_2 &= 2 \\ d_1 a\alpha + d_2 \beta &= a \end{aligned} \tag{2.23}$$

lineer denklem sistemi elde edilir. İki bilinmeyenli iki denklemden oluşan Eş. 2.23 lineer denklem sisteminin katsayılar matrisinin determinantı;

$$\begin{vmatrix} a & 1 \\ a\alpha & \beta \end{vmatrix} = a\beta - a\alpha = a(\beta - \alpha) = -a\sqrt{a^2+4}$$

dir. $a \in Z^+$ olduğundan $-a\sqrt{a^2+4} \neq 0$ dır. O halde Eş. 2.23, Cramer sistemidir. Buna göre;

$$d_1 = \frac{\begin{vmatrix} 2 & 1 \\ a & \beta \end{vmatrix}}{\begin{vmatrix} a & 1 \\ a\alpha & \beta \end{vmatrix}} = \frac{2\beta - a}{-a\sqrt{a^2+4}} = \frac{a - \sqrt{a^2+4} - a}{-a\sqrt{a^2+4}} = \frac{1}{a}$$

bulunur. Benzer şekilde,

$$d_2 = \frac{\begin{vmatrix} a & 2 \\ a\alpha & a \end{vmatrix}}{\begin{vmatrix} a & 1 \\ a\alpha & \beta \end{vmatrix}} = \frac{a^2 - 2a\alpha}{-a\sqrt{a^2+4}} = \frac{a^2 - \sqrt{a^2+4} - a^2}{-a\sqrt{a^2+4}} = 1$$

bulunur. d_1 ve d_2' nin bulunan değerleri Eş. 2.20'de yerine yazılırsa;

$$V_n = \alpha^n + \beta^n \tag{2.24}$$

elde edilir.

Çizelge 2.1.'de, a'ya vereceğimiz pozitif tamsayı değerleri için U_n sayılarını görebiliriz.

Çizelge 2.1. U_n Sayıları

n / a	-5	-4	-3	-2	-1	0	1	2	3	4	5
1	**5**	**-3**	**2**	**-1**	**1**	**0**	**1**	**1**	**2**	**3**	**5**
2	**29**	**-12**	**5**	**-2**	**1**	**0**	**1**	**2**	**5**	**12**	**29**
3	**109**	**-33**	**10**	**-3**	**1**	**0**	**1**	**3**	**10**	**33**	**109**
4	**305**	**-72**	**17**	**-4**	**1**	**0**	**1**	**4**	**17**	**72**	**305**
5	**701**	**-135**	**26**	**-5**	**1**	**0**	**1**	**5**	**26**	**135**	**701**

Çizelge 2.1.'den de görüleceği üzere negatif ve pozitif U_n sayıları arasında aşağıdaki eşitlik verilebilir.

$$U_n = (-1)^{n+1} U_{-n} \tag{2.25}$$

Şimdi, Eş. 2.25'in doğruluğunu gösterelim.

Eş. 2.25'de, Eş. 2.8'i kullanacak olursak;

$$(-1)^{n+1} U_{-n} = (-1)^{n+1} \left(\frac{\alpha^{-n} - \beta^{-n}}{\alpha - \beta} \right)$$

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

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

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

$$= U_n$$

elde edilir.

Benzer şekilde Çizelge 2.2.'de, a'ya vereceğimiz pozitif tamsayı değerleri için V_n sayılarını görebiliriz.

Çizelge 2.2. V_n Sayıları

n / a	-5	-4	-3	-2	-1	0	1	2	3	4	5
1	**-11**	**7**	**-4**	**3**	**-1**	**2**	**1**	**3**	**4**	**7**	**11**
2	**-82**	**34**	**-14**	**6**	**-2**	**2**	**2**	**6**	**14**	**34**	**82**
3	**-393**	**119**	**-36**	**11**	**-3**	**2**	**3**	**11**	**36**	**119**	**393**
4	**-1364**	**322**	**-76**	**18**	**-4**	**2**	**4**	**18**	**76**	**322**	**1364**
5	**-3775**	**727**	**-140**	**27**	**-5**	**2**	**5**	**27**	**140**	**727**	**3775**

Çizelge 2.2. 'den de görüleceği üzere negatif ve pozitif V_n sayıları arasında,

$$V_n = (-1)^n V_{-n} \tag{2.26}$$

şeklinde bir genelleştirme yapabiliriz.

Gerçekten; Eş. 2.24'ü kullanarak,

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

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

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

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

$$= V_n$$

eşitliğini elde ederiz.

U_n ve V_n dizileri arasındaki bazı ilişkileri aşağıdaki teoremle görmek mümkündür.

2.2. Teorem

U_n ve V_n dizileri arasında aşağıdaki bağıntılar vardır:

i) $V_n + \sqrt{a^2 + 4} U_n = 2\alpha^n$ (2.27)

ii) $V_n - \sqrt{a^2 + 4} U_n = 2\beta^n$ (2.28)

iii) $\left(a^2 + 4\right) U_n^2 - V_n^2 = 4(-1)^n$ (2.29)

iv) $U_{n+m} + (-1)^m U_{n-m} = U_n V_m$ (2.30)

v) $U_{n+m} - (-1)^m U_{n-m} = V_n U_m$ (2.31)

vi) $V_{n+m} + (-1)^m V_{n-m} = V_m V_n$ (2.32)

vii) $V_{n+m} - (-1)^m V_{n-m} = (a^2+4) U_n U_m$ (2.33)

viii) $U_{2n} = U_n V_n$ (2.34)

ix) $2V_{2n} = V_n^2 + (a^2+4) U_n^2$ (2.35)

x) $U_{n+1} U_{n-1} - U_n^2 = (-1)^n$ (2.36)

xi) $V_{n+1} V_{n-1} - V_n^2 = (-1)^{n-1} (a^2+4)$ (2.37)

xii) $V_{2n} - V_n^2 = 2(-1)^{n+1}$ (2.38)

xiii) $U_{n+1} + U_{n-1} = V_n$ (2.39)

xiv) $aU_n + V_n = 2U_{n+1}$ (2.40)

xv) $U_{n+1} U_{m+1} + U_n U_m = U_{n+m+1}$ (2.41)

İspat

Verilen bağıntıların doğruluğunu Eş. 2.8 ve Eş. 2.24 genel formüllerini kullanarak gösterelim.

i) $$V_n + \sqrt{a^2+4} U_n = \alpha^n + \beta^n + \sqrt{a^2+4} \left(\frac{\alpha^n - \beta^n}{\alpha - \beta} \right)$$

$$= \alpha^n + \beta^n + \sqrt{a^2+4} \left(\frac{\alpha^n - \beta^n}{\sqrt{a^2+4}} \right)$$

$$= \alpha^n + \beta^n + \alpha^n - \beta^n$$

$$= 2\alpha^n$$

ii) $V_n - \sqrt{a^2+4}U_n = \alpha^n + \beta^n - \sqrt{a^2+4}\left(\frac{\alpha^n - \beta^n}{\alpha - \beta}\right)$

$$= \alpha^n + \beta^n - \sqrt{a^2+4}\left(\frac{\alpha^n - \beta^n}{\sqrt{a^2+4}}\right)$$

$$= \alpha^n + \beta^n - \alpha^n + \beta^n$$

$$= 2\beta^n$$

iii) $\left(a^2+4\right)U_n^2 - V_n^2 = \left(a^2+4\right)\left(\frac{\alpha^n - \beta^n}{\alpha - \beta}\right)^2 - \left(\alpha^n + \beta^n\right)$

$$= \left(a^2+4\right)\frac{\left(\alpha^n - \beta^n\right)^2}{\left(a^2+4\right)} - \left(\alpha^n + \beta^n\right)^2$$

$$= (\alpha^n - \beta^n + \alpha^n + \beta^n)\left(\alpha^n - \beta^n - \alpha^n - \beta^n\right)$$

$$= 2\alpha^n(-2)\beta^n$$

$$= 4(-1)^{n+1}$$

iv) $U_{n+m} + (-1)^m U_{n-m} = \frac{\alpha^{n+m} - \beta^{n+m}}{\alpha - \beta} + (-1)^m\left(\frac{\alpha^{n-m} - \beta^{n-m}}{\alpha - \beta}\right)$

$$= \frac{\left(\alpha^n - \beta^n\right)\left(\alpha^m + \beta^m\right) - \alpha^n\beta^m + \alpha^m\beta^n}{\alpha - \beta} + (-1)^m\left(\frac{\frac{\alpha^n}{\alpha^m} - \frac{\beta^n}{\beta^m}}{\alpha - \beta}\right)$$

$$= U_n V_m + \frac{\alpha^m\beta^n - \alpha^n\beta^m}{\alpha - \beta} + (-1)^m\left(\frac{\alpha^n\beta^m - \alpha^m\beta^n}{(-1)^m(\alpha - \beta)}\right)$$

$$= U_n V_m + \frac{\alpha^m\beta^n - \alpha^n\beta^m}{\alpha - \beta} + \frac{\alpha^n\beta^m - \alpha^m\beta^n}{\alpha - \beta}$$

$$= U_n V_m$$

v) $U_{n+m}-(-1)^m U_{n-m} = \dfrac{(\alpha^n+\beta^n)(\alpha^m-\beta^m)+\alpha^n\beta^m-\alpha^m\beta^n}{\alpha-\beta}-(-1)^m\left(\dfrac{\frac{\alpha^n}{\alpha^m}-\frac{\beta^n}{\beta^m}}{\alpha-\beta}\right)$

$$= V_n U_m + \frac{\alpha^n\beta^m-\alpha^m\beta^n}{\alpha-\beta}-(-1)^m\left(\frac{\alpha^n\beta^m-\alpha^m\beta^n}{(-1)^m(\alpha-\beta)}\right)$$

$$= V_n U_m + \frac{\alpha^n\beta^m-\alpha^m\beta^n}{\alpha-\beta}-\left(\frac{\alpha^n\beta^m-\alpha^m\beta^n}{\alpha-\beta}\right)$$

$$= V_n U_m$$

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

$$= (\alpha^n+\beta^n)(\alpha^m+\beta^m)-\alpha^n\beta^m-\alpha^m\beta^n+(-1)^m\left(\frac{\alpha^n}{\alpha^m}+\frac{\beta^n}{\beta^m}\right)$$

$$= V_n V_m - \alpha^n\beta^m-\alpha^m\beta^n+(-1)^m\left(\frac{\alpha^n\beta^m+\alpha^m\beta^n}{(-1)^m}\right)$$

$$= V_n V_m - \alpha^n\beta^m-\alpha^m\beta^n+\alpha^n\beta^m+\alpha^m\beta^n$$

$$= V_n V_m$$

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

$$= (\alpha^n-\beta^n)(\alpha^m-\beta^m)+\alpha^n\beta^m+\alpha^m\beta^n-(-1)^m\left(\frac{\alpha^n}{\alpha^m}+\frac{\beta^n}{\beta^m}\right)$$

$$= (a^2+4)U_n U_m + \alpha^n\beta^m+\alpha^m\beta^n-(-1)^m\left(\frac{\alpha^n\beta^m+\alpha^m\beta^n}{(-1)^m}\right)$$

$$= (a^2+4)U_n U_m + \alpha^n\beta^m+\alpha^m\beta^n-(\alpha^n\beta^m+\alpha^m\beta^n)$$

$$= (a^2+4)U_n U_m$$

viii) $U_{2n} = \left(\dfrac{\alpha^{2n}-\beta^{2n}}{\alpha-\beta}\right)$

$$= \left(\frac{\alpha^n - \beta^n}{\alpha - \beta} \right) \left(\alpha^n + \beta^n \right)$$

$$= U_n V_m$$

ix) $2V_{2n} = 2\left(\alpha^{2n} + \beta^{2n} \right)$

$$= \alpha^{2n} + 2\alpha^n \beta^n + \beta^{2n} + \alpha^{2n} - 2\alpha^n \beta^n + \beta^{2n}$$

$$= \left(\alpha^n + \beta^n \right)^2 + \left(\frac{\alpha^n - \beta^n}{\alpha - \beta} \right)^2 \left(a^2 + 4 \right)$$

$$= V_n^2 + \left(a^2 + 4 \right) U_n^2$$

x) $U_{n+1} U_{n-1} - U_n^2 = \left(\frac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta} \right) \left(\frac{\alpha^{n-1} - \beta^{n-1}}{\alpha - \beta} \right) - \left(\frac{\alpha^n - \beta^n}{\alpha - \beta} \right)^2$

$$= \frac{\alpha^{2n} - \alpha^{n+1}\beta^{n-1} - \alpha^{n-1}\beta^{n+1} + \beta^{2n}}{a^2 + 4} - \frac{\alpha^{2n} - 2\alpha^n \beta^n + \beta^{2n}}{a^2 + 4}$$

$$= \frac{-\alpha^2 (-1)^{n-1} - \beta^2 (-1)^{n-1} + 2(-1)^n}{a^2 + 4}$$

$$= \frac{(-1)^n \left(a^2 + 4 \right)}{a^2 + 4}$$

$$= (-1)^n$$

xi) $V_{n+1} V_{n-1} - V_n^2 = \left(\alpha^{n+1} + \beta^{n+1} \right) \left(\alpha^{n-1} + \beta^{n-1} \right) - \left(\alpha^n + \beta^n \right)^2$

$$= \alpha^{2n} + \alpha^{n+1}\beta^{n-1} + \alpha^{n-1}\beta^{n+1} - \alpha^{2n} - 2\alpha^n \beta^n - \beta^{2n}$$

$$= \alpha^2 (-1)^{n-1} + \beta^2 (-1)^{n-1} + 2(-1)^{n+1}$$

$$= (-1)^{n-1} \left(\alpha^2 + \beta^2 + 2(-1)^2 \right)$$

$$= (-1)^{n-1} \left(a^2 + 4 \right)$$

xii) $V_{2n} - V_n^2 = \left(\alpha^{2n} + \beta^{2n} \right) - \left(\alpha^n + \beta^n \right)^2$

$$= \alpha^{2n} + \beta^{2n} - \alpha^{2n} - 2\alpha^n\beta^n - \beta^{2n}$$

$$= -2(\alpha\beta)^n$$

$$= 2(-1)^{n+1}$$

xiii) $U_{n+1} + U_{n-1} = \dfrac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta} + \dfrac{\alpha^{n-1} - \beta^{n-1}}{\alpha - \beta}$

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

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

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

$$= \frac{(\alpha - \beta)\left(\alpha^n + \beta^n\right)}{\alpha - \beta}$$

$$= V_n$$

xiv) $aU_n + V_n = a\left(\dfrac{\alpha^n - \beta^n}{\alpha - \beta}\right) + \alpha^n + \beta^n$

$$= a\left(\frac{\alpha^n - \beta^n}{\alpha - \beta}\right) + \frac{\left(\alpha^n + \beta^n\right)(\alpha - \beta)}{(\alpha - \beta)}$$

$$= a\left(\frac{\alpha^n - \beta^n}{\alpha - \beta}\right) + \frac{\alpha^{n+1} - \alpha^n\beta + \alpha\beta^n - \beta^{n+1}}{(\alpha - \beta)}$$

$$= \frac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta} + a\left(\frac{\alpha^n - \beta^n}{\alpha - \beta}\right) + \frac{\alpha^{n-1} - \beta^{n-1}}{\alpha - \beta}$$

$$= U_{n+1} + aU_n + U_{n-1}$$

$$= 2U_{n+1}$$

xv) $U_{n+1}U_{m+1} + U_nU_m = \left(\dfrac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta}\right)\left(\dfrac{\alpha^{m+1} - \beta^{m+1}}{\alpha - \beta}\right) + \left(\dfrac{\alpha^n - \beta^n}{\alpha - \beta}\right)\left(\dfrac{\alpha^m - \beta^m}{\alpha - \beta}\right)$

$$= \frac{\alpha^{m+n+2} - \alpha^{n+1}\beta^{m+1} - \alpha^{m+1}\beta^{n+1} + \beta^{m+n+2} + \alpha^{m+n} - \alpha^{n}\beta^{m} - \alpha^{m}\beta^{n} + \beta^{m+n}}{(\alpha-\beta)^2}$$

$$= \frac{\alpha^{m+n+1}\left(\alpha + \frac{1}{\alpha}\right) + \beta^{m+n+1}\left(\beta + \frac{1}{\beta}\right) + \alpha^{n}\beta^{m} + \alpha^{m}\beta^{n} - \alpha^{n}\beta^{m} - \beta^{n}\alpha^{n}}{(\alpha-\beta)^2}$$

$$= \frac{\alpha^{m+n+1}(\alpha-\beta) - \beta^{m+n+1}(\alpha-\beta)}{(\alpha-\beta)^2}$$

$$= \frac{\left(\alpha^{m+n+1} - \beta^{m+n+1}\right)(\alpha-\beta)}{(\alpha-\beta)^2}$$

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

$$= U_{m+n+1}$$

2.3. U^n Matrisi ve Genel Özellikleri

U matrisi $[1]$'de aşağıdaki gibi tanımlanmıştır:

$$U = \begin{bmatrix} a & 1 \\ 1 & 0 \end{bmatrix} \tag{2.42}$$

U matrisi; $a = 1$ alındığında $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$ Fibonacci matrisine, $a = 2$ alındığında ise $\begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}$ Pell matrisine dönüşür$[1-16]$.

$n \in \mathbf{Z}^+$ olmak üzere Eş. 2.42 ile verilen U matrisinin n. kuvveti aşağıdaki gibidir$[1]$:

$$U^n = \begin{bmatrix} U_{n+1} & U_n \\ U_n & U_{n-1} \end{bmatrix} \tag{2.43}$$

Eş. 2.43 matrisinde, Eş. 2.2 başlangıç şartlarıyla verilen Eş. 2.1 reküransını kullanırsak;

$$U^n = \begin{bmatrix} U_{n+1} & U_n \\ U_n & U_{n-1} \end{bmatrix}$$

$$= \begin{bmatrix} aU_n + U_{n-1} & aU_{n-1} + U_{n-2} \\ aU_{n-1} + U_{n-2} & aU_{n-2} + U_{n-3} \end{bmatrix}$$

$$= a\begin{bmatrix} U_n & U_{n-1} \\ U_{n-1} & U_{n-2} \end{bmatrix} + \begin{bmatrix} U_{n-1} & U_{n-2} \\ U_{n-2} & U_{n-3} \end{bmatrix}$$

$$U^n = aU^{n-1} + U^{n-2} \tag{2.44}$$

eşitliği elde edilir.

Eş. 2.43'ün doğruluğunun tümevarımla da gösterilebileceğini hatırlatalım.

U matrisleri, matrislerde çarpma işlemine göre değişme özelliğine sahiptir. Bunu aşağıdaki teoremle ifade edelim.

2.3. Teorem

m, n pozitif tamsayıları için;

$$U^m U^n = U^n U^m = U^{m+n} \tag{2.45}$$

dir.

İspat

$$U^m U^n = \begin{bmatrix} U_{m+1} & U_m \\ U_m & U_{m-1} \end{bmatrix} \begin{bmatrix} U_{n+1} & U_n \\ U_n & U_{n-1} \end{bmatrix}$$

$$= \begin{bmatrix} U_{m+1}U_{n+1} + U_m U_n & U_{m+1}U_n + U_m U_{n-1} \\ U_m U_{n+1} + U_{m-1}U_n & U_m U_n + U_{m-1}U_{n-1} \end{bmatrix} \tag{2.46}$$

Eş. 2.46'de, Eş. 2.41 kullanılırsa;

$$U^m U^n = \begin{bmatrix} U_{m+n+1} & U_{m+n} \\ U_{m+n} & U_{m+n-1} \end{bmatrix}$$

$$U^m U^n = U^{m+n} \tag{2.47}$$

elde edilir. Benzer şekilde;

$$U^n U^m = \begin{bmatrix} U_{n+1} & U_n \\ U_n & U_{n-1} \end{bmatrix} \begin{bmatrix} U_{m+1} & U_m \\ U_m & U_{m-1} \end{bmatrix}$$

$$= \begin{bmatrix} U_{n+1}U_{m+1} + U_n U_m & U_{n+1}U_m + U_n U_{m-1} \\ U_n U_{m+1} + U_{n-1}U_m & U_n U_m + U_{n-1}U_{m-1} \end{bmatrix} \tag{2.48}$$

dir. Eş. 2.48'de Eş. 2.41 kullanılırsa;

$$U^n U^m = \begin{bmatrix} U_{n+m+1} & U_{n+m} \\ U_{n+m} & U_{n+m-1} \end{bmatrix}$$

$$U^n U^m = U^{n+m} \tag{2.49}$$

elde edilir. Eş. 2.47 ve Eş. 2.49 birlikte düşünüldüğünde;

$$U^n U^m = U^m U^n = U^{n+m}$$

yazılır. Böylece ispat tamamlanır.

Şimdi, Eş. 2.43 ile verilen U^n matrisinin determinantını hesaplayalım:

$$\det U^n = U_{n+1}U_{n-1} - U_n^2 \tag{2.50}$$

dir. Eş. 2.50'de, Eş. 2.36 kullanılırsa;

$$\det U^n = (-1)^n \tag{2.51}$$

bulunur. Yani $\det U^n \neq 0$ dır. O halde U^n matrisinin ters matrisi olan U^{-n}'den bahsedebiliriz.

Çizelge 2.3.'te $n = 0, \pm 1, \pm 2, \pm 3, \ldots$ tamsayıları ve a pozitif tamsayıları için U^n matrisleri ve U^{-n} ters matrisleri verilmiştir.

Çizelge 2.3. U^n ve U^{-n} Matrisleri

n	0	1	2	3	4
U^n	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} a^2+1 & a \\ a & 1 \end{pmatrix}$	$\begin{pmatrix} a^3+2a & a^2+1 \\ a^2+1 & a \end{pmatrix}$	$\begin{pmatrix} a^4+3a^2+1 & a^3+2a \\ a^3+2a & a^2+1 \end{pmatrix}$
U^{-n}	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & -a \end{pmatrix}$	$\begin{pmatrix} 1 & -a \\ -a & a^2+1 \end{pmatrix}$	$\begin{pmatrix} -a & a^2+1 \\ a^2+1 & -(a^3+2a) \end{pmatrix}$	$\begin{pmatrix} a^2+1 & -(a^3+2a) \\ -(a^3+2a) & a^4+3a^2+1 \end{pmatrix}$

Çizelge 2.3.' ten de görüleceği üzere k pozitif tamsayıları için $n = 2k+1$ aldığımızda; U^n matrisinin tersi bulunurken, esas köşegen üzerindeki elemanlar yer ve işaret değiştirir. Yani;

$$U^{2k+1} = \begin{bmatrix} U_{2k+2} & U_{2k+1} \\ U_{2k+1} & U_{2k} \end{bmatrix} \tag{2.52}$$

matrisinin ters matrisi;

$$U^{-(2k+1)} = \begin{bmatrix} -U_{2k} & U_{2k+1} \\ U_{2k+1} & -U_{2k+2} \end{bmatrix} \tag{2.53}$$

dir. Benzer şekilde, k pozitif tamsayıları için $n = 2k$ aldığımızda; U^n matrisinin tersi bulunurken, esas köşegen üzerindeki elemanlar yer değiştirir, diğer köşegen üzerindeki elemanlar ise işaret değiştirir. Yani;

$$U^{2k} = \begin{bmatrix} U_{2k+1} & U_{2k} \\ U_{2k} & U_{2k-1} \end{bmatrix} \tag{2.54}$$

matrisinin ters matrisi;

$$U^{-2k} = \begin{bmatrix} U_{2k-1} & -U_{2k} \\ -U_{2k} & U_{2k+1} \end{bmatrix} \tag{2.55}$$

dir.

3. SİMETRİK HİPERBOLİK U VE V FOKSİYONLARI

3.1. Hiperbolik Fonksiyonlar

$y = e^x$ ve $y = e^{-x}$ fonksiyonlarını göz önüne alalım. Bu iki fonksiyon yardımıyla yeni fonksiyonlar tanımlanabilir. Bunlar; $\sinh : R \to R$ tanımlanan sinüs hiperbolik fonksiyonu,

$$\sinh nx = \frac{e^{nx} - e^{-nx}}{2} \tag{3.1}$$

ve $\cosh : R \to [1, \infty)$ tanımlanan cosinüs hiperbolik fonksiyonu;

$$\cosh nx = \frac{e^{nx} + e^{-nx}}{2} \tag{3.2}$$

dir. Eş. 3.1 ve Eş. 3.2'de argüment $\frac{n}{2}\ln\frac{\tau}{\sigma}$ seçilirse, hiperbolik fonksiyonların özellikleri ile Fibonacci ve Lucas dizilerinin özellikleri arasında çok yakın bir benzerlik olduğu $[14]$'te gösterilmiştir. (Burada τ ve σ; Fibonacci dizileri için tanımlanan $x^2 = x + 1$ karakteristik denkleminin kökleridir.) Biz de bu bölümde U_n ve V_n dizileri ile hiperbolik fonksiyonlar arasındaki benzerliğe değineceğiz.

Eş. 3.1 ve Eş. 3.2'de argümenti $\frac{n}{2}\ln\frac{\alpha}{\beta}$ seçersek (α ve β Eş. 2.3 karakteristik denkleminin kökleridir.)

$$\sinh nx = \frac{e^{\frac{n}{2}\ln\frac{\alpha}{\beta}} - e^{-\frac{n}{2}\ln\frac{\alpha}{\beta}}}{2}$$

$$= \frac{\left(\frac{\alpha}{\beta}\right)^{\frac{1}{2}n} - \left(\frac{\alpha}{\beta}\right)^{-\frac{1}{2}n}}{2}$$

$$= \frac{1}{2}\left[\frac{\alpha^n - \beta^n}{(\alpha\beta)^{\frac{1}{2}n}}\right]$$

$$\sinh nx = \frac{U_n\sqrt{a^2+4}}{2i^n} \tag{3.3}$$

ve

$$\cos hnx = \frac{e^{\frac{n}{2}\ln\frac{\alpha}{\beta}} + e^{-\frac{n}{2}\ln\frac{\alpha}{\beta}}}{2}$$

$$= \frac{\left(\frac{\alpha}{\beta}\right)^{\frac{1}{2}n} + \left(\frac{\alpha}{\beta}\right)^{-\frac{1}{2}n}}{2}$$

$$= \frac{1}{2}\left[\frac{\alpha^n + \beta^n}{i^n}\right]$$

$$\cosh nx = \frac{V_n}{2i^n} \tag{3.4}$$

dir. Eş. 3.3 ve Eş. 3.4 kullanarak hiperbolik fonksiyonlarla U_n ve V_n dizileri arasındaki bazı ilişkileri aşağıdaki gibi verebiliriz:

i) $\cosh nx + \sinh nx = e^{nx}$

$$\frac{V_n}{2i^n} + \frac{U_n\sqrt{a^2+4}}{2i^n} = \frac{\alpha^n + \beta^n}{2i^n} + \frac{\alpha^n - \beta^n}{2i^n}$$

$$\frac{V_n}{2i^n} + \frac{U_n\sqrt{a^2+4}}{2i^n} = \frac{2\alpha^n}{2i^n}$$

$$V_n + U_n\sqrt{a^2+4} = 2\alpha^n \qquad \text{(Eş. 2.27)}$$

ii) $\cosh nx - \sinh nx = e^{-nx}$

$$\frac{V_n}{2i^n} - \frac{U_n\sqrt{a^2+4}}{2i^n} = \frac{\alpha^n + \beta^n}{2i^n} - \frac{\alpha^n - \beta^n}{2i^n}$$

$$\frac{V_n}{2i^n} - \frac{U_n\sqrt{a^2+4}}{2i^n} = \frac{2\beta^n}{2i^n}$$

$$V_n - U_n\sqrt{a^2+4} = 2\beta^n \qquad \text{(Eş. 2.28)}$$

iii) $\cosh^2 nx + \sinh^2 nx = 1$

$$\left[\frac{V_n}{2i^n}\right]^2 - \left[\frac{U_n\sqrt{a^2+4}}{2i^n}\right]^2 = \frac{{V_n}^2}{4(-1)^n} - \frac{{U_n}^2(a^2+4)}{4(-1)^n}$$

$$= \frac{(a^2+4)U_n^2 - V_n^2}{4(-1)^{n+1}} \qquad \text{(Eş. 2.29)}$$

$$= 1$$

iv) Hiperbolik fonksiyonlarla ilgili,

$$\sinh(m+n)x + \cosh(m+n)x = 2\sinh mx\cosh nx$$

$$\sinh(m+n)x - \cosh(m+n)x = 2\cosh mx\sinh nx$$

$$\cosh(m+n)x + \cosh(m-n)x = 2\cosh mx\cosh nx$$

$$\cosh(m+n)x - \cosh(m-n)x = 2\sinh mx\sinh nx$$

eşitlikleri ile daha önce doğruluğunu gösterdiğimiz;

$$U_{n+m}+(-1)^m U_{n-m}=U_n V_m \qquad \text{(Eş. 2.30)}$$

$$U_{n+m}-(-1)^m U_{n-m}=V_n U_m \qquad \text{(Eş. 2.31)}$$

$$V_{n+m}+(-1)^m V_{n-m}=V_m V_n \qquad \text{(Eş. 2.32)}$$

$$V_{n+m}-(-1)^m V_{n-m}=(a^2+4)U_m U_n \qquad \text{(Eş. 2.33)}$$

eşitlikleri arasında dikkat çekici bir benzerlik vardır.

v) $\sinh 2nx = 2\sinh nx \cosh nx$

$\cosh 2nx = \cosh^2 + \sinh^2 nx$

$$U_{2n}=U_n V_n \qquad \text{(Eş. 2.34)}$$

$$2V_{2n}=V_n^{\,2}+(a^2+4)U_n^2 \qquad \text{(Eş. 2.35)}$$

vi) $\sinh(n+1)x \sinh(n-1)x-(\sinh nx)^2=5(-1)^n$

$$U_{n+1}U_{n-1}-U_n^2=(a^2+4)(-1)^n \qquad \text{(Eş.2.36)}$$

3.2. Simetrik Hiperbolik Fonksiyonlar

Fibonacci dizisinin karakteristik denklemi $x^2=x+1$'in pozitif kökü olan $\tau=\frac{1+\sqrt{5}}{2}$, yi kullanarak $k=0,\pm1,\pm2,\pm3,\pm,4...$ tamsayıları için Fibonacci ve Lucas dizilerini aşağıdaki şekilde düşünebiliriz:

$$F_n = \begin{cases} \dfrac{\tau^{2k} + \tau^{-2k}}{\sqrt{5}} & ; \quad n = 2k \\ \dfrac{\tau^{2k+1} - \tau^{-(2k+1)}}{\sqrt{5}} & ; \quad n = 2k+1 \end{cases} \tag{3.5}$$

$$L_n = \begin{cases} \tau^{2k} + \tau^{-2k} & ; \quad n = 2k \\ \tau^{2k+1} - \tau^{-(2k+1)} & ; \quad n = 2k+1 \end{cases} \tag{3.6}$$

Eş. 3.3 ve Eş. 3.4'te tamsayı değişkeni k yerine, reel değerli x değişkeni alındığında sürekli hiperbolik Fibonacci ve Lucas fonksiyonları $[15]$'te aşağıdaki şekilde tanımlanmıştır:

Hiperbolik Fibonacci sinüs fonksiyonu;

$$sF(x) = \frac{\tau^{2x} - \tau^{-2x}}{\sqrt{5}} \tag{3.7}$$

dir. Hiperbolik Fibonacci cosinüs fonksiyonu;

$$cF(x) = \frac{\tau^{2x+1} + \tau^{-(2x+1)}}{\sqrt{5}} \tag{3.8}$$

dir. Benzer şekilde, hiperbolik Lucas sinüs fonksiyonu;

$$sL(x) = \tau^{2x+1} - \tau^{-(2x+1)} \tag{3.9}$$

dir. Hiperbolik Lucas cosinüs fonksiyonu ise;

$$cL(x) = \tau^{2x} + \tau^{-2x} \tag{3.10}$$

dir. [15]'te Eş. 3.7-Eş. 3.10 ile tanımlanan fonksiyonlar; Fibonacci ve Lucas fonksiyonlarını sürekli fonksiyonlara dönüştürmesi açısından önemlidir.

Eş. 3.5, Eş. 3.6 Binet formülleri ve Eş. 3.1, Eş. 3.2 klasik hiperbolik fonksiyonlar aracılığıyla hiperbolik Fibonacci ve Lucas fonksiyonlarının farklı bir formu olan simetrik hiperbolik Fibonacci ve Lucas fonksiyonlarını tanımlayabiliriz[15]. Buna göre simetrik hiperbolik Fibonacci sinüs fonksiyonu;

$$sFs(x) = \frac{\tau^x - \tau^{-x}}{\sqrt{5}} \tag{3.11}$$

dir. Simetrik hiperbolik Fibonacci cosinüs fonksiyonu;

$$cFs(x) = \frac{\tau^x + \tau^{-x}}{\sqrt{5}} \tag{3.12}$$

dir. Simetrik hiperbolik Lucas sinüs fonksiyonu;

$$sLs(x) = \tau^x - \tau^{-x} \tag{3.13}$$

dir. Simetrik hiperbolik Lucas cosinüs fonksiyonu ise;

$$cLs(x) = \tau^x + \tau^{-x} \tag{3.14}$$

dir.

Eş. 3.11-Eş. 3.14 simetrik hiperbolik Fibonacci ve Lucas fonksiyonları ile klasik Fibonacci ve Lucas fonksiyonları arasında aşağıdaki gibi bir ilişki vardır[15].

$$F_n = \begin{cases} sFs(n); & n = 2k \\ cFs(n); & n = 2k+1 \end{cases} \tag{3.15}$$

$$L_n = \begin{cases} cLs(n); & n = 2k \\ sLs(n); & n = 2k+1 \end{cases} \tag{3.16}$$

Bu kısımda, daha önce verdiğimiz U_n, V_n dizilerinin genel formülleri ve klasik hiperbolik fonksiyonlar aracılığıyla tanımlanan bazı fonksiyonları ifade edelim.

Eş. 2.3 karakteristik denkleminin pozitif kökü olan α'yı kullanarak $k = 0, \pm 1, \pm 2, \pm 3, \ldots.$ tamsayıları için Eş. 2.8, Eş. 2.24 ile tanımlanan U_n ve V_n dizilerini aşağıdaki formda yazabiliriz:

$$U_n = \begin{cases} \dfrac{\alpha^{2k} - \alpha^{-2k}}{\sqrt{a^2+4}} & ; \quad n = 2k \\ \dfrac{\alpha^{2k+1} + \alpha^{-(2k+1)}}{\sqrt{a^2+4}}; & n = 2k+1 \end{cases} \tag{3.17}$$

$$V_n = \begin{cases} \alpha^{2k} + \alpha^{-2k} & ; \quad n = 2k \\ \alpha^{2k+1} - \alpha^{-(2k+1)}; & n = 2k+1 \end{cases} \tag{3.18}$$

Eş. 3.17 ve Eş. 3.18'de k tamsayı değişkeni yerine reel sayılarda değer alan x değişkenini kullandığımızda sürekli hiperbolik U ve V fonksiyonlarını aşağıdaki gibi tanımlayabiliriz:

Hiperbolik U sinüs fonksiyonu;

$$sU(x) = \frac{\alpha^{2x} - \alpha^{-2x}}{\sqrt{a^2+4}} \tag{3.19}$$

dir. Hiperbolik U cosinüs fonksiyonu;

$$cU(x)=\frac{\alpha^{2x+1}+\alpha^{-(2x+1)}}{\sqrt{a^2+4}} \tag{3.20}$$

dir. Hiperbolik V sinüs fonksiyonu;

$$sV(x)=\alpha^{2x+1}-\alpha^{-(2x+1)} \tag{3.21}$$

dir. Hiperbolik V cosinüs fonksiyonu ise;

$$cV(x)=\alpha^{2x}+\alpha^{-2x} \tag{3.22}$$

dir. Eş. 3.15-Eş. 3.22; Eş. 2.8 ve Eş. 2.24 ile tanımlanan U_n ve V_n dizilerini sürekli fonksiyonlara dönüştürmesi açısından önemlidir.

Eş. 3.17, Eş.3.18 genel formülleri ve Eş. 3.1, Eş. 3.2 klasik hiperbolik fonksiyonlar aracılığıyla Eş. 3.17-Eş. 3.22; hiperbolik U ve V fonksiyonlarını farklı bir formda yazabiliriz. Buna göre simetrik hiperbolik U sinüs fonksiyonu;

$$sUs(x)=\frac{\alpha^{x}-\alpha^{-x}}{\sqrt{a^2+4}} \tag{3.23}$$

dir. Simetrik hiperbolik U cosinüs fonksiyonu;

$$cUs(x)=\frac{\alpha^{x}+\alpha^{-x}}{\sqrt{a^2+4}} \tag{3.24}$$

dir. Simetrik hiperbolik V sinüs fonksiyonu;

$$sVs(x) = \alpha^{x} - \alpha^{-x} \tag{3.25}$$

dir. Simetrik hiperbolik V cosinüs fonksiyonu ise;

$$cVs(x) = \alpha^{x} + \alpha^{-x} \tag{3.26}$$

dir. Böylelikle simetrik hiperbolik U ve V fonksiyonları ile U_n ve V_n dizileri arasında $k = 0, \pm 1, \pm 2, \pm 3, \ldots$ tamsayıları için aşağıdaki gibi bir ilişki kurulabilir.

$$U_n = \begin{cases} sUs(n); & n = 2k \\ cUs(n); & n = 2k+1 \end{cases} \tag{3.27}$$

$$V_n = \begin{cases} cVs(n); & n = 2k \\ sVs(n); & n = 2k+1 \end{cases} \tag{3.28}$$

Simetrik hiperbolik U , V fonksiyonları ve hiperbolik fonksiyonlar arasındaki bazı ilişkileri aşağıdaki teorem ile verelim.

3.1. Teorem

Simetrik hiperbolik U ve V fonksiyonları ile klasik hiperbolik fonksiyonlar arasında aşağıdaki bağıntılar vardır:

i) $$sUs(x) = \frac{2}{\sqrt{a^2+4}} sh\left[(\ln \alpha)x\right] \tag{3.29}$$

ii) $$cUs(x) = \frac{2}{\sqrt{a^2+4}} ch\left[(\ln \alpha)x\right] \tag{3.30}$$

iii) $sVs(x) = 2sh[(\ln\alpha)x]$ (3.31)

iv) $cVs(x) = 2ch[(\ln\alpha)x]$ (3.32)

İspat

i) Eş. 3.1 klasik hiperbolik sinüs fonksiyonunda argümenti $(\ln\alpha)x$ olarak seçersek;

$$\frac{2}{\sqrt{a^2+4}}\,\mathrm{s}h[(\ln\alpha)x] = \frac{2}{\sqrt{a^2+4}}\frac{e^{(\ln\alpha)x} - e^{-(\ln\alpha)x}}{2}$$
$$= \frac{\alpha^x - \alpha^{-x}}{\sqrt{a^2+4}}$$
$$= sUs(x)$$

Benzer şekilde diğer özelliklerin doğruluğunu gösterebiliriz.

3.3. Simetrik Hiperbolik U ve V Fonksiyonlarının Özellikleri

Simetrik hiperbolik U, V fonksiyonlarının özelliklerini ve bu fonksiyonların birbirleriyle olan ilişkilerini aşağıdaki teoremlerle açıklayalım.

3.2. Teorem

Simetrik hiperbolik U ve V fonksiyonları için $x \to \infty$ ve $x \to -\infty$ olduğunda aşağıdaki eşitlikler yazılabilir.

i) $\lim_{x\to\infty} \frac{cUs(2x+1)}{sUs(2x)} = \alpha$ (3.33)

ii) $$\lim_{x\to-\infty}\frac{cUs(2x+1)}{sUs(2x)}=-\frac{1}{\alpha} \tag{3.34}$$

iii) $$\lim_{x\to\infty}\frac{sVs(2x+1)}{cVs(2x)}=\alpha \tag{3.35}$$

iv) $$\lim_{x\to-\infty}\frac{sVs(2x+1)}{cVs(2x)}=-\frac{1}{\alpha} \tag{3.36}$$

İspat

i) $$\lim_{x\to\infty}\frac{cUs(2x+1)}{sUs(2x)}=\lim_{x\to\infty}\frac{\frac{\alpha^{2x+1}+\alpha^{-(2x+1)}}{\sqrt{a^2+4}}}{\frac{\alpha^{2x}-\alpha^{-2x}}{\sqrt{a^2+4}}}$$

$$=\lim_{x\to-\infty}\frac{\alpha^{2x+1}+\alpha^{-(2x+1)}}{\alpha^{2x}-\alpha^{-2x}}$$

$$=\lim_{x\to\infty}\frac{\alpha^{2x+1}\left(1+\alpha^{-4x-2}\right)}{\alpha^{2x}\left(1-\alpha^{-4x}\right)}$$

$$=\lim_{x\to\infty}\frac{\alpha\left(1+\frac{1}{\alpha^{4x+2}}\right)}{\left(1-\frac{1}{\alpha^{4x}}\right)}$$

$$=\alpha$$

ii) $$\lim_{x\to-\infty}\frac{cUs(2x+1)}{sUs(2x)}=\lim_{x\to-\infty}\frac{\frac{\alpha^{2x+1}+\alpha^{-(2x+1)}}{\sqrt{a^2+4}}}{\frac{\alpha^{2x}-\alpha^{-2x}}{\sqrt{a^2+4}}}$$

$$=\lim_{x\to-\infty}\frac{\alpha^{2x+1}+\alpha^{-(2x+1)}}{\alpha^{2x}-\alpha^{-2x}}$$

$$=\lim_{x\to-\infty}\frac{\alpha^{-2x-1}\left(\alpha^{4x+2}+1\right)}{\alpha^{-2x}\left(\alpha^{4x}-1\right)}$$

$$= \lim_{x\to-\infty} \frac{\alpha^{-1}\left(\frac{\alpha^2}{\alpha^{-4x}}+1\right)}{\left(\frac{1}{\alpha^{-4x}}-1\right)}$$

$$= -\frac{1}{\alpha}$$

iii) $$\lim_{x\to\infty} \frac{sVs(2x+1)}{cVs(2x)} = \frac{\alpha^{2x+1}-\alpha^{-(2x+1)}}{\alpha^{2x}-\alpha^{-2x}}$$

$$= \frac{\alpha^{2x+1}\left(1-\alpha^{-4x-2}\right)}{\alpha^{2x}\left(1+\alpha^{-4x}\right)}$$

$$= \frac{\alpha\left(1-\frac{1}{\alpha^{4x+2}}\right)}{\left(1+\frac{1}{\alpha^{4x}}\right)}$$

$$= \alpha$$

iv) $$\lim_{x\to-\infty} \frac{sVs(2x+1)}{cVs(2x)} = \frac{\alpha^{2x+1}-\alpha^{-(2x+1)}}{\alpha^{2x}-\alpha^{-2x}}$$

$$= \frac{\alpha^{-2x-1}\left(\alpha^{4x+2}-1\right)}{\alpha^{-2x}\left(\alpha^{4x}+1\right)}$$

$$= \frac{\alpha^{-1}\left(\frac{\alpha^2}{\alpha^{-4x}}-1\right)}{\left(\frac{1}{\alpha^{-4x}}+1\right)}$$

$$= -\frac{1}{\alpha}$$

3.3. Teorem

Simetrik hiperbolik U fonksiyonlarıyla,

$$U_{n+2} = aU_{n+1} + U_n$$

rekürans bağıntısına benzer aşağıdaki bağıntılar yazılabilir.

i) $sUs(x+2) = acUs(x+1) + sUs(x)$ (3.37)

ii) $cUs(x+2) = asUs(x+1) + cUs(x)$ (3.38)

İspat

$$\text{i) } acUs(x+1) + sUs(x) = a\left(\frac{\alpha^{x+1} + \alpha^{-(x+1)}}{\sqrt{a^2+4}}\right) + \left(\frac{\alpha^x - \alpha^{-x}}{\sqrt{a^2+4}}\right)$$

$$= \frac{a\alpha^{x+1} + a\alpha^{-x-1} + \alpha^x - \alpha^{-x}}{\sqrt{a^2+4}}$$

$$= \frac{\alpha^x(a\alpha+1) - \alpha^{-x}(1-a\alpha^{-1})}{\sqrt{a^2+4}}$$

$$= \frac{\alpha^x\alpha^2 + \alpha^{-x}\alpha^{-2}}{\sqrt{a^2+4}}$$

$$= \frac{\alpha^{x+2} - \alpha^{-(x+2)}}{\sqrt{a^2+4}}$$

$$= sUs(x+2)$$

$$\text{ii) } asUs(x+1) + cUs(x) = a\left(\frac{\alpha^{x+1} - \alpha^{-(x+1)}}{\sqrt{a^2+4}}\right) + \left(\frac{\alpha^x + \alpha^{-x}}{\sqrt{a^2+4}}\right)$$

$$= \frac{a\alpha^{x+1} - a\alpha^{-x-1} + \alpha^x + \alpha^{-x}}{\sqrt{a^2+4}}$$

$$= \frac{\alpha^x(a\alpha+1) + \alpha^{-x}(1-a\alpha^{-1})}{\sqrt{a^2+4}}$$

$$= \frac{\alpha^x \alpha^2 + \alpha^{-x} \alpha^{-2}}{\sqrt{a^2+4}}$$
$$= \frac{\alpha^{x+2} + \alpha^{-(x+2)}}{\sqrt{a^2+4}}$$
$$= cUs(x+2)$$

3.4. Teorem

Simetrik hiperbolik V fonksiyonlarıyla,

$$V_{n+2} = aV_{n+1} + V_n$$

rekürans bağıntısına benzer aşağıdaki bağıntılar yazılabilir.

i) $sVs(x+2) = acVs(x+1) + sVs(x)$ (3.39)

ii) $cVs(x+2) = asVs(x+1) + cVs(x)$ (3.40)

İspat

i) $acVs(x+1) + sVs(x) = a\left(\alpha^{x+1} + \alpha^{-(x+1)}\right) + \left(\alpha^x - \alpha^{-x}\right)$
$$= a\alpha^{x+1} + a\alpha^{-(x+1)} + \alpha^x - \alpha^{-x}$$
$$= \alpha^x (a\alpha + 1) - \alpha^{-x}\left(1 - a\alpha^{-1}\right)$$
$$= \alpha^x \alpha^2 - \alpha^{-x}\alpha^{-2}$$
$$= \alpha^{x+2} - \alpha^{-(x+2)}$$
$$= sVs(x+2)$$

ii) $asVs(x+1) + cVs(x) = a\left(\alpha^{x+1} - \alpha^{-(x+1)}\right) + \left(\alpha^x + \alpha^{-x}\right)$

$$= a\alpha^{x+1} - a\alpha^{-(x+1)} + \alpha^{x} + \alpha^{-x}$$
$$= \alpha^{x}\left(a\alpha + 1\right) + \alpha^{-x}\left(1 - a\alpha^{-1}\right)$$
$$= \alpha^{x}\alpha^{2} - \alpha^{-x}\alpha^{-2}$$
$$= \alpha^{x+2} - \alpha^{-(x+2)}$$
$$= cVs\left(x+2\right)$$

3.5. Teorem

Simetrik hiperbolik U fonksiyonları arasında,

$$U_{n+1}U_{n-1} - U_n^2 = (-1)^n$$

bağıntısına benzer aşağıdaki bağıntılar vardır.

i) $$cUs\left(x+1\right)cUs\left(x-1\right) - \left[sUs\left(x\right)\right]^2 = 1 \qquad (3.41)$$

ii) $$sUs\left(x+1\right)sUs\left(x-1\right) - \left[cUs\left(x\right)\right]^2 = -1 \qquad (3.42)$$

İspat

i)

$$cUs\left(x+1\right)cUs\left(x-1\right) - \left[sUs\left(x\right)\right]^2 = \left(\frac{\alpha^{x+1} + \alpha^{-(x+1)}}{\sqrt{a^2+4}}\right)\left(\frac{\alpha^{x-1} + \alpha^{-(x-1)}}{\sqrt{a^2+4}}\right) - \left(\frac{\alpha^{x} - \alpha^{-x}}{\sqrt{a^2+4}}\right)^2$$
$$= \frac{\alpha^{2x} + \alpha^{2} + \alpha^{-2} + \alpha^{-2x} - \alpha^{2x} + 2 - \alpha^{-2x}}{a^2+4}$$
$$= \frac{\alpha^{2} + \alpha^{-2} + 2}{a^2+4}$$
$$= \frac{1 + a\alpha + 1 - a\alpha^{-1} + 2}{a^2+4}$$

$$= \frac{4 + a\left(\alpha - \alpha^{-1}\right)}{a^2 + 4}$$

$$= \frac{a^2 + 4}{a^2 + 4}$$

$$= 1$$

ii) $sUs(x+1)\,sUs(x-1) - \left[cUs(x)\right]^2 = \left(\frac{\alpha^{x+1} - \alpha^{-(x+1)}}{\sqrt{a^2+4}}\right)\left(\frac{\alpha^{x-1} - \alpha^{-(x-1)}}{\sqrt{a^2+4}}\right) - \left(\frac{\alpha^x + \alpha^{-x}}{\sqrt{a^2+4}}\right)^2$

$$= \frac{-\left(\alpha^2 + \alpha^{-2} + 2\right)}{a^2 + 4}$$

$$= -\frac{\left[1 + a\alpha + 1 - a\alpha^{-1} + 2\right]}{a^2 + 4}$$

$$= \frac{-\left[4 + a\left(\alpha - \alpha^{-1}\right)\right]}{a^2 + 4}$$

$$= -\frac{a^2 + 4}{a^2 + 4}$$

$$= -1$$

3.6. Teorem

Simetrik hiperbolik V fonksiyonları arasında

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

bağıntısına benzer aşağıdaki bağıntılar mevcuttur.

i) $cVs(2x) = \left[sVs(x)\right]^2 + 2$ (3.43)

ii) $cVs(2x) = \left[cVs(x)\right]^2 - 2$ (3.44)

İspat

i) $\left[sVs(x)\right]^2+2=\left(\alpha^x-\alpha^{-x}\right)^2+2$

$$=\alpha^{2x}-2+\alpha^{-2x}+2$$

$$=cVs(2x)$$

ii) $\left[cVs(x)\right]^2-2=\left(\alpha^x+\alpha^{-x}\right)^2-2$

$$=\alpha^{2x}+2+\alpha^{-2x}-2$$

$$=cVs(2x)$$

3.7. Teorem

Simetrik hiperbolik U ve V fonksiyonları arasında,

$$U_{n+1}+U_{n-1}=V_n$$

bağıntısına benzer aşağıdaki bağıntılar vardır.

i) $cUs(x+1)+cUs(x-1)=cVs(x)$ (3.44)

ii) $sUs(x+1)+sUs(x-1)=sVs(x)$ (3.45)

İspat

i) $cUs(x+1)+cUs(x-1)=\dfrac{\alpha^{x+1}+\alpha^{-(x+1)}}{\sqrt{a^2+4}}+\dfrac{\alpha^{x-1}+\alpha^{-(x-1)}}{\sqrt{a^2+4}}$

$$=\frac{\alpha^x\left(\alpha+\alpha^{-1}\right)+\alpha^{-x}\left(\alpha+\alpha^{-1}\right)}{\sqrt{a^2+4}}$$

$$=\frac{\alpha^x\sqrt{a^2+4}+\alpha^{-x}\sqrt{a^2+4}}{\sqrt{a^2+4}}$$

$$= \frac{\sqrt{a^2+4}\left(\alpha^x + \alpha^{-x}\right)}{\sqrt{a^2+4}}$$

$$= \left(\alpha^x + \alpha^{-x}\right)$$

$$= cVs(x)$$

ii) $$sUs(x+1) + sUs(x-1) = \frac{\alpha^{x+1} - \alpha^{-(x+1)}}{\sqrt{a^2+4}} + \frac{\alpha^{x-1} - \alpha^{-(x-1)}}{\sqrt{a^2+4}}$$

$$= \frac{\alpha^x\left(\alpha + \alpha^{-1}\right) - \alpha^{-x}\left(\alpha + \alpha^{-1}\right)}{\sqrt{a^2+4}}$$

$$= \frac{\alpha^x\sqrt{a^2+4} - \alpha^{-x}\sqrt{a^2+4}}{\sqrt{a^2+4}}$$

$$= \frac{\sqrt{a^2+4}\left(\alpha^x - \alpha^{-x}\right)}{\sqrt{a^2+4}}$$

$$= \left(\alpha^x - \alpha^{-x}\right)$$

$$= sVs(x)$$

3.9. Teorem

Simetrik hiperbolik U ve V fonksiyonları arasında,

$$aU_n + V_n = 2U_{n+1}$$

bağıntısına benzer aşağıdaki bağıntılar mevcuttur.

i) $$acUs(x) + cVs(x) = 2cUs(x+1) \tag{3.47}$$

ii) $$asUs(x) + sVs(x) = 2sUs(x+1) \tag{3.48}$$

İspat

i) $acUs(x)+cVs(x)=a\left(\frac{\alpha^x+\alpha^{-x}}{\sqrt{a^2+4}}\right)+\left(\alpha^x+\alpha^{-x}\right)$

$$=a\left(\frac{\alpha^x+\alpha^{-x}}{\sqrt{a^2+4}}\right)+\frac{\left(\alpha^x+\alpha^{-x}\right)\left(\alpha+\alpha^{-1}\right)}{\sqrt{a^2+4}}$$

$$=a\left(\frac{\alpha^x+\alpha^{-x}}{\sqrt{a^2+4}}\right)+\frac{\alpha^{x+1}+\alpha^{x-1}+\alpha^{-x+1}+\alpha^{-(x+1)}}{\sqrt{a^2+4}}$$

$$=\frac{\alpha^{x+1}+\alpha^{-(x+1)}}{\sqrt{a^2+4}}+a\left(\frac{\alpha^x+\alpha^{-x}}{\sqrt{a^2+4}}\right)+\frac{\alpha^{x-1}+\alpha^{-(x-1)}}{\sqrt{a^2+4}}$$

$$=cUs(x+1)+acUs(x)+cUs(x-1)$$

$$=2cUs(x+1)$$

ii) $asUs(x)+sVs(x)=a\left(\frac{\alpha^x-\alpha^{-x}}{\sqrt{a^2+4}}\right)+\left(\alpha^x-\alpha^{-x}\right)$

$$=a\left(\frac{\alpha^x-\alpha^{-x}}{\sqrt{a^2+4}}\right)+\frac{\left(\alpha^x-\alpha^{-x}\right)\left(\alpha+\alpha^{-1}\right)}{\sqrt{a^2+4}}$$

$$=a\left(\frac{\alpha^x-\alpha^{-x}}{\sqrt{a^2+4}}\right)+\frac{\alpha^{x+1}+\alpha^{x-1}-\alpha^{-x+1}-\alpha^{-(x+1)}}{\sqrt{a^2+4}}$$

$$=\frac{\alpha^{x+1}-\alpha^{-(x+1)}}{\sqrt{a^2+4}}+a\left(\frac{\alpha^x-\alpha^{-x}}{\sqrt{a^2+4}}\right)+\frac{\alpha^{x-1}-\alpha^{-(x-1)}}{\sqrt{a^2+4}}$$

$$=sUs(x+1)+asUs(x)+sUs(x-1)$$

$$=2sUs(x+1)$$

3.9. Teorem

Simetrik hiperbolik U ve V fonksiyonları arasında,

$ch^2(x)-sh^2(x)=1$

bağıntısına benzer aşağıdaki bağıntılar mevcuttur.

$$\text{i)}\left[cUs(x)\right]^2-\left[sUs(x)\right]^2=\frac{4}{a^2+4} \tag{3.50}$$

$$\text{ii)}\left[cVs(x)\right]^2-\left[sVs(x)\right]^2=4 \tag{3.51}$$

İspat

$$\begin{aligned}\text{i)}\left[cUs(x)\right]^2-\left[sUs(x)\right]^2&=\left(\frac{\alpha^x+\alpha^{-x}}{\sqrt{a^2+4}}\right)^2-\left(\frac{\alpha^x-\alpha^{-x}}{\sqrt{a^2+4}}\right)^2\\&=\frac{\alpha^{2x}+2+\alpha^{-2x}-\alpha^{2x}+2-\alpha^{-2x}}{a^2+4}\\&=\frac{4}{a^2+4}\end{aligned}$$

$$\begin{aligned}\text{ii)}\left[cVs(x)\right]^2-\left[cVs(x)\right]^2&=\left(\alpha^x+\alpha^{-x}\right)^2-\left(\alpha^x-\alpha^{-x}\right)^2\\&=\alpha^{2x}+2+\alpha^{-2x}-\alpha^{2x}+2-\alpha^{-2x}\\&=4\end{aligned}$$

3.10. Teorem

Simetrik hiperbolik U ve V fonksiyonları arasında,

$$ch(x+y)=ch(x)ch(y)+sh(x)sh(y)$$

$$ch(x-y)=ch(x)ch(y)-sh(x)sh(y)$$

$$sh(x+y)=sh(x)ch(y)+sh(y)ch(x)$$

$$sh(x-y)=sh(x)ch(y)-sh(y)ch(x)$$

bağıntılarına benzer aşağıdaki bağıntılar mevcuttur.

i) $$\frac{2}{\sqrt{a^2+4}}cUs(x+y)=cUs(x)cUs(y)+sUs(x)sUs(y) \tag{3.52}$$

ii) $$\frac{2}{\sqrt{a^2+4}}cUs(x-y)=cUs(x)cUs(y)-sUs(x)sUs(y) \tag{3.53}$$

iii) $$\frac{2}{\sqrt{a^2+4}}sUs(x+y)=sUs(x)cUs(y)+sUs(y)cUs(x) \tag{3.53}$$

iv) $$\frac{2}{\sqrt{a^2+4}}sUs(x-y)=sUs(x)cUs(y)-sUs(y)cUs(x) \tag{3.54}$$

v) $$2cVs(x+y)=cVs(x)cVs(y)+sVs(x)sVs(y) \tag{3.55}$$

vi) $$2cVs(x-y)=cVs(x)cVs(y)-sVs(x)sVs(y) \tag{3.56}$$

vii) $$2sVs(x+y)=sVs(x)cVs(y)+sVs(y)cVs(x) \tag{3.57}$$

viii) $$2sVs(x-y)=sVs(x)cVs(y)-sVs(y)cVs(x) \tag{3.58}$$

İspat

i)

$$cUs(x)cUs(y)+sUs(x)sUs(y)=\left(\frac{\alpha^x+\alpha^{-x}}{\sqrt{a^2+4}}\right)\left(\frac{\alpha^y+\alpha^{-y}}{\sqrt{a^2+4}}\right)+\left(\frac{\alpha^x-\alpha^{-x}}{\sqrt{a^2+4}}\right)\left(\frac{\alpha^y-\alpha^{-y}}{\sqrt{a^2+4}}\right)$$

$$= \frac{\alpha^{x+y} + \alpha^{x-y} + \alpha^{-x+y} + \alpha^{-(x+y)} + \alpha^{x+y} - \alpha^{x-y} - \alpha^{-x+y} + \alpha^{-(x+y)}}{a^2+4}$$

$$= \frac{2\left(\alpha^{x+y} + \alpha^{-(x+y)}\right)}{a^2+4}$$

$$= \frac{2}{\sqrt{a^2+4}} cUs(x+y)$$

ii)

$$cUs(x)cUs(y) - sUs(x)sUs(y) = \left(\frac{\alpha^x + \alpha^{-x}}{\sqrt{a^2+4}}\right)\left(\frac{\alpha^y + \alpha^{-y}}{\sqrt{a^2+4}}\right) - \left(\frac{\alpha^x - \alpha^{-x}}{\sqrt{a^2+4}}\right)\left(\frac{\alpha^y - \alpha^{-y}}{\sqrt{a^2+4}}\right)$$

$$= \frac{\alpha^{x+y} + \alpha^{x-y} + \alpha^{-x+y} + \alpha^{-(x+y)} - \alpha^{x+y} + \alpha^{x-y} + \alpha^{-x+y} - \alpha^{-(x+y)}}{a^2+4}$$

$$= \frac{2\left(\alpha^{x-y} + \alpha^{-(x-y)}\right)}{a^2+4}$$

$$= \frac{2}{\sqrt{a^2+4}} cUs(x-y)$$

iii)

$$sUs(x)cUs(y) + sUs(y)cUs(x) = \left(\frac{\alpha^x - \alpha^{-x}}{\sqrt{a^2+4}}\right)\left(\frac{\alpha^y + \alpha^{-y}}{\sqrt{a^2+4}}\right) + \left(\frac{\alpha^y - \alpha^{-y}}{\sqrt{a^2+4}}\right)\left(\frac{\alpha^x + \alpha^{-x}}{\sqrt{a^2+4}}\right)$$

$$= \frac{\alpha^{x+y} + \alpha^{x-y} - \alpha^{-x+y} - \alpha^{-(x+y)} + \alpha^{x+y} - \alpha^{x-y} + \alpha^{-x+y} - \alpha^{-(x+y)}}{a^2+4}$$

$$= \frac{2\left(\alpha^{x+y} - \alpha^{-(x+y)}\right)}{a^2+4}$$

$$= \frac{2}{\sqrt{a^2+4}} sUs(x+y)$$

iv)

$$sUs(x)cUs(y) - sUs(y)cUs(x) = \left(\frac{\alpha^x - \alpha^{-x}}{\sqrt{a^2+4}}\right)\left(\frac{\alpha^y + \alpha^{-y}}{\sqrt{a^2+4}}\right) - \left(\frac{\alpha^y - \alpha^{-y}}{\sqrt{a^2+4}}\right)\left(\frac{\alpha^x + \alpha^{-x}}{\sqrt{a^2+4}}\right)$$

$$= \frac{\alpha^{x+y} + \alpha^{x-y} - \alpha^{-x+y} - \alpha^{-(x+y)} - \alpha^{x+y} + \alpha^{x-y} - \alpha^{-x+y} + \alpha^{-(x+y)}}{a^2+4}$$

$$= \frac{2\left(\alpha^{x-y} - \alpha^{-(x-y)}\right)}{a^2+4}$$

$$= \frac{2}{\sqrt{a^2+4}} sUs(x-y)$$

v) $cVs(x)cVs(y) + sVs(x)sVs(y) = \left(\alpha^x + \alpha^{-x}\right)\left(\alpha^y + \alpha^{-y}\right) + \left(\alpha^x - \alpha^{-x}\right)\left(\alpha^y - \alpha^{-y}\right)$

$$= \alpha^{x+y} + \alpha^{x-y} + \alpha^{-x+y} + \alpha^{-(x+y)} + \alpha^{x+y} - \alpha^{x-y} - \alpha^{-x+y} + \alpha^{-(x+y)}$$

$$= 2\left(\alpha^{x+y} + \alpha^{-(x+y)}\right)$$

$$= 2cVs(x+y)$$

vi) $cVs(x)cVs(y) - sVs(x)sVs(y) = \left(\alpha^x + \alpha^{-x}\right)\left(\alpha^y + \alpha^{-y}\right) - \left(\alpha^x - \alpha^{-x}\right)\left(\alpha^y - \alpha^{-y}\right)$

$$= \alpha^{x+y} + \alpha^{x-y} + \alpha^{-x+y} + \alpha^{-(x+y)} - \alpha^{x+y} + \alpha^{x-y} + \alpha^{-x+y} - \alpha^{-(x+y)}$$

$$= 2\left(\alpha^{x-y} + \alpha^{-(x-y)}\right)$$

$$= 2cVs(x-y)$$

vii) $sVs(x)cVs(y) + sVs(y)cVs(x) = \left(\alpha^x - \alpha^{-x}\right)\left(\alpha^y + \alpha^{-y}\right) + \left(\alpha^y - \alpha^{-y}\right)\left(\alpha^x + \alpha^{-x}\right)$

$$= \alpha^{x+y} + \alpha^{x-y} - \alpha^{-x+y} - \alpha^{-(x+y)} + \alpha^{x+y} - \alpha^{x-y} + \alpha^{-x+y} - \alpha^{-(x+y)}$$

$$= 2\left(\alpha^{x+y} - \alpha^{-(x+y)}\right)$$

$$= 2sVs(x+y)$$

viii) $sVs(x)cVs(y) - sVs(y)cVs(x) = \left(\alpha^x - \alpha^{-x}\right)\left(\alpha^y + \alpha^{-y}\right) - \left(\alpha^y - \alpha^{-y}\right)\left(\alpha^x + \alpha^{-x}\right)$

$$= \alpha^{x+y} + \alpha^{x-y} - \alpha^{-x+y} - \alpha^{-(x+y)} - \alpha^{x+y} + \alpha^{x-y} - \alpha^{-x+y} + \alpha^{-(x+y)}$$

$$= 2\left(\alpha^{x-y} - \alpha^{-(x-y)}\right)$$

$$= 2sVs(x-y)$$

3.11. Teorem

Simetrik hiperbolik U ve V fonksiyonlarının türevleri aşağıdaki gibidir.

$$\text{i)}\left[cUs(x)\right]^{(n)}=\begin{cases}(\ln\alpha)^n\, sUs(x); & n=2k\\ (\ln\alpha)^n\, cUs(x); & n=2k+1\end{cases} \tag{3.60}$$

$$\text{ii)}\left[sUs(x)\right]^{(n)}=\begin{cases}(\ln\alpha)^n\, cUs(x); & n=2k\\ (\ln\alpha)^n\, sUs(x); & n=2k+1\end{cases} \tag{3.61}$$

$$\text{iii)}\left[cVs(x)\right]^{(n)}=\begin{cases}(\ln\alpha)^n\, sVs(x); & n=2k\\ (\ln\alpha)^n\, cVs(x); & n=2k+1\end{cases} \tag{3.62}$$

$$\text{iv)}\left[sVs(x)\right]^{(n)}=\begin{cases}(\ln\alpha)^n\, cVs(x); & n=2k\\ (\ln\alpha)^n\, sVs(x); & n=2k+1\end{cases} \tag{3.63}$$

İspat

i)-ii) $\left[cUs(x)\right]'=\left(\dfrac{\alpha^x+\alpha^{-x}}{\sqrt{a^2+4}}\right)'$

$$=\frac{\alpha^x\ln\alpha-\alpha^{-x}\ln\alpha}{\sqrt{a^2+4}}$$

$$=\ln\alpha\left(\frac{\alpha^x-\alpha^{-x}}{\sqrt{a^2+4}}\right)$$

$$=\ln\alpha\, sUs(x)$$

$$\left[sUs(x)\right]'=\left(\frac{\alpha^x-\alpha^{-x}}{\sqrt{a^2+4}}\right)'$$

$$= \frac{\alpha^x \ln\alpha + \alpha^{-x} \ln\alpha}{\sqrt{a^2+4}}$$

$$= \ln\alpha \left(\frac{\alpha^x + \alpha^{-x}}{\sqrt{a^2+4}} \right)$$

$$= \ln\alpha cUs(x)$$

$$\left[cUs(x) \right]'' = \left[\ln\alpha sUs(x) \right]'$$

$$= \ln\alpha \ln\alpha cUs(x)$$

$$= (\ln\alpha)^2 cUs(x)$$

$$\left[sUs(x) \right]'' = \left[\ln\alpha cUs(x) \right]'$$

$$= \ln\alpha \ln\alpha sUs(x)$$

$$= (\ln\alpha)^2 sUs(x)$$

Türev almaya devam edersek;

$$\left[cUs(x) \right]^{(n)} = \begin{cases} (\ln\alpha)^n sUs(x); & n = 2k \\ (\ln\alpha)^n cUs(x); & n = 2k+1 \end{cases}$$

$$\left[sUs(x) \right]^{(n)} = \begin{cases} (\ln\alpha)^n cUs(x); & n = 2k \\ (\ln\alpha)^n sUs(x); & n = 2k+1 \end{cases}$$

eşitlikleri elde edilir.

iii)-iv) $\left[cVs(x) \right]' = \left(\alpha^x + \alpha^{-x} \right)'$

$$= \alpha^x \ln\alpha - \alpha^{-x} \ln\alpha$$

$$= \ln\alpha\left(\alpha^{x} - \alpha^{-x}\right)$$

$$= \ln\alpha sVs(x)$$

$$\left[sVs(x)\right]' = \left(\alpha^{x} - \alpha^{-x}\right)'$$

$$= \alpha^{x}\ln\alpha + \alpha^{-x}\ln\alpha$$

$$= \ln\alpha\left(\alpha^{x} + \alpha^{-x}\right)$$

$$= \ln\alpha cVs(x)$$

$$\left[cVs(x)\right]'' = \left(\ln\alpha sVs(x)\right)'$$

$$= \ln\alpha\ln\alpha cVs(x)$$

$$= \left(\ln\alpha\right)^{2} cVs(x)$$

$$\left[sVs(x)\right]'' = \left(\ln\alpha cVs(x)\right)'$$

$$= \ln\alpha\ln\alpha sVs(x)$$

$$= \left(\ln\alpha\right)^{2} cVs(x)$$

Türev almaya devam edersek;

$$\left[cVs(x)\right]^{(n)} = \begin{cases} \left(\ln\alpha\right)^{n} sVs(x); & n = 2k \\ \left(\ln\alpha\right)^{n} cVs(x); & n = 2k+1 \end{cases}$$

$$\left[sVs(x)\right]^{(n)} = \begin{cases} \left(\ln\alpha\right)^{n} cVs(x); & n = 2k \\ \left(\ln\alpha\right)^{n} sVs(x); & n = 2k+1 \end{cases}$$

eşitliklerini elde ederiz.

3.12. Teorem

$$\left(r\cos\theta + ri\sin\theta\right)^n = r^n\left(\cos n\theta + i\sin n\theta\right)$$

"De Moivre Formülü"ne benzer olarak simetrik hiperbolik U ve V fonksiyonları için aşağıdaki eşitlikleri yazabiliriz.

$$\text{i)}\left[cUs(x)\pm sUs(x)\right]^n = \left(\frac{2}{\sqrt{a^2+4}}\right)^{n-1}\left[cUs(nx)\pm sUs(nx)\right] \tag{3.64}$$

$$\text{ii)}\left[cVs(x)\pm sVs(x)\right]^n = (2)^{n-1}\left[cVs(nx)\pm sVs(nx)\right] \tag{3.65}$$

İspat

i) Özelliğin doğruluğunu n üzerinden tümevarımla gösterelim.

$n=1$ için,

$$cUs(x)\pm sUs(x) = \left(\frac{2}{\sqrt{a^2+4}}\right)^0\left[cUs(x)\pm sUs(x)\right]$$

eşitliği doğrudur.

$n=k$ için Eş. 3.64'ün doğru olduğunu kabul edelim. Yani;

$$\left[cUs(x)\pm sUs(x)\right]^k = \left(\frac{2}{\sqrt{a^2+4}}\right)^{k-1}\left[cUs(kx)\pm sUs(kx)\right]$$

eşitliği doğru olsun. O halde, Eş. 3.64'ün $n=k+1$ için doğruluğunu gösterelim.

$$\left[cUs(x)\pm sUs(x)\right]^{k+1}=\left[cUs(x)\pm sUs(x)\right]^{k}\left[cUs(x)\pm sUs(x)\right]$$

$$=\left(\frac{2}{\sqrt{a^2+4}}\right)^{k-1}\left[cUs(kx)\pm sUs(kx)\right]\left[cUs(x)\pm sUs(x)\right]$$

$$=\left(\frac{2}{\sqrt{a^2+4}}\right)^{k-1}\left(\frac{\alpha^{kx}+\alpha^{-kx}}{\sqrt{a^2+4}}\pm\frac{\alpha^{kx}-\alpha^{-kx}}{\sqrt{a^2+4}}\right)\left(\frac{\alpha^{x}+\alpha^{-x}}{\sqrt{a^2+4}}\pm\frac{\alpha^{x}-\alpha^{-x}}{\sqrt{a^2+4}}\right)$$

$$=\left(\frac{2}{\sqrt{a^2+4}}\right)^{k-1}\left(\begin{array}{l}\dfrac{\alpha^{kx+x}+\alpha^{kx-x}+\alpha^{-kx+x}+\alpha^{-(kx+x)}}{\sqrt{a^2+4}}\pm\dfrac{\alpha^{kx+x}-\alpha^{kx-x}+\alpha^{-kx+x}-\alpha^{-(kx+x)}}{\sqrt{a^2+4}}\pm\\ \dfrac{\alpha^{kx+x}+\alpha^{kx-x}-\alpha^{-kx+x}-\alpha^{-(kx+x)}}{\sqrt{a^2+4}}+\dfrac{\alpha^{kx+x}-\alpha^{kx-x}-\alpha^{-kx+x}+\alpha^{-(kx+x)}}{\sqrt{a^2+4}}\end{array}\right)$$

$$=\left(\frac{2}{\sqrt{a^2+4}}\right)^{k-1}\left[2\left(\frac{\alpha^{kx+x}+\alpha^{-(kx+x)}}{\sqrt{a^2+4}}\right)\pm 2\left(\frac{\alpha^{kx+x}+\alpha^{-(kx+x)}}{\sqrt{a^2+4}}\right)\right]$$

$$=\left(\frac{2}{\sqrt{a^2+4}}\right)^{k}\left(cUs\left[(k+1)x\right]\pm sUs\left[(k+1)x\right]\right)$$

Böylece Eş. 3.64'ün doğruluğu gösterilmiş olur.

ii) Özelliğin doğruluğunu n üzerinden tümevarımla gösterelim.

$n=1$ için,

$$cVs(x)\pm sVs(x)=2^{0}\left[cVs(x)\pm sVs(x)\right]$$

eşitliği doğrudur.

$n=k$ için Eş. 3.65'in doğru olduğunu kabul edelim. Yani;

$$\left[cVs(x)\pm sVs(x)\right]^{k}=(2)^{k-1}\left[cVs(kx)\pm sVs(kx)\right]$$

eşitliği doğru olsun. O halde, $n=k+1$ için Eş. 3.65'in doğru olduğunu gösterelim.

$$\begin{aligned}
\left[cVs(x)\pm sVs(x)\right]^{k+1} &= \left[cVs(x)\pm sVs(x)\right]^{k}\left[cVs(x)\pm sVs(x)\right] \\
&= 2^{k-1}\left[cVs(kx)\pm sVs(kx)\right]\left[cVs(x)\pm sVs(x)\right] \\
&= 2^{k-1}\left[\left(\alpha^{kx}+\alpha^{-kx}\right)\pm\left(\alpha^{kx}-\alpha^{-kx}\right)\right]\left[\left(\alpha^{x}+\alpha^{-x}\right)\pm\left(\alpha^{x}-\alpha^{-x}\right)\right] \\
&= 2^{k-1}\begin{bmatrix}\alpha^{kx+x}+\alpha^{kx-x}+\alpha^{-kx+x}+\alpha^{-(kx+x)}\pm\alpha^{kx+x}-\alpha^{kx-x}+\alpha^{-kx+x}-\alpha^{-(kx+x)} \\ \pm\alpha^{kx+x}+\alpha^{kx-x}-\alpha^{-kx+x}-\alpha^{-(kx+x)}+\alpha^{kx+x}-\alpha^{kx-x}-\alpha^{-kx+x}+\alpha^{-(kx+x)}\end{bmatrix} \\
&= 2^{k-1}\left[2\left(\alpha^{kx+x}+\alpha^{-(kx+x)}\right)\pm 2\left(\alpha^{kx+x}-\alpha^{-(kx+x)}\right)\right] \\
&= 2^{k}\left(cVs\left[(k+1)x\right]\pm sVs\left[(k+1)x\right]\right)
\end{aligned}$$

Çizelge 3.1.' de U_n ve V_n dizileri arasındaki bağıntılarla simetrik hiperbolik U ve V fonksiyonları arasındaki bağıntılar karşılaştırılmıştır. Çizelge 3.2.'de ise klasik hiperbolik fonksiyonlar arasındaki bağıntılarla simetrik hiperbolik U ve V fonksiyonları arasındaki bağıntılar karşılaştırılmıştır.

Çizelge 3.1. U_n ve V_n Dizileri ile Simetrik Hiperbolik U ve V Fonksiyonlarının Karşılaştırılması

U ve V Dizileri Arasındaki Bağıntılar	Simetrik Hiperbolik U ve V Fonksiyonları Arasındaki Bağıntılar
$U_{n+2} = aU_{n+1} + U_n$	$sUs(x+2) = acUs(x+1) + sUs(x)$
$U_n = (-1)^{n+1} U_{-n}$	$cUs(x+2) = asUs(x+1) + cUs(x)$
$U_{n+1}U_{n-1} - U_n^2 = (-1)^n$	$sUs(x) = -sUs(-x)$
$U_{2n+1} = U_{n+1}^2 + V_n^2$	$cUs(x) = cUs(-x)$
$V_{n+2} = aV_{n+1} + V_n$	$sUs(x+1)sUs(x-1) - [cUs(x)]^2 = -1$
$V_n = (-1)^n V_{-n}$	$cUs(x+1)cUs(x-1) - [sUs(x)]^2 = 1$
$V_{n+1}V_{n-1} - V_n^2 = (a^2+4)(-1)^{n+1}$	$sUs(2x+1) = [cUs(x+1)]^2 + [sUs(x)]^2$
$V_{n-1} + V_{n-1} = (a^2+4)U_n$	$cUs(2x+1) = [sUs(x+1)]^2 + [cUs(x)]^2$
$V_n + (a^2+4)U_n = 2V_{n-1}$	$sVs(x+2) = acVs(x+1) + sVs(x)$
$V_{n+1}^2 + V_n^2 = (a^2+4)U_{2n+1}$	$cVs(x+2) = asVs(x+1) + cVs(x)$
	$sVs(x) = -sVs(-x)$
	$cVs(x) = cVs(-x)$
	$[sVs(x)]^2 + 2 = cVs(2x)$
	$[cVs(x)]^2 - 2 = cVs(2x)$
	$[sVs(x)]^2 - sVs(x+1)sVs(x-1) = a^2+4$
	$cVs(x+1)cVs(x-1) - [cVs(x)]^2 = a^2+4$
	$sVs(x+1) + sVs(x-1) = (a^2+4)sUs(x)$
	$cVs(x+1) + cVs(x-1) = (a^2+4)cUs(x)$
	$asVs(x) + (a^2+4)cUs = 2cVs(x+1)$
	$acVs(x) + (a^2+4)sUs = 2sVs(x+1)$
	$[sVs(x+1)]^2 + [sVs(x)]^2 = (a^2+4)cUs(2x+1)$
	$[cVs(x+1)]^2 + [cVs(x)]^2 = (a^2+4)sUs(2x+1)$

Çizelge 3.2. Klasik Hiperbolik Fonksiyonlarla Simetrik Hiperbolik U ve V Fonksiyonlarının Karşılaştırılması

Klasik Hiperbolik Fonksiyonlar Arasındaki Bağıntılar	Simetrik Hiperbolik U ve V Fonksiyonları Arasındaki Bağıntılar
$ch^2(x)-sh^2(x)=1$	$\left[cUs(x)\right]^2-\left[sUs(x)\right]^2=\frac{4}{a^2+4}$
$ch(x\pm y)=ch(x)ch(y)\pm sh(x)sh(y)$	$\left[cVs(x)\right]^2-\left[sVs(x)\right]^2=4$
$sh(x\pm y)=sh(x)ch(y)\pm sh(y)ch(x)$	$\frac{2}{\sqrt{a^2+4}}cUs(x\pm y)=cUs(x)cUs(y)\pm sUs(x)sUs(y)$
$ch(2x)=ch^2(x)+sh^2(x)$	$\frac{2}{\sqrt{a^2+4}}sUs(x\pm y)=sUs(x)cUs(y)\pm sUs(y)cUs(x)$
$sh(2x)=2sh(x)ch(x)$	$2cVs(x\pm y)=cVs(x)cVs(y)\pm sVs(x)sVs(y)$
$\left[ch(x)\right]^{(n)}=\begin{cases}sh(x) & ;n=2k+1\\ ch(x) & ;n=2k\end{cases}$	$2sVs(x\pm y)=sVs(x)cVs(y)\pm sVs(y)cVs(x)$
$\left[sh(x)\right]^{(n)}=\begin{cases}ch(x) & ;n=2k+1\\ sh(x) & ;n=2k\end{cases}$	$\frac{2}{\sqrt{a^2+4}}cUs(2x)=\left[cUs(x)\right]^2+\left[sUs(x)\right]^2$
$\iint_n ch(x)dx=\begin{cases}sh(x) & ;n=2k+1\\ ch(x) & ;n=2k\end{cases}$	$\frac{1}{\sqrt{a^2+4}}sUs(2x)=sUs(x)cUs(x)$
$\iint_n sh(x)dx=\begin{cases}ch(x) & ;n=2k+1\\ sh(x) & ;n=2k\end{cases}$	$2cVs(2x)=\left[cVs(x)\right]^2+\left[sVs(x)\right]^2$
	$sVs(2x)=sVs(x)cVs(x)$
	$\left[cUs(x)\right]^{(n)}=\begin{cases}\left[\ln\alpha\right]^n sUs(x) & ;n=2k+1\\ \left[\ln\alpha\right]^n cUs(x) & ;n=2k\end{cases}$
	$\left[sUs(x)\right]^{(n)}=\begin{cases}\left[\ln\alpha\right]^n cUs(x) & ;n=2k+1\\ \left[\ln\alpha\right]^n sUs(x) & ;n=2k\end{cases}$
	$\left[cVs(x)\right]^{(n)}=\begin{cases}\left[\ln\alpha\right]^n sVs(x) & ;n=2k+1\\ \left[\ln\alpha\right]^n cVs(x) & ;n=2k\end{cases}$
	$\iint_n cUs(x)dx=\begin{cases}\left[\ln\alpha\right]^{-n} sUs(x) & ;n=2k+1\\ \left[\ln\alpha\right]^{-n} cUs(x) & ;n=2k\end{cases}$
	$\iint_n sUs(x)dx=\begin{cases}\left[\ln\alpha\right]^{-n} cUs(x) & ;n=2k+1\\ \left[\ln\alpha\right]^{-n} sUs(x) & ;n=2k\end{cases}$
	$\iint_n cVs(x)dx=\begin{cases}\left[\ln\alpha\right]^{-n} sVs(x) & ;n=2k+1\\ \left[\ln\alpha\right]^{-n} cVs(x) & ;n=2k\end{cases}$
	$\iint_n sVs(x)dx=\begin{cases}\left[\ln\alpha\right]^{-n} cVs(x) & ;n=2k+1\\ \left[\ln\alpha\right]^{-n} sVs(x) & ;n=2k\end{cases}$

3.4. Genelleştirilmiş Altın Matrisler

$(2x2)$ tipindeki Fibonacci matrisini düşünelim.

$$Q=\begin{bmatrix}1 & 1\\ 1 & 0\end{bmatrix} \tag{3.66}$$

$n\in\mathbb{N}$ olmak üzere, Eş. 3.66 ile verilen matrisin $n.$ kuvveti;

$$Q^n=\begin{bmatrix}F_{n+1} & F_n\\ F_n & F_{n-1}\end{bmatrix} \tag{3.67}$$

dir $[2-16]$.

Eş. 3.67'de $k\in\mathbb{Z}^+$ için $n=2k$ ve $n=2k+1$ alındığında ise sırasıyla;

$$Q^{2k}=\begin{bmatrix}F_{2k+1} & F_{2k}\\ F_{2k} & F_{2k-1}\end{bmatrix} \tag{3.68}$$

$$Q^{2k+1}=\begin{bmatrix}F_{2k+2} & F_{2k+1}\\ F_{2k+1} & F_{2k}\end{bmatrix} \tag{3.69}$$

matrisleri elde edilir. Eş. 3.68 ve Eş. 3.69 ile verilen matrislerin elemanlarını Eş. 3.15, hiperbolik Fibonacci fonksiyonlarından seçersek;

$$Q^{2k}=\begin{bmatrix}cFs(2k+1) & sFs(2k)\\ sFs(2k) & cFs(2k-1)\end{bmatrix} \tag{3.70}$$

$$Q^{2k+1}=\begin{bmatrix}sFs(2k+2) & cFs(2k+1)\\ cFs(2k+1) & sFs(2k)\end{bmatrix} \tag{3.71}$$

matrislerini elde ederiz. Eş. 3.70 ve Eş. 3.71 ile verilen matrislerde, tamsayı k değişkeni yerine reel değerli x değişkenini alırsak; elemanları x değişkeninin sürekli fonksiyonları olan matrisleri elde ederiz. Bu matrisler $[16]$'da;

$$Q^{2x} = \begin{bmatrix} cFs(2x+1) & sFs(2x) \\ sFs(2x) & cFs(2x-1) \end{bmatrix} \tag{3.72}$$

$$Q^{2x+1} = \begin{bmatrix} sFs(2x+2) & cFs(2x+1) \\ cFs(2x+1) & sFs(2x) \end{bmatrix} \tag{3.73}$$

olarak tanımlanmış Altın matrislerdir. Açıktır ki; Eş. 3.72 ve Eş. 3.73 ile verilen matrisler, Eş. 3.67 ile verilen matrisin tanım kümesini sürekli hale getiren bir genelleştirmedir. Altın matrisler birçok matematiksel özelliğe sahiptir. Örneğin $x = \frac{1}{4}$ alındığında Eş. 3.72 ile verilen matris aşağıdaki gibidir.

$$Q^{\frac{1}{2}} = \begin{bmatrix} cFs\left(\frac{1}{4}\right) & sFs\left(\frac{1}{2}\right) \\ sFs\left(\frac{1}{2}\right) & cFs\left(-\frac{1}{2}\right) \end{bmatrix} \tag{3.74}$$

Burada $Q^{\frac{1}{2}}$ matrisiyle kastedilen Q matrisinin karekökü yani $\sqrt{Q}$ değildir. Sadece şaşırtıcı bir Fibonacci özelliğidir$[16]$.

Biz de bu bölümde $[16]$'da tanımlanan Altın matrislerin bir genelleştirmesini tanımlayacağız.

Eş. 2.43 ile verilen U^n matrisini düşünelim.

$$U^n = \begin{bmatrix} U_{n+1} & U_n \\ U_n & U_{n-1} \end{bmatrix}$$

U^n matrisinde, $k \in Z^+$ olmak üzere, $n = 2k$ ve $n = 2k+1$ seçersek;

$$U^{2k} = \begin{bmatrix} U_{2k+1} & U_{2k} \\ U_{2k} & U_{2k-1} \end{bmatrix} \tag{3.75}$$

$$U^{2k+1} = \begin{bmatrix} U_{2k+2} & U_{2k+1} \\ U_{2k+1} & U_{2k} \end{bmatrix} \tag{3.76}$$

olur. Eş. 3.75 ve Eş. 3.76 ile verilen matrislerin elemanlarını, Eş. 3.27 ile tanımladığımız simetrik hiperbolik U fonksiyonlarından seçersek, $k = 0, \pm 1, \pm 2, \pm 3, \ldots$ için;

$$U^{2k} = \begin{bmatrix} cUs(2k+1) & sUs(2k) \\ sUs(2k) & cUs(2k-1) \end{bmatrix} \tag{3.77}$$

$$U^{2k+1} = \begin{bmatrix} sUs(2k+2) & cUs(2k+1) \\ cUs(2k+1) & sUs(2k) \end{bmatrix} \tag{3.78}$$

matrislerini elde ederiz. Eş. 3.77 ve Eş. 3.78'de k tamsayı değişkeni yerine reel değerli x değişkenini seçersek; elemanları x değişkeninin sürekli fonksiyonları olan Genelleştirilmiş Altın Matrisleri elde ederiz.

$$U^{2x} = \begin{bmatrix} cUs(2x+1) & sUs(2x) \\ sUs(2x) & cUs(2x-1) \end{bmatrix} \tag{3.79}$$

$$U^{2x+1} = \begin{bmatrix} sUs(2x+2) & cUs(2x+1) \\ cUs(2x+1) & sUs(2x) \end{bmatrix} \tag{3.80}$$

Bu matrisler $[16]$'da tanımlanan Altın matrislerin a pozitif tamsayıları için bir genelleştirmesidir.

Belirtmek gereklidir ki; Eş. 3.79 ve Eş. 3.80 ile tanımladığımız Genelleştirilmiş Altın Matrisler; Eş. 1.43 ile verilen U^n matrisinin tanım kümesini sürekli hale getiren bir genelleştirmedir.

Eş. 3.79 ve Eş. 3.80 ile tanımladığımız Genelleştirilmiş Altın Matrislerin determinantlarını hesaplayalım. Eş. 3.41 ve Eş. 3.42 gereği;

$$\det U^{2x} = cUs(2x+1)\,cUs(2x-1) - \left[sUs(2x)\right]^2 = 1$$

$$\det U^{2x+1} = sUs(2x+2)\,sUs(2x) - \left[cUs(2x+1)\right]^2 = -1$$

dir. U^{2x} ve U^{2x+1} matrislerinin determinantları sıfırdan farklı olduğu için bu matrislerin ters matrislerinden bahsedebiliriz.

$$U^{-2x} = \begin{bmatrix} cUs(2x-1) & -sUs(2x) \\ -sUs(2x) & cUs(2x+1) \end{bmatrix} \tag{3.81}$$

$$U^{-(2x+1)} = \begin{bmatrix} -sUs(2x) & cUs(2x+1) \\ cUs(2x+1) & -sUs(2x+2) \end{bmatrix} \tag{3.82}$$

dir. Şimdi U^{-2x} ve $U^{-(2x+1)}$ matrislerinin sırasıyla U^{2x} ve U^{2x+1} matrislerinin ters matrisleri olduğunu gösterelim.

$$U^{2x}U^{-2x} = \begin{bmatrix} cUs(2x+1) & sUs(2x) \\ sUs(2x) & cUs(2x-1) \end{bmatrix}\begin{bmatrix} cUs(2x-1) & -sUs(2x) \\ -sUs(2x) & cUs(2x+1) \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

$$a_{11} = cUs(2x+1)\,cUs(2x-1) - \left[sUs(2x)\right]^2$$

$$a_{12} = -cUs(2x+1)\,sUs(2x) + cUs(2x+1)\,sUs(2x)$$

$$a_{21} = cUs(2x+1)\,sUs(2x) - cUs(2x+1)\,sUs(2x)$$

$$a_{22} = -\left[sUs(2x)\right]^2 + cUs(2x-1)\,cUs(2x+1)$$

Burada a_{12} ve a_{21} elemanlarının sıfıra eşit olacağı açıktır. Eş. 3.41 gereği;

$$a_{11} = a_{22} = 1$$

dir. O halde;

$$U^{2x}U^{-2x} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

bulunur. Yani U^{-2x}, U^{2x} matrisinin ters matrisidir.

$$U^{2x+1}U^{-(2x+1)} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

eşitliğinin doğru olduğu da benzer şekilde gösterilebilir.

Belirtmek gereklidir ki U^{2x} ve U^{2x+1} matrislerinin ters matrisleri bulunurken; simetrik hiperbolik U sinüs fonksiyonlarının bulunduğu köşegendeki elemanlar yer ve işaret, simetrik hiperbolik U cosinüs fonksiyonlarının bulunduğu köşegendeki elemanlar ise sadece yer değiştirir. Çünkü sinüs tek, cosinüs ise çift fonksiyondur.

4. BİR KRİPTOGRAFİK UYGULAMA

4.1. Ön Bilgiler

Eski çağlardan beri haberleşmede gizlilik, üzerinde durulan önemli bir kavramdır. Gizlilikten maksat; ilgili mesajı alıcısından başka kimsenin anlamamasıdır. Gizli haberleşme yaklaşık olarak 4000 yıl önce kullanılmaya başlanmış, özellikle askeri ve diplomasi haberleşmelerinde ön planda tutulmuş ve modern savaşlarda önemli rol oynamıştır. İlk olarak eski Mısırlıların hiyeroglif yazılarının bazılarında karşılaşılan şifreleme daha sonra İbranilerin kitaplarındaki belirli kelimelerde görülmüştür. 2000 yıl önce Eski Roma İmparatoru Julius Ceasar, "Ceasar Şifreleme" olarak bilinen simetrik anahtar şifrelemenin klasik bir örneği olan basit yerine koyma şifrelemesini haberleşmelerinde kullanmıştır.

Rager Bucon; 1200'lerde şifreleme için metotlar geliştirmeye başlamış, Leon Albert; 1460'larda şifreleme tekerleği tasarlamış, 1585 yılında Blaise De Vigenere kriptografi üzerine bir kitap yayınlamış ve polialfabetik yerine koyma metodunu vermiştir. 1790 yılında "Jefferson Silindiri" geliştirilmiş, 1860'lı yıllarda Wheatstone; polialfabetik şifre oluşturmak için ortak merkezli iki daireden oluşan bir makine icat etmiştir.

II. Dünya Savaşı'nda Almanlar, şifre makinelerinin önemli bir sınıfı olan Engima Rotor makinelerini kullanmışlardır. Günümüzde elektronik bankacılığın yaygınlaşması ve elektronik ticaretin kullanılmaya başlanması; gizliliği bu alanda da ön plana çıkarmıştır. Dolayısıyla kriptolojiye büyük çapta bir ilgi doğmuştur. Bilgisayarların hızlı bir şekilde yaygınlaşması, haberleşme sistemlerinin gelişmesi, özel sektörün de dijital formda bilgiyi koruma ve güvenlik sağlama isteğini beraberinde getirmiştir. 1970'lerin başında IBM'de çalışmaya başlanan ve ABD Teknoloji Standartları Enstitüsü NIST tarafından her dört yılda bir güvenliği onaylanan "Veri Şifreleme Standardı" DES; bilinen en iyi kriptolojik mekanizmadır.

Kriptolojinin en güçlü gelişmesi, Diffie ve Hellman'ın "New Directions in Criptography" isimli kitapları yayınlandığında olmuştur. 1978'de Rivest Shamir ve

Adleman, RSA olarak ifade edilen ilk açık anahtar şifreleme ve imza tasarısını bulmuşlardır. RSA tasarısı, zor matematiksel problemlere dayanır. Güçlü ve pratik açık anahtar tasarılarının bir başka sınıfı 1985'te El Gamal tarafından bulunmuştur.

Konuyla ilgili bazı terminolojileri açıklayalım:

Gizlilik sistemlerinin bağlı bulunduğu bilim dalına *kriptoloji* denir. *Kriptografi* ise; gizlilik sistemlerinin tasarım ve araçlarıyla ilgili olan, kriptolojinin özel bir parçasıdır. Gizli şekle çevrilecek metin *açık metin,* birtakım özel dönüşümler uygulayarak açık metindeki harfleri ve ya sembolleri değiştirme işlemi *şifreleme;* şifrelenmiş metin de *şifre metin* olarak adlandırılır. Şifre metnin tekrar anlaşılır hale getirilmesine *deşifre etme* denir. Şifreleme; *açık anahtar şifreleme* ve *simetrik(gizli) anahtar şifreleme* olarak ikiye ayrılır. Sadece şifrelemede kullanılan, deşifrelemede kullanılmayan anahtar açık anahtar; hem şifreleme hem de deşifre etmede kullanılan anahtar ise simetrik anahtardır. Şifreleme anahtarlarını bilerek deşifreleme anahtarlarını; deşifreleme anahtarlarını bilerek de şifreleme anahtarlarını bulmak mümkündür.

A:= Tanımlı alfabe olarak adlandırılan sonlu bir kümedir.

M:= Mesaj uzayı olarak adlandırılan sonlu bir kümedir. Tanımlı bir alfabenin sembollerinin sıralanışından oluşur. Her bir elemanı açık metin olarak adlandırılır.

C:= Şifre uzayı olarak adlandırılan bir kümeyi gösterir. Tanımlanmış alfabeden oluşur. Fakat bu alfabe *M* için tanımlanmış alfabeden farklıdır. Her bir elemanı şifre metin olarak adlandırılır.

K:= Anahtar uzayı olarak adlandırılır. *K*'nın her bir elemanına anahtar denir.

$\forall e \in K$ için $E_e : M \rightarrow C$ olarak gösterilen birebir örten fonksiyonu *şifreleme fonksiyonu* olarak adlandırılır.

$\forall d \in K$ için, $D_d : C \to M$ olarak gösterilen birebir örten fonksiyonu *deşifreleme fonksiyonu* olarak adlandırılır. Buna göre; $m \in M$ mesajına E_e fonksiyonunun uygulanma işlemine *m mesajının şifrelenmesi,* $c \in C$ şifresine D_d fonksiyonunun uygulanma işlemine de *c şifresinin deşifrelenmesi* denir.

Bir şifreleme tasarısı; şifreleme fonksiyonlarının bir kümesi $\{E_e : e \in K\}$ ve $\{D_d : d \in K\}$ kümelerinden oluşur. Burada $\forall e \in K$ için $D_d = E_e^{-1}$ yani $D_d(E_e(M)) = m$ olacak şekilde bir tek $d \in K$ vardır. e ve d' ye *şifreleme/deşifreleme anahtar çifti* denir ve (e,d) ile gösterilir.

(e,d) anahtar çifti hakkında önceden bir bilgisi olmaksızın üçüncü bir şahıs bazı denemelerle şifre metne karşılık gelen açık metni çözerse, şifreleme tasarısı *kırılabilirdir* denir.

Açık anahtar şifrelemenin sağladığı en önemli yararlardan biri dijital imzadır. Dijital imzalar mesajın gerçekten istenilen göndericiden geldiğini doğrulamak için kullanılan bir işlemdir.

4.2. *U* Kriptografik Metot

Bu bölümde [16]'da çalışılan Eş. 3.72 ve Eş. 3.73 Altın Matrisleri ile bu matrislerle terslerinin bir uygulaması olan Altın Kriptografik Metot'un bir genelleştirilmesinden bahsedeceğiz. Bu yeni kriptografik metot Eş. 3.79 ve Eş. 3.80 ile tanımladığımız Genelleştirilmiş Altın Matrisler ile bu matrislerin terslerinin bir uygulaması olarak karşımıza çıkar.

Başlangıç mesajı, pozitif reel sayıların herhangi bir dizisi olan dijital bir sinyal olarak karşımıza çıksın. Dijital telefon, dijital televizyon, dijital ölçüm sistemleri gibi birçok dijital sinyal örneği vardır.

$$m_1, m_2, m_3, m_4, m_5, m_6, m_7, ... \tag{4.1}$$

$$\forall i \geq 1 \text{ için } m_i \geq 0 \tag{4.2}$$

Eş. 4.1 ile verilen dijital sinyalin heackerlardan koruma problemi genellikle kriptografik metotların uygulamalarıyla çözülür.

Genelleştirilmiş Altın Matrislerin bir uygulaması olan U Kriptografik Metot'u tanıtalım.

Eş. 4.1 ile verilen dijital sinyalin ilk dört elemanını seçerek M $(2x2)$ kare matrisine yerleştirelim.

$$M = \begin{bmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{bmatrix} \tag{4.3}$$

Belirtmek gereklidir ki, m_1, m_2, m_3, m_4 elemanlarının M matrisine yerleştirilmesi $4! = 24$ farklı şekilde yapılabilir. Bizim seçimimiz bu 24 farklı permütasyondan herhangi birisidir. Böylece kriptografik korumanın ilk adımı m_1, m_2, m_3, m_4 elemanları için $P_i\,(i = 1, 2, ..., 24)$ permütasyonlarından herhangi birinin seçimidir.

Kriptografik korumanın ikinci adımı ise a pozitif tamsayısının belirlenmesidir. Daha sonra, belirlenen a tamsayısı için Eş. 3.79, Eş.3.80; Genelleştirilmiş Altın Matrisleri ile bu matrislerin ters matrisleri teşkil edilir. U Kriptografik Metot'a göre şifreleme için Eş. 3.79, Eş. 3.80 ile tanımladığımız matrisleri; deşifreleme içinse Eş. 3.81, Eş. 3.82 ile tanımladığımız matrisleri kullanırız.

Çizelge 4.1. ile U Kriptografik Metot'un şifreleme ve deşifreleme algoritmaları verilmiştir.

Çizelge 4.1. Şifreleme ve Deşifreleme Algoritmaları

Şifreleme	Deşifreleme
$MU^{2x} = E_1(x)$	$E_1(x)U^{-2x} = M$
$MU^{2x+1} = E_2(x)$	$E_2(x)U^{-(2x+1)} = M$

Çizelge 4.1.'den görüleceği üzere U Kriptografik Metot'un şifreleme/deşifreleme algoritmaları matris çarpımına bağlıdır. Burada U^{2x} ve U^{2x+1}; şifreleme matrisleri, $E_1(x)$, $E_2(x)$; şifre metinler, $U^{-2x}, U^{-(2x+1)}$ ise deşifreleme matrisleridir. Bu algoritmalardaki x değişkenini kriptografik anahtar olarak kullanabiliriz. Böylece x anahtarının alabileceği değerlere bağlı olarak M mesaj metninden $E(x)$ şifre metnine sonsuz çoklukta dönüşüm yapılabilir.

U kriptografik metotta $K=\{P_i, a, x, c/s\}$; P_i permütasyonları, pozitif a tamsayısı, reel değerli x değişkenleri ve c veya s sembollerinden herhangi biri olmak üzere dört kısımdan oluşur. K anahtarındaki c veya s sembollerinin seçimi, Çizelge 4.1. ile verilen şifreleme/deşifreleme algoritmalarında kullanacağımız U matrisine bağlıdır. Şifreleme/deşifreleme için U^{2x} kullanılacaksa $K=\{P_i, x, a, c\}$ anahtarını, U^{2x+1} kullanılacaksa $K=\{P_i, x, a, s\}$ anahtarını tercih edeceğiz.

Çizelge 4.1. ile verilen şifreleme algoritmasını kullanarak M matrisinden $E(x)$ matrisini; deşifreleme algoritmasını kullanarak da $E(x)$ matrisinden tekrar M matrisini elde etmeye çalışalım.

U şifreleme;

$$MU^{2x}=\begin{bmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{bmatrix}\begin{bmatrix} cUs(2x+1) & sUs(2x) \\ sUs(2x) & cUs(2x-1) \end{bmatrix}=\begin{bmatrix} e_{11} & e_{12} \\ e_{21} & e_{22} \end{bmatrix}=E(x) \tag{4.4}$$

dir. :Burada,

$$e_{11}=m_{11}cUs(2x+1)+m_{12}sUs(2x) \tag{4.5}$$

$$e_{12}=m_{11}sUs(2x)+m_{12}cUs(2x-1) \tag{4.6}$$

$$e_{21}=m_{21}cUs(2x+1)+m_{22}sUs(2x) \tag{4.7}$$

$$e_{22}=m_{21}sUs(2x)+m_{22}cUs(2x-1) \tag{4.8}$$

dir. U deşifreleme ise;

$$E(x)U^{-2x}=\begin{bmatrix} e_{11} & e_{12} \\ e_{21} & e_{22} \end{bmatrix}\begin{bmatrix} cUs(2x-1) & -sUs(2x) \\ -sUs(2x) & cUs(2x+1) \end{bmatrix}=\begin{bmatrix} d_{11} & d_{12} \\ d_{21} & d_{22} \end{bmatrix}=D(x) \tag{4.9}$$

dir. Burada,

$$d_{11}=e_{11}cUs(2x-1)-e_{12}sUs(2x) \tag{4.10}$$

$$d_{12}=-e_{11}sUs(2x)+e_{12}cUs(2x+1) \tag{4.11}$$

$$d_{21}=e_{21}cUs(2x-1)-e_{22}sUs(2x) \tag{4.12}$$

$$d_{22}=-e_{21}sUs(2x)+e_{22}cUs(2x+1) \tag{4.13}$$

dir. Eş. 4.10-Eş. 4.12 ile verilen matris elemanlarını hesaplarken Eş. 4.5-Eş. 4.8, Eş. 3.41 ve Eş. 3.42'yi kullanırsak;

$$\begin{aligned} d_{11} &= e_{11}\left[m_1 cUs(2x+1)+m_2 sUs(2x)\right]cUs(2x-1)- \\ &\quad \left[m_1 sUs(2x)+m_2 sUs(2x)\right]sUs(2x) \\ &= m_1\left[cUs(2x+1)cUs(2x-1)-\left[sUs(2x)\right]^2\right]+ \\ &\quad m_2\left[sUs(2x)cUs(2x-1)-cUs(2x-1)sUs(2x)\right] \end{aligned}$$

$$d_{11} = m_{11} \tag{4.14}$$

bulunur. Benzer hesaplamalarla;

$$d_{12} = m_{12} \tag{4.15}$$

$$d_{21} = m_{21} \tag{4.16}$$

$$d_{22} = m_{22} \tag{4.17}$$

bulunabilir. Eş. 4.14-Eş. 4.17'nin Eş. 4.9'da kullanılmasıyla;

$$D(x) = \begin{bmatrix} d_{11} & d_{12} \\ d_{21} & d_{22} \end{bmatrix} = \begin{bmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{bmatrix} = M$$

elde edilir.

U Kriptografik Metodu bir örnekle açıklamaya çalışalım.

Örnek

Alfabemizdeki harfleri sırasıyla 1'den 29'a kadar olan tamsayılarla eşleyelim

Çizelge 4.2. Alfabemizdeki Harflerin Kodlanması

A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z
16	17	18	19	20	21	22	23	24	25	26	27	28	29

U Kriptografik Metot'a göre şifreleyeceğimiz mesaj kelimesi "ÖZGE" olsun. Bu mesaj, Çizelge 4.2.'ye göre m=19 29 8 6 olarak kodlanır. m mesajını 2×2 tipindeki M matrisine yerleştirelim. U Kriptografik Metot'a göre bu işlem $4!=24$ farklı şekilde yapılabilir.

$$P_1 \begin{bmatrix} 19 & 29 \\ 8 & 6 \end{bmatrix} \quad P_2 \begin{bmatrix} 8 & 19 \\ 6 & 29 \end{bmatrix} \quad P_3 \begin{bmatrix} 6 & 8 \\ 29 & 19 \end{bmatrix} \quad P_4 \begin{bmatrix} 29 & 6 \\ 19 & 8 \end{bmatrix}$$

$$P_5 \begin{bmatrix} 29 & 19 \\ 8 & 6 \end{bmatrix} \quad P_6 \begin{bmatrix} 19 & 8 \\ 6 & 29 \end{bmatrix} \quad P_7 \begin{bmatrix} 8 & 6 \\ 29 & 19 \end{bmatrix} \quad P_8 \begin{bmatrix} 6 & 29 \\ 19 & 8 \end{bmatrix}$$

$$P_9 \begin{bmatrix} 19 & 29 \\ 6 & 8 \end{bmatrix} \quad P_{10} \begin{bmatrix} 8 & 19 \\ 29 & 6 \end{bmatrix} \quad P_{11} \begin{bmatrix} 6 & 8 \\ 19 & 29 \end{bmatrix} \quad P_{12} \begin{bmatrix} 29 & 6 \\ 8 & 19 \end{bmatrix}$$

$$P_{13} \begin{bmatrix} 29 & 19 \\ 6 & 8 \end{bmatrix} \quad P_{14} \begin{bmatrix} 19 & 8 \\ 29 & 6 \end{bmatrix} \quad P_{15} \begin{bmatrix} 8 & 6 \\ 19 & 29 \end{bmatrix} \quad P_{16} \begin{bmatrix} 6 & 29 \\ 8 & 19 \end{bmatrix}$$

$$P_{17} \begin{bmatrix} 8 & 29 \\ 19 & 6 \end{bmatrix} \quad P_{18} \begin{bmatrix} 6 & 19 \\ 8 & 29 \end{bmatrix} \quad P_{19} \begin{bmatrix} 29 & 8 \\ 6 & 19 \end{bmatrix} \quad P_{20} \begin{bmatrix} 19 & 6 \\ 29 & 8 \end{bmatrix}$$

$$P_{21} \begin{bmatrix} 19 & 6 \\ 8 & 29 \end{bmatrix} \quad P_{22} \begin{bmatrix} 8 & 29 \\ 6 & 19 \end{bmatrix} \quad P_{23} \begin{bmatrix} 6 & 19 \\ 29 & 8 \end{bmatrix} \quad P_{24} \begin{bmatrix} 29 & 8 \\ 19 & 6 \end{bmatrix}$$

M matrisi 7. permütasyon olsun.

$$M = \begin{bmatrix} 8 & 6 \\ 29 & 19 \end{bmatrix}$$

a pozitif tamsayısını 2, x reel sayısını 1, şifreleme matrisini U^{2x} seçerek U Kriptografik Metot'un $K = \{P_7, 2, 1, c\}$ şifreleme anahtarını ve $U^2 = \begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix}$ şifreleme matrisini oluşturabiliriz.

Çizelge 4.1.'deki şifreleme algoritmasını K anahtarına uygun olarak kullandığımızda;

$$MU^2 = \begin{bmatrix} 8 & 6 \\ 29 & 19 \end{bmatrix} \begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix}$$

$$E = \begin{bmatrix} 52 & 22 \\ 183 & 77 \end{bmatrix}$$

şifre metnini elde ederiz. Böylece, m=19 29 8 6 mesaj kelimesinden e=52 22 183 77 şifre kelimesini elde etmiş olduk.

E matrisinin elemanlarını $\bmod 29$ 'a göre düzenleyelim.

$52 \equiv 23 \pmod{29}$

$22 \equiv 22 \pmod{29}$

$183 \equiv 9 \pmod{29}$

$77 \equiv 19 \pmod{29}$

Elde ettiğimiz sonuçlar için Çizelge 4.2.'yi kullanırsak, "ÖZGE" mesajının "ŞSĞÖ" olarak şifrelendiğini görmüş oluruz.

Alıcı, Çizelge 4.1.'deki deşifreleme algoritmalarını kullanarak E şifre metninden M mesaj metnine ulaşmaya çalışır. Alıcının deşifreleme için kullanacağı anahtar, $K=\{P_7, 2, 1, c\}$, şifreleme için kullandığımız anahtarla aynıdır.

Alıcı, Çizelge 4.1.'e göre;

$$EU^{-2} = \begin{bmatrix} 52 & 22 \\ 183 & 77 \end{bmatrix} \begin{bmatrix} 1 & -2 \\ -2 & 5 \end{bmatrix}$$

$$M = \begin{bmatrix} 8 & 6 \\ 29 & 19 \end{bmatrix}$$

mesaj metnine ulaşır. K anahtarında yer alan 7. permütasyonu dikkate aldığında, M matrisinden m= 19 29 8 6 mesaj kelimesine ulaşır. Çizelge 4.2.'ye göre deşifre edilen mesaj "ÖZGE" dir.

Belirtmek gereklidir ki şifreleyeceğimiz mesaj kelimesi dört uzunluklu parçalara ayrılarak mesaj matrisine yerleştirilir. Eğer mesaj matrisine yerleştirilecek kelimenin uzunluğu dörtten azsa dolgu yöntemi kullanılabilir. Örneğin; şifreleyeceğimiz kelime "AZ" ise bu kelime mesaj matrisine "AZZZ" olarak yerleştirilebilir.

4.3. U Kriptografik Metodun Kontrol Elemanları

Çizelge 4.1. ile verilen şifreleme algoritmalarını kullanarak $E_1(x)$ ve $E_2(x)$ matrislerinin determinantlarını hesaplayalım.

$$\det E_1(x) = \det\left[MU^{2x}\right] = \det M \det U^{2x} \tag{4.18}$$

$$\det E_2(x) = \det\left[MU^{2x+1}\right] = \det M \det U^{2x+1} \tag{4.19}$$

eşitlikleri yazılır. Eş. 4.18 ve Eş. 4.19'da Eş. 3.41 ve Eş. 3.42'yi kullanırsak;

$$\det E_1(x) = \det M \tag{4.20}$$

$$\det E_2(x) = -\det M \tag{4.21}$$

olarak bulunur. Böylece Eş. 4.20 ve Eş. 4.21, U Kriptografik Metot'un ilk kontrol elemanı olur.

U Kriptografik Metot'un diğer kontrol elemanları ise $E(x)$ matrisinin elemanları arasındaki bağıntılardır.

Seçilen pozitif x reel sayısı için Eş. 4.2'nin kullanılmasıyla Eş. 4.10-Eş. 4.13;

$$e_{11}cUs(2x-1) - e_{12}sUs(2x) > 0 \tag{4.22}$$

$$-e_{11}sUs(2x) + e_{12}cUs(2x+1) > 0 \tag{4.23}$$

$$e_{21}cUs(2x-1) - e_{22}sUs(2x) > 0 \tag{4.24}$$

$$-e_{21}sUs(2x) + e_{22}cUs(2x+1) > 0 \tag{4.25}$$

eşitsizliklerine dönüşür. Eş. 4.22 ve Eş. 4.23'ün birlikte düşünülmesiyle;

$$e_{12}\frac{sUs(2x)}{cUs(2x-1)} < e_{11} < e_{12}\frac{cUs(2x+1)}{sUs(2x)} \tag{4.26}$$

eşitsizliği elde edilir. Eş. 4.26'da $x \to \infty$ için Eş. 3.33'ün kullanılmasıyla;

$$e_{11} \approx \alpha e_{12} \tag{4.27}$$

yaklaşık eşitliği bulunur. Benzer şekilde Eş. 4.24 ve Eş. 4.25'in birlikte düşünülmesiyle;

$$e_{22}\frac{sUs(2x)}{cUs(2x-1)} < e_{21} < e_{22}\frac{cUs(2x+1)}{sUs(2x)} \tag{4.28}$$

eşitsizliği elde edilir. $x \to \infty$ için Eş. 3.33'ün kullanılmasıyla;

$$e_{21} \approx \alpha e_{22} \tag{4.29}$$

yaklaşık eşitliği bulunur.

x değişkenini negatif reel sayılardan seçersek $x \to -\infty$ için Eş. 3.34'ün kullanılmasıyla Eş. 4.27 ve Eş. 4.29;

$$e_{11} \approx -\frac{1}{\alpha}e_{12} \tag{4.30}$$

$$e_{21} \approx -\frac{1}{\alpha}e_{22} \tag{4.31}$$

yaklaşık eşitliklerine dönüşür.

Böylece $x \to \infty$ için Eş. 4.27 ve Eş. 4.29 ile verilen yaklaşık eşitlikler ile Eş. 4.20 ve Eş. 4.21; $x \to -\infty$ için Eş. 4.30 ve Eş. 4.31 ile verilen yaklaşık eşitlikler ile Eş. 4.20 ve Eş. 4.21; U Kriptografik Metot'un kontrol elemanları olarak karşımıza çıkar.

4.4. Hata Bulma ve Düzeltme

U Kriptografik Metot, E şifre metninde oluşabilecek hataları bulmak ve düzeltmek için farklı bağıntılar kullanır. Mesaj matrisine uygulanan Çizelge 4.1.'deki şifreleme algoritmaları sonrasında oluşabilecek herhangi bir hataya karşı Eş. 4.20 veya Eş. 4.21

kontrol bağıntısı olarak rol oynar. E şifre metninin alıcıya gönderilmesi sırasında oluşabilecek herhangi bir hataya karşı ise pozitif x reel değerleri için Eş. 4.27 ve Eş. 4.29, negatif x değerleri için Eş. 4.30 ve Eş. 4.31 ile verilen yaklaşık eşitlikleri kontrol bağıntısı olarak rol oynar.

$\det E \neq \det M$ ise E matrisi hatalıdır. İlk hipotezimiz alıcıya gönderilen E matrisinde tek hata olmasıdır. E matrisinde 4 farklı tek hatanın olacağı açıktır.

$$\begin{bmatrix} k & e_{12} \\ e_{21} & e_{22} \end{bmatrix} \qquad \begin{bmatrix} e_{11} & l \\ e_{21} & e_{22} \end{bmatrix} \qquad \begin{bmatrix} e_{11} & e_{12} \\ m & e_{22} \end{bmatrix} \qquad \begin{bmatrix} e_{11} & e_{12} \\ e_{21} & n \end{bmatrix}$$

Burada k, l, m, n elemanları bozulmuş(hatalı) elemanlardır. Eş. 4.27, Eş. 4.29 veya Eş. 4.30, Eş. 4.31 ile verilen yaklaşık eşitlikleri kullanarak bu hataları düzeltmeye çalışırız. Kontrol bağıntılarını sağlayan çözümler elde edemezsek hipotezimizi değiştirmek zorunda kalırız.

İkinci hipotezimiz E şifre metninde iki hata olmasıdır. E şifre metninde $\binom{4}{2} = 6$ farklı iki hata mevcuttur.

Örnek olarak aşağıdaki iki hataya sahip E matrisini inceleyelim.

$$E = \begin{bmatrix} k & l \\ e_{21} & e_{22} \end{bmatrix}$$

İlk kontrol elemanı Eş. 4.20 veya Eş. 4.21 kullanılarak aşağıdaki cebirsel denklemleri yazabiliriz.

$$\begin{aligned} ke_{22} - le_{21} &= \det M \\ ke_{22} - le_{21} &= -\det M \end{aligned} \qquad (4.32)$$

İkinci kontrol elemanı olarak Eş. 4.27 veya Eş. 4.30'u kullanarak k ve l arasında aşağıdaki bağıntıları yazabiliriz.

$$k \approx \alpha l \qquad (x \to \infty)$$
$$k \approx \frac{-1}{\alpha} l \qquad (x \to -\infty) \tag{4.33}$$

Belirtmek gereklidir ki, Eş. 4.32 ile verilen denklemler diafont denklemlerdir ve sonsuz çözüme sahiptir. Biz bu çözümler arasından Eş. 4.33 ile verilen yaklaşık eşitlikleri sağlayan çözümleri arayacağız. Bulacağımız çözümler kontrol bağıntılarını sağlamazsa E şifre metninde üç hata olduğu sonucuna varırız. Benzer yaklaşımlarla E şifre metnindeki tüm üç hataya sahip durumları tespit ederek bu hataları düzeltebiliriz. Bu durumda da çözümlerimiz kontrol bağıntılarını sağlayan çözümler değilse ya $\det M$ hatalıdır ya da E şifre metninde dört hata vardır yani E şifre metni düzeltilemez durumdadır.

m mesaj kelimesinin alıcıya gönderilmesi sırasında, E şifre metninde oluşabilecek hataları nasıl bulup düzelteceğimizi, aşağıdaki örneklerle açıklayalım.

Örnek

Beklediğimiz mesaj, $K=\{P_7, 2, 1, c\}$ anahtarı ile $E = \begin{bmatrix} 52 & 22 \\ 183 & 7 \end{bmatrix}$ olarak gelmiş olsun. $\det M = -22$ olduğuna göre; E şifre metnindeki hatayı bulup düzelterek, mesaj kelimesine ulaşalım.

Şifreleme anahtarı $K=\{P_7, 2, 1, c\}$ olduğundan, E şifre metnindeki hatayı bulup düzeltmek için Eş. 4.20, Eş. 4.27 ve Eş. 4.29 kontrol bağıntılarını kullanacağız.

İlk kontrol bağıntısı Eş. 4.20'ye göre;

$$\det E = -3662 \neq -22 = \det M$$

olduğundan E şifre metni hatalıdır. Diğer kontrol bağıntıları Eş. 4.27 ve Eş. 4.29'a göre;

$$52 \approx \left(1+\sqrt{2}\right)22$$
$$183 \approx \left(1+\sqrt{2}\right)7$$

olmalıdır. Fakat Eş. 4.29'un sağlanmadığı açıktır. Bu durumda e_{21} veya e_{22} elemanlarının hatalı olabileceğini tespit ederiz. Hipotezimiz ilk olarak, E şifre metninde tek hatanın varlığına ilişkin kuralım.

Kabul edelim ki, e_{21} elemanı hatalı olsun. O halde e_{21};

$$\det E = \det M$$
$$e_{11}e_{22} - e_{12}e_{21} = \det M$$
$$e_{21} = \frac{e_{11}e_{22} - \det M}{e_{12}} \tag{4.34}$$

denklemi ile Eş. 4.29 ile verilen kontrol bağıntısını sağlayan pozitif bir tamsayı olmak zorundadır.

Eş. 4.34'e göre;

$$e_{21} = \frac{52.7 + 22}{22} = 17,545 \notin Z^{+}$$

olduğundan kabulümüz yanlıştır. Bu durumda e_{22} elemanının hatalı olduğunu kabul ederiz. e_{22};

$$e_{22} = \frac{e_{12}e_{21} + \det M}{e_{11}} \tag{4.35}$$

denklemi ile Eş. 4.29 ile verilen kontrol bağıntısını sağlayan pozitif bir tamsayı olmak zorundadır.

Eş. 4.35'e göre; $e_{22} = 77 \in Z^+$ dır. Aynı zamanda, $\frac{183}{77} = 2,376 \approx 1+\sqrt{2}$ olup, Eş. 4.29 ile verilen kontrol bağıntısı da sağlanır.

Çizelge 4.1.'deki deşifreleme algoritmasını K anahtarına uygun olarak kullandığımızda;

$$EU^{-2} = \begin{bmatrix} 52 & 22 \\ 183 & 77 \end{bmatrix} \begin{bmatrix} 1 & -2 \\ -2 & 5 \end{bmatrix}$$

$$M = \begin{bmatrix} 8 & 6 \\ 29 & 19 \end{bmatrix}$$

M mesaj matrisine ulaşırız. K anahtarındaki 7. permütasyonu dikkate aldığımızda; m=19 29 8 6 mesaj kelimesine ulaşırız.

Örnek

Beklediğimiz mesaj, $K=\{P_7, 2, 1, c\}$ anahtarı ile $E = \begin{bmatrix} 52 & 2 \\ 18 & 77 \end{bmatrix}$ olarak gelmiş olsun. $\det M = -22$ olduğuna göre; E şifre metnindeki hatayı bulup düzelterek, mesaj kelimesine ulaşalım.

Şifreleme anahtarı $K=\{P_7, 2, 1, c\}$ olduğundan; E şifre metnindeki hatayı düzeltmek için, Eş. 4.20, Eş. 4.27 ve Eş. 4.29 ile verilen kontrol bağıntılarını kullanacağız.

İlk kontrol bağıntısı Eş. 4.20'ye göre;

$$\det E = 3968 \neq -22 = \det M$$

olduğundan, E şifre metni hatalıdır. Diğer kontrol bağıntıları Eş. 4.27 ve Eş. 4.29'a göre;

$$52 \approx \left(1+\sqrt{2}\right)2$$

$$18 \approx \left(1+\sqrt{2}\right)77$$

yaklaşık eşitliklerinin ikisinin birden sağlanmadığı açıktır. O halde, E şifre metninde en az iki hata vardır.

Hipotezimizi ilk olarak, E şifre metninde iki hatanın varlığına ilişkin kuralım. Eş. 4.27 ve Eş. 4.29 kontrol bağıntılarının ikisi birden sağlanmadığından, hatalı elemanlar E matrisinin her iki satırında da birer tanedir. Bu durumda, E şifre metninde $\binom{2}{1}\binom{2}{1}=4$ farklı iki hata vardır.

İlk olarak e_{11} ve e_{21} elemanlarının hatalı olduğunu düşünelim. e_{11} ve e_{21};

$$e_{11} = \frac{-22+2e_{21}}{77} \tag{4.36}$$

$$e_{21} = \frac{22+77e_{11}}{2} \tag{4.37}$$

denklemleri ile Eş. 4.27 ve Eş. 4.29 ile verilen kontrol bağıntılarını sağlayan pozitif tamsayılar olmak zorundadır.

Eş. 4.36 ve Eş. 4.37'den;

$$77e_{11} - 2e_{21} = -22 \tag{4.38}$$

diafont denklemi elde edilir. $(77,-2)=1$ ve $1|-22$ olduğundan, Eş. 4.38'in tamsayılarda çözümü vardır.

$$1=77.1+(-2)38$$
$$-22=77(-22)+(-2)(-836)$$

olup, $e_{11}=-22$ ve $e_{21}=-836$ Eş. 4.38'in bir çözümüdür. Ayrıca $t\in Z$ için;

$$e_{11}=-22-2t \tag{4.39}$$

$$e_{21}=-836+77t \tag{4.40}$$

olacak şekilde, sonsuz çoklukta (e_{11},e_{21}) ikilisine ulaşabiliriz. e_{11} ve e_{21} in pozitif tamsayı değerleri için $t\in\left[(-\infty,-11)\cup\left[11,\infty\right)\right]$ olmalıdır. Eş. 4.29 ile verilen kontrol bağıntısına göre;

$$e_{11}\approx\left(1+\sqrt{2}\right)2$$

yaklaşık eşitliğinin de sağlanması gerekir. Bu durumda $e_{11}=5$'tir. Fakat Eş. 4.39'a göre, $e_{11}=5$'i sağlayan $t\in Z$ bulunamaz. Benzer durum, Eş. 4.29 kontrol bağıntısını kullanarak Eş. 4.40 için de görülebilir. O halde, kabulümüz yanlıştır.

e_{12} ve e_{21} hatalı olsun. e_{12} ve e_{21};

$$4026=e_{12}e_{21}$$

denklemi ile Eş. 4.27 ve Eş. 4.29 ile verilen kontrol bağıntılarını sağlayan pozitif çözümler olmak zorundadır.

4026'yı asal çarpanlarına ayırırsak;

$$e_{12}e_{21} = 2.3.11.61 \tag{4.41}$$

olur. Ayrıca Eş. 4.27 ile verilen kontrol bağıntısına göre;

$$52 \approx \left(1+\sqrt{2}\right)e_{12}$$

olmalıdır. Eş. 4.41'i dikkate aldığımızda $e_{12} = 22$ dir. Bu durumda $e_{21} = 183$ bulunur. Eş. 4.29 ile verilen kontrol bağıntısına göre;

$$183 \approx \left(1+\sqrt{2}\right)77$$

yaklaşık eşitliği de sağlanır. Böylece E şifre metnindeki hataları tespit etmiş ve düzeltmiş oluruz.

U Kriptografik Metot'un deşifreleme algoritmasını kullanırsak; m=19 29 8 6 mesaj kelimesine ulaşırız.

Örnek

Beklediğimiz mesaj, $K=\{P_7, 2, 1, c\}$ anahtarı ile $E = \begin{bmatrix} 52 & 2 \\ 18 & 7 \end{bmatrix}$ olarak gelmiş olsun. $\det M = -22$ olduğuna göre; E şifre metnindeki hatayı bulup düzelterek, mesaj kelimesine ulaşmaya çalışalım.

Şifreleme anahtarı $K=\{P_7, 2, 1, c\}$ olduğundan, E şifre metnindeki hatayı düzeltmek için Eş. 4.20, Eş. 4.27 ve Eş. 4.29 ile verilen kontrol bağıntılarını kullanırız.

İlk kontrol bağıntısı Eş. 4.20'ye göre;

$$\det E = 328 \neq -22 = \det M$$

olduğundan E şifre metni hatalıdır. Diğer kontrol bağıntıları Eş. 4.27 ve Eş. 4.29'a göre;

$$52 \approx \left(1+\sqrt{2}\right)2$$
$$18 \approx \left(1+\sqrt{2}\right)7$$

yaklaşık eşitliklerinin her ikisinin de sağlanmadığı açıktır. Bu durumda E şifre metninde en az iki hata vardır. Her bir hata durumu bir önceki örnekte olduğu gibi incelenirse, bulunan çözümlerin Eş. 4.20, Eş. 4.27 ve Eş. 4.29 ile verilen kontrol bağıntılarını sağlamadığı görülür. Bu yüzden hipotezimizi E şifre metninde üç hatanın varlığına ilişkin kurmalıyız.

E şifre metninde, $\binom{4}{3} = 4$ farklı üç hata olma durumu vardır.

Kabul edelim ki E matrisinin e_{11}, e_{12} ve e_{21} elemanları hatalı olsun. e_{11}, e_{12} ve e_{21};

$$e_{12}e_{21} - 7e_{11} = 22 \tag{4.42}$$

denklemi ile Eş. 4.27 ve Eş. 4.29 ile verilen kontrol bağıntılarını sağlayan pozitif tamsayılar olmak zorundadır.

$(1,-7) = 1$ ve $1 \mid 22$ olduğundan Eş. 4.41'in tamsayılarda çözümü vardır.

$$1 = 1.8 + (-7)1$$
$$22 = 1.176 + (-7)22$$

olup, $e_{12}e_{21}=176$ ve $e_{11}=22$ Eş. 4.42'nin bir çözümüdür. Ayrıca $t\in Z$ için;

$$e_{12}e_{21}=176-7t \tag{4.43}$$

$$e_{11}=22+t \tag{4.44}$$

olacak şekilde sonsuz çoklukta $(e_{11},e_{12}e_{21})$ ikilinse ulaşabiliriz. e_{11},e_{12} ve e_{21} pozitif tamsayılar olacağı için $t\in[-21,25]$ olmalıdır. Eş. 4.29 ile verilen kontrol bağıntısına göre;

$$e_{21}\approx\left(1+\sqrt{2}\right)7$$

olmalıdır. O halde,

$$e_{21}=17$$

dir. Bu durumda Eş. 4.42;

$$17e_{12}-7e_{11}=22$$

diafont denklemine dönüşür. Bu denklem bir önceki örnekte olduğu gibi çözülürse, bulunan e_{11} ve e_{12} değerlerinin Eş. 4.27 ile verilen kontrol bağıntısını sağlamadığı görülür. Kabulümüz yanlıştır.

e_{12},e_{21} ve e_{22} hatalı olsun. e_{12},e_{21} ve e_{22};

$$52e_{22}-e_{12}e_{21}=-22 \tag{4.45}$$

denklemi ve Eş. 4.27, Eş. 4.39 ile verilen kontrol bağıntılarını sağlayan pozitif tamsayılar olmak zorundadır. Eş. 4.27 ile verilen kontrol bağıntısına göre;

$$52 \approx \left(1+\sqrt{2}\right) e_{12}$$

olmalıdır. O halde,

$$e_{12} = 22$$

dir. Bu durumda Eş. 4.45;

$$52e_{22} - 22e_{21} = -22 \tag{4.46}$$

diafont denklemine dönüşür. $(52,-22) = 2$ ve $2 \mid -22$ olduğundan Eş. 4.46'nın tamsayılarda çözümü vardır.

$$2 = 52.3 + (-22)7$$
$$-22 = 52(-33) + (-22)(-77)$$

olup, $e_{22} = -33$ ve $e_{21} = -77$; Eş. 4.46'nın bir çözümüdür. Ayrıca $t \in Z$ için;

$$e_{22} = -33 - 11t \tag{4.47}$$

$$e_{21} = -77 - 26t \tag{4.48}$$

olacak şekilde sonsuz çoklukta (e_{12}, e_{22}) ikilisine ulaşabiliriz. e_{21} ve e_{22} pozitif tamsayılar olacağı için $t \in (-\infty, -4]$ olmalıdır. Eş. 4.29 ile verilen kontrol bağıntısına göre;

$$e_{21} \approx \left(1+\sqrt{2}\right) e_{22}$$

olmalıdır. $t = -11$ seçersek, Eş. 4.47 ve Eş. 4.48'e göre;

$$e_{21} = 183$$

$$e_{22} = 77$$

bulunur. Böylece E şifre metnindeki hatalı elemanları tespit etmiş ve düzeltmiş oluruz.

U Kriptografik Metot'un deşifreleme algoritmasını kullanarak m= 19 29 8 6 mesaj kelimesine ulaşırız.

4.5. Şifreleme ve Deşifreleme Zamanı

Eş. 4.4' e göre şifreleme $e_{11}, e_{12}, e_{21}, e_{22}$ elemanlarının hesaplanmasından oluşur.

Eş. 4.5-Eş. 4.8'e göre her bir elemanın hesaplanması için iki çarpma ve bir toplama işlemi gereklidir. Böylece tüm şifreleme zamanı;

$$T_e = 8\Delta t_m + 4\Delta t_a \tag{4.49}$$

olarak yazılır. Burada Δt_m; bir çarpma işleminin zamanı ve Δt_a ise bir toplama işleminin zamanıdır.

Benzer şekilde Eş. 4.10-Eş. 4.13'ü kullanarak tüm deşifreleme zamanı;

$$T_d = 8\Delta t_m + 4\Delta t_a \tag{4.50}$$

olarak yazılır.

Eş. 4.32 ve Eş. 4.33; bize U Kriptografik Metot'un çok hızlı bir metot olduğunu gösterir. Yani U Kriptografik Metot $[16]$ ile verilen Altın Kriptografik Metot'a benzer olarak reel zaman aralığında dijital sinyallerin kriptografik korunmasını sağlar.

4.6. Kriptografik Korumanın Geliştirilmesi

Şifreleme ve deşifreleme çiftlerini kullanarak kriptografik korumayı geliştirebiliriz. Şifrelemenin ilk adımı anahtarı kullanmaktır.

$$K_1 = \{P_i, a_1, x_1, c/s\} \tag{4.51}$$

anahtarı değişken değerler alabilen herhangi bir P_i permütasyonu, herhangi bir a_1 pozitif tamsayısı, herhangi bir x_1 reel sayısı ve c yada s sembolünden oluşur. Şifreleme sonucunda $E(P_i, a_1, x_1, c/s)$ matrisini elde ederiz. $E(P_i, a_1, x_1, c/s)$ matrisini kullanarak şifrelemenin ikinci adımını gerçekleştirebiliriz. Bunun için,

$$K_2 = \{P_j, a_2, x_2, c/s\} \tag{4.52}$$

kriptografik anahtarı kullanılır. Burada P_j, P_i den farklı bir permütasyon; a_2, a_1' den farklı bir pozitif tamsayı ve x_2, x_1'den farklı bir reel sayıdır. K_1 ve K_2 anahtarlarını kullanarak elde edilen yeni şifre matrisi;

$$E\left(E = \{P_i, a_1, x_1, c/s; P_j, a_2, x_2, c/s\}\right) \tag{4.53}$$

dir.

n farklı $P_i, P_j, ..., P_k$ permütasyonlarını, $a_1, a_2, ..., a_n$ pozitif tamsayılarını ve $x_1, x_2, ..., x_n$ reel değişkenlerini kullanarak elde edilen kriptografik anahtar;

$$K_n = \{P_i, a_1, x_1, c/s; P_j, a_2, x_2, c/s; ...; P_k, a_n, x_n, c/s\} \quad (4.54)$$

dir. Çizelge 4.1. ile verilen şifreleme algoritmalarını kullanarak $E = E(K)$ şifre matrisini elde ederiz.

Deşifreleme için ise kriptografik anahtar K_n den elde edilen ters kriptografik anahtar K_n^{-1} i kullanırız. Yani;

$$K_n^{-1} = \{P_k, a_n, x_n, c/s; P_r, a_{n-1}, x_{n-1}, c/s; ...; P_j, a_2, x_2, c/s; P_i, a_1, x_1, c/s\} \quad (4.55)$$

ters kriptografik anahtarı deşifreleme için kullanılır. Böylece $D = D(K^{-1})$ deşifreleme matrisini elde etmiş oluruz.

5. SONUÇ

Modern bilim son yıllarda Fibonacci sayı teorisi ve altın oranla aydınlanmaya başladı. Teorik fizik, geometri, astronomi ve bilgisayar bilimlerinin vazgeçilmez yapısı olan hiperbolik fonksiyonlar ve matrisler bu çalışmayla yeni bir boyut kazandı. Keyfi a pozitif tamsayısı için teşkil edeceğimiz U_n dizileri, U^n matrisleri ve simetrik hiperbolik U fonksiyonları ile Fibonacci sayı teoriye katkı sağlamak sunulan çalışmanın temel amacıdır. Ayrıca $[16]$'da bahsedilen Altın Kriptografik Metot'un bir genelleştirilmesi olan U Kriptografik Metot; U_n dizileri, U^n matrisleri ve simetrik hiperbolik U fonksiyonlarının bir uygulaması olarak karşımıza çıkar.

U Kriptografik Metot birkaç yönden $[16]$'da bahsedilen kriptografik metottan daha iyi sonuç verir.

i) U Kriptografik Metot'un anahtarı $K=\{P_i, a_1, x_1, c/s\}$ olmak üzere dört, Altın Kriptografik Metot'un anahtarı $K=\{P_i, x_1\}$ olmak üzere iki parçadan oluşur. U Kriptografik Metot'ta eklenen yeni değişken keyfi a pozitif tamsayısı ile K anahtarı, şifreleme ve deşifreleme matrislerinin sonsuz çeşitlilikteki seçimine imkân sağlar. Oysaki Altın Kriptografik Metot'ta Q^{2x} veya Q^{2x+1} ile Q^{-2x} veya $Q^{-(2x+1)}$ matrisleri olmak üzere bir tek çeşit şifreleme/deşifreleme matrisi vardır. Ayrıca, Altın Kriptografik Metot'ta şifreleme ve deşifreleme matrisi olarak Q^{2x} veya Q^{2x+1} matrislerinden hangisinin kullanılacağı belirsizdir. Bu durum şifreleme ve deşifreleme işlemleri sırasında problemlere yol açar. U Kriptografik Metot'ta ise K anahtarına eklenen c/s sembolüyle şifreleme ve deşifreleme işlemleri için U^{2x} veya U^{2x+1} matrislerinden hangisinin kullanılacağı belirlenmiş olur.

ii) U Kriptografik Metot'ta mesaj metin ile şifre metin matrislerinin determinantını kıyaslayan Eş. 4.20, Eş. 4.21'in yanı sıra; şifre metnin elemanlarını kıyaslayan pozitif x değerleri için Eş. 4.27, Eş. 4.29; negatif x değerleri için Eş. 4.30, Eş. 4.31 yaklaşık

eşitlikleri kontrol bağıntısı olarak rol oynar. Altın Kriptografik Metot'ta ise şifreleme ve deşifreleme algoritmalarını kontrol eden, şifre metin ile mesaj metin matrislerinin determinantlarını kıyaslayan bir tek kontrol bağıntısı vardır.

iii) Sahip olduğu kontrol bağıntıları vasıtasıyla U Kriptografik Metot, bir şifre metin matrisinde meydana gelebilecek bir, iki ya da üç hatanın düzeltilmesine imkân sağlar.

$$E = \begin{bmatrix} e_{11} & e_{12} \\ e_{21} & e_{22} \end{bmatrix}$$

matrisinde $2^4 - 1 = 15$ farklı hata olma durumu vardır. U Kriptografik Metot; $\binom{4}{1} + \binom{4}{2} + \binom{4}{3} = 14$ farklı hatayı düzeltmeye imkan sağladığından $\frac{14}{15} = \%93,33$ düzeltilebilirdir. Bu ise U Kriptografik Metot'un diğer kriptografik metotlara nazaran daha iyi çalıştığını gösterir. Çünkü son yıllarda geliştirilen asimetrik kriptoloji $[17]$'de çok karmaşık şifreleme ve deşifreleme algoritmaları kullanıldığından, şifreleme ve deşifrelemenin hatasız elde edilemeyeceğini garanti eden bir teori ileri sürer.

KAYNAKLAR

1. Ercolano J., "Matrix Generator of Pell Sequence", ***Fibonacci Quarterly***, 17(1): 71-77 (1979).

2. Halıcı, S., Daşdemir, A., "On Same Relationships Among Pell , Pell-Lucas and Modified Pell Sequences", ***SAÜ Fen Bilimleri Dergisi*****,** 14(2): 141-145 (2010).

3. Hoggat, W.E., Marjorie, B., "Fibonacci Matrices and Lambda Functions The ***Fibonacci Quarterly,*** 2(1): 29-32 (1964).

4. Hoggat, W.E., " The Fibonacci and Lucas Numbers ", ***Haugton Mifflen***, ***Boston*** 1-70 (1969).

5. Horodam, A. F., Pell İdentities", ***Fibonacci Quarterly,*** 9(3): 245-252 (1971).

6. Horadam, A. F., " Generalized Fibonacci Sequence", ***Amer. Math. Monthly*****,** 68(5): 455–459 (1961).

7. Koshy, T.,"Fibonacci and Lucas Numbers with Applications", ***Jhon Wiley & Sons,*** New York (2001).

8. Matham, R., "Sums Involving Fibonacci and Pell Numbers", ***Portugliae Math.,*** 56(3): 309-317 (1999).

9. Stakhov, A.P., Rozin, B."Theory of Binet Formulas for Fibonacci and Lucas p-Numbers", ***Choas, Solitons and Fractals*** 27: 1162-1177 (2006).

10. Stakhov, A.P., "The Generalized Golden Sections and a New Approach to The Geometric Defination of a Number", ***Ukr Math J,*** 56(8):1143-50 (2004).

11. Stakhov, A.P., "Fundamentals of a New Kind of Mathematics Based on The Golden Section", ***Choas, Solitons and Fractals,*** 27: 1124-1146 (2006).

12. Stakhov, A.P., "Fibonacci Matrices A Generalization of The Cassini Formula and A New Coding Theory", ***Chaos, Solitons and Fractals,*** 30: 55-56 (2006).

13. Vajda, S., "Fibonacci and Lucas Numbers And The Golden Section", ***Halsted Pres, New York***, 9-51 (1989).

14. Vajda, S., "Fibonacci & Lucas Numbers and Theory", ***Jhon Wiley & Sons,*** New York (1989).

15. Stakhov, A.P, Rozin, B., " On a New Class of Hyperbolic Functions", ***Chaos, Solitions and Fractals,*** 23: 379-59 (2004).

16. Stakhov, A.P., "The Golden Matrices a New Kind of Criptography", ***Choas***,

Solitons and Fractals, 32: 1138-1146 (2007).

17. Seberry J., Pieprzyk J., "Criptography an Introduction to Cumpeter Securitiy", ***Prentice Hall,*** (1989).

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı	: BOSTANCI, Özge
Uyruğu	: T.C.
Doğum tarihi ve yeri	: 21.02.1985 Ankara
Medeni hali	: Bekar
Telefon	: 0 506 851 55 49
e-mail	: mat_ozge_5@hotmail.com

Eğitim

Derece	**Eğitim Birimi**
Lisans	Atatürk Üniversitesi Kazım Karabekir Eğitim Fakültesi / Ortaöğretim Matematik Öğretmenliği
Lise	Amasya Anadolu Öğretmen Lisesi

Yabancı Dil

İngilizce