ANKARA
HACI BAYRAM VELİ ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

Perrin Sayılarının Kodlama Teorisinde Uygulanması

Yüksek Lisans Tezi

Satı Yılmaz

Matematik Anabilim Dalı
Cebir ve Sayılar Teorisi Programı
Ankara, 2025

Perrin Sayılarının Kodlama Teorisinde Uygulanması

Satı YILMAZ

Tez Danışmanı Prof. Dr. Fatih YILMAZ

Tez Jürisi

Prof. Dr. Mustafa ÖZKAN

Prof. Dr. Fatih YILMAZ

Dr. Öğr. Üyesi Düriye KORKMAZ DÜZGÜN

YÜKSEK LİSANS TEZİ

MATEMATİK ANABİLİM DALI

CEBİR VE SAYILAR TEORİSİ BİLİM DALI

Ankara - 2025

ETİK BEYAN

Ankara Hacı Bayram Veli Üniversitesi Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında; tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi, tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu, tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi, kullanılan verilerde herhangi bir değişiklik yapmadığımı, bu tezde sunduğum çalışmanın özgün olduğunu, bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Satı YILMAZ

22/06/2025

ONAY

Ankara Hacı Bayram Veli Üniversitesi Lisansüstü Eğitim Enstitüsü Matematik Anabilim Dalı Yüksek Lisans Programı Yüksek Lisans Öğrencisi Satı YILMAZ tarafından hazırlanan Perrin Sayılarının Kodlama Teorisinde Uygulanması Başlıklı tez çalışması 16/06/2025 tarih ve 00:00 saatinde yapılan tez savunma sınavında aşağıdaki jüri tarafından OY BİRLİĞİ ile YÜKSEK LİSANS TEZİ olarak KABUL edilmiştir.

	Kabul	**Ret**
Başkan (Unvan/Ad-Soyad/Kurum):		
Prof. Dr. Mustafa ÖZKAN	☒	☐
Gazi Üniversitesi		
Üye (Unvan/Ad-Soyad/Kurum):		
Prof. Dr. Fatih YILMAZ	☒	☐
Ankara Hacı Bayram Veli Üniversitesi		
Üye (Unvan/Ad-Soyad/Kurum):		
Dr. Öğr. Üyesi Düriye KORKMAZ DÜZGÜN	☒	☐
Ankara Hacı Bayram Veli Üniversitesi		

Perrin Sayılarının Kodlama Teorisinde Uygulanması

Satı YILMAZ

Yüksek Lisans Tezi

Danışman: Prof. Dr. Fatih YILMAZ
T.C. Ankara Hacı Bayram Veli Üniversitesi Lisansüstü Eğitim Enstitüsü
Matematik Anabilim Dalı
2025, Ankara

ÖZET

Perrin dizileri üzerine yapılan bu çalışmada, birinci bölümde rekürans bağıntılarına ilişkin temel tanımlar ve teoremlere yer verilmiştir. Ayrıca Perrin sayılarına ait rekürans bağıntısı tanımlanmış ve bu sayıların matris gösterimleri sunulmuştur. Bu bölümde ayrıca kuaterniyon ve Perrin kuaterniyon kavramları tanıtılmış, son olarak grafik teorisine dair bazı temel tanımlar verilmiştir. İkinci bölümde, Perrin sayılarına dayalı olarak kodlama yöntemleri geliştirilmiştir. Multiplicative Perrin dizilerinin pozitif ve negatif indeksli halleri tanımlanmış ve bu dizilerin çeşitli özellikleri ele alınmıştır. Bu sayıların kullanımıyla kodlama işlemleri gerçekleştirilmiştir. Ayrıca grafların matris gösterimleri incelenerek, Perrin sayıları kullanılarak şifreleme yöntemleri uygulanmıştır. Özetle, bu çalışmada Perrin dizileri ile kodlama teorisine ilişkin yöntemler sunulmuş ve bu yöntemlere dair uygulama örnekleri verilmiştir. Çalışmanın amacı, Perrin dizilerinin matematiksel özelliklerini incelemek ve bu dizilerin kodlama teorisindeki potansiyel kullanım alanlarını ortaya koymaktır.

Anahtar Kelimeler: Kodlama teorisi, Perrin sayıları, Multplicative Perrin

Application of Perrin Number in Coding Theory

Satı YILMAZ

Master's Thesis

Supervisor: Prof. Dr. Fatih YILMAZ
Ankara Hacı Bayram Veli University, Institute of Graduate Programs
Department of Mathematic
2025, Ankara

ABSTRACT

In this study on Perrin sequences, the first chapter includes fundamental definitions and theorems related to recurrence relations. Additionally, a recurrence relation for Perrin numbers is defined, and their matrix representations are presented. This chapter also introduces the concepts of quaternions and Perrin quaternions, and finally, some basic definitions from graph theory are provided. In the second chapter, coding methods based on Perrin numbers are developed. The positive and negative indexed forms of multiplicative Perrin sequences are defined, and various properties of these sequences are discussed. Coding processes are carried out using these numbers. Furthermore, by examining the matrix representations of graphs, encryption methods based on Perrin numbers are applied. In summary, this study presents methods related to coding theory using Perrin sequences and provides application examples of these methods. The aim of the study is to examine the mathematical properties of Perrin sequences and to reveal their potential applications in coding theory.

Keywords: Coding theory, Perrin numbers, Multiplicative Perrin

TEŞEKKÜR

Bu tez çalışmasının hazırlanmasında katkılarını esirgemeyen birçok kişi ve kuruma teşekkür etmek isterim.

Öncelikle, çalışmam boyunca bilgi, deneyim ve desteğiyle her zaman yanımda olan değerli tez danışmanım Prof. Dr. Fatih Yılmaz'a sonsuz teşekkürlerimi sunarım. Yol göstericiliği ve sabrı sayesinde bu çalışmayı başarıyla tamamlayabildim.

Akademik hayatım boyunca bilgi ve motivasyon kazanmamda katkısı olan tüm hocalarıma teşekkür ederim. Ayrıca, araştırmam süresince bana destek olan arkadaşlarıma ve tüm sevdiklerime minnettarım.

Son olarak, her koşulda yanımda olan, bana inanan ve desteğini hiç eksik etmeyen aileme en derin şükranlarımı sunuyorum. Varlığınız, bu süreci benim için çok daha anlamlı kıldı.

İÇİNDEKİLER

Sayfa

Özet iv
Abstract v
Teşekkür vi
İçindekiler vii
Tabloların Listesi viii
Şekillerin Listesi ix
Simgeler Dizini x
1. GİRİŞ 1
2. PERRİN SAYILARIYLA KODLAMA TEORİSİ ALANINDA UYGULAMALAR 29
2.1. Perrin Üreteç Matrisini Kullanarak Şifreleme 29
2.2. Affine Cipher Yöntemi ile Perrin Dizisi ve Perrin Katsayılı Kuaterniyonları Kullanarak Şifreleme 36
2.3. Multiplicative Perrin Sayıları ve Şifreleme 41
2.4. Grafların Matris Gösterimleri ve Perrin Sayıları ile Şifreleme 48
3. SONUÇ 53
Extended Abstract 55
Kaynaklar 57
Özgeçmiş 61

TABLOLARIN LİSTESİ

Sayfa

Tablo 1.1. Bazı İkinci Dereceden Özel Sayı Dizileri 9
Tablo 1.2. Bazı Genelleştirilmiş Tribonacci Sayılarının Özel Durumları 11
Tablo 1.3. Bazı Pozitif ve Negatif n Değerleri İçin Perrin Sayıları 14
Tablo 1.4. Perrin Sayıları İçin Rekürans Bağıntıları 16
Tablo 1.5. Reel Kuaterniyonlar İçin Birimlerin Çarpımı 19
Tablo 1.6. Split Kuaterniyonlar İçin Birimlerin Çarpımı 22
Tablo 1.7. Genelleştirilmiş Kuaterniyonlar İçin Birimlerin Çarpımı 22
Tablo 1.8. Genelleştirilmiş Kuaterniyonların Sınıflandırılması 23
Tablo 1.9. Bazı Perrin Genelleştirilmiş Kuaterniyon Örnekleri 24
Tablo 2.1. ASCII ve 8-Bit Binary Tablosu 31
Tablo 2.2. ASCII Tablosu 37
Tablo 2.3. Perrin ve Multiplicative Perrin Sayılarının Tablosu 42

ŞEKİLLERİN LİSTESİ

Sayfa

Şekil 2.1. Graf 1 48
Şekil 2.2. Graf 2 50

SİMGELER DİZİNİ

Bu çalışmada kullanılmış kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Simgeler	Açıklamalar
$\widetilde{\boldsymbol{R_n}}$	Genelleştirimiş Perrin Kuaterniyonları
$+_*$	Multiplicative(çarpımsal) Toplama
$\cdot_*$,	Multiplicative(çarpımsal) Çarpım
$\mathbb{Z}^+$	Pozitif Tam Sayılar Kümesi
$\boldsymbol{MR_n}$	Multiplicative Perrin Sayıları
$\boldsymbol{P_n}$	Padovan Sayıları
$\boldsymbol{R_n}$	Perrin Sayıları
$\boldsymbol{\mathcal{R}_{\alpha\beta}}$	Perrin Genelleştirilmiş Kuaterniyonlar Kümesi
$\mathbb{N}$	Doğal Sayılar Kümesi
$\mathbb{Z}$	Tam Sayılar Kümesi
$\boldsymbol{G = (V, E)}$	Graf

1. GİRİŞ

Sayılar ve sayı sistemleri, yalnızca matematiksel düşüncenin temel yapı taşları değil, aynı zamanda fizik, mühendislik, bilgisayar bilimi, ekonomi ve astronomi gibi birçok disiplinde hayati öneme sahiptir. İnsanlık tarihinin erken dönemlerinden beri sayılar farklı kültürler tarafından çeşitli şekillerde temsil edilmiştir. MÖ 3000 civarında Mısırlılar sayıları hiyeroglif yazı sistemiyle ifade etmeye başladılar. Bu ilk sistem, bir kavramı veya nesneyi temsil etmek için kullandı ve sonunda modern sayı sistemlerinin yolunu açtı. Mezopotamya'daki Sümerler ve Babilliler, günümüzde zaman ve açı ölçümü gibi birçok alanda kullanılan 60 tabanlı sayı sistemini geliştirdiler. Yunanlılar, sayılarla ilgili hesaplamalarını harflerle yaparak matematiksel düşünceyi geometri üzerine kurdular. Roma İmparatorluğu'nda sayıların temsili Roma rakamlarıyla şekillendirildi. Çin'de sayıları ifade etmek için dikey ve yatay çubuklar kullanıldı; bu sistem sayıları görsel olarak düzenlemeye dayalı bir sistemdi. Öte yandan Hindistan, sıfır kavramını geliştiren ve ondalık sistemin temellerini atan bir medeniyet olarak matematiğin evriminde kritik bir rol oynamıştır. Hindistan'dan sonra sayılar ve aralarındaki ilişkiler üzerine yapılan çalışmalar sayı teorisinin ve modern matematiğin temellerini atmıştır. Her biri kendi döneminde sayıların işlevini ve temsilini farklı şekillerde yorumlamıştır, ancak tüm bu katkılar bir araya gelerek günümüzün matematik ve bilim dünyasını şekillendirmede önemli bir rol oynamıştır. [(Anonim), (Dantzig, 1930)]

Matematiksel yapılar modern bilim ve mühendislikte önemli uygulamalar bulmuş ve özellikle sayı teorisi ve dizileri üzerine yapılan çalışmalar birçok disiplinde temel yapı taşları haline gelmiştir. Bu bağlamda özel sayı dizileri, sayı sistemleri ve bunların genellemeleri teorik araştırmaların yanı sıra pratik uygulamalarda da büyük önem taşımaktadır. Belirli bir tekrarlama ilişkisine sahip sayı dizilerinin tanımı matematiksel modeller ve algoritmalara ışık tutmaktadır. İkinci dereceden tekrarlama dizileri gibi temel yapılar bilgisayar bilimi ve kodlama teorisi gibi alanlarda hata düzeltme, güvenlik ve veri iletimi gibi alanlarda önemli rol oynamaktadır.

Matematikte özel bir yere sahip olan bazı sayılar, doğada, sanatta ve bilimde önemli uygulama alanları bulmuştur. Altın oran (1.61803...) ve plastik oran (1.32471...) gibi sayılar, bu tür matematiksel yapılar arasında öne çıkmaktadır [(Sloane N. J.)]. Altın oran, antik çağlardan günümüze kadar matematikçilerin, fizikçilerin, filozofların, sanatçıların ve müzisyenlerin ilgisini çekmiş; estetik ve simetri anlayışının temel taşlarından biri olmuştur. Plastik oran ise, altın orana benzer şekilde, mimari ve matematiksel yapılarda belirgin bir yer edinmiştir. Plastik

oran, $x^3 - x - 1 = 0$ denkleminin tek reel kökü olup, matematiksel düzenin önemli örneklerinden biridir.[(Sloane N. J.)] Bu denklem, dikkat çekici bir şekilde, rekürans ilişkileriyle tanımlanan Padovan ve Perrin sayı dizilerinin de karakteristik denklemi olarak karşımıza çıkmaktadır. Rekürans dizileri, ardışık terimlerin belirli kurallara göre oluşturulduğu diziler olup, birçok bilimsel ve mühendislik uygulamasında kullanılmaktadır. Perrin sayıları, özellikle üçlü rekürans ilişkisiyle tanımlanan ve belirli asal sayılarla olan ilişkisi nedeniyle matematiksel olarak büyük ilgi çeken bir dizidir. Perrin sayıları,

$$R_n = R_{n-2} + R_{n-3}$$

rekürans bağıntısıyla tanımlanır ve başlangıç koşulları $R_0 = 3, R_1 = 0, R_2 = 2$ olarak verilir [(Yılmaz N. , 2015)]. Perrin dizisi, özellikle asal sayılar, grafik teorisi ve kombinatoryal yapılarla ilgili olarak büyüleyici matematiksel özellikler sergiler. Benzersiz tekrarlama formülü, önemsiz olmayan cebirsel özelliklere sahip dizilerin hata düzeltme ve kriptografik yöntemleri geliştirebildiği kodlama teorisindeki uygulamalar için onu bir aday yapar.

Kodlama teorisi alanı, güvenilir veri iletimi ve hata düzeltme sağlamak için büyük bir öneme sahiptir. Hamming ve Reed-Solomon gibi geleneksel kodlar yaygın olarak kullanılmakla birlikte, verimli ve yenilikçi kodlama yöntemlerine olan ihtiyaç devam etmektedir. Kodlama yöntemlerinin tasarlanması, genellikle cebirsel yapılar, sayı dizileri ve modüler aritmetik üzerine kuruludur. Fibonacci dizisine benzerliğiyle dikkat çeken Perrin sayıları, kodlama teorisinde yenilikçi uygulamaların keşfedilmesine olanak sağlayan potansiyel bir araç olarak öne çıkmaktadır.

Kodlama teorisi, bilgiyi belirli sembollerle ifade ederek, verilerin hatalara karşı dayanıklı bir şekilde saklanmasını ve iletilmesini sağlayan matematiksel bir disiplindir. Bu alan, özellikle gürültülü iletişim kanallarında hata tespit ve düzeltme teknikleri geliştirmeye odaklanır. Kodlama teorisinin temelleri, Claude Shannon'ın 1948 yılında yayımladığı "A Mathematical Theory of Communication" adlı çalışmasıyla atılmıştır. Shannon, bir iletişim kanalında hatasız veri iletimi sağlamak için kanal kapasitesi kavramını tanımlamış ve uygun kodlama yöntemlerinin önemini vurgulamıştır (Shannon, 1948). Bu çalışma, bilgi kuramının da temel taşlarından biri olarak kabul edilir.

Kodlama teorisi, günümüz teknolojisinin pek çok alanında kritik bir rol oynamaktadır. Örneğin, dijital haberleşmede verilerin doğru bir şekilde iletilmesini sağlayan hata düzeltme kodları, kodlama teorisinin en önemli uygulamalarından biridir. Bu kodlar, iletim sırasında oluşabilecek hataları otomatik olarak algılayıp düzelterek verinin doğruluğunu garanti eder.

Örneğin, Reed-Solomon kodları, CD ve DVD'lerdeki veri bütünlüğünü sağlamak için yaygın olarak kullanılmaktadır. Ayrıca, uzay iletişiminde, düşük güçlü sinyallerle uzak mesafelere veri göndermek için de hata düzeltme teknikleri büyük önem taşır. NASA'nın Voyager 1 ve 2 uzay araçlarında kullanılan Turbo kodlar, derin uzaydan gelen verilerin doğru bir şekilde Dünya'ya iletilmesini mümkün kılmıştır.

Kodlama teorisi ile kriptografi arasında önemli bir fark bulunmaktadır. Kodlama teorisinin temel amacı, verinin hatasız bir şekilde iletilmesini sağlarken, kriptografi verinin gizliliğini ve güvenliğini korumayı hedefler. Örneğin, blok şifreleme yöntemleri ve açık anahtarlı şifreleme sistemleri (RSA, ElGamal, ECC) kriptografinin temel uygulamaları arasındadır. Kodlama teorisi ise, örneğin QR kodlarında veya mobil iletişim sistemlerinde kullanılan ileri düzey hata düzeltme kodları gibi, daha çok verinin güvenilir iletimi ile ilgilenir. Kriptografi ve kodlama teorisi her ne kadar benzer matematiksel kavramlara dayansa da, hedefleri ve uygulama alanları farklıdır.

Kodlama teorisinin tarihsel gelişimi, matematiksel fikirlerin pratik mühendislik sorunlarına çözüm getirdiği bir süreçtir. Richard W. Hamming, 1950'lerde geliştirdiği Hamming kodları ile hata tespit ve düzeltme alanında büyük bir adım atmıştır. Hamming kodları, günümüzde bilgisayar hafızalarında veri güvenliği sağlamak amacıyla yaygın bir şekilde kullanılmaktadır. 1970'lerde ise, convolutional kodlar ve daha sonra geliştirilen LDPC (Low-Density Parity-Check) kodları, modern kablosuz iletişimde devrim yaratmıştır.

Kodlama teorisi, yalnızca haberleşme sistemlerinde değil, aynı zamanda veri saklama teknolojilerinde de önemli bir yere sahiptir. Örneğin, RAID (Redundant Array of Independent Disks) sistemleri, hata toleransını artırarak büyük veri merkezlerinde veri güvenliğini sağlamak için kodlama tekniklerinden yararlanır. Bunun yanı sıra, veri sıkıştırma algoritmaları da kodlama teorisi ile doğrudan ilişkilidir. MP3, JPEG ve MPEG gibi formatlar, verinin daha az yer kaplamasını sağlamak amacıyla kayıplı ve kayıpsız sıkıştırma yöntemleri kullanır. Bu sayede, büyük boyutlu dosyalar, daha az bant genişliği kullanılarak iletilebilir.

Kodlama teorisinin bir diğer önemli matematiksel yönü, sayı dizileri ve kombinatorik yapılarla olan ilişkisidir. Örneğin, Perrin sayıları kodlama teorisinde çeşitli uygulamalar için kullanılabilir. Perrin sayıları, şeklinde tanımlanan bir rekürsif dizidir ve belirli kalıpların analizi için güçlü bir araç olarak görülebilir. Özellikle hata düzeltme kodlarının tasarımında ve doğrulama süreçlerinde Perrin dizisinin sunduğu kombinatorik özelliklerden yararlanılabilir.

Ayrıca, bazı özel kodlama tekniklerinde bu sayı dizisinin modüler aritmetikteki özellikleri kullanılarak güvenli anahtar üretimi gibi uygulamalar gerçekleştirilebilir.

Perrin sayıları, ayrıca güvenli veri iletimi ile ilgili çeşitli kriptografik protokollerde de araştırılmaktadır. Sayının asal olup olmadığını belirlemede kullanılan Perrin testi, özellikle büyük asal sayıların belirlenmesi açısından önemlidir. Kriptografi ve kodlama teorisi arasındaki bu tür kesişimler, matematiğin teorik ve uygulamalı alanlarını birbirine bağlayan yenilikçi çözümler sunmaktadır.

Kodlama teorisi, haberleşme, veri güvenliği, sıkıştırma ve hata düzeltme gibi birçok alanda kritik bir rol oynamaktadır. Modern dijital sistemlerin güvenilir çalışmasını sağlamak için matematiksel yapıların mühendislik uygulamalarıyla birleştiği bu alan, teknolojinin gelişmesiyle birlikte daha da önem kazanmaktadır. Perrin sayıları gibi özel matematiksel yapılar, kodlama teorisinin daha güçlü ve verimli sistemler geliştirmesine katkıda bulunarak, gelecekteki araştırmalara yön vermektedir.

Her harfi sayısal bir değere dönüştüren Affine şifreleme, belirli matematiksel işlemlerle şifreleyen ve tekrar bir harfe dönüştüren bir tür ikame şifrelemesidir. Bir harfi başka bir harfe dönüştürerek yeni bir metin elde edilir. Şifreleme işlemi aşağıdaki formülle yapılır:

$$Y = (mQ + b) \ \ modn$$

Burada, n alfabedeki harf sayısı, m çarpan değeri, b miktarını ifade eder. Yukarıdaki denklemdeki çarpan m, n'ye göre nispeten asal olmalıdır, aksi takdirde şifre çözme imkansızdır. [(Mezaal & Abdulkareem, 2017)]

Çözme işlemi için şu formül kullanılır:

$$Q = m^{-1}(Y - b)\, modn$$

burada m^{-1}, aşağıdaki denklemi sağlayan bir modül n'nin modüler çarpımsal tersidir:

$$1 = mm^{-1} \ \ modn$$

(Mezaal & Abdulkareem, 2017)

Bir graf, $G = (V, E)$ gibi gösterilen ve $E \subseteq [V]^2$ koşulunu sağlayan bir düğüm ve kenar kümesi çiftidir olarak tanımlanır. Graf tabanlı şifreleme yöntemleri, veriyi yönlendirilmiş veya ağırlıklı graf yapıları üzerinden güvenli bir şekilde dönüştürmeye dayanır. Bu yöntemlerde düğümler genellikle anahtar bileşenleri temsil ederken, kenarlar şifreleme adımlarını belirler.

Bu alanda çalışma yapan (Domada, Ashok, Kumar, & Chaya, 2024) şifreleme ve deşifreleme yöntemini şu şekilde vermiştir.

Şifreleme Prosedürü:

1. Adım: Bir grafı ele alın ve komşuluk matrisini oluşturun. Ardından, mesajı alın ve mesajdaki karakterlere karşılık gelen sayısal değerleri kullanarak bir diyagonal matris oluşturun.

2. Adım: İlk şifreleme katmanını elde etmek için ortaya çıkan iki matrisi çarpın.

3. Adım: Sonra, bu ürünü ikinci şifreleme katmanı için aynı mertebeden bir Perrin matrisine ekleyin.

4. Adım: Son olarak, ortaya çıkan matris iki seviyeli bir şifrelenmiş matrisdir.

Şifre Çözme Prosedürü

Adım 1: Sağlanan matrisi kullanarak, alıcı karşılık gelen olay matrisini oluşturabilir.

Adım 2: İkinci adımda, aynı mertebeden bir Perrin matrisini çıkarın.

Adım 3: Son olarak, bu matrisi orijinal bitişiklik matrisinin tersiyle çarparak mesajı alın.

Bazı Temel Tanımlar

Bu bölümde bazı genel tanımlar ile ileriki bölümlerde kullanılacak tanım ve teoremlere yer verilecektir. Bu bağlamda, rekürans bağıntılarının temel kavramları ele alınarak, ikinci ve üçüncü dereceden bazı özel sayı dizileri incelenecektir. Rekürans bağıntıları, bir dizinin her teriminin kendisinden önceki belirli sayıdaki terimlerle ifade edilmesini sağlayan matematiksel formüllerdir ve özellikle sayı teorisi, lineer cebir ve kodlama teorisi gibi birçok alanda önemli uygulamalara sahiptir. Ayrıca, rekürans bağıntılarının matris gösterimi ile nasıl modellenebileceği açıklanacaktır. Bu kapsamda, companion (eş) matris kavramı tanıtılarak, bu matrisin temel özellikleri ve rekürans dizileri ile olan ilişkisi detaylandırılacaktır. Companion matrisler, rekürans ilişkilerine sahip dizilerin özelliklerini anlamada güçlü bir araç olup, özellikle karakteristik denklemler ve özdeğer analizleri açısından büyük önem taşımaktadır.

Rekürans bağıntıları, bir sayı dizisinin önceki veya sonraki terimlerinin belirlenmesini sağlayan ilişkiler olarak bilinir. Bir rekürans bağıntısının lineer olması, dizinin her teriminin kendinden önceki terimlerin lineer bir kombinasyonu şeklinde ifade edilebilmesi anlamına gelir [(Tan, 2015)]. Lineer rekürans bağıntıları ise iki kategoriye ayrılır: homojen ve homojen olmayan bağıntılar. Homojen rekürans bağıntılarında her terim yalnızca önceki terimlerin

katsayılı toplamı şeklinde ifade edilirken, homojen olmayan bağıntılarda buna ek olarak sabit ya da değişken terimler de bulunabilir [(Tan, 2015)].

Tanım 1.1:

$m \in \mathbb{Z}^+$ ve $a_1, a_2, \dots a_m \in \mathbb{R}$ olmak üzere $\forall n \geq m$ için,

$$u_n = a_1 u_{n-1} + a_2 u_{n-2} + \cdots + a_m u_{n-m} \qquad (1.1)$$

Sabit katsayılara sahip bir lineer homojen rekürans bağıntısı, her terimin kendinden önceki belirli sayıda terimlerin lineer kombinasyonu ile ifade edildiği bir bağıntı türüdür [(Tan, 2015), (Everest, Poorten, Shparliaski, & Ward, 2003)].

Burada, u_n terimi önceki m-adet terime bağlı olarak tanımlandığından, bu rekürans bağıntısının derecesi "m" olarak adlandırılır [(Tan, 2015)]. Bir sayı dizisinin tam olarak belirlenebilmesi için, (1.1) numaralı eşlikte verilen rekürans bağıntısının yanı sıra başlangıç koşullarının da tanımlanması gerekmektedir. Yani, dizinin belirli bir düzene göre oluşturulabilmesi için $u_0, u_1, \dots u_{m-1}$ başlangıç değerlerinin (toplam m- adet) bilinmesi gerekir [(Tan, 2015)].

Tanım 1.2:

$m \in \mathbb{Z}^+$ ve$a_1, a_2, \dots a_m \in \mathbb{R}$, $a_m \neq 0$ olmak üzere $\forall n \geq m$ için $u_0, u_1, \dots u_{m-1}$ başlangıç değerlerine sahip ve (1.1) eşliği $u_n = a_1 u_{2-1} + a_2 u_{n-2} + \cdots + a_m u_{n-m}$ ile verilen homojen lineer rekürans bagıntısını gerçekleyen diziye lineer rekürans dizisi denir [(Tan, 2015), (Everest, Poorten, Shparliaski, & Ward, 2003)].

Rekürans bağıntıları, bir dizinin tanımlanmasında kritik bir rol oynarsa da özellikle büyük indeksli terimlere doğrudan ulaşmak her zaman kolay olmayabilir. Örneğin, bir tavşan popülasyonunun büyümesini ifade eden bir rekürans dizisini ele alalım. Eğer belirli bir ayda toplam tavşan sayısını hesaplamak istiyorsak, tüm önceki aylardaki popülasyon değerlerini bilmemiz gerekir. Ancak, 200. ayda kaç tavşan olacağını bulmak için ilk 200 terimini tek tek hesaplamak oldukça zahmetli olacaktır. Bu nedenle, dizinin doğrudan hesaplanmasını sağlayacak kapalı bir formül elde etmek önemlidir. Bu tür bir eşitlik, rekürans bağıntılarının temel yapısı kullanılarak aşağıdaki gibi oluşturulabilir [(Tan, 2015)]. (1.1) numaralı eşlikte u_n yerine x^n yazıldığında, şu eşitlik elde edilir.

$$x^n = a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_m x^{n-m}$$

Daha sonra elde edilen son eşitlik x^{n-m} ile bölünerek sadeleştirilir ve ifade yeniden düzenlenirse, aşağıdaki form elde edilir. Bu işlem, rekürans bağıntısının karakteristik denklemini elde etmek ve dizinin genel terimini belirlemek için önemli bir adımdır.

$$x^m - a_1 x^{m-1} - a_2 x^{m-2} - \cdots - a_m = 0$$

Bu son elde edilen eşitliğe, dizinin rekürans bağıntısının karakteristik denklemi denir. Karakteristik denklem, dizinin genel terimini belirlemek için kullanılan önemli bir araçtır. Burada,

$$g(x) = x^m - a_1 x^{m-1} - a_2 x^{m-2} - \cdots - a_m \qquad (1.2)$$

Bu ifadeye dizinin rekürans bağıntısının karakteristik polinomu denir. Karakteristik polinomun kökleri, dizinin genel çözümünü belirlemekte önemli bir rol oynar. Eğer x_1 karakteristik polinomun bir kökü ise, x_1^m değeri de (1.1) numaralı eliği sağlar [(Tan, 2015)]. Bu kökler kullanılarak, dizinin genel terimi kapalı bir formda ifade edilebilir ve büyük indeksli terimlere doğrudan ulaşmak mümkün hale gelir.

Teorem 1.1:

Karakteristik polinomun farklı kökleri $x_1, x_2, \ldots, x_m$ ve $A_1, A_2, \ldots, A_m$ katsayıları sabit olmak üzere, karakteristik denklemin genel çözümü

$$u_n = A_1 x_1^n + A_2 x_2^n + \cdots + A_m x_m^n$$

Bu ifade, Binet (veya Binet-benzeri) formülü olarak adlandırılan bir kapalı formül verir [(Tan, 2015), (Everest, Poorten, Shparliaski, & Ward, 2003)]. Bu formül, özellikle Fibonacci ve Perrin gibi bazı özel rekürans dizilerinin genel terimlerini doğrudan hesaplamak için kullanılır.

Buna ek olarak, üreteç fonksiyonu, homojen lineer rekürans bağıntılarının çözümünde etkili yöntemlerden biridir [(Tan, 2015)]. Üreteç fonksiyonları, bir dizinin terimlerini tek bir cebirsel ifade içinde toplu olarak ifade etmeye yardımcı olur ve birçok kombinatoryal ve cebirsel problemde güçlü bir araç olarak kullanılır.

Üreteç fonksiyonunun, karakteristik polinomun katsayılarının sırasının ters çevrilmesiyle oluşturulan bir fonksiyon olduğu görülmektedir. Yani, eğer karakteristik polinom (1.2) eşliği karakteristik polinom şeklinde olursa:

$$f(x) = 1 - a_1 x - a_2 x^2 - \cdots - a_m x^m$$

olarak ifade edilir [(Tan, 2015)]. Üreteç fonksiyonunun genel formu, aşağıdaki teorem ile tanımlanabilir:

Kalman [(Kalman, 1982)], bir dizinin $(n+k)$. teriminin, kendisinden önce gelen k terimin lineer bir birleşimi olarak yazılabileceği fikrinden hareketle, rekürans dizileri için matris temelli eşitlikler geliştirmiştir [(DEVECİ, Akuzum, & Karaduman, 2015)]. Bu yaklaşım doğrultusunda, katsayılar $c_0, c_1, \dots, c_{k-1} \in \mathbb{R}$ olmak üzere,

$$a_{n+k} = c_0 a_n + c_1 a_{n+1} + \cdots + c_{k-1} a_{n+k-1}$$

şeklindedir. [(Kalman, 1982)] çalışmasında eş matris,

$$A_k = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ c_0 & c_1 & c_2 & \cdots & c_{k-2} & c_{k-1} \end{bmatrix}$$

gösterimi yukarıdaki şekilde olup

$$A_k^n \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{k-1} \end{pmatrix} = \begin{pmatrix} a_0 \\ a_{n-1} \\ \vdots \\ a_{n+k-1} \end{pmatrix}$$

eşliği verilmiştir.

Tanım 1.3:

Horadam sayıları, başlangıç koşulları $w_0, w_1 \in \mathbb{R}$ olmak üzere,

$$w_n = r w_{n-1} + s w_{n-2} \qquad (1.3)$$

şeklinde ikinci dereceden lineer bir rekürans bağıntısına sahiptir, burada $n \geq 2, r, s \in \mathbb{R}$ [(Horadam, 1965), (Horadam, 1965), (Soykan Y. , 2020)].

Bu sayı dizisi negatif indeksler için şu rekürans bağıntısıyla ifade edilebilir [(Soykan Y. , 2020)]:

$$w_{-n} = \frac{1}{s} w_{-(n-2)} - \frac{r}{s} w_{-(n-1)}, s \neq 0$$

Buradan, (1.3) rekürans bağıntısı $\forall$ n $\in \mathbb{Z}$ için geçerlidir [(Soykan Y. , 2020)].

Örnek olarak, bu aileye ait bazı sayılar aşağıdaki gibi incelenebilir. Burada, $n = 2$ olduğu açıkça görülmektedir:

- Fibonacci Sayı Dizisi; f_n: n. Fibonacci sayısı ve $f_0 = 0$, $f_1 = 1$, rekürans bağıntısı:

$$f_n = f_{n-1} + f_{n-2}, n \geq 2$$

burada, $a_1 = 1, a_2 = 1$ 'dir.

- Pell Sayı Dizisi; p_n: n. Pell sayısı ve $p_0 = 0$, $p_1 = 1$, rekürans bağıntısı:

$$p_n = 2p_{n-1} + p_{n-2}, n \geq 2$$

burada, $a_1 = 2, a_2 = 1$ 'dir.

- Jacobsthal Sayı Dizisi; j_n: n. Jacobsthal sayısı ve $j_0 = 0$, $j_1 = 1$, rekürans bağıntısı:

$$j_n = j_{n-1} + 2j_{n-2}, n \geq 2$$

burada, $a_1 = 1, a_2 = 2$ 'dir.

İkinci dereceden rekürans bağıntısına sahip Horadam sayılarının r, s ve başlangıç değerlerine bağlı olarak ortaya çıkan özel durumlar, Tablo 1.1'de gösterilmektedir. Bu sayılar arasındaki fark, özellikle başlangıç değerleri ve r, s katsayılarının farklı olmasından kaynaklanmaktadır.

Tablo 1.1. Bazı İkinci Dereceden Özel Sayı Dizileri

İsim	$\{w_n\} = \{w_n(w_0, w_1; r, s)\}$	Rekürans Bağıntısı
Fibonacci	$\{f_n\} = \{w_n(1,1;1,1)\}$	$f_n = f_{n-1} + f_{n-2}$
Lucas	$\{l_n\} = \{w_n(2,1;1,1)\}$	$l_n = l_{n-2} + l_{n-3}$
Pell	$\{p_n\} = \{w_n(0,1;2,1)\}$	$p_n = 2p_{n-1} + p_{n-2}$
Pell-Lucas	$\{pl_n\} = \{w_n(2,2;1,2)\}$	$pl_n = 2pl_{n-1} + pl_{n-2}$
Jacobsthal	$\{j_n\} = \{w_n(0,1;1,2)\}$	$j_n = j_{n-1} + 2j_{n-2}$
Jacobsthal-Lucas	$\{jl_n\} = \{w_n(2,1;1,2)\}$	$jl_n = jl_{n-1} + 2jl_{n-2}$

Horadam sayılarını karakteristik denklemi

$$x^2 - rx - s = 0$$

olmak üzere, bu denklemin kökleri

$$a_1 = \frac{r + \sqrt{\Delta}}{2}, a_2 = \frac{r - \sqrt{\Delta}}{2}, \Delta = r^2 + 4s$$

olarak verilmiştir. [(Soykan Y. , 2020)]. Horadam sayılarının Binet formülü

$$w_n = A_1\alpha_1^n + A_2\alpha_2^n \qquad (1.4)$$

olmak üzere, burada

$$A_1 = \frac{w_1 - \alpha_2 w_0}{\alpha_1 - \alpha_2}, A_2 = \frac{w_1 - \alpha_1 w_0}{\alpha_2 - \alpha_1}$$

Bu eşlikler geçerlidir [(Soykan Y. , 2020)]. Ayrıca, negatif indisli Horadam sayıları için Binet formülü de verilebilir [(Soykan Y. , 2020)]. (1.4) numaralı eşlikteki Binet formülü, ∀ n ∈ ℤ için geçerlidir; bu sonuca, Howard ve Saidak [(Howard & Saidak, 2010)] çalışmalarında ulaşılmıştır [(Soykan Y. , 2020)].

Bunlara ek olarak, Horadam sayıları için üreteç fonksiyonu da tanımlanabilir [(Soykan Y. , 2020)].

$$\sum_{n=0}^{\infty} w_n x^n = \frac{w_0 + (w_1 - r w_0)}{1 - rx - sx^2}$$

Horadam sayıları için aşağıdaki matris formülü, Kalman'ın [(Kalman, 1982)] çalışmasındaki benzer şekilde ifade edilebilir:

$$\begin{pmatrix} w_n \\ w_{n+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ r & s \end{pmatrix}^n \begin{pmatrix} w_0 \\ w_1 \end{pmatrix}$$

ve 2 × 2 tipindeki

$$\begin{pmatrix} r & s \\ 1 & 0 \end{pmatrix}$$

matrisi ile verilmiştir [(Soykan Y. , 2020)].

Tanım 2.3:

Genelleştirilmiş Tribonacci sayıları, $V_0 = a, V_1 = b, V_2 = c \in \mathbb{Z}$ ve $r, s, t \in \mathbb{R}$ olmak üzere,

$$V_n = rV_{n-1} + sV_{n-2} + tV_{n-3}, n \geq 3 \quad (1.5)$$

şeklinde üçüncü dereceden lineer bir rekürans bağıntısına sahiptir [(Sloane N. J.), (Shannon & Horadam, 1972), (Adegoke, 2019), (C.C.Yalavigi, 1972), (Cereceda, 2015), (Adegoke, 2019)].

Benzer şekilde, negatif indisli genelleştirilmiş Tribonacci sayıları için rekürans bağıntısı ise:

$$V_{-n} = \frac{1}{t} V_{-(n-3)} - \frac{s}{t} V_{-(n-1)} - \frac{r}{t} V_{-(n-2)}, \forall\, n \in \mathbb{Z}^+, t \neq 0$$

şeklindedir [(Soykan Y. , 2020)]. Böylece, bu rekürans bağıntısı $\forall n \in \mathbb{Z}$ için geçerlidir [(Waddill M. E., 1991), (SOYKAN, 2020)].

Örnek olarak, bu aileye ait bazı sayılar aşağıdaki gibi incelenebilir. Burada $n = 3$ olduğu açıkça görülmektedir.

- Tribonacci Sayı Dizisi; A_n: n. Fibonacci sayısı ve $A_0 = 1, A_1 = 1, A_2 = 1$ rekürans bağıntısı:

$$A_n = A_{n-1} + A_{n-2} + A_{n-2}, n \geq 3$$

burada, $a_1 = 1, a_2 = 1, a_3 = 1$ 'dir.

- Padovan Sayı Dizisi; P_n: n. Padovan sayısı ve $P_0 = P_1 = P_2 = 1$ rekürans bağıntısı:

$$P_n = P_{n-2} + P_{n-3}, n \geq 3$$

olmak üzere, $a_1 = 0, a_2 = 1, a_3 = 1$ 'dir.

- Perrin Sayı Dizisi; R_n: n. Perrin sayısı ve $R_0 = 3, R_1 = 0, R_2 = 2$

$$R_n = R_{n-2} + R_{n-3}, n \geq 3$$

olmak üzere, $a_1 = 0, a_2 = 1, a_3 = 1$ 'dir.

Üçüncü dereceden rekürans bağıntısına sahip Horadam sayılarının r, s, t ve başlangıç değerlerine bağlı olarak ortaya çıkan özel durumlar, Tablo 1.2'de gösterilmektedir. Örnek olarak, tez çalışmasının konusu olan Perrin sayıları, Tablo 1.2'nin ikinci satırında yer alan genelleştirilmiş Padovan alt ailesine aittir. Bu gruplandırma ve özel durumlar hakkında daha detaylı bilgiler, [(Adegoke, 2019), (Cerda-Morales, 2017), (C.C.Yalavigi, 1972)] çalışmalarıyla elde edilebilir.

Tablo 1.2. Bazı Genelleştirilmiş Tribonacci Sayılarının Özel Durumları

İsim	$\{V_n\} = \{V_n(V_0, V_1, V_2; r, s, t)\}$	Rekürans Bağıntısı
Tribonacci	$\{A_n\} = \{V_n(0,1,1; 1,1,1)\}$	$A_n = A_{n-1} + A_{n-2} + A_{n-2}$
Tribonacci-Perrin	$\{C_n\} = \{V_n(3,0,2; 1,1,1)\}$	$C_n = C_{n-1} + C_{n-2} + C_{n-2}$
Padovan	$\{P_n\} = \{V_n(1,1,1; 0,1,1)\}$	$P_n = P_{n-2} + P_{n-3}$
Perrin	$\{R_n\} = \{V_n(3,0,2; 0,1,1)\}$	$R_n = R_{n-2} + R_{n-3}$
Padovan-Perrin	$\{J_n\} = \{V_n(0,0,1; 0,1,1)\}$	$J_n = J_{n-2} + J_{n-3}$
Pell-Perrin	$\{N_n\} = \{V_n(3,0,2; 0,2,1)\}$	$N_n = 2N_{n-2} + N_{n-3}$

Bu bilgilere ek olarak, genelleştirilmiş Tribonacci sayılarının karakteristik denklemi

$$x^3 - rx^2 - sx - t = 0 \qquad (1.6)$$

¸şeklinde olup, bu denklemin kökleri aşağıda verilmi¸stir (Cerda-Morales, 2017):

$$x_1 = \frac{r}{3} + \breve{\alpha} + \breve{\beta}, x_2 = \frac{r}{3} + \varepsilon\breve{\alpha} + \varepsilon^2\breve{\beta}, x_3 = \frac{r}{3} + \varepsilon^2\breve{\alpha} + \varepsilon\breve{\beta}$$

Burada,

$$\begin{cases} \breve{\alpha} = \sqrt{\frac{r^3}{27} + \frac{rs}{6} + \frac{t}{2} + \sqrt{\mu}}, \\ \breve{\beta} = \sqrt{\frac{r^3}{27} + \frac{rs}{6} + \frac{t}{2} - \sqrt{\mu}}, \\ \varepsilon = \frac{-1 + i\sqrt{3}}{2}, \\ \mu = \frac{r^3 t}{27} - \frac{r^2 s^2}{108} + \frac{rst}{6} - \frac{s^3}{27} + \frac{t^2}{4}, \end{cases}$$

ve

$$x_1 + x_2 + x_3 = r, x_1x_2 + x_1x_3 + x_2x_3 = -s, \qquad x_1x_2x_3 = t,$$

şeklindedir. μ>0 olmak şartıyla, (1.5) eşliğinde verilen rekürans bağıntısının karakteristik denkleminin bir reel ve iki reel olmayan çözümü vardır (Cerda-Morales, 2017). Genelleştirilmiş Tribonacci sayıları için Binet (Binet-benzeri) formülü:

$$V_n = \frac{\breve{P}\, x_1^n}{(x_1 - x_2))(x_1 - x_3)} + \frac{\breve{R}\, x_2^n}{(x_2 - x_1)(x_2 - x_3)} + \frac{\breve{S}\, x_3^n}{(x_3 - x_1)(x_3 - x_2)} \quad (1.7)$$

şeklinde olup, buradan

$$\begin{cases} \breve{P} = V_2 - (x_2 + x_3)V_1 + x_2x_3V_0 \\ \breve{R} = V_2 - (x_1 + x_3)V_1 + x_1x_3V_0 \\ \breve{S} = V_2 - (x_1 + x_2)V_1 + x_1x_2V_0 \end{cases}$$

dir (Cerda-Morales, 2017). Negatif indisli genelleştirilmiş Tribonacci sayıları için Binet formülü de verilmiştir (Soykan Y. , 2020). (1.7) eşliği $\forall\, n \in \mathbb{Z}$ için sağlanmaktadır. Bunlara ek olarak, genelleştirilmiş Tribonacci sayıları için üreteç fonksiyonu;

$$\sum_{n=0}^{\infty} V_n\, x^n = \frac{V_0 + (V_1 - rV_0)x + (V_2 - rV_1 - sV_0)x^2}{1 - rx - sx^2 - t^3}$$

olarak verilmektedir (Soykan Y. , 2020).

Ayrıca, genelleştirilmiş Tribonacci sayılarının matris formları da incelenmiş olup, bu konu üzerine çeşitli çalışmalar gerçekleştirilmiştir. Bu çalışmalar, Tribonacci dizilerinin matris

temsilleri aracılığıyla daha sistematik bir şekilde ele alınmasını sağlamış ve bu sayede dizinin genel teriminin hesaplanmasında ve özelliklerinin analiz edilmesinde önemli bir yöntem sunmuştur [(Waddill M. , 1993), (Shannon & Horadam, 1972), (Waddill M. E., 1991), (Waddill M. E., 1967), (Soykan Y. , 2020)].

V_n dizisini üretmenin alternatif bir yolu olan S-matrisi, Shannon ve Horadam tarafından incelenmiş olup [(Shannon & Horadam, 1972)], bu matrisin daha genel bir versiyonu olan R-matrisi ise Waddill ve Sacks tarafından çalışılmıştır [(Waddill M. E., 1991), (Waddill M. E., 1967)]. S- matrisi;

$$S = \begin{pmatrix} r & s & t \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

şeklinde gösterilir. Aşağıdaki matris formülü verilebilir [(Waddill M. E., 1991), (Waddill M. E., 1967)]:

$$\begin{pmatrix} r & s & t \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}^{n-2} \begin{pmatrix} V_2 \\ V_1 \\ V_0 \end{pmatrix} = \begin{pmatrix} V_n \\ V_{n-1} \\ V_{n-2} \end{pmatrix}$$

Bu konuda daha detaylı bilgi için [(Shannon & Horadam, 1972), (Waddill M. E., 1991), (Cerda-Morales G. , 2018), (Waddill M. E., 1967)] çalışmalarına göz atılabilir.

Üçüncü mertebeden özel bir sayı dizisi olan Perrin sayıları (OEIS: A001608, A078712 [(Sloane N. J., tarih yok)]), ilk olarak 1876 yılında Fransız matematikçi Édouard Lucas (1842-1891) tarafından incelenmiştir [(Yılmaz N. , 2015), (Lucas, 1878)]. Ancak, bu özel sayı dizisi üzerine François Olivier Raoul Perrin (1841-1910) de 1899 yılında çalışmalar yapmış olup, dizi onun adıyla anılmaktadır [(Perrin, 1899)]. Perrin sayıları, sayılar teorisi ve kombinatorik alanlarında çeşitli uygulamalara sahip olup, özellikle asal sayılarla ilişkisi açısından dikkat çekmektedir. Bu sayı dizisi üzerine yapılan detaylı çalışmalar, literatürde geniş bir yer kaplamakta olup, daha fazla bilgi için [(Sloane N. J., tarih yok), (Adegoke, 2019), (Yılmaz & Taşkara, 2013), (Sokhuma, 2013), (M. Mangueira, Alves, & Catarino, 2020), (Shtayat & Al-Kateeb, 2021), (Adegoke, 2019), (Yılmaz & D. Bozkurt, 2011) (Irmak, 2019), (Kaygısız & D. Bozkurt, 2012)] kaynakları incelenebilir.

Tanım 1.4:

$n \geq 3$ için, Perrin sayıları dizisi,

$$R_n = R_{n-2} + R_{n-3} \qquad (1.8)$$

$\{R_n\}_{n\geq 0}$ rekürans bağıntısıyla tanımlanır. Başlangıç koşulları $R_0 = 3, R_1 = 0, R_2 = 2$ olmak üzere, R_n, n. Perrin sayısını temsil etmektedir [(Yılmaz & Taşkara, 2013), (Yılmaz N. , 2015), (Shannon, Anderson, & Horadam, 2006)].

Negatif indisli Perrin sayıları, aşağıdaki tekrarlama ilişkisi,

$$R_{-n} = R_{-n+2} + R_{-n+3}$$

şeklinde tanımlanıp, R_{-n} negatif indisli Perrin sayısını temsil etmektedir [(Soykan Y. , 2020), (Yılmaz N. , 2015), (Sloane N. J., tarih yok)]. Perrin sayılarının kümesi $\mathscr{R}$ ile temsil edilecektir.

Tablo 1.3'de bazı pozitif ve negatif n değerleri için Perrin sayıları örnek olarak verilmiştir.

Tablo 1.3. Bazı Pozitif ve Negatif n Değerleri İçin Perrin Sayıları

R_n	…	-1	-2	4	-3	2	1	-1	3	0	2	3	2	5	5	7	…

$\forall n \in \mathbb{N}$ için,

$$\alpha = \sqrt[3]{\frac{1}{2}+\frac{1}{6}\sqrt{\frac{23}{3}}} + \sqrt[3]{\frac{1}{2}-\frac{1}{6}\sqrt{\frac{23}{3}}},$$

$$\beta = -\sqrt[3]{\frac{1}{16}+\frac{1}{48}\sqrt{\frac{23}{3}}} - \sqrt[3]{\frac{1}{16}-\frac{1}{48}\sqrt{\frac{23}{3}}} + i\frac{\sqrt{3}}{2}\left(\sqrt[3]{\frac{1}{2}+\frac{1}{6}\sqrt{\frac{23}{3}}} + \sqrt[3]{\frac{1}{2}-\frac{1}{6}\sqrt{\frac{23}{3}}}\right),$$

$$\gamma = -\sqrt[3]{\frac{1}{16}+\frac{1}{48}\sqrt{\frac{23}{3}}} - \sqrt[3]{\frac{1}{16}-\frac{1}{48}\sqrt{\frac{23}{3}}} - i\frac{\sqrt{3}}{2}\left(\sqrt[3]{\frac{1}{2}+\frac{1}{6}\sqrt{\frac{23}{3}}} + \sqrt[3]{\frac{1}{2}-\frac{1}{6}\sqrt{\frac{23}{3}}}\right) \text{(Sloane N. J.).}$$

Perrin sayılarının karakteristik denklemi,

$$x^3 - x - 1 = 0$$

bu eşitlikle gösterilir [(Laisant & Lemoine, 1894) , (Yılmaz N. , 2015)]. Kökleri $\alpha, \beta, \gamma = \bar{\beta}$ şeklindedir, burada

$$\alpha = \frac{\omega_1 + \omega_2}{6}, \beta = \frac{-\omega_1 - \omega_2 + i\sqrt{3}(\omega_1 - \omega_2)}{12},$$

Ve

$$\omega_1 = \sqrt[3]{108 + 12\sqrt{69}},\ \omega_2 = \sqrt[3]{108 - 12\sqrt{69}}$$

şu notasyonları kullanalım:

$$c_\alpha = \frac{(1-\beta)(1-\gamma)}{(\alpha-\beta)(\alpha-\gamma)} = \frac{1+\alpha}{-\alpha^2+3\alpha+1},$$
$$c_\gamma = \frac{(1-\alpha)(1-\beta)}{(\gamma-\alpha)(\gamma-\beta)} = \frac{1+\gamma}{-\gamma^2+3\gamma+1} = \overline{c_\beta}.$$

Bu özel sayı dizisi için parametreler $\alpha = 0, \beta = 1, \gamma = 1$ olarak belirlenmiştir. Bu durum, genelleştirilmiş Tribonacci sayı dizisinin karakteristik denklemi olan (1.6) eşitliğinde $\alpha = 0, \beta = 1, \gamma = 1$ değerleri yerine konulduğunda açıkça doğrulanmaktadır.

Perrin sayıları için Binet-benzeri formülü;

$R_n = \alpha^n + \beta^n + \gamma^n$, tüm $n \geq 0$ için. (1.9)

olarak verilir (Yılmaz N. , 2015). $\forall\, n \in \mathbb{N}$ için negatif indisli Perrin sayılarının Binet-benzeri formülü;

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

şeklindedir (Taskara & Yilmaz, 2014). (1.9) eşliğindeki Perrin sayıları için Binet-benzeri formülü, $\forall\, n \in \mathbb{Z}$ için geçerlidir (Soykan Y. , 2020). Perrin sayılarının üreteç fonksiyonu,

$$\sum_{n=1}^{\infty} R_n y^{n-1} = \frac{3-y^2}{1-y^2-y^3}$$

şeklinde ifade edilir (Shannon, Anderson, & Horadam, Properties of Cordonnier,Perrin and Van der Laan numbers, 2006). [(Yılmaz & Taşkara, 2013), (Yılmaz N. , 2015)] çalışmalarında Perrin matris dizileri incelenmiş ve bu matris dizileri aracılığıyla Perrin sayıları için alternatif bir ifade elde edilmiştir. Bu yaklaşım, Perrin sayılarını farklı bir biçimde ifade eden aşağıdaki üreteç fonksiyonunun türetilmesine olanak sağlamıştır:

$$\sum_{n=1}^{\infty} R_{n-1} x^n = \frac{-1+3x+x^2}{1-x^2-x^3}$$

Bu üreteç fonksiyonu, Perrin sayılarının karakteristik denklemi ile tutarlıdır ve seriye ait terimlerin sistematik olarak üretilmesini sağlar. [(Taskara & Yilmaz, 2014), (Yılmaz N. , 2015)] çalışmalarında negatif indisli Perrin matris dizileri incelenmiş ve bu dizilerden hareketle negatif indisli Perrin sayıları için aşağıdaki üreteç fonksiyonu elde edilmiştir.

$$\sum_{n=1}^{\infty} R_{-n-1}x^n = \frac{-1+3x^2}{1+x-x^3}$$

Bu üreteç fonksiyonu, negatif indisli Perrin sayılarını sistematik olarak üretmek için kullanılır ve pozitif indisli Perrin sayılarının üreteç fonksiyonu ile benzer bir yapıya sahiptir. Negatif indisli terimlerin belirli bir örüntüye göre türediği bu fonksiyon, dizinin genişletilmesinde önemli bir araç olarak değerlendirilmiştir.

Padovan ve Perrin sayıları arasındaki ilişki göz önüne alındığında (farklı başlangıç koşulları ancak aynı rekürans bağıntısı), Cerda-Morales'in [(Cerda-Morales G. , 2019)] çalışmasında sunulan Tablo 2.9, Perrin sayıları için de uygulanabilir.

Yani, $\forall\, n \in \mathbb{N}$ olmak üzere, Perrin sayıları için şu eşitlik sağlanmaktadır:

$$R_n = \rho_a R_{n-a} + \sigma_a R_{n-2a} + R_{n-3a} \qquad (1.10)$$

Burada $(\rho_a, \sigma_a), \rho_a, \sigma_a \in \mathbb{Z}, 0 \leq a \leq 8, a \in \mathbb{N}$ 'dir.

Tablo 1.4. Perrin Sayıları İçin Rekürans Bağıntıları

α		(ρ_a, σ_a)	$R_n = \rho_a R_{n-a} + \sigma_a R_{n-2a} + R_{n-3a}$
1		(0,1)	$R_n = R_{n-2} + R_{n-3}$
2		$(2,-1)$	$R_n = 2R_{n-2} - R_{n-4} + R_{n-6}$
3		$(3,-2)$	$R_n = 3R_{n-2} - 2R_{n-6} + R_{n-9}$
4		(2,3)	$R_n = 2R_{n-4} + 3R_{n-8} + R_{n-12}$
5		$(5,-4)$	$R_n = 5R_{n-5} - 4R_{n-10} + R_{n-15}$
6		(5,2)	$R_n = 5R_{n-6} + 2R_{n-12} + R_{n-18}$
7		(7,1)	$R_n = 7R_{n-7} + R_{n-14} + R_{n-21}$

Kaynak: Cerda-Morales G. , 2019

(1.10) eşitliği R_{-n} olmak üzere $\forall\, n \geq 1$ için de geçerlidir (Cerda-Morales G. , 2019). Perrin matris dizisinin *n*. genel matris gösterimi,

$$\mathcal{R}_n = \begin{pmatrix} R_{n-5} & R_{n-3} & R_{n-4} \\ R_{n-4} & R_{n-2} & R_{n-3} \\ R_{n-3} & R_{n-1} & R_{n-2} \end{pmatrix}, \forall\, n \in \mathbb{N},$$

şeklindedir [(Yılmaz N. , 2015), (Yılmaz & Taşkara, 2013)].

$\forall n \geq 1$ için Perrin sayıları için matris formüllerini aşağıdaki gibidir [(M. Mangueira, Alves, & Catarino, 2020)]:

$$(R_0 \quad R_2 \quad R_1)\begin{pmatrix}0 & 1 & 0\\ 0 & 0 & 1\\ 1 & 1 & 0\end{pmatrix}^n = (R_n \quad R_{n+2} \quad R_{n+1}), \tag{1.11}$$

$$(R_2 \quad R_0 \quad R_1)\begin{pmatrix}0 & 0 & 1\\ 1 & 0 & 0\\ 1 & 1 & 0\end{pmatrix}^n = (R_{n+2} \quad R_n \quad R_{n+1}), \tag{1.12}$$

$$(R_0 \quad R_1 \quad R_2)\begin{pmatrix}0 & 0 & 1\\ 1 & 0 & 1\\ 0 & 1 & 0\end{pmatrix}^n = (R_n \quad R_{n+1} \quad R_{n+2}) \tag{1.13}$$

$$(R_1 \quad R_2 \quad R_0)\begin{pmatrix}0 & 1 & 1\\ 1 & 0 & 0\\ 0 & 1 & 0\end{pmatrix}^n = (R_{n+1} \quad R_{n+2} \quad R_n), \tag{1.14}$$

$$(R_2 \quad R_1 \quad R_0)\begin{pmatrix}0 & 1 & 0\\ 1 & 0 & 1\\ 1 & 0 & 0\end{pmatrix}^n = (R_{n+2} \quad R_{n+1} \quad R_n), \tag{1.15}$$

$$(R_1 \quad R_0 \quad R_2)\begin{pmatrix}0 & 1 & 1\\ 0 & 0 & 1\\ 1 & 0 & 0\end{pmatrix}^n = (R_{n+1} \quad R_n \quad R_{n+2}), \tag{1.16}$$

Yukarıda (1.11)- (1.16) eşitliklerinde ([(M. Mangueira, Alves, & Catarino, 2020)]) n. kuvveti görülen matrisler, sırasıyla [(Sokhuma., 2013)] ve [(Seenukul, Netmanee, Panyakhun, Ausiseekaen, & Muangchan, 2015)] çalışmalarında kullanılan $Q_0, Q_1, Q_2, Q_{3,}, Q_4, Q_5$ matrisleri ile aynıdır. Bu altı eşitlikten de açıkça görülebilir ki, n = 1 alındığında R_0, R_1, R_2 değerlerinin bulunduğu 1 × 3 boyutundaki matrislerdeki sıralama her değiştiğinde, ilgili matris de değişmektedir. Sonuç olarak, altı farklı eşitlik ve altı farklı matris elde edilmektedir (3! = 6).

$\forall n > 0$ olmak üzere negatif indisli Perrin sayıları için matris formülleri aşağıdaki gibidir [(M. Mangueira, Alves, & Catarino, 2020)]:

$$(R_0 \quad R_2 \quad R_1)\begin{pmatrix}-1 & 0 & 1\\ 1 & 0 & 0\\ 0 & 1 & 0\end{pmatrix}^n = (R_{-n} \quad R_{-n+2} \quad R_{-n+1}), \tag{1.17}$$

$$(R_2 \quad R_0 \quad R_1)\begin{pmatrix}0 & 1 & 0\\ 0 & -1 & 0\\ 1 & 0 & 0\end{pmatrix}^n = (R_{-n+2} \quad R_{-n} \quad R_{-n+1}), \tag{1.18}$$

$$(R_0 \quad R_1 \quad R_2)\begin{pmatrix}-1 & 1 & 0\\ 0 & 0 & 1\\ 1 & 0 & 0\end{pmatrix}^n = (R_{-n} \quad R_{-n+1} \quad R_{-n+2}) \tag{1.19}$$

$$(R_1 \quad R_2 \quad R_0)\begin{pmatrix}0 & 1 & 0\\ 0 & 0 & 1\\ 1 & 0 & -1\end{pmatrix}^n = (R_{-n+1} \quad R_{-n+2} \quad R_{-n}), \text{ (1.20)}$$

$$(R_2 \quad R_1 \quad R_0)\begin{pmatrix}0 & 0 & 1\\ 1 & 0 & 0\\ 0 & 1 & -1\end{pmatrix}^n = (R_{-n+2} \quad R_{-n+1} \quad R_{-n}), \text{ (1.21)}$$

$$(R_1 \quad R_0 \quad R_2)\begin{pmatrix}0 & 0 & 1\\ 1 & -1 & 0\\ 0 & 1 & 0\end{pmatrix}^n = (R_{-n+1} \quad R_{-n} \quad R_{-n+2}), \text{ (1.22)}$$

Benzer şekilde yukarıdaki (1.17) -(1.22) eşitliklerinde ([(M. Mangueira, Alves, & Catarino, 2020)]) n. kuvveti görülen matrisler, sırasıyla, $Q_0, Q_1, Q_2, Q_3, Q_4, Q_5$ matrislerinin tersleridir.

Padovan ve Perrin sayıları arasındaki ilişki ise,

$$R_n = 3P_{n-5} + 2P_{n-4}$$

'dır (Sloane N. J., tarih yok).

Kuaterniyonlar, kompleks sayıların daha yüksek boyutlara genelleştirilmesi fikriyle ortaya çıkmış, dört boyutlu bir sayı sistemidir. İlk olarak 1843 yılında İrlandalı matematikçi William Rowan Hamilton tarafından keşfedilen kuaterniyonlar, skaler ve vektör bileşenlerden oluşur ve üç boyutlu uzayda dönüşümleri temsil etmek için güçlü bir matematiksel araç sağlar [(Hamilton, 1844)]. Kuaterniyonların geniş bir kullanım alanı bulunmaktadır. Geometri ve mekanikte dönüşümleri modellemek için kullanılırken, bilgisayar grafiklerinde ve oyun motorlarında nesnelerin döndürülmesini sağlamak amacıyla yaygın olarak tercih edilir. Ayrıca robotik ve animasyon teknolojisinde hareket simülasyonlarında önemli bir rol oynar. Fizik ve mühendislikte kuantum mekaniği, elektromanyetizma ve akışkanlar dinamiği gibi alanlarda da kuaterniyonlar faydalanılır. Kinematik analizlerde ve uzay navigasyon sistemlerinde de kritik bir öneme sahiptir.

Tanım 1.5:

$q_1, q_2, q_3, q_4 \in \mathbb{R}$ olmak üzere, bir q reel kuaterniyonu $q = q_1 + iq_2 + jq_3 + kq_4$ şeklinde ifade edilir. Reel kuaterniyonlar kümesi $\mathbb{H}$ ile temsil edilir ve

$$\mathbb{H} = \{q = q_1 + iq_2 + jq_3 + kq_4 | i^2 = j^2 = k^2 = -1, \text{ijk} = -1, q_1, q_2, q_3, q_4 \in \mathbb{R}\}$$

şeklinde tanımlanır [(Özdemir, 2020), (Hamilton W. R., 1853), (Hamilton W. R., 1969)].

Burada kuaterniyonik i, j, k birimleri Tablo 2.5 'deki özellikleri sağlamaktadır.

Tablo 1.5. Reel Kuaterniyonlar İçin Birimlerin Çarpımı

.	1	*i*	*j*	*k*
1	1	*i*	*j*	*k*
i	*i*	-1	*k*	-*j*
j	*j*	-*k*	-1	*i*
k	*k*	*j*	-*i*	-1

Kaynak: Hamilton, 1844, 1853

Kuaterniyonlar kümesi çarpma işlemine göre birleşmeli ancak değişmeli değildir.

$$q = q_1 + iq_2 + jq_3 + kq_4 \in \mathbb{R}^4$$

olmak üzere burada,

$$1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, i = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, j = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, k = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

olup, q kuaterniyonu,

$$q = \begin{pmatrix} q_1 \\ q_2 \\ q_3 \\ q_4 \end{pmatrix}$$

şeklinde matris gösterimi yapılabilir (Hamilton W. R., 1969).

$q = q_1 + iq_2 + jq_3 + kq_4, p = p_1 + ip_2 + jp_3 + kp_4 \in \mathbb{H}$ olmak üzere, reel kuaterniyonlar için bazı temel tanım ve cebirsel özellikleri aşağıdaki şekildedir (Özdemir, 2020):

- Kuaterniyonun Vektörel Kısmı: q kuaterniyonun vektörel kısmı $\overrightarrow{V_q}$ ile gösterilir ve $\overrightarrow{V_q} = iq_2 + jq_3 + kq_4$ şeklinde tanımlanır.
- Kuaterniyonun Skaler Kısmı: q kuaterniyonunun skaler kısmı S_q ile gösterilir ve $S_q = q_1$ şeklinde ifade edilir. Böylece $\mathrm{q} = S_q + \overrightarrow{V_q}$ yazılabilir.

- Has (Pür) Kuaterniyon: Eğer $S_q = 0$ ise q kuaterniyonunu has kuaterniyon veya pür kuaterniyon olarak adlandırılır. Bu durumdan hareketle, $\mathbb{R}^3$ uzayındaki her vektörün aslında bir has kuaterniyon olarak düşünülebileceği söylenebilir.

Genel olarak, kuaterniyonlar $\mathbb{R}^4$ uzayı ile, kuaterniyonların vektörel (saf) kısmı ise $\mathbb{R}^3$ ile özdeşleştirilir. Bu bağlamda, kuaterniyonların skaler bileşeni uzaya dördüncü bir boyut ekleyerek dönüşüm ve hesaplamalarda daha geniş bir ifade gücü sunar.

- Eşlenik: Bir q reel kuaterniyonunun eşleniği $\bar{q}$ ile temsil edilir ve

$$\bar{q} = q_1 - iq_2 - jq_3 - kq_4$$

olarak tanımlanır.

- Kuaterniyon Normu: $q \in \mathbb{H}$ olmak üzere,

$$\|.\|: \mathbb{H} \to \mathbb{R}^+ \cup 0$$

$$q \to \|q\| = \sqrt{q\bar{q}} = \sqrt{\bar{q}q} = \sqrt{q_1^2 + q_2^2 + q_3^2 + q_4^2}$$

olarak ifade edilir.

- Eşitlik: $q, p \in \mathbb{H}$ olmak üzere,

$$q = p \Leftrightarrow q_1 = p_1, q_2 = p_2, q_3 = p_3, q_4 = p_4 q_4$$

ifadesiyle gösterilir.

- Toplama/Çıkarma: $q, p \in \mathbb{H}$ olmak üzere,

$$q \pm p = (q_1 + iq_2 + jq_3 + kq_4) \pm (p_1 + ip_2 + jp_3 + kp_4)$$

$$= q_1 \pm p_1 + i(q_2 \pm p_2) + j(q_3 \pm p_3) + k(q_4 \pm p_4)$$

Ayrıca,

$$S_{q \pm p} = q_1 \pm p_1 = S_q \pm S_p$$

ve

$$\overrightarrow{V_{q \pm p}} = i(q_2 \pm p_2) + j(q_3 \pm p_3) + k(q_4 \pm p_4) = \overrightarrow{V_q} + \overrightarrow{V_p}$$

ifadeleri sağlanır.

- Skaler ile Çarpma: $q \in \mathbb{H}$ olmak üzere,

$$cq = c(q_1 + iq_2 + jq_3 + kq_4) = cq_1 + icq_2 + jcq_3 + kcq_4, c \in \mathbb{R}$$

şeklinde ifade edilir.

- Çarpma: $q, p \in \mathbb{H}$ olmak üzere,

$$qp = (q_1 + iq_2 + jq_3 + kq_4)(p_1 + ip_2 + jp_3 + kp_4)$$

$$= q_1p_1 - q_2p_2 - q_3p_3 - q_4p_4 + i(q_1p_2 + q_2p_1 + q_3p_4 - q_4p_3)$$
$$+ j(q_1p_3 - q_2p_4 + q_3p_1 + q_4p_2) + k(q_1p_4 + q_2p_3 - q_3p_2 + q_4p_1)$$

şeklindedir. Çarpma işlemi yapılırken Tablo 1.5 'den yararlanılmıştır. Kuaterniyon çarpımı bir diğer şekilde de ifade edilir:

$$qp = \left(S_q + \overrightarrow{V_q}\right)\left(S_p + \overrightarrow{V_p}\right)$$

$$= S_qS_p - \langle \overrightarrow{V_q}, \overrightarrow{V_p} \rangle + S_q\overrightarrow{V_p} + S_p\overrightarrow{V_q} + \overrightarrow{V_q} \times \overrightarrow{V_p}.$$

Burada Öklid iç çarpımı ve Öklid vektörel çarpımı kullanılmıştır. Ayrıca, q, p has kuaterniyonlar olması durumunda,

$$qp = -\langle \overrightarrow{V_q}, \overrightarrow{V_p} \rangle + \overrightarrow{V_q} \times \overrightarrow{V_p}$$

elde edilir.

Split kuaterniyonlar 1849 yılında İngiliz matematikçi James Cockle (1819-1895) tarafından literatüre kazandırılmıştır. Klasik reel kuaterniyonlardan farklı olarak, split kuaterniyonlar $j^2 = k^2 =$ ijk $= 1$ koşulu sağlanarak tanımlanır (Cockle, 1849). Split kuaterniyonlardaki cebirsel özellikler, reel kuaterniyonlardaki ifadelere oldukça benzerdir. Split kuaterniyonlar, standart kuaterniyonlar gibi dört boyutlu bir cebirsel yapı oluşturur; ancak, farklı iç çarpım yapısına sahiptir ve Lorentzian geometri ile bağlantılıdır. Bu özellikleri nedeniyle özel görelilik, hiperbolik geometri ve diferansiyel denklemler gibi alanlarda önemli uygulamalara sahiptir. Özellikle, Lorentz dönüşümlerinin kuaterniyon temelli bir yorumu olarak kullanılması, teorik fizik ve mühendislikte split kuaterniyonların kullanım alanlarını genişletmiştir (Cockle, 1849). Ayrıca, split kuaterniyonlar klasik kuaterniyonlar gibi dönüşüm ve rotasyon işlemlerinde kullanılabilirken, hiperbolik uzayda simetri ve izometri analizlerinde de önemli bir matematiksel araç olarak öne çıkar.

Tanım 1.6:

$q_1, q_2, q_3, q_4 \in \mathbb{R}$ olmak üzere, bir q split kuaterniyonu $q = q_1 + iq_2 + jq_3 + kq_4$ şeklinde ifade edilir. Burada kuaterniyonik i, j, k birimleri Tablo 1.6 'daki özellikleri sağlamaktadır.

Tablo 1.6. Split Kuaterniyonlar İçin Birimlerin Çarpımı

.	1	*i*	*j*	*K*
1	1	*i*	*j*	*K*
i	*i*	-1	*k*	*-j*
j	*j*	*-k*	1	*-I*
k	*k*	*j*	*i*	1

Kaynak: Cockle, 1849

Split kuaterniyonlar kümesi $\mathbb{H}_S$ ile temsil edilir ve,

$$\mathbb{H}_S = \{q = q_1 + iq_2 + jq_3 + kq_4 | i^2 = -1, j^2 = k^2 = \text{ijk} = 1, q_1, q_2, q_3, q_4 \in \mathbb{R}\}$$

şeklinde tanımlanır. Bu kümenin her bir elemanına split kuaterniyon adı verilir [(Özdemir, 2020), (Cockle, 1849)]. Split kuaterniyonlar kümesi çarpma işlemine göre birleşmeli ancak değişmeli değildir.

Genelleştirilmiş Kuaterniyonlar (Generalized Quaternions), klasik kuaterniyonların bir genellemesidir ve daha geniş bir sayı sistemi olarak tanımlanır. Genelleştirilmiş kuaterniyonlar, kuaterniyonlar sisteminin sınırlarını aşarak daha fazla boyutta vektörel ve skaler bileşenler içerebilen yapılar oluştururlar. Bu genelleme, kuaterniyonların dört bileşeni (bir skaler ve üç vektörel bileşen) yerine daha fazla bileşene sahip olan yapıların ele alınmasını sağlar. Klasik kuaterniyonlar $\mathbb{R}^4$ uzayında bir yapı oluştururken, genelleştirilmiş kuaterniyonlar $\mathbb{R}^n$ uzayında daha geniş boyutlu yapılar şeklinde tanımlanabilir. (Cockle, 1849) (Hamilton, 1844)

Tanım 1.7:

$q_1, q_2, q_3, q_4 \in \mathbb{R}$ olmak üzere, bir q genelleştirilmiş kuaterniyonu $q = q_1 + iq_2 + jq_3 + kq_4$ şeklinde ifade edilir. $\alpha, \beta \in \mathbb{R}$ için kuaterniyonik i, j, k birimleri Tablo 1.7 'deki özellikleri sağlamaktadır.

Tablo 1.7. Genelleştirilmiş Kuaterniyonlar İçin Birimlerin Çarpımı

.	1	i	j	K
1	1	i	j	K
i	I	-α	k	-αj
j	J	−k	−β	Bi
k	K	αj	-βi	-αβ

Kaynak: Dickson, 1924; Griffiths, 1928

Genelleştirilmiş kuaterniyonlar kümesi $\mathbb{H}_{\alpha\beta}$ ile temsil edilir ve,

$$\mathbb{H}_{\alpha\beta} = \{q = q_1 + iq_2 + jq_3 + kq_4 | i^2 = -1, j^2 = k^2 = \text{ijk} = 1, q_1, q_2, q_3, q_4 \in \mathbb{R}\}$$

şeklinde tanımlanır. Bu kümenin her bir elemanına genelleştirilmiş kuaterniyon adı verilir [(Özdemir, 2020), (Cockle, 1849), (Dickson, 1924), (Griffiths, 1928)]. Tablo 1.8'de genelleştirilmiş kuaterniyonların özel α ve β değerlerine göre sınıflandırılması verilmektedir.

Tablo 1.8. Genelleştirilmiş Kuaterniyonların Sınıflandırılması

α, β	$\mathbb{H}_{\alpha\beta}$ Kümesi	**α, β**	$\mathbb{H}_{\alpha\beta}$ Kümesi
$\alpha = \beta = 1$	Reel Kuaterniyon	$\alpha = 1, \beta = 0$	Semi-Kuaterniyon
$\alpha = 1, \beta = -1$	Split Kuaterniyon	$\alpha = -1, \beta = 0$	Split Semi-Kuaterniyon

Kaynak: Jafari, 2015; Jafari & Yaylı, 2015

Genelleştirilmiş kuaterniyonlarda cebirsel özellikler gerçek kuaterniyonlarda olduğu gibi ifade edilir. Ancak,

$$pq = S_p S_q - g(\overrightarrow{V_p}, \overrightarrow{V_q}) + S_p \overrightarrow{V_q} + S_q \overrightarrow{V_p} + \overrightarrow{V_p} \times \overrightarrow{V_q},$$

ifadesi incelenirse burada $g(\overrightarrow{V_p}, \overrightarrow{V_q})$ ve $\overrightarrow{V_p} \times \overrightarrow{V_q}$ genelleştirilmiş iç çarpım ve genelleştirilmiş vektör çarpımdır. Bu çarpımları şu şekilde ifade ederiz [(Özdemir, 2020), (JAFARI, 2015)]:

$$u = (u_1, u_2, u_3) = iu_1 + ju_2 + ku_3, v = (v_1, v_2, v_3) = iv_1 + jv_2 + kv_3 \in \mathbb{R}^3, \alpha, \beta \in \mathbb{R}^+$$

olmak üzere, genelleştirilmiş iç çarpım,

$$g(u, v) = \alpha u_1 v_1 + \beta u_2 v_2 + \alpha\beta u_3 v_3$$

olarak tanımlanır. Genelleştirilmiş vektörel çarpım ise,

$$u \times v = \begin{vmatrix} \beta i & \alpha j & k \\ u_1 & u_2 & u_3 \\ v_1 & v_2 & v_3 \end{vmatrix} = i(\beta u_2 v_3 - \beta u_3 v_2) + j(\alpha u_3 v_1 - \alpha u_1 v_3) + k(u_1 v_2 - u_2 v_1)$$

olarak tanımlanır. Bir genelleştirilmiş kuaterniyonun normu ise aşağıdaki şekilde ifade edilir (Jafari & Yaylı, 2015):

$$N_q = |q\bar{q}| = |\bar{q}q| = |q_1^2 + \alpha q_2^2 + \beta q_3^2 + \alpha\beta q_4^2|$$

Tanım 1.8:

$\forall n \in \mathbb{N}$ olmak üzere, n. Perrin genelleştirilmiş kuaterniyon

$$\widetilde{R_n} = R_n + iR_{n-1} + jR_{n-2} + kR_{n-3}$$

şeklinde tanımlanır ve $\widetilde{R_n}$ ile temsil edilir. (Z & N., 2022)

Negatif indisli $(-n.)$ Perrin genelleştirilmiş kuaterniyon, $\forall n \in \mathbb{Z}^+$ olmak üzere,

$$\widetilde{R_{-n}} = R_{-n} + iR_{-n+1} + jR_{-n+2} + kR_{-n+3}$$

şeklinde tanımlanır. (Z & N., 2022) Burada, R_n; n. Perrin sayısı, R_{-n} ise $-n.$ (negatif indisi) Perrin sayısıdır, (R_n , $R_{-n} \in \mathscr{R}$). Ayrıca, i, j, k kuaterniyonik birimleri Tablo 1.7'deki kuralları sağlar. Perrin genelleştirilmiş kuaterniyonlar kümesi $\mathcal{R}_{\alpha\beta}$ ile temsil edilecektir. (Z & N., 2022)

Tablo 1.9. Bazı Perrin Genelleştirilmiş Kuaterniyon Örnekleri

n		R_n	R_{-n}
0		$3 + 2j + 3k$	$3 + 2j + 3k$
1		$2 + i + 3j + 2k$	$-1 + 3i + 2k$
2		$2 + 3i + 2j + 5k$	$1 - i + 3jk$
3		$3 + 2i + 5j + 5k$	$2 + i - j + 3k$
4		$2 + 5i + 5j + 7k$	$-3 + 2i + j - k$

Kaynak: Z & N., 2022

Tanım 1.9:

$\mathbb{R}_* = (0, \infty)$ olsun. $\mathbb{R}_*$ kümesinde multiplicative(çarpımsal) toplamayı veya $*$ toplama $+_*$,

$$a +_* b = ab, \qquad a, b \in \mathbb{R}_*$$

şekinde tanımlanır. (Georgiev & Zennir, 2022)

Tanım 1.10:

$\mathbb{R}_*$ kümesinde multiplicative(çarpımsal) çarpım veya $*$ çarpımı $\cdot_*$,

$$a \cdot_* b = e^{loga\, logb}$$

şu şekilde tanımlarız. (Georgiev & Zennir, 2022)

Tanım 1.11:

$x, y \in \mathbb{R}_*$ için çarpımsal çıkarmayı veya $*$ toplamayı $-_*$,

$$x -_* y = a +_* (-_* b)$$

şu şekilde tanımlarız. (Georgiev & Zennir, 2022)

Güç fonksiyonu şu şekilde tanımlanır:

$$x^{k_*} = x \cdot_* \cdot_* \cdots \cdot_* x$$

burada $x \in \mathbb{R}_*$ve $k \in \mathbb{N}$. Ayrıca, çarpımsal sıfır ve çarpımsal birim sırasıyla $0_* = 1$ ve $1_* = e$ olarak tanımlanmıştır.

Tanım 1.12:

Bir graf $G = (V, E)$ için olay matrisi $B = (b_{ij})_{n\times m}$ şu şekilde tanımlanır:

- $V = \{v_1, v_2, \dots, v_n\}$ (düğümler kümesi)
- $E = \{e_1, e_2, \dots, e_m\}$ (kenarlar kümesi)

Bu matris, F_2 üzerinde aşağıdaki şekilde tanımlanır:

$$b_{ij} = \begin{cases} 1, & eğer\ v_i\ düğümü\ e_j\ kenarına\ aitse, \\ 0, & aksi\ halde. \end{cases}$$

Genellikle B^t (B'nin transpozesi) matrisinin transpozesi olarak gösterilir. B ve B^t sırasıyla aşağıdaki doğrusal dönüşümleri tanımlar:

$$B: \mathcal{E}(G) \to \mathcal{V}(G)$$

$$B^t: \mathcal{V}(G) \to \mathcal{E}(G)$$

Bu dönüşümler, standart bazlar göz önünde bulundurularak tanımlanır. (Diestel, 2005)

Bir grafın bitişiklik(adjacency) matrisi $A = (a_{ij})_{n\times n}$ şu şekilde tanımlanır:

$$a_{ij} = \begin{cases} 1, & eğer\ v_i, v_j\ \in E\ ise, \\ 0, & aksi\ halde. \end{cases}$$

Son olarak, A ve B matrisleri arasında basit bir bağlantı bulunmaktadır. D ile $d(v_i)$ değerlerini içeren gerçek (real) köşegen matrisini tanımlayalım:

$$D = (d_{ij})_{n\times n}$$

Burada, $d_{ii} = d(v_i)$ ve $d_{ij} = 0 \ \ (i \neq j)$.

Rekürans bağıntılarıyla ilgili bazı özelliklere (Stevic, 2004), (Tan, 2015), (Everest, Poorten, Shparliaski, & Ward, 2003), (Poorten, 1989) bu çalışmalar incelenerek ulaşılabilir. (Waddill M. , 1993) k. mertebeden lineer rekürans dizilerinin matris özelliklerini çalışmıştır. (Spickerman & & Joyner, 1984) çalışmasında k. mertebeden lineer rekürans dizileri için Binet formülü konusunda çalışılmıştır. (Wyler, 1965), (Brooke, Saucedo, & Xu, 2017), (Chowla, Dunton, & Lewis, 1961) çalışmalarında ikinci dereden rekürans bağıntılarıyla ilgili detaylı bilgilere ulaşılabilir. Üçüncü dereceden rekürans bağıntılarını ile ilgili bilgiler ve teoremler (Rabinowitz, 1996) çalışmasında verilmiştir. (Jarden, 1966) üçüncü dereceden rekürans dizilerini ele almıştır., (A & A, 1971), (Shannon & Horadam, 1972), ve (Adegoke, 2019) çalışmalarında üçüncü rekürans bağıntılarının bazı özelliklerini, matris formüllerini, ve rekürans dizilerinin kuvvetlerinin üreteç fonksiyonları ele alınmıştır. (Cerda-Morales, 2017), (Cereceda, 2015), (Cerda-Morales G. , 2018), ve (Waddill M. E., 1991) çalışmalarında Tribonacci sayılarının bazı özellikleri, Tribonacci dizisi ve matrisleri, Tribonacci Binet formülleri üzerinedir. (Vieira, Alves, & Catarino, 2020) çalışmasında Padovan sayılarıyla ilgili tanımlar ve matris gösterimleri verilmiştir. (Sokhuma., 2013) Padovan Q matris ve bu matrisin genelleştirilmesi üzerinedir. (Adegoke, 2019) bu makalede, Padovan ve Perrin toplam formüllerini incelemiştir. Padovan ve Perrin sayılarının cebirsel özellikleri ve matris özellikleriyle ilgili (Sokhuma, 2013), (Taskara & Yilmaz, 2014), ve (Irmak, 2019) çalışmalar yapmışlardır.

1876 yılında Edouard Lucas tarafından dolaylı olarak dile getirilmiş olsa da, Perrin dizisini ancak 1899 yılında François Perrin tanımlamıştır (Perrin, 1899). (M. Mangueira, Alves, & Catarino, 2020) çalışmasında Perrin dizisinin pozitif tam sayıları için matrisler incelenerek ve matris formunun genelleştirilmesi yapılarak, negatif tam sayılar alanına genişletilmesi sağlanmıştır. (Shannon, Anderson, & Horadam, 2006) bu makalede Cordonnier, Perrin ve van der Laan sayılarının üçüncü dereceden dizilerinin bazı özelliklerini araştırmışlardır.

(Taş, Uçar, Özgür, & Kaymak, 2018) çalışmasında Fibonacci Q matrislerini kullanarak yeni bir kodlama/kod çözme algoritmaları yöntemi sunulmuştur. (Aydınyuz & & Aşcı, 2023) k-mertebeden Gauss Fibonacci polinomları için tanımlanan kodlama teorisi x = 1 alınarak yeniden düzenlenmiştir ve bu kodlama teorisine k-mertebeden Gauss Fibonacci Kodlama Teorisi adını vermişlerdir. (Shtayat & Al-Kateeb, 2019) Padovan Q-matrisleri kullanarak yeni bir kodlama/kod çözme algoritması önermişlerdir. (Shtayat & Al-Kateeb, 2021) çalışmasında

Perrin sayı dizilerinin bazı özelliklerini incelenmiş, ve Padovan Q-matrisi ve Perrin R-matrisine dayalı bir kriptografi modeli verilmiştir.

Tezin Amacı

Bu tezde, üçüncü dereceden doğrusal tekrarlama dizileri arasında yer alan Perrin sayıları ve Perrin kuaterniyonları ele alınacak ve bu sayıların özellikleri ve karakteristik denklemleri incelenecektir. Bu sayı dizisinin matematiksel yapısı Perrin tekrarlama ilişkisine dayalı olarak detaylandırılacak ve çeşitli sayı sistemleriyle ilişkisi araştırılacaktır.

Ayrıca Perrin sayılarının ve kuaterniyonlarının kodlama teorisi açısından uygulamaları incelenecek ve hata tespiti ve düzeltme algoritmalarındaki rolleri değerlendirilecektir. Özellikle Perrin sayı dizisinin güvenli veri iletimi, kriptografi ve hata düzeltme kodları gibi alanlarda nasıl kullanıldığı ve kullanım potansiyelinin ne olduğu ortaya konulacaktır.

Bu bağlamda çalışmada hem teorik hem de uygulamalı bir yaklaşım benimsenerek literatürdeki mevcut çalışmalar derinlemesine incelenecek ve yeni katkılar sunulması amaçlanacaktır.

2. PERRİN SAYILARIYLA KODLAMA TEORİSİ ALANINDA UYGULAMALAR

Bu bölümde, Perrin sayılarına dayalı çeşitli şifreleme yöntemleri ele alınacak, her bir yöntemin temel yapısı ve şifreleme-deşifreleme süreçleri detaylandırılacaktır. Ayrıca, Multiplicative Perrin sayıları tanıtılacak ve bu sayıların bazı kombinatoriyel özellikleri detaylı bir şekilde ortaya konulacaktır.

2.1. Perrin Üreteç Matrisini Kullanarak Şifreleme

Perrin üreteç matrisi, Perrin sayılarını ardışık olarak üreten bir matristir ve genellikle üçüncü dereceden bir fark denklemini temel alır. Bu matris, Perrin dizisinin lineer cebirsel temsili olarak kullanılır ve şifreleme algoritmalarında dönüşüm aracı olarak işlev görür. Bu bağlamda, üreteç matrisinin kuvvetleri aracılığıyla mesaj matrisleri üzerinde çeşitli doğrusal işlemler uygulanabilir ve bu işlemler geri dönüşümlü olduğu için çözümleme işlemi de mümkündür.

Şifreleme Prosedürü:

1. Adım: Bir başlangıç mesajını alın ve mesajdaki karakterlere karşılık gelen sayısal değerleri kullanarak 3. mertebeden M matris oluşturun.

2. Adım: Kodlama ve kod çözme işlemlerimizi basitleştirmek için Perrin matrisi R_n 'yi kodlama matrisi olarak alıyoruz.

3. Adım: İlk şifreleme katmanını elde etmek için ortaya çıkan iki matrisi çarpın. $M \times R_n = C$.

3. Adım: Sonra, bu ürünü ikinci şifreleme katmanı için kodlama matrisini aynı mertebeden bir mesaj matrisindeki harflerin binary kodlarının matris gösterimini olan matrisini ekleyin. $P = C + B_m$.

4. Adım: Son olarak, ortaya çıkan matris iki seviyeli bir şifrelenmiş matrisdir.

Şifre Çözme Prosedürü

Adım 1: Birinci adımda, P matrisinden B_m matrisini çıkararak C matrisini elde ediyoruz. $C = P - B_m$.

Adım 2: Son olarak, bu matrisi Perrin matrisinin tersiyle çarparak deşifrelemeyi tamamlıyoruz. $M = C \times R_n^{-1}$. Bu kod çözme süreciyle orijinal mesaj matrisi 'yi elde ediyoruz.

Teorem 2.1: $n \geq 1$ ve R'nin n 'inci Perrin sayısı olduğunu varsayalım. Eğer

$$Q = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}, K = \begin{bmatrix} R_{-5} & R_{-3} & R_{-4} \\ R_{-4} & R_{-2} & R_{-3} \\ R_{-3} & R_{-1} & R_{-2} \end{bmatrix}, \text{ve } R_n = \begin{bmatrix} R_{n-5} & R_{n-3} & R_{n-4} \\ R_{n-4} & R_{n-2} & R_{n-3} \\ R_{n-3} & R_{n-1} & R_{n-2} \end{bmatrix}$$

ise

$$KQ^n = R_n \qquad (2.1)$$

eşliği tüm $n \in \mathbb{Z}^+$ için geçerlidir.

İspat: Bunu Matematiksel Tümevarım İlkesini kullanarak kanıtlayalım. $n = 1$ için ifadenin doğrulandığını görmek kolaydır. Teoremin $n = k$ durumu için geçerli olduğunu varsayalım, yani:

$$KQ^k = R_k$$

Şimdi, teoremi $n = k + 1$için kanıtlamalıyız. Yani:

$$KQ^{k+1} = R_{k+1}$$

Şu şekilde yeniden yazılabilir:

$$KQ^{k+1} = KQ^kQ$$

Tümevarım hipotezini ve matris çarpımını kullanarak sonucu doğrulamak kolaydır. Yani, ispat tamamlanmıştır.

Teorem 2.2: $n \geq 1$ için,

$$\det(R_n) = 23$$

dir.

İspat:

$$\begin{aligned} \det R_n &= \det(KQ^n) = \det(K)\det(Q)^n \\ &= 23 \end{aligned}$$

Teorem 2.2: $n \geq 1$ için,

$$(R_n)^{-1} =$$

$$\frac{1}{|R_n|}\begin{bmatrix} R_{n-2}^2 - R_{n-3}R_{n-1} & R_{n-4}R_{n-1} - R_{n-3}R_{n-2} & R_{n-3}^2 - R_{n-4}R_{n-2} \\ R_{n-3}^2 - R_{n-4}R_{n-2} & R_{n-5}R_{n-2} - R_{n-4}R_{n-3} & R_{n-4}^2 - R_{n-5}R_{n-3} \\ R_{n-4}R_{n-1} - R_{n-2}R_{n-3} & R_{n-3}^2 - R_{n-5}R_{n-1} & R_{n-5}R_{n-2} - R_{n-3}R_{n-4} \end{bmatrix}.$$

İspat: Bilinen matris tersi alma formülü kullanarak $(R_n)^{-1}$ kolayca elde edilebilir:

$$(R_n)^{-1} = \frac{1}{\det(R_n)} \operatorname{adj}(R_n).$$

Örnek: "ALGORITHM" mesajını alarak şifreleme ve deşifreleme aşamalarını yapalım.

- Adım 1: Mesaj matrisini oluşturalım:

Tablo 2.1. ASCII ve 8-Bit Binary Tablosu

Harf	ASCII	$8-Bit\ Binary$	Harf	ASCII	$8-Bit\ Binary$
A	65	01000001	T	84	01010100
L	76	01001100	H	72	01001000
G	71	01000111	M	77	01001101
O	79	01001111			
R	82	01010010			
I	73	01001001			

$$M = \begin{bmatrix} A & L & G \\ O & R & I \\ T & H & M \end{bmatrix}_{3\times 3} = \begin{bmatrix} 65 & 76 & 71 \\ 79 & 82 & 73 \\ 84 & 72 & 77 \end{bmatrix}.$$

• Adım 2: Her harf için ASCII değerinden başlayan Perrin dizisini kullanarak bir matris oluşturuyoruz. Her harfin ASCII değerine bağlı olarak farklı bir R_n matrisi kullanırsak, her harf ayrı bir şekilde şifrelenir ve güvenlik seviyesi çok daha yüksek olacaktır. "A" harfi için ($n = 65$), "L" harfi için ($n = 76$), "G" harfi için ($n = 71$), "O" harfi için ($n = 79$), "R" harfi için ($n = 82$), "I" harfi için ($n = 73$) "T" harfi için ($n = 84$), "H" harfi için ($n = 72$), "M" harfi için ($n = 77$) R_n matris gösterimleri:

$$R_A = R_{65} = \mathrm{K}Q^{65} = \begin{bmatrix} 21252274 & 37295141 & 28153269 \\ 28153269 & 49405543 & 37295141 \\ 37295141 & 65448410 & 10365448410 \end{bmatrix}.$$

$$R_L = R_{76} = \mathrm{K}Q^{76} = \begin{bmatrix} 468557684 & 822261415 & 620706778 \\ 620706778 & 1089264462 & 822261415 \\ 822261415 & 1442968193 & 1089264462 \end{bmatrix}.$$

$$R_G = R_{71} = \mathrm{K}Q^{71} = \begin{bmatrix} 114853953 & 201554637 & 152149094 \\ 152149094 & 267003047 & 201554637 \\ 201554637 & 353703731 & 267003047 \end{bmatrix}.$$

$$R_O = R_{79} = \mathrm{K}Q^{79} = \begin{bmatrix} 1089264462 & 1911525877 & 1442968193 \\ 1442968193 & 2532232655 & 1911525877 \\ 1911525877 & 3354494070 & 2532232655 \end{bmatrix}.$$

$$R_R = R_{82} = \mathrm{K}Q^{82} = \begin{bmatrix} 2532232655 & 4443758532 & 3354494070 \\ 3354494070 & 5886726725 & 4443758532 \\ 4443758532 & 7798252602 & 5886726725 \end{bmatrix}.$$

$$R_I = R_{73} = \mathrm{K}Q^{73} = \begin{bmatrix} 201554637 & 353703731 & 267003047 \\ 267003047 & 468557684 & 353703731 \\ 353703731 & 620706778 & 468557684 \end{bmatrix}.$$

$$R_T = R_{84} = \mathrm{K}Q^{84} = \begin{bmatrix} 4443758532 & 7798252602 & 5886726725 \\ 5886726725 & 10330485257 & 7798252602 \\ 7798252602 & 13684979327 & 10330485257 \end{bmatrix}.$$

$$R_H = R_{72} = \mathrm{K}Q^{72} = \begin{bmatrix} 152149094 & 267003047 & 201554637 \\ 201554637 & 353703731 & 267003047 \\ 267003047 & 468557684 & 353703731 \end{bmatrix}.$$

$$R_M = R_{77} = \mathrm{K}Q^{77} = \begin{bmatrix} 620706778 & 1089264462 & 822261415 \\ 822261415 & 1442968193 & 1089264462 \\ 1089264462 & 1911525877 & 1442968193 \end{bmatrix}.$$

• Adım 3: 1. seviye kodlama:

$$C = R \times M$$

Matris çarpımı ile her harf için farklı bir kod mesajı elde ediyoruz.

$$C_A = R_A \times M = \begin{bmatrix} 6692588545 & 6700409754 & 6399258460 \\ 8865792226 & 8876153122 & 8477212595 \\ 11744674167 & 11758399432 & 11229915752 \end{bmatrix}$$

$$C_L = R_L \times M = \begin{bmatrix} 147554270597 & 147726708030 & 141087100765 \\ 195467791928 & 195696222892 & 186900615919 \\ 258939694030 & 259242300630 & 247590602128 \end{bmatrix}$$

$$C_G = R_G \times M = \begin{bmatrix} 36168847164 & 36211115430 & 34583599402 \\ 47913521331 & 47969514862 & 45813515154 \\ 63471902102 & 63546077738 & 60689986209 \end{bmatrix}$$

$$C_O = R_O \times M = \begin{bmatrix} 343022062525 & 343422930922 & 327987716684 \\ 454407485958 & 454938523522 & 434491218047 \\ 601961756555 & 602665231552 & 575578318812 \end{bmatrix}$$

$$C_R = R_R \times M = \begin{bmatrix} 797429548483 & 798361454444 & 762478934731 \\ 1056369242513 & 1057603755074 & 1010069536859 \\ 1399391305038 & 1401026685996 & 1338057253543 \end{bmatrix}$$

$$C_I = R_I \times M = \begin{bmatrix} 63471902102 & 63546077738 & 60689986209 \\ 84082368495 & 84180630292 & 80397114556 \\ 111385423433 & 111515592600 & 106503501363 \end{bmatrix}$$

$$C_T = R_T \times M = \begin{bmatrix} 1399391305038 & 1401026685996 & 1338057253543 \\ 1853798790996 & 1855965209518 & 1772548471590 \\ 2455760547551 & 2458630441070 & 2348126790402 \end{bmatrix}$$

$$C_H = R_H \times M = \begin{bmatrix} 47913521331 & 47969514862 & 45813515154 \\ 63471902102 & 63546077738 & 60689986209 \\ 84082368495 & 84180630292 & 80397114556 \end{bmatrix}$$

$$C_M = R_M \times M = \begin{bmatrix} 195467791928 & 195696222892 & 186900615919 \\ 258939694030 & 259242300630 & 247590602128 \\ 343022062525 & 343422930922 & 327987716684 \end{bmatrix}$$

2. seviye kodlama:

$$P = C + B_m$$

"A","L", "G", "O", "R", "I", "T", "H","M" harfleri için binary matris B_m gösterimleri:

$$B_A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & ? \end{bmatrix}. B_L = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & ? \end{bmatrix}. B_G = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & ? \end{bmatrix}.$$

$$B_O = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & ? \end{bmatrix}. B_R = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & ? \end{bmatrix}. B_I = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & ? \end{bmatrix}.$$

$$B_T = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & ? \end{bmatrix}. B_H = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & ? \end{bmatrix}. B_M = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & ? \end{bmatrix}.$$

8 bitlik bir binary dizisini 3×3 boyutundaki bir matrise yerleştirdiğimizden 1 hücre boş kalıyor — yani $c_{3,3}$ (matrisin sağ alt köşesi). O hücreyi tamamlamak için '?' eklendi. '?' ASCII kod tablosunda 63' e denk gelmektedir.

$$P_A = C_A + B_A = \begin{bmatrix} 6692588545 & 6700409755 & 6399258460 \\ 8865792226 & 8876153122 & 8477212595 \\ 11744674167 & 11758399433 & 11229915815 \end{bmatrix}$$

$$P_L = C_L + B_L = \begin{bmatrix} 147554270597 & 147726708031 & 141087100765 \\ 195467791928 & 195696222892 & 186900615920 \\ 258939694030 & 259242300630 & 247590602191 \end{bmatrix}$$

$$P_G = C_G + B_G = \begin{bmatrix} 36168847164 & 36211115431 & 34583599402 \\ 47913521331 & 47969514862 & 45813515155 \\ 63471902103 & 63546077739 & 60689986272 \end{bmatrix}$$

$$P_O = C_O + B_O = \begin{bmatrix} 343022062525 & 343422930923 & 327987716684 \\ 454407485958 & 454938523523 & 434491218048 \\ 601961756556 & 602665231553 & 575578318875 \end{bmatrix}$$

$$P_R = C_R + B_R = \begin{bmatrix} 797429548483 & 798361454445 & 762478934731 \\ 1056369242514 & 1057603755074 & 1010069536859 \\ 1399391305039 & 1401026685996 & 1338057253606 \end{bmatrix}$$

$$P_I = C_I + B_I = \begin{bmatrix} 63471902102 & 63546077739 & 60689986209 \\ 84082368495 & 84180630293 & 80397114556 \\ 111385423433 & 111515592601 & 106503501426 \end{bmatrix}$$

$$P_T = C_T + B_H = \begin{bmatrix} 1399391305038 & 1401026685997 & 1338057253543 \\ 1853798790997 & 1855965209518 & 1772548471591 \\ 2455760547551 & 2458630441070 & 2348126790465 \end{bmatrix}$$

$$P_H = C_H + B_H = \begin{bmatrix} 47913521331 & 47969514863 & 45813515154 \\ 63471902102 & 63546077739 & 60689986209 \\ 84082368495 & 84180630292 & 80397114619 \end{bmatrix}$$

$$P_M = C_M + B_M = \begin{bmatrix} 195467791928 & 195696222893 & 186900615919 \\ 258939694030 & 259242300631 & 247590602129 \\ 343022062525 & 343422930923 & 327987716747 \end{bmatrix}$$

Mesajı çözmek için bulduğumuz kodlama matrislerini deşifrelemenin Adım 1 $C = P - B_m$ ve Adım 2 $M = C \times R_n^{-1}$. aşamalarını inceleyelim:

Adım 1: P_n matrislerinden B_m matrislerini çıkarıyoruz ve C_n matrislerini elde ediyoruz.

$$C_A = P_A - B_A = \begin{bmatrix} 6692588545 & 6700409754 & 6399258460 \\ 8865792226 & 8876153122 & 8477212595 \\ 11744674167 & 11758399432 & 11229915752 \end{bmatrix},$$

$$C_L = P_L - B_L = \begin{bmatrix} 147554270597 & 147726708030 & 141087100765 \\ 195467791928 & 195696222892 & 186900615919 \\ 258939694030 & 259242300630 & 247590602128 \end{bmatrix},$$

$$C_G = P_G - B_G = \begin{bmatrix} 36168847164 & 36211115430 & 34583599402 \\ 47913521331 & 47969514862 & 45813515154 \\ 63471902102 & 63546077738 & 60689986209 \end{bmatrix},$$

$$C_O = P_O - B_O = \begin{bmatrix} 343022062525 & 343422930922 & 327987716684 \\ 454407485958 & 454938523522 & 434491218047 \\ 601961756555 & 602665231552 & 575578318812 \end{bmatrix},$$

$$C_R = P_R - B_R = \begin{bmatrix} 797429548483 & 798361454444 & 762478934731 \\ 1056369242513 & 1057603755074 & 1010069536859 \\ 1399391305038 & 1401026685996 & 1338057253543 \end{bmatrix},$$

$$C_I = P_I - B_I = \begin{bmatrix} 63471902102 & 63546077738 & 60689986209 \\ 84082368495 & 84180630292 & 80397114556 \\ 111385423433 & 111515592600 & 106503501363 \end{bmatrix},$$

$$C_T = P_T - B_T = \begin{bmatrix} 1399391305038 & 1401026685996 & 1338057253543 \\ 1853798790996 & 1855965209518 & 1772548471590 \\ 2455760547551 & 2458630441070 & 2348126790402 \end{bmatrix},$$

$$C_H = P_H - B_H = \begin{bmatrix} 47913521331 & 47969514862 & 45813515154 \\ 63471902102 & 63546077738 & 60689986209 \\ 84082368495 & 84180630292 & 80397114556 \end{bmatrix},$$

$$C_M = P_M - B_M = \begin{bmatrix} 195467791928 & 195696222892 & 186900615919 \\ 258939694030 & 259242300630 & 247590602128 \\ 343022062525 & 343422930922 & 327987716684 \end{bmatrix}.$$

Adım 2: Öncelikle R_n^{-1} matrislerini yazıyoruz.

$$R_A^{-1} = \frac{1}{23}\begin{bmatrix} -50961 & -14273 & 39814 \\ 39814 & -11147 & -14273 \\ -14273 & 25541 & -11147 \end{bmatrix}$$

$$R_L^{-1} = \frac{1}{23}\begin{bmatrix} -23651 & 178424 & -121211 \\ -121211 & -144862 & 178424 \\ 178424 & 57213 & -144862 \end{bmatrix}$$

$$R_G^{-1} = \frac{1}{23}\begin{bmatrix} 33562 & 90775 & -87649 \\ -87649 & -54087 & 90775 \\ 90775 & 3126 & -54087 \end{bmatrix}$$

$$R_O^{-1} = \frac{1}{23}\begin{bmatrix} 299635 & 202075 & -323286 \\ -323286 & -23651 & 202075 \\ 202075 & -121211 & -23651 \end{bmatrix}$$

$$R_R^{-1} = \frac{1}{23}\begin{bmatrix} 525361 & -97560 & -225726 \\ -225726 & 299635 & -97560 \\ -97560 & -323286 & 299635 \end{bmatrix}$$

$$R_I^{-1} = \frac{1}{23}\begin{bmatrix} -144862 & 33562 & 57213 \\ 57213 & -87649 & 33562 \\ 33562 & 90775 & -87649 \end{bmatrix}$$

$$R_T^{-1} = \frac{1}{23}\begin{bmatrix} 397195 & 525361 & -622921 \\ -622921 & -225726 & 525361 \\ 525361 & -97560 & -225726 \end{bmatrix}$$

$$R_H^{-1} = \frac{1}{23}\begin{bmatrix} 57213 & -87649 & 33562 \\ 33562 & 90775 & -87649 \\ -87649 & -54087 & 90775 \end{bmatrix}$$

$$R_M^{-1} = \frac{1}{23}\begin{bmatrix} 202075 & -121211 & -23651 \\ -23651 & 178424 & -121211 \\ -121211 & -144862 & 178424 \end{bmatrix}.$$

Şimdi R_n^{-1} ile karşılık gelen C_n matrisini çarpıyoruz.

$$M = R_A^{-1} \times C_A = \begin{bmatrix} 65 & 76 & 71 \\ 79 & 82 & 73 \\ 84 & 72 & 77 \end{bmatrix} = \begin{bmatrix} A & L & G \\ O & R & I \\ T & H & M \end{bmatrix}_{3\times 3}$$

$$M = R_L^{-1} \times C_L = \begin{bmatrix} 65 & 76 & 71 \\ 79 & 82 & 73 \\ 84 & 72 & 77 \end{bmatrix} = \begin{bmatrix} A & L & G \\ O & R & I \\ T & H & M \end{bmatrix}_{3\times 3}$$

$$M = R_G^{-1} \times C_G = \begin{bmatrix} 65 & 76 & 71 \\ 79 & 82 & 73 \\ 84 & 72 & 77 \end{bmatrix} = \begin{bmatrix} A & L & G \\ O & R & I \\ T & H & M \end{bmatrix}_{3\times3}$$

$$M = R_O^{-1} \times C_O = \begin{bmatrix} 65 & 76 & 71 \\ 79 & 82 & 73 \\ 84 & 72 & 77 \end{bmatrix} = \begin{bmatrix} A & L & G \\ O & R & I \\ T & H & M \end{bmatrix}_{3\times3}$$

$$M = C_R \times R_R^{-1} = \begin{bmatrix} 65 & 76 & 71 \\ 79 & 82 & 73 \\ 84 & 72 & 77 \end{bmatrix} = \begin{bmatrix} A & L & G \\ O & R & I \\ T & H & M \end{bmatrix}_{3\times3}$$

$$M = C_I \times R_I^{-1} = \begin{bmatrix} 65 & 76 & 71 \\ 79 & 82 & 73 \\ 84 & 72 & 77 \end{bmatrix} = \begin{bmatrix} A & L & G \\ O & R & I \\ T & H & M \end{bmatrix}_{3\times3}$$

$$M = C_T \times R_T^{-1} = \begin{bmatrix} 65 & 76 & 71 \\ 79 & 82 & 73 \\ 84 & 72 & 77 \end{bmatrix} = \begin{bmatrix} A & L & G \\ O & R & I \\ T & H & M \end{bmatrix}_{3\times3}$$

$$M = C_H \times R_H^{-1} = \begin{bmatrix} 65 & 76 & 71 \\ 79 & 82 & 73 \\ 84 & 72 & 77 \end{bmatrix} = \begin{bmatrix} A & L & G \\ O & R & I \\ T & H & M \end{bmatrix}_{3\times3}$$

$$M = C_M \times R_M^{-1} = \begin{bmatrix} 65 & 76 & 71 \\ 79 & 82 & 73 \\ 84 & 72 & 77 \end{bmatrix} = \begin{bmatrix} A & L & G \\ O & R & I \\ T & H & M \end{bmatrix}_{3\times3}$$

Buradan deşifreleme işlemi tamamlanır ve mesaj matrisimiz olan M'yi elde etmiş oluruz.

2.2. Affine Cipher Yöntemi ile Perrin Dizisi ve Perrin Katsayılı Kuaterniyonları Kullanarak Şifreleme

Bu kısımda verilen mesajdaki harfi ASCII'den bir polinom kullanarak şifreleyeceğiz.

$$\mathrm{E(x)} = \mathrm{a} \times \mathrm{R}_n + \mathrm{b}\ \mathrm{mod} p$$

Burada R_n, Perrin dizisinin elemanlarını temsil eder. a ve b parametreleri de mesajın karakterleri ile değişebilir. n ifadesini mesajın ASCII ifadelerine göre değiştirerek Perrin sayılarında kullanıyoruz. Bu şekilde farklı ve çözülmesi daha zor olan bir şifreleme yöntemi elde ediyoruz.

Örnek: "UYGULAMA" mesajını alarak Affine cipher ve Perrin dizisini kullanarak şifreleyelim ve ardından geri çözelim.

Tablo 2.2. ASCII Tablosu

Harf	ASCII	Harf	ASCII
U	85	A	65
Y	89	M	77
G	71	A	65
U	85		
L	76		

Seçilen değerler:

• $a = 4, b = 6, ve\ p = 256$ dır.

$$U \rightarrow n = 85 \rightarrow Y_U = 4 \times R_{85} + 6\ mod256 = 4 \times (24015464584) + 6 + 85\ mod256$$

$$= 96061858427\ mod256 = 123 \rightarrow \{$$

$$Y \rightarrow n = 89 \rightarrow Y_Y = 4 \times R_{89} + 6\ mod256 = 4 \times (73957919629) + 6 + 89\ mod256$$

$$= 295831678611\ mod256 = 147 \rightarrow M - \hat{}S$$

$$G \rightarrow n = 71 \rightarrow Y_G = 4 \times R_{71} + 6\ mod256 = 4 \times (468557684) + 6 + 71\ mod256$$

$$= 1874230813\ mod256 = 29 \rightarrow GS$$

$$U \rightarrow n = 85 \rightarrow Y_U = 4 \times R_{85} + 6\ \ mod256 = 4 \times (24015464584) + 6 + 85\ mod256$$

$$= 96061858427\ mod256 = 123 \rightarrow \{$$

$$L \rightarrow n = 76 \rightarrow Y_L = 4 \times R_{76} + 6\ mod256 = 4 \times (1911525877) + 6 + 76\ mod256$$

$$= 7646103590\ mod256 = 38 \rightarrow \&$$

$$A \rightarrow n = 65 \rightarrow Y_A = 4 \times R_{65} + 6\ mod256 = 4 \times (86700684) + 6 + 65\ mod256$$

$$= 346802807\ mod256 = 119 \rightarrow w$$

$$M \rightarrow n = 77 \rightarrow Y_M = 4 \times R_{77} + 6\ mod256 = 4 \times (2532232655) + 6 + 77\ mod256$$

$$= 10128930703\ mod256 = 143 \rightarrow M - \hat{}O$$

$$A \rightarrow n = 65 \rightarrow Y_A = 4 \times R_{65} + 6\ mod256 = 4 \times (86700684) + 6 + 65\ mod256$$

$$= 346802807 \bmod 256 = 119 \rightarrow \mathrm{w}$$

‘UYGULAMA’ mesajının şifrelenmiş ifadesi buradan ‘{M-^SGS{&wM-^Ow’ şeklinde elde edilir.

Deşifrelemek için:

$$\mathrm{ASCII} = (\mathrm{Y} - \mathrm{a} \times \mathrm{R}_n - \mathrm{b}) \bmod \mathrm{p}$$

kullanırız.

$$\{\rightarrow \mathrm{ASCII} = 96061858427 - 4 \times (2532232655) - 6 \bmod 256$$

$$= 85 \bmod 256 = 85 \rightarrow \mathrm{U}$$

$$\mathrm{M} - \mathrm{\hat{}S} \rightarrow \mathrm{ASCII} = 295831678611 - 4 \times (73957919629) - 6 \bmod 256$$

$$= 89 \bmod 256 = 89 \rightarrow \mathrm{Y}$$

$$\mathrm{GS} \rightarrow \mathrm{ASCII} = 1874230813 - 4 \times (468557684) \bmod 256$$

$$= 71 \bmod 256 = 71 \rightarrow \mathrm{G}$$

$$\{\rightarrow \mathrm{ASCII} = 96061858427 - 4 \times (2532232655) - 6 \bmod 256$$

$$= 85 \bmod 256 = 85 \rightarrow \mathrm{U}$$

$$\& \rightarrow \mathrm{ASCII} = 7646103590 - 4 \times (1911525877) - 6 \bmod 256$$

$$= 76 \bmod 256 = 76 \rightarrow \mathrm{L}$$

$$\mathrm{w} \rightarrow \mathrm{ASCII} = 346802807 - 4 \times (86700684) - 6 \bmod 256$$

$$= 65 \bmod 256 = 65 \rightarrow \mathrm{A}$$

$$\mathrm{M} - \mathrm{\hat{}O} \rightarrow \mathrm{ASCII} = 10128930703 - 4 \times (2532232655) - 6 \bmod 256$$

$$= 77 \bmod 256 = 77 \rightarrow \mathrm{M}$$

$$\mathrm{w} \rightarrow \mathrm{ASCII} = 346802807 - 4 \times (86700684) - 6 \bmod 256$$

$$= 65 \bmod 256 = 65 \rightarrow \mathrm{A}$$

Deşifrelemeyi yaptığımızda orijinal mesajımız olan ‘UYGULAMA’yı elde etmiş oluruz.

Örnek: "UYGULAMA" mesajını alarak Affine cipher ve Perrin kuaterniyonları kullanarak şifreleyelim ve ardından geri çözelim.

Şifrelemek için:

$$\mathrm{E(x)} = \mathrm{a} \times \widetilde{R_n} + \mathrm{b}\ \mathrm{mod p}$$

kullanırız.

Seçilen değerler:

- $\mathrm{a} = 2, b = 4, ve\ p = 256$ dır.

$$\mathrm{U} \rightarrow \mathrm{n} = 85 \rightarrow Y_U = 2 \times \widetilde{R_{85}} + 4\ mod256 = 2 \times (24015464584 + 31813717186i + 42144202443j + 55829181770k) + 4 + 85\ \mathrm{mod256}$$

$$= 63627434372i + 84288404886j + 111658363540k + 48030929257\ mod256$$
$$= 132i + 150j + 148k + 105$$

$$\mathrm{Y} \rightarrow \mathrm{n} = 89 \rightarrow Y_Y = 2 \times \widetilde{R_{89}} + 4\ mod256 = 2 \times (73957919629 + 97973384213i + 129787101399j + 171931303842k) + 4 + 89\ \mathrm{mod256}$$

$$= 195946768426i + 259574202798j + 343862607684k + 147915839351\ mod256$$
$$= 42i + 174j + 68k + 119$$

$$\mathrm{G} \rightarrow \mathrm{n} = 71 \rightarrow Y_G = 2 \times \widetilde{R_{71}} + 4\ mod256 = 2 \times (468557684 + 620706778i + 822261415j + 1089264462k) + 4 + 71\ \mathrm{mod256}$$

$$= 1241413556i + 1644522830j + 2178528924k + 937115443\ mod256$$
$$= 180i + 78j + 156k + 51$$

$$\mathrm{U} \rightarrow \mathrm{n} = 85 \rightarrow Y_U = 2 \times \widetilde{R_{85}} + 4\ mod256 = 2 \times (24015464584 + 31813717186i + 42144202443j + 55829181770k) + 4 + 85\ \mathrm{mod256}$$

$$= 63627434372i + 84288404886j + 111658363540k + 48030929257\ mod256$$
$$= 132i + 150j + 148k + 105$$

$$\mathrm{L} \rightarrow \mathrm{n} = 76 \rightarrow Y_L = 2 \times \widetilde{R_{76}} + 4\ mod256 = 2 \times (1911525877 + 2532232655i + 3354494070j + 4443758532k) + 4 + 76\ \mathrm{mod256}$$

$$= 5064465310i + 6708988140j + 8887517064k + 3823051834\ mod256$$
$$= 158i + 236j + 136k + 58$$

$$\mathrm{A} \rightarrow \mathrm{n} = 65 \rightarrow Y_A = 2 \times \widetilde{R_{65}} + 4\ mod256 = 2 \times (86700684 + 114853953i + 152149094j + 201554637k) + 4 + 65\ \mathrm{mod256}$$

$$= 229707906i + 304298188j + 403109274k + 173401437\ mod256$$
$$= 130i + 204j + 154k + 93$$

$$\mathrm{M} \to \mathrm{n} = 77 \ \to Y_M = 2 \times \widetilde{R_{77}} + 4\ mod256 = 2 \times (22532232655 + 3354494070i + 4443758532j + 5886726725k) + 4 + 77 \bmod 256$$

$$= 6708988140i + 8887517064j + 11773453450k + 45064465391\ mod256$$

$$= 236i + 136j + 138k + 239$$

$$\mathrm{A} \to \mathrm{n} = 65 \ \to Y_A = 2 \times \widetilde{R_{65}} + 4\ mod256 = 2 \times (86700684 + 114853953i + 152149094j + 201554637k) + 4 + 65 \bmod 256$$

$$= 229707906i + 304298188j + 403109274k + 173401437\ mod256$$

$$= 130i + 204j + 154k + 93$$

Deşifrelemek için:

$$\mathrm{ASCII} = (\mathrm{Y} - \mathrm{a} \times \widetilde{R_n} - \mathrm{b}) \bmod \mathrm{p}$$

kullanırız.

$$132i + 150j + 148k + 105 \to \mathrm{ASCII} = 63627434372i + 84288404886j + 111658363540k + 48030929257 \ - 2 \times (24015464584 + 31813717186i + 42144202443j + 55829181770k) - 4 \bmod 256$$

$$= 85 \bmod 256 = 85 \ \to \mathrm{U}$$

$$42i + 174j + 68k + 119 \to \mathrm{ASCII} = 195946768426i + 259574202798j + 343862607684k + 147915839351 - 2 \times (73957919629 + 97973384213i + 129787101399j + 171931303842k) - 4 \bmod 256$$

$$= 89 \bmod 256 = 89 \ \to \mathrm{Y}$$

$$180i + 78j + 156k + 51 \to \mathrm{ASCII} = 1241413556i + 1644522830j + 2178528924k + 937115443 - 2 \times (468557684 + 620706778i + 822261415j + 1089264462k) - 4 \bmod 256$$

$$= 71 \bmod 256 = 71 \ \to \mathrm{G}$$

$$132i + 150j + 148k + 105 \to \mathrm{ASCII} = 63627434372i + 84288404886j + 111658363540k + 48030929257 \ - 2 \times (24015464584 + 31813717186i + 42144202443j + 55829181770k) - 4 \bmod 256$$

$$= 85 \bmod 256 = 85 \ \to \mathrm{U}$$

$$158i + 236j + 136k + 58 \rightarrow \text{ASCII} = 5064465310i + 6708988140j + 8887517064k + 3823051834 - 2 \times (1911525877 + 2532232655i + 3354494070j + 4443758532k) - 4 \bmod 256$$

$$= 76 \bmod 256 = 76 \rightarrow \text{L}$$

$$130i + 204j + 154k + 93 \rightarrow \text{ASCII} = 229707906i + 304298188j + 403109274k + 173401437 - 2 \times (86700684 + 114853953i + 152149094j + 201554637k) - 4 \bmod 256$$

$$= 65 \bmod 256 = 65 \rightarrow \text{A}$$

$$236i + 136j + 138k + 239 \rightarrow \text{ASCII} = 6708988140i + 8887517064j + 11773453450k + 45064465391 - 2 \times (22532232655 + 3354494070i + 4443758532j + 5886726725k) - 4 \bmod 256$$

$$= 77 \bmod 256 = 7 \rightarrow \text{A}$$

$$130i + 204j + 154k + 93 \rightarrow \text{ASCII} = 229707906i + 304298188j + 403109274k + 173401437 - 2 \times (86700684 + 114853953i + 152149094j + 201554637k) - 4 \bmod 256$$

$$= 65 \bmod 256 = 65 \rightarrow \text{A}$$

Deşifrelemeyi yaptığımızda orijinal mesajımız olan ‘UYGULAMA’yı elde etmiş oluruz.

2.3. Multiplicative Perrin Sayıları ve Şifreleme

Multiplicative Kalkülüs (veya non-Newtonian Calculus) Michael Grossman ve Robert Katz tarafından 1960 larda çıkarma ve toplamanın rollerini bölme ve çarpmaya taşıyarak yeni bir kalkülüs kurmasıyla ortaya çıkmış bir çalışma alanıdır. Multiplicative Kalkülüs özellikle ekonomi ve finans için yararlı bir matematiksel araçtır.

Bu kısımda, öncelikle multiplicative kalkülüste tanımlanan işlemler göz önüne alarak multiplicative Perrin sayılarını tanımlıyoruz ve bazı özellikleri sunulacaktır. Bu multiplicative Perrin dizisi için üreten matrisin n'inci kuvveti belirlenecek ve bu dizinin bazı temel özellikleri matris yöntemleriyle elde edilecektir.

Tanım: $n \geq 1$ için multiplicative Perrin sayılarını aşağıdaki rekürans ilişkisiyle

$$MR_n = MR_{n-2} +_* MR_{n-3}$$

tanımlanır. Burada MR_n başlangıç koşulları $MR_0 = e^3, MR_1 = 1$ ve $MR_0 = e^2$ olan n'inci multiplicative Perrin sayısını belirtir.

Tanım 2.1: $n \geq 3$ için negatif multiplicative Perrin sayılarını aşağıdaki rekürans ilişkisiyle

$$MR_{-n} = MR_{-n+3} -_* MR_{-n+1}$$

tanımlanır. Burada MR_n başlangıç koşulları $MR_0 = e^3, MR_{-1} = e^{-1}$ ve $MR_{-2} = e$ olan n'inci multiplicative Perrin sayısını belirtir. Perrin sayılarının ilk birkaç pozitif ve negatif sayı değerlerini tabloda bulunacaktır.

Tablo 2.3. Perrin ve Multiplicative Perrin Sayılarının Tablosu

n	0	1	2	3	4	5	6	7	8	…
R_n	3	0	2	3	2	5	5	7	10	...
MR_n	e^3	1	e^2	e^3	e^2	e^5	e^5	e^7	e^{10}	...
R_{-n}	3	-1	1	2	-3	4	-2	-1	5	...
MR_{-n}	e^3	e^{-1}	e	e^2	e^{-3}	e^4	e^{-2}	e^{-1}	e^5	...

Aşağıdaki matrisleri tanımlayalım:

$$Q = \begin{bmatrix} 1 & e & e \\ e & 1 & 1 \\ 1 & e & 1 \end{bmatrix} \text{ and } K = \begin{bmatrix} MR_2 & MR_0 & MR_1 \\ MR_1 & MR_{-1} & MR_0 \\ MR_0 & MR_{-2} & MR_{-1} \end{bmatrix}$$

burada Q, multiplicative Perrin dizisi için üreteç matris olarak adlandırılır. Buna göre aşağıdaki teoremi elde edilecektir.

Teorem 2.3: Her $n \geq 3$ değerleri için,

$$Q^n \cdot_* \mathrm{K} = \begin{bmatrix} MR_{n+2} & MR_n & MR_{n+1} \\ MR_{n+1} & MR_{n-1} & MR_n \\ MR_n & MR_{n-2} & MR_{n-1} \end{bmatrix}$$

burada MR_n, n'inci multiplicative Perrin sayısıdır.

İspat: Bunu n üzerinde matematiksel tümevarımla kanıtlayalım. Eğer $n = 3$ ise,

$$K \cdot_* Q^3 = \begin{bmatrix} e^2 & e^3 & 1 \\ 1 & e^{-1} & e^3 \\ e^3 & e & e^{-1} \end{bmatrix} \cdot_* \begin{bmatrix} e & e & e \\ e & e & 1 \\ 1 & e & e \end{bmatrix}$$
$$= \begin{bmatrix} e \cdot_* e^2 +_* e \cdot_* 1 +_* e \cdot_* e^3 & e \cdot_* e^3 +_* e \cdot_* e^{-1} +_* e \cdot_* e & e \cdot_* 1 +_* e \cdot_* e^3 +_* e \cdot_* e^{-1} \\ e \cdot_* e^2 +_* e \cdot_* 1 +_* 1 \cdot_* e^3 & e \cdot_* e^3 +_* e \cdot_* e^{-1} +_* 1 \cdot_* e & e \cdot_* 1 +_* e \cdot_* e^3 +_* 1 \cdot_* e^{-1} \\ 1 \cdot_* e^2 +_* e \cdot_* 1 +_* e \cdot_* e^3 & 1 \cdot_* e^3 +_* e \cdot_* e^{-1} +_* e \cdot_* e & 1 \cdot_* 1 +_* e \cdot_* e^3 +_* e \cdot {}_* e^{-1} \end{bmatrix}$$
$$= \begin{bmatrix} e^5 & e^3 & e^2 \\ e^2 & e^2 & e^3 \\ e^3 & 1 & e^2 \end{bmatrix} = \begin{bmatrix} MR_5 & MR_3 & MR_4 \\ MR_4 & MR_2 & MR_3 \\ MR_3 & MR_1 & MR_2 \end{bmatrix}.$$

bu doğrudur. $n = k$ için geçerli olduğunu varsayalım, yani:

$$Q^k \cdot_* K = \begin{bmatrix} 1 & e & e \\ e & 1 & 1 \\ 1 & e & 1 \end{bmatrix}^n \cdot_* \begin{bmatrix} MR_2 & MR_0 & MR_1 \\ MR_1 & MR_{-1} & MR_0 \\ MR_0 & MR_{-2} & MR_{-1} \end{bmatrix} = \begin{bmatrix} MR_{k+2} & MR_k & MR_{k+1} \\ MR_{k+1} & MR_{k-1} & MR_k \\ MR_k & MR_{k-2} & MR_{k-1} \end{bmatrix}$$

Şimdi $n = k + 1$ için doğrulandığını göstermeliyiz. Başka bir deyişle,

$$Q^{k+1} \cdot_* K = K \cdot_* Q^k \cdot_* Q$$
$$= \begin{bmatrix} MR_{k+2} & MR_k & MR_{k+1} \\ MR_{k+1} & MR_{k-1} & MR_k \\ MR_k & MR_{k-2} & MR_{k-1} \end{bmatrix} \cdot_* \begin{bmatrix} 1 & e & e \\ e & 1 & 1 \\ 1 & e & 1 \end{bmatrix}$$
$$= \begin{bmatrix} MR_{k+3} & MR_{k+1} & MR_{k+2} \\ MR_{k+2} & MR_k & MR_{k+1} \\ MR_{k+1} & MR_{k-1} & MR_k \end{bmatrix}$$

dir ve istenilen elde edilmiş olunur.

Lemma: Q matrisinin multiplicative determinantı

$$\det(Q) = e \cdot_* 1 \cdot_* 1 -_* 1 \cdot_* e \cdot_* e +_* e \cdot_* e \cdot_* e -_* 1 \cdot_* 1 \cdot_* e +_* 1 \cdot_* 1 \cdot_* 1 -_* e \cdot_* 1 \cdot_* e = e.$$

dir.

Lemma: $n \geq 3$ için,

$$\det(Q^n) = e$$

İspat: İfadesi $\det(Q^n) = [\det(Q)]^n = [e]^n = e$ buradan açıkça görülecektir.

Lemma: $n \geq 3$ için,

$$\det(K) = e^3 \cdot_* e^3 \cdot_* e^3 -_* e^{-1} \cdot_* e^3 \cdot_* 1 +_* 1 \cdot_* 1 \cdot_* e -_* e^2 \cdot_* e^3 \cdot_* e +_* e^{-1} \cdot {}_* e^2 \cdot_* e^{-1} -_* 1 \cdot_* e^3 \cdot_* e^{-1} = e^{23}$$

dir.

Lemma : $n \geq 1$ için,

$$\det MR_n = \det(K \cdot_* Q^n) = \det(K) \cdot_* \det(Q)^n = e^{23} \cdot_* e = e^{23}$$

Multiplicative Perrin sayılarının tanımı gereği, aşağıdaki vektör rekürans ilişkisini yazılabilecektir:

$$\begin{bmatrix} MR_{n+2} \\ MR_{n+1} \\ MR_n \end{bmatrix} = Q \cdot_* \begin{bmatrix} MR_2 \\ MR_1 \\ MR_0 \end{bmatrix}$$

Buradan zaman aşağıdaki teorem ortaya çıkar.

Teorem 2.4. $n \geq 2$ için,

$$\begin{bmatrix} MR_{n+2} \\ MR_{n+1} \\ MR_n \end{bmatrix} = \begin{bmatrix} 1 & e & e \\ e & 1 & 1 \\ 1 & e & 1 \end{bmatrix}^n \cdot_* \begin{bmatrix} MR_2 \\ MR_1 \\ MR_0 \end{bmatrix}$$

Dir.

İspat: Bunu n üzerinde matematiksel tümevarımla kanıtlayalım. Eğer $n = 2$ ise,

$$\begin{bmatrix} 1 & e & e \\ e & 1 & 1 \\ 1 & e & 1 \end{bmatrix}^2 \cdot_* \begin{bmatrix} e^2 \\ 1 \\ e^3 \end{bmatrix} = \begin{bmatrix} e & e & 1 \\ 1 & e & e \\ e & 1 & 1 \end{bmatrix} \cdot_* \begin{bmatrix} e^2 \\ 1 \\ e^3 \end{bmatrix} = \begin{bmatrix} e^2 \\ e^3 \\ e^2 \end{bmatrix} = \begin{bmatrix} MR_4 \\ MR_3 \\ MR_2 \end{bmatrix}.$$

$$\begin{bmatrix} MR_{n+2} \\ MR_{n+1} \\ MR_n \end{bmatrix} = \begin{bmatrix} 1 & e & e \\ e & 1 & 1 \\ 1 & e & 1 \end{bmatrix} \cdot_* \begin{bmatrix} MR_2 \\ MR_1 \\ MR_0 \end{bmatrix}.$$

tümevarımsal bir argümanla ve Multiplicative Perrin sayılarının tanımından hareketle ispat tamamlanır.

Multiplicative Perrin sayılarının çarpımsal toplamını aşağıdaki gibi ele alalım:

$$S_n = \sum_{k=0}^{n_*} MR_k = MR_0 +_* MR_1 +_* MR_2 +_* \cdots +_* MR_n$$

Daha sonra aşağıdaki lemma doğrulanacaktır.

Lemma:. $n \geq 3$ için,

$$S_n = e^2 +_* S_{n-2} +_* S_{n-3}$$

İspat: n üzerinde tümevarım yapılarak ispat tamamlanır.

Aşağıdaki matrisleri ele alalım:

$$A=\begin{bmatrix}1_* & 0_* & 0_* & 0_*\\ 1_* & 0_* & 1_* & 1_*\\ 0_* & 1_* & 0_* & 0_*\\ 0_* & 0_* & 1_* & 0_*\end{bmatrix}=\begin{bmatrix}e & 1 & 1 & 1\\ e & 1 & e & e\\ 1 & e & 1 & 1\\ 1 & 1 & e & 1\end{bmatrix}, T=\begin{bmatrix}e & 1 & 1 & 1\\ e^3 & MR_2 & MR_0 & MR_1\\ e & MR_1 & MR_{-1} & MR_0\\ e & MR_0 & MR_{-2} & MR_{-1}\end{bmatrix}$$

$$\text{ve } B_n=\begin{bmatrix}e & 1 & 1 & 1\\ S_n & MR_{n+2} & MR_n & MR_{n+1}\\ S_{n-1} & MR_{n+1} & MR_{n-1} & MR_n\\ S_{n-2} & MR_n & MR_{n-2} & MR_{n-1}\end{bmatrix}$$

Burada $S_n=\sum_{k=0}^{n-2_*} MR_k$ dır. Buna göre aşağıdaki teoremi verilecektir.

Teorem 2.5: $n\geq 3$ için,

$$A^n \cdot_* T = B_n$$

Dir.

İspat: $n=2$ için,

$$A^2 \cdot_* T=\begin{bmatrix}e & 1 & 1 & 1\\ e & e & e & 1\\ e & 1 & e & e\\ 1 & e & 1 & 1\end{bmatrix}\cdot_*\begin{bmatrix}e & 1 & 1 & 1\\ e^3 & e^2 & e^3 & 1\\ e & 1 & e^{-1} & e^3\\ e & e^3 & e & e^{-1}\end{bmatrix}$$

$$=\begin{bmatrix}e & 1 & 1 & 1\\ e^5 & e^2 & e^2 & e^3\\ e^3 & e^3 & 1 & e^2\\ e^3 & e^2 & e^3 & 1\end{bmatrix}$$

$$=\begin{bmatrix}1_* & 0_* & 0_* & 0_*\\ S_2 & MR_4 & MR_2 & MR_3\\ S_1 & MR_3 & MR_1 & MR_2\\ S_0 & MR_2 & MR_0 & MR_1\end{bmatrix}.$$

$n=3$ için,

$$A^3 \cdot_* T=\begin{bmatrix}e & 1 & 1 & 1\\ e^2 & e & e & e\\ e & e & e & 1\\ e & 1 & e & e\end{bmatrix}\cdot_*\begin{bmatrix}e & 1 & 1 & 1\\ e^3 & e^2 & e^3 & 1\\ e & 1 & e^{-1} & e^3\\ e & e^3 & e & e^{-1}\end{bmatrix}$$

$$=\begin{bmatrix}e & 1 & 1 & 1\\ e^8 & e^5 & e^3 & e^2\\ e^5 & e^2 & e^2 & e^3\\ e^3 & e^3 & 1 & e^2\end{bmatrix}$$

$$=\begin{bmatrix}1_* & 0_* & 0_* & 0_*\\ S_3 & MR_5 & MR_3 & MR_4\\ S_2 & MR_4 & MR_2 & MR_3\\ S_1 & MR_3 & MR_1 & MR_2\end{bmatrix}.$$

n için geçerli olduğunu varsayalım,

$$A^n \cdot_* T = \begin{bmatrix} e & 1 & 1 & 1 \\ S_n & MR_{n+2} & MR_n & MR_{n+1} \\ S_{n-1} & MR_{n+1} & MR_{n-1} & MR_n \\ S_{n-2} & MR_n & MR_{n-2} & MR_{n-1} \end{bmatrix}$$

Bunu $n+1$ için doğrulayalım. Başka bir deyişle,

$$\begin{aligned} A^{n+1} &= A^n \cdot_* T \cdot_* A \\ &= \begin{bmatrix} e & 1 & 1 & 1 \\ S_n & MR_{n+2} & MR_n & MR_{n+1} \\ S_{n-1} & MR_{n+1} & MR_{n-1} & MR_n \\ S_{n-2} & MR_n & MR_{n-2} & MR_{n-1} \end{bmatrix} \cdot_* \begin{bmatrix} e & 1 & 1 & 1 \\ e & 1 & e & e \\ 1 & e & 1 & 1 \\ 1 & 1 & e & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1_* & 0_* & 0_* & 0_* \\ S_{n+1} & MR_{n+3} & MR_{n+1} & MR_{n+2} \\ S_n & MR_{n+2} & MR_n & MR_{n+1} \\ S_{n-1} & MR_{n+1} & MR_{n-1} & MR_n \end{bmatrix} \\ &= B_{n+1} \end{aligned}$$

istenileni elde etmiş oluruz.

Örnek: "ALGORITHM" mesajını alarak şifreleme ve deşifreleme aşamalarını yapalım.

• Adım 1: Multiplicative mesaj matrisini oluşturalım:

$$M = \begin{bmatrix} A & L & G \\ O & R & I \\ T & H & M \end{bmatrix} = \begin{bmatrix} e^{65} & e^{76} & e^{71} \\ e^{79} & e^{82} & e^{73} \\ e^{84} & e^{72} & e^{77} \end{bmatrix}.$$

• Adım 2: $MR_n = \mathrm{K}Q^n$

n = 3 için,

$$MR_3 = K \cdot_* Q^3 = \begin{bmatrix} e^5 & e^3 & e^2 \\ e^2 & e^2 & e^3 \\ e^3 & 1 & e^2 \end{bmatrix}$$

• Adım 3: Kod mesajı;

$$C = M +_* MR_3$$

$$= \begin{bmatrix} e^{65} & e^{76} & e^{71} \\ e^{79} & e^{82} & e^{73} \\ e^{84} & e^{72} & e^{77} \end{bmatrix} +_* \begin{bmatrix} e^5 & e^3 & e^2 \\ e^2 & e^2 & e^3 \\ e^3 & 1 & e^2 \end{bmatrix}$$

$$= \begin{bmatrix} e^{65} +_* e^5 & e^{76} +_* e^3 & e^{71} +_* e^2 \\ e^{79} +_* e^2 & e^{82} +_* e^2 & e^{73} +_* e^3 \\ e^{84} +_* e^3 & e^{72} +_* 1 & e^{77} +_* e^2 \end{bmatrix} = \begin{bmatrix} e^{65} \cdot e^5 & e^{76} \cdot e^3 & e^{71} \cdot e^2 \\ e^{79} \cdot e^2 & e^{82} \cdot e^2 & e^{73} \cdot e^3 \\ e^{84} \cdot e^3 & e^{72} \cdot 1 & e^{77} \cdot e^2 \end{bmatrix}$$

$$= \begin{bmatrix} e^{70} & e^{79} & e^{73} \\ e^{81} & e^{84} & e^{76} \\ e^{87} & e^{72} & e^{79} \end{bmatrix}$$

• Adım 4: Kod çözme mesajı;

$$M = C -_* MR_3$$

$$= \begin{bmatrix} e^{70} & e^{79} & e^{73} \\ e^{81} & e^{84} & e^{76} \\ e^{87} & e^{72} & e^{79} \end{bmatrix} -_* \begin{bmatrix} e^{5} & e^{3} & e^{2} \\ e^{2} & e^{2} & e^{3} \\ e^{3} & 1 & e^{2} \end{bmatrix}$$

$$= \begin{bmatrix} e^{70} -_* e^{5} & e^{79} -_* e^{3} & e^{73} -_* e^{2} \\ e^{81} -_* e^{2} & e^{84} -_* e^{2} & e^{76} -_* e^{3} \\ e^{87} -_* e^{3} & e^{72} -_* 1 & e^{79} -_* e^{2} \end{bmatrix} = \begin{bmatrix} e^{70}/e^{5} & e^{79}/e^{3} & e^{73}/e^{2} \\ e^{81}/e^{2} & e^{84}/e^{2} & e^{76}/e^{3} \\ e^{87}/e^{3} & e^{72}/1 & e^{79}/e^{2} \end{bmatrix}.$$

$$= \begin{bmatrix} e^{65} & e^{76} & e^{71} \\ e^{79} & e^{82} & e^{73} \\ e^{84} & e^{72} & e^{77} \end{bmatrix} = \begin{bmatrix} A & L & G \\ O & R & I \\ T & H & M \end{bmatrix}.$$

Örnek: "QUADRATIC" mesajını alarak şifreleme ve deşifreleme aşamalarını yapalım.

• Adım 1: Multiplicative mesaj matrisini oluşturalım:

$$M = \begin{bmatrix} Q & U & A \\ D & R & A \\ T & I & C \end{bmatrix} = \begin{bmatrix} e^{81} & e^{85} & e^{65} \\ e^{68} & e^{82} & e^{65} \\ e^{84} & e^{73} & e^{67} \end{bmatrix}.$$

• Adım 2: $MR_n = \mathrm{K}Q^n$

n = 4 için,

$$MR_4 = K \cdot_* Q^4 = \begin{bmatrix} e^{5} & e^{2} & e^{5} \\ e^{5} & e^{3} & e^{2} \\ e^{2} & e^{2} & e^{3} \end{bmatrix}$$

• Adım 3: Kod mesajı;

$$C = M +_* MR_4$$

$$= \begin{bmatrix} e^{81} & e^{85} & e^{65} \\ e^{68} & e^{82} & e^{65} \\ e^{84} & e^{73} & e^{67} \end{bmatrix} +_* \begin{bmatrix} e^{5} & e^{2} & e^{5} \\ e^{5} & e^{3} & e^{2} \\ e^{2} & e^{2} & e^{3} \end{bmatrix}$$

$$= \begin{bmatrix} e^{81} +_* e^{5} & e^{85} +_* e^{2} & e^{65} +_* e^{5} \\ e^{68} +_* e^{5} & e^{82} +_* e^{3} & e^{65} +_* e^{2} \\ e^{84} +_* e^{2} & e^{73} +_* e^{2} & e^{67} +_* e^{3} \end{bmatrix} = \begin{bmatrix} e^{81} \cdot e^{5} & e^{85} \cdot e^{2} & e^{65} \cdot e^{5} \\ e^{68} \cdot e^{5} & e^{82} \cdot e^{3} & e^{65} \cdot e^{2} \\ e^{84} \cdot e^{2} & e^{73} \cdot e^{2} & e^{67} \cdot e^{3} \end{bmatrix}$$

$$= \begin{bmatrix} e^{86} & e^{87} & e^{70} \\ e^{73} & e^{85} & e^{67} \\ e^{86} & e^{75} & e^{70} \end{bmatrix}.$$

• Adım 4: Kod çözme mesajı;

$$M = C -_* MR_4$$

$$= \begin{bmatrix} e^{86} & e^{87} & e^{70} \\ e^{73} & e^{85} & e^{67} \\ e^{86} & e^{75} & e^{70} \end{bmatrix} -_* \begin{bmatrix} e^{5} & e^{2} & e^{5} \\ e^{5} & e^{3} & e^{2} \\ e^{2} & e^{2} & e^{3} \end{bmatrix}$$

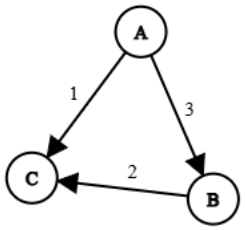
$$= \begin{bmatrix} e^{86} -_* e^{5} & e^{87} -_* e^{2} & e^{70} -_* e^{5} \\ e^{73} -_* e^{5} & e^{85} -_* e^{3} & e^{67} -_* e^{2} \\ e^{86} -_* e^{2} & e^{75} -_* e^{2} & e^{70} -_* e^{3} \end{bmatrix} = \begin{bmatrix} e^{86}/e^{5} & e^{87}/e^{2} & e^{70}/e^{5} \\ e^{73}/e^{5} & e^{85}/e^{3} & e^{67}/e^{2} \\ e^{86}/e^{2} & e^{75}/e^{2} & e^{70}/e^{3} \end{bmatrix}.$$

$$= \begin{bmatrix} e^{81} & e^{85} & e^{65} \\ e^{68} & e^{82} & e^{65} \\ e^{84} & e^{73} & e^{67} \end{bmatrix} = \begin{bmatrix} Q & U & A \\ D & R & A \\ T & I & C \end{bmatrix}.$$

2.4. Grafların Matris Gösterimleri ve Perrin Sayıları ile Şifreleme

Graf teori günlük hayatımızda farkına varmadan da olsa birçok alanda kullandığımız bir çalışma alanıdır. Bu kısımda, 3 düğümlü yönlü bir graf kullanılarak basit bir Perrin sayıları kullanılarak şifreleme yöntemi ele alınmaktadır. Grafın kenarları, Perrin dizisinin belirli elemanlarıyla ilişkilendirilerek bir dönüşüm matrisi oluşturulmakta ve bu matris, metin verisini şifrelemek için kullanılmaktadır. Bu yaklaşım, klasik matris tabanlı şifreleme yöntemlerine alternatif olarak graf teorisini ve sayı teorisini birleştirerek daha karmaşık ve güvenli sistemler tasarlamaya olanak tanır.

Örnek: "TEK" mesajını alarak verilen 3 düğümlü yönlü grafı graf tabanlı Perrin şifreleme kullanarak şifreleyelim ve ardından geri çözelim.



Şekil 2.1. Graf 1

Bu grafın ilişki (incidence) matrisi aşağıdaki şekilde verilir:

$$A = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$

Verilen mesaja karşılık gelen diyagonal matris ASCII kodlama sistemine göre şudur:

$$B = \begin{bmatrix} T & 0 & 0 \\ 0 & E & 0 \\ 0 & 0 & K \end{bmatrix} = \begin{bmatrix} 84 & 0 & 0 \\ 0 & 69 & 0 \\ 0 & 0 & 75 \end{bmatrix}.$$

Birinci seviye şifreleme:

$$C = A \times B = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix} \times \begin{bmatrix} 84 & 0 & 0 \\ 0 & 69 & 0 \\ 0 & 0 & 75 \end{bmatrix} = \begin{bmatrix} 84 & 0 & 75 \\ 0 & 69 & 75 \\ 84 & 69 & 0 \end{bmatrix}.$$

Şimdi Perrin Matrisi'ni ele alalım.

$$E = \begin{bmatrix} R_0 & R_1 & R_2 \\ R_3 & R_4 & R_5 \\ R_6 & R_7 & R_8 \end{bmatrix} = \begin{bmatrix} 3 & 0 & 2 \\ 3 & 2 & 5 \\ 5 & 7 & 10 \end{bmatrix}.$$

İkinci seviye şifreleme:

$$R = C + E = \begin{bmatrix} 84 & 0 & 75 \\ 0 & 69 & 75 \\ 84 & 69 & 0 \end{bmatrix} + \begin{bmatrix} 3 & 0 & 2 \\ 3 & 2 & 5 \\ 5 & 7 & 10 \end{bmatrix} = \begin{bmatrix} 87 & 0 & 77 \\ 3 & 71 & 80 \\ 89 & 76 & 10 \end{bmatrix}.$$

Birinci Şifre Çözme Seviyesinde paylaşılan grafın komşuluk matrisi hesaplanır.

$$R = \begin{bmatrix} 87 & 0 & 77 \\ 3 & 71 & 80 \\ 89 & 76 & 10 \end{bmatrix}$$

İkinci şifre çözme aşamasında bu komşuluk matrisi aynı mertebeden E matrisi çıkarılır ve C matrisi elde edilir.

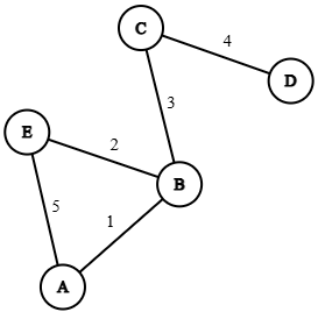
$$C = R - E = \begin{bmatrix} 84 & 0 & 75 \\ 0 & 69 & 75 \\ 84 & 69 & 0 \end{bmatrix} - \begin{bmatrix} 3 & 0 & 2 \\ 3 & 2 & 5 \\ 5 & 7 & 10 \end{bmatrix} = \begin{bmatrix} 84 & 0 & 75 \\ 0 & 69 & 75 \\ 84 & 69 & 0 \end{bmatrix}.$$

Son aşamada alıcı bu matrisi A matrisinin tersiyle çarparak mesajı diyagonal matris biçiminde elde eder.

$$B = A^{-1} \times C = \begin{bmatrix} \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \end{bmatrix} \times \begin{bmatrix} 84 & 0 & 75 \\ 0 & 69 & 75 \\ 84 & 69 & 0 \end{bmatrix} = \begin{bmatrix} 84 & 0 & 0 \\ 0 & 69 & 0 \\ 0 & 0 & 75 \end{bmatrix} = \begin{bmatrix} T & 0 & 0 \\ 0 & E & 0 \\ 0 & 0 & K \end{bmatrix}.$$

Deşifrelemeyi yaptığımızda orijinal mesajımız olan ‘TEK’ i elde etmiş oluruz.

Örnek: "Limit" mesajını alarak verilen 5 düğümlü yönlü grafı graf tabanlı Perrin şifreleme kullanarak şifreleyelim ve ardından geri çözelim.



Şekil 2.2. Graf 2

Bu grafın ilişki (incidence) matrisi aşağıdaki şekilde verilir:

$$A = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

Verilen mesaja karşılık gelen diyagonal matris ASCII kodlama sistemine göre şudur:

$$B = \begin{bmatrix} L & 0 & 0 & 0 & 0 \\ 0 & i & 0 & 0 & 0 \\ 0 & 0 & m & 0 & 0 \\ 0 & 0 & 0 & i & 0 \\ 0 & 0 & 0 & 0 & t \end{bmatrix} = \begin{bmatrix} 76 & 0 & 0 & 0 & 0 \\ 0 & 105 & 0 & 0 & 0 \\ 0 & 0 & 109 & 0 & 0 \\ 0 & 0 & 0 & 105 & 0 \\ 0 & 0 & 0 & 0 & 116 \end{bmatrix}.$$

Birinci seviye şifreleme:

$$C = A \times B = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 76 & 0 & 0 & 0 & 0 \\ 0 & 105 & 0 & 0 & 0 \\ 0 & 0 & 109 & 0 & 0 \\ 0 & 0 & 0 & 105 & 0 \\ 0 & 0 & 0 & 0 & 116 \end{bmatrix}$$

$$= \begin{bmatrix} 76 & 0 & 0 & 0 & 116 \\ 76 & 105 & 109 & 0 & 0 \\ 0 & 0 & 109 & 105 & 0 \\ 0 & 0 & 0 & 0 & 116 \\ 0 & 105 & 0 & 0 & 116 \end{bmatrix}.$$

Şimdi Perrin Matrisi'ni ele alalım.

$$E = \begin{bmatrix} R_0 & R_1 & R_2 & R_3 & R_4 \\ R_5 & R_6 & R_7 & R_8 & R_9 \\ R_{10} & R_{11} & R_{12} & R_{13} & R_{14} \\ R_{15} & R_{16} & R_{17} & R_{18} & R_{19} \\ R_{20} & R_{21} & R_{22} & R_{23} & R_{24} \end{bmatrix} = \begin{bmatrix} 3 & 0 & 2 & 3 & 2 \\ 5 & 5 & 7 & 10 & 12 \\ 17 & 22 & 29 & 39 & 51 \\ 68 & 90 & 119 & 158 & 209 \\ 277 & 367 & 486 & 644 & 853 \end{bmatrix} mod256$$

$$= \begin{bmatrix} 3 & 0 & 2 & 3 & 2 \\ 5 & 5 & 7 & 10 & 12 \\ 17 & 22 & 29 & 39 & 51 \\ 68 & 90 & 119 & 158 & 209 \\ 21 & 111 & 230 & 132 & 85 \end{bmatrix}.$$

İkinci seviye şifreleme:

$$R = C + E = \begin{bmatrix} 76 & 0 & 0 & 0 & 116 \\ 76 & 105 & 109 & 0 & 0 \\ 0 & 0 & 109 & 105 & 0 \\ 0 & 0 & 0 & 0 & 116 \\ 0 & 105 & 0 & 0 & 116 \end{bmatrix} + \begin{bmatrix} 3 & 0 & 2 & 3 & 2 \\ 5 & 5 & 7 & 10 & 12 \\ 17 & 22 & 29 & 39 & 51 \\ 68 & 90 & 119 & 158 & 209 \\ 21 & 111 & 230 & 132 & 85 \end{bmatrix}$$

$$= \begin{bmatrix} 76 & 0 & 2 & 3 & 118 \\ 81 & 110 & 116 & 10 & 12 \\ 17 & 22 & 138 & 144 & 51 \\ 68 & 90 & 119 & 158 & 325 \\ 21 & 216 & 230 & 132 & 201 \end{bmatrix} mod256 = \begin{bmatrix} 76 & 0 & 2 & 3 & 118 \\ 81 & 110 & 116 & 10 & 12 \\ 17 & 22 & 138 & 144 & 51 \\ 68 & 90 & 119 & 158 & 69 \\ 21 & 216 & 230 & 132 & 201 \end{bmatrix}.$$

Birinci Şifre Çözme Seviyesinde paylaşılan grafın komşuluk matrisi hesaplanır.

$$R = \begin{bmatrix} 76 & 0 & 2 & 3 & 118 \\ 81 & 110 & 116 & 10 & 12 \\ 17 & 22 & 138 & 144 & 51 \\ 68 & 90 & 119 & 158 & 69 \\ 21 & 216 & 230 & 132 & 201 \end{bmatrix}.$$

İkinci şifre çözme aşamasında bu komşuluk matrisi aynı mertebeden E matrisi çıkarılır ve C matrisi elde edilir.

$$C = R - E = \begin{bmatrix} 76 & 0 & 2 & 3 & 118 \\ 81 & 110 & 116 & 10 & 12 \\ 17 & 22 & 138 & 144 & 51 \\ 68 & 90 & 119 & 158 & 69 \\ 21 & 216 & 230 & 132 & 201 \end{bmatrix} - \begin{bmatrix} 3 & 0 & 2 & 3 & 2 \\ 5 & 5 & 7 & 10 & 12 \\ 17 & 22 & 29 & 39 & 51 \\ 68 & 90 & 119 & 158 & 209 \\ 21 & 111 & 230 & 132 & 85 \end{bmatrix}$$

$$= \begin{bmatrix} 76 & 0 & 0 & 0 & 116 \\ 76 & 105 & 109 & 0 & 0 \\ 0 & 0 & 109 & 105 & 0 \\ 0 & 0 & 0 & 0 & 116 \\ 0 & 105 & 0 & 0 & 116 \end{bmatrix}.$$

Son aşamada alıcı bu matrisi A matrisinin tersiyle çarparak mesajı diyagonal matris biçiminde elde eder.

$$B = A^{-1} \times C = \begin{bmatrix} 1 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 & 1 \\ -1 & 1 & 0 & 2 & -1 \\ 1 & -1 & 1 & -2 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \times \begin{bmatrix} 76 & 0 & 0 & 0 & 116 \\ 76 & 105 & 109 & 0 & 0 \\ 0 & 0 & 109 & 105 & 0 \\ 0 & 0 & 0 & 0 & 116 \\ 0 & 105 & 0 & 0 & 116 \end{bmatrix}$$

$$= \begin{bmatrix} 76 & 0 & 0 & 0 & 0 \\ 0 & 105 & 0 & 0 & 0 \\ 0 & 0 & 109 & 0 & 0 \\ 0 & 0 & 0 & 105 & 0 \\ 0 & 0 & 0 & 0 & 116 \end{bmatrix} = \begin{bmatrix} L & 0 & 0 & 0 & 0 \\ 0 & i & 0 & 0 & 0 \\ 0 & 0 & m & 0 & 0 \\ 0 & 0 & 0 & i & 0 \\ 0 & 0 & 0 & 0 & t \end{bmatrix}.$$

Deşifrelemeyi yaptığımızda orijinal mesajımız olan ‘Limit’ i elde etmiş oluruz.

3. SONUÇ

Bu çalışmada, Perrin dizilerinin matematiksel özellikleri incelenmiş ve bu dizilerin kodlama teorisindeki potansiyel kullanım alanları araştırılmıştır. Çalışmanın ilk bölümünde, rekürans bağıntılarına ilişkin temel tanımlar ve teoremler sunulmuş; Perrin sayılarına ait rekürans bağıntısı tanımlanarak matris gösterimleri ortaya konmuştur. Ayrıca, kuaterniyon ve Perrin kuaterniyon kavramları açıklanmış, grafik teorisine dair temel kavramlarla teorik altyapı desteklenmiştir.

İkinci bölümde, Perrin dizileri esas alınarak çeşitli kodlama ve şifreleme yöntemleri geliştirilmiştir. Multiplicative Perrin dizilerinin hem pozitif hem de negatif indeksli biçimleri tanımlanmış; bu dizilerin karakteristik özellikleri analiz edilmiştir. Söz konusu dizilerden yararlanılarak veri kodlama uygulamaları gerçekleştirilmiş ve grafların matris temsilleri aracılığıyla Perrin sayılarına dayalı şifreleme yöntemleri uygulanmıştır.

Elde edilen bulgular, Perrin dizilerinin yalnızca kuramsal açıdan değil, aynı zamanda uygulamalı kriptografi ve bilgi güvenliği alanlarında da kullanılabilir olduğunu göstermektedir. Bu çerçevede, Perrin dizilerinin yapısal özelliklerinden yararlanarak daha gelişmiş kodlama algoritmalarının geliştirilmesi mümkündür. Gelecekte yapılacak çalışmalar, bu dizilerin farklı matematiksel yapılara entegrasyonu ve diğer modern kriptografik yöntemlerle karşılaştırılması açısından önemli katkılar sağlayabilir.

EXTENDED ABSTRACT

Application of Perrin Numbers in Coding Theory

In today's world, with the rapid development of communication technologies and the growing importance of data transmission and security, the use of mathematical structures in coding theory and cryptography has become an increasingly relevant field of study. Among these structures, number sequences defined by recurrence relations are particularly significant due to their easily analyzable structures and their adaptability to algorithmic processes. This study focuses on a special type of recursive number sequence known as the Perrin sequence. The mathematical properties of Perrin sequences are investigated in depth, and their applicability in the field of coding theory is explored.

The Perrin sequence, first introduced by French mathematician Raoul Perrin, is defined by the recurrence relation:

$$R_n = R_{n-2} + R_{n-3}$$

with initial values typically taken as $R_0 = 3, R_1 = 0$, and $R_2 = 2$. This recursive structure endows Perrin numbers with a specific regularity, making them suitable for various mathematical and applied contexts. Unlike more widely studied sequences such as Fibonacci and Lucas numbers, the Perrin sequence has a notable feature: if n is a prime number, it often satisfies the condition $R_n \ modn \ \equiv 0$. This property suggests that Perrin numbers may be useful in primality testing and number-theoretic algorithms.

The first part of this study presents fundamental definitions and theorems related to recurrence relations. Recurrence relations are mathematical expressions in which each term of a sequence is defined in terms of previous terms. The matrix representation of such sequences plays an important role in analyzing their behavior and implementing them efficiently in algorithms. The Perrin sequence is expressed in matrix form, and its closed-form solution is explored using characteristic polynomials. These representations facilitate faster computations and enhance the practical usability of the sequence in algorithmic design.

Additionally, the concept of quaternions and a new structure referred to as Perrin quaternions are introduced. Quaternions are hypercomplex numbers in four dimensions and are widely used in 3D transformations and rotations. Perrin quaternions extend this classical structure by incorporating Perrin numbers into the quaternionic framework, offering a new perspective that can potentially contribute to encryption algorithms and algebraic modeling in applied mathematics.

Basic concepts from graph theory are also discussed in the first chapter, as they provide a theoretical foundation for subsequent applications. The matrix representations of graphs, such as adjacency and Laplacian matrices, are particularly useful in modeling data structures in coding and encryption processes. When combined with the numerical structure of a sequence like the Perrin sequence, these matrix forms provide a meaningful framework for secure data transformation.

In the second chapter, original coding methods based on Perrin sequences are developed. Coding theory aims to enable the secure and error-resistant transmission of data using mathematical techniques. In this context, a new concept referred to as Multiplicative Perrin sequences is introduced. These sequences represent multiplicative versions of the classical Perrin sequence, and their positive and negative indexed terms are analyzed in detail. The study finds that the negatively indexed forms provide insights into the symmetry and inverse behavior of the sequence, contributing further to its algebraic richness.

These extended structures are used to construct novel coding algorithms. The algorithms developed in this study leverage the periodic and recursive structure of the Perrin sequence to match data blocks with sequence elements. Modular arithmetic is used during encoding, providing both security and verification capabilities. These algorithms demonstrate the potential for Perrin-based systems in encoding applications requiring both speed and robustness.

On the applied side, encryption methods are proposed using the matrix representations of graphs and Perrin sequences. These methods integrate graph-based data structures with Perrin numbers to offer dual-layered security mechanisms in both coding and data encryption. For instance, the adjacency matrix of a graph is modified using elements of the Perrin sequence through modular operations to produce encrypted data. This approach may be particularly applicable in areas such as network security, sensor networks, and blockchain technologies, where secure and structured communication is essential.

In conclusion, this study presents a comprehensive approach to the Perrin sequence, addressing both its theoretical foundations and applied aspects. The mathematical properties of Perrin numbers are examined through algebraic and matrix formulations, expanded through quaternion-based generalizations, and contextualized within graph theory. On the applied side, the development of coding and encryption methods based on these structures provides innovative and practical solutions for secure data transmission and integrity.

The results indicate that although Perrin sequences have been less explored compared to other recursive sequences, they offer unique properties that make them highly suitable for various applications. In particular, their connection to prime numbers enhances their potential in cryptographic protocols. Furthermore, their matrix representations allow for efficient implementation in software and hardware systems, making real-time applications feasible.

Future work may focus on integrating Perrin sequences with other algebraic structures such as polynomial rings or Galois fields to develop advanced cryptographic systems. In addition, further analysis of the sequence's randomness properties within the framework of information theory may yield insights into its suitability for secure key generation. Comparative studies of Perrin sequences with other well-known recursive sequences in terms of performance, security, and efficiency would also contribute significantly to the existing literature.

Beyond its theoretical appeal, the application of Perrin sequences in real-world systems offers promising interdisciplinary opportunities. In the realm of digital communications, Perrin-based coding schemes can be integrated into error-correcting codes for wireless and satellite transmissions, where robustness against noise and interference is critical. Similarly, in cryptographic systems, the structure of Perrin sequences may be employed in symmetric and asymmetric key generation, adding an additional layer of unpredictability. In computer science, the use of Perrin-based algorithms in data compression, watermarking, or steganography can lead to innovative approaches that balance efficiency and security. Moreover, because of the recursive and self-referential nature of Perrin sequences, their implementation aligns well with modern programming paradigms such as functional programming and recursive algorithm design, making them not only mathematically rich but also computationally feasible for large-scale applications.

Their deterministic yet nontrivial structure enables secure pattern generation, which can be leveraged in lightweight cryptography, especially for resource-constrained environments like IoT devices. As computational demands grow and data security becomes more essential, further exploration into hardware-optimized Perrin-based cryptosystems could lead to efficient, scalable, and secure encryption models for future digital infrastructure.

KAYNAKLAR

A, S., & A, H. (1971). Generating Functions for Powers of Third Order Recurrence Sequences. *Duke Mathematical Journal, 38, 4, 791-4.*

Adegoke, K. (2019). Basic properties of a generalized third order sequence of numbers. *ArXiv:1906.00788v3 [math.NT], 12 pages.*

Adegoke, K. (2019). Summation identities involving Padovan and Perrin numbers. *arXiv:1812.03241v2 [math.CO]*, s. 18 pages.

Anonim. (tarih yok). *Sayıların Tarihçesi.* Ankara Üniversitesi Açık Ders Malzemeleri: https://acikders.ankara.edu.tr/mod/resource/view.php?id=77430 adresinden alındı

Aydınyuz, S., & & Aşcı, M. (. (2023). Error detection and correction for coding theory on k-order Gaussian Fibonacci matrices. . *Mathematical Biosciences and Engineering.*

Brooke, K., Saucedo, D., & Xu, C. (2017). Second-Order Linear Recurrence Relations and Periodicity. *The Onyx Review: The Interdisciplinary Research Journal*, s. 7-12.

C.C.Yalavigi. (1972). Properties of Tribonacci numbers. *Fibonacci Quarterly, vol. 10*, s. 231–246.

Cerda-Morales. (2017, Kasım). G. On a Generalization for Tribonacci Quaternions. *Mediterr. J. Math.*

Cerda-Morales, G. (2018). *A three-by-three matrix representation of a generalized Tribonacci sequence*. arXiv preprint arXiv:1807.03340. adresinden alındı

Cerda-Morales, G. (2019). New identities for Padovan numbers. *arXiv:1904.05492v1 [math.CO]*, s. 9 pages.

Cereceda, J. L. (2015). Binet's formula for generalized Tribonacci numbers. *International Journal of Mathematical Education in Science and Technology, vol. 46*, s. 1235–1243.

Chowla, S., Dunton, M., & Lewis, D. J. (1961). Linear recurrences of order two.

Cockle, J. (1849). On systems of algebra involving more than one imaginary; and on equations of the fifth degree. *Philosophical Magazine, vol. 35,* , s. 434–437.

Dantzig, T. (1930). *Number, the language of science; a critical survey written for the cultured non-mathematician.* New York: The Macmillan Company.

DEVECİ, Ö., Akuzum, Y., & Karaduman, E. (2015). The Pell-Padovan p-sequences and its applications. *Utilitas Mathematica, 98.*

Dickson, L. E. (1924). On the theory of numbers and generalized quaternions. *American Journal of Mathematics, vol. 46*, s. 1–16, 1924.

Diestel, R. (2005). *Graph Theory.* Springer-Verlag Heidelberg: http://www.dcs.fmph.uniba.sk/~macajova/TG/DiestelGraphTheoryIII.pdf adresinden alındı

Domada, T., Ashok, G., Kumar, S. A., & Chaya, D. (2024). Super-encryption technique of graphs via matricial approach. *Journal of Discrete Mathematical Sciences and Cryptography, 27:4*, s. 1215–1222, DOI: 10.47974/JDMSC-1976.

Everest, G., Poorten, A., Shparliaski, I., & Ward, T. (2003). Recurrence Sequences. *American Mathematical Society*.

Georgiev, S., & Zennir, K. (2022). *Multiplicative Differential Calculus (1st ed.).* Chapman and Hall/CRC. https://doi.org/10.1201/9781003299080.

Griffiths, L. W. (1928). Generalized quaternion algebras and the theory of numbers. *American Journal of Mathematics, vol. 50*, s. 303–314.

Hamilton, W. R. (1844). On quaternions; or on a new system of imaginaries in algebra. *Philosophical Magazine, vol. 25*, s. 489–495.

Horadam, A. F. (1965). Basic properties of a certain generalized sequence of numbers. *Fibonacci Quarterly, vol. 14, pp. 161–176, 1965*, s. 161-176.

Horadam, A. F. (1965). Special properties of the sequence W_n(a, b; p, q). *Fibonacci Quarterly, vol. 3*, s. 161-176.

Howard, F. T., & Saidak, F. I. (2010). Zhou's theory of constructing identities. *In Congress Numer Vol. 200*, s. 225-237.

Irmak, N. (2019). On factorials in Perrin and Padovan sequences. *Turkish Journal of Mathematics, vol. 43*, s. pp. 2602–2609.

JAFARI, M. (2015). *MATRIX FORMULATION OF REAL QUATERNIONS.* EÜFBED - Fen Bilimleri Enstitüsü Dergisi.

Jafari, M., & Yaylı, Y. (2015). Generalized quaternions and rotation in 3-space E^{3}_{alfabeta}. *TWMS Journal of Pure and Applied Mathematics, vol. 6*, s. 224–232.

Jafari, M., & Yaylı, Y. (2015). Generalized quaternions and their algebraic properties. *Communications Faculty of Sciences University of Ankara Series A1 Mathematics and Statistics, vol. 64*, s. 15–27.

Jarden, D. (. (1966). Third order recurring sequences. *his Recurring Sequences*, s. 86-89.

Kalman, D. (1982). Generalized Fibonacci numbers by matrix methods. *Fibonacci Quarterly*, s. vol. 20; pp. 73–76.

Kaygısız, K., & D. Bozkurt. (2012). k-generalized order-k Perrin number presentation by matrix method. *Ars Combinatoria, vol. 105*, s. pp. 95–101.

Laisant, C. A., & Lemoine, E. M. (1894). L'Interm´ediaire des mathematiciens (Vol. 1). . *Gauthier-Villars et F*.

Lucas, E. (1878). Théorie des fonctions numériques simplement périodiques. s. pp. 289–321.

M. Mangueira, R. V., Alves, F., & Catarino, P. M. (2020). A generalização da forma matricial da sequência de Perrin. *Revista Sergipana de Matemática e Educação Matemática, vol. 5*, s. pp. 384–392.

Mezaal, Y. S., & Abdulkareem, S. F. (2017). Affine cipher cryptanalysis using genetic algorithms. *JP Journal of Algebra, Number Theory and Applications, 39(5),*, s. 785-802.

Özdemir, M. (2020). *Kuaterniyonlar ve Geometri.* Altın Nokta.

Perrin, R. (1899). Query 1484. *L'Intermédiaire des Mathématiciens, vol. 6*, s. pp. 76–77.

Poorten, A. J. (1989). Notes on continued fractions and recurrence sequences. J. H. Loxton içinde, *Number Theory and Cryptography, vol. 154* (s. pp. 86–97). Cambridge University Press.

Rabinowitz, S. (1996). Algorithmic manipulation of third-order linear recurrences. *The Fibonacci Quarterly, 34(5)*, s. 447-464.

Seenukul, P., Netmanee, S., Panyakhun, T., Ausiseekaen, R., & Muangchan, S. ..-A. (2015). Matrices which have similar properties to Padovan Q-matrix and its generalized relations. *SNRU Journal of Science and Technology, vol. 7*, s. 90-94.

Shannon, A. G., & Horadam, A. F. (1972). Some properties of third-order recurrence. *Fibonacci Quarterly,vol. 10*, s. pp. 135–146.

Shannon, A. G., Anderson, P. G., & Horadam, A. F. (2006). Properties of Cordonnier,Perrin and Van der Laan numbers. s. pp. 825–831, 2006.

Shtayat, J., & Al-Kateeb, A. (2019). An Encoding-Decoding algorithm based on Padovan numbers. *arXiv preprint arXiv:1907.02007*.

Shtayat, J., & Al-Kateeb, A. (2021). The Perrin R-matrix and more properties with an application. *Journal of Discrete Mathematical Sciences & Cryptography*, s. pp. 11-12.

Sloane, N. J. (tarih yok). "Sequence A001622 (Decimal expansion of golden ratio phi (or tau) = (1 + sqrt(5))/2)". *The On-Line Encyclopedia of Integer Sequences. OEIS Foundation.*

Sloane, N. J. (tarih yok). *The on-line encyclopedia of integer sequences*. OEIS: https://oeis.org/ adresinden alındı

Sloane, N. J. (tarih yok). *The on-line encyclopedia of integer sequences*. OEIS: https://oeis.org/. adresinden alındı

Sokhuma, K. (2013). Matrices formula for Padovan and Perrin sequences. *Applied Mathematical Sciences, vol. 7*, s. pp. 7093–7096.

Sokhuma., K. (2013). Padovan Q-matrix and the generalized relations. *Applied Mathematical Sciences, vol. 7*, s. 2777–2780.

SOYKAN, Y. (2020). On sum formulas for generalized Tribonacci sequence.

Soykan, Y. (2020, Ocak). "A study on generalized (r,s, t)-numbers". *MathLAB Journal, vol. 7*, s. 101–129.

Soykan, Y. (2020). On generalized (r,s)-numbers. *International Journal of Advances in Applied Mathematics and Mechanics*, s. 1-14.

Spickerman, W. R., & & Joyner, R. N. (1984). Binet's Formula for the Recursive Sequence of Order K. *The Fibonacci Quarterly, 22(4)*, s. 327-331. https://doi.org/10.1080/00150517.1984.12429868.

Stevic, S. (2004). More on a rational recurrence relation. *Appl. Math. E-Notes,4(1)*, s. 80-85.

Tan, E. (2015). Rekürans Bağıntılar ve Rasyonel Yaklaşımlar. *Ankara Üniversitesi, Fen Bilimleri Enstitüsü*.

Taskara, N., & Yilmaz, N. (2014). On the negatively subscripted Padovan and Perrin matrix sequences. *Communications in Mathematics and Applications, vol. 5*, s. pp. 59–72.

Taş, N., Uçar, S., Özgür, N. Y., & Kaymak, Ö. Ö. (2018). A new coding/decoding algorithm using Fibonacci numbers. *Discrete Mathematics, Algorithms and Applications, 10(02), 1850028.*

Vieira, R. P., Alves, F. R., & Catarino, P. M. (2020). A historical analysis of the Padovan sequence. *International Journal of Trends in Mathematics Education Research, 3(1)*, s. 8-12.

Waddill, M. (1993). Using Matrix Techniques to Establish Properties of k-Order Linear Recursive Sequences. P. A. G.E. içinde, *Applications of Fibonacci Numbers* (s. pp. 601–615). Springer, Dordrecht.

Waddill, M. E. (1967). Another generalized Fibonacci sequence. *Fibonacci Quarterly, vol. 5*, s. pp. 209–222.

Waddill, M. E. (1991). Using matrix techniques to establish properties of a generalized Tribonacci sequence. *Applications of Fibonacci Numbers, vol. 4*, s. pp. 299–308.

Wyler, O. (1965). On Second-Order Recurrences. *The American Mathematical Monthly,72(5)*, s. 500–506. https://doi.org/10.1080/00029890.1965.11970558.

Yılmaz, F., & D. Bozkurt. (2011). Hessenberg matrices and the Pell and Perrin numbers. *Journal of Number Theory, vol. 13*, s. pp. 1390–1396. https : / / moam . info / perrin - matrix - sequences _ adresinden alındı

Yılmaz, N. (2015). Padovan ve Perrin Sayılarının Matris Temsilleri. *Selçuk Üniversitesi,*.

Yılmaz, N., & Taşkara, N. (2013). Matrix sequences in terms of Padovan and Perrin numbers. *Journal of Applied Mathematics, vol. 2013, 7 pages*.

Z, İ., & N., G. (2022). Padovan and Perrin generalized quaternions. *Math Meth Appl Sci. 45(18): 12060–12076. https://doi.org/10.1002/mma.7495*.

ÖZGEÇMİŞ

Kişisel Bilgiler

SOYAD, Ad	YILMAZ, Satı

Eğitim

Derece	**Eğitim Birimi**	**Mezuniyet**
Lisans	Ankara Hacı Bayram Veli Üniversitesi Matematik Bölümü	2022
Yüksek Lisans	Ankara Hacı Bayram Veli Üniversitesi Lisansüstü Eğitim Enstitüsü Matematik Anabilim Dalı	Devam ediyor

İş Deneyimi

Yıl	**Yer**	**Görev**
2025	Vakıfbank	Memur

Yayınlar

Kitap	Recent Developments in Mathematics	Pegem / 2024

ankara
HBM