

T.C.
RECEP TAYYİP ERDOĞAN ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

FARK KÜMELERİ VE İKİLİ DİZİ OLUŞTURMADAKİ
UYGULAMALARI

TUĞBA NAVDAR GÜNAY

TEZ DANIŞMANI
DR. ÖĞR. ÜYESİ EMEK DEMİRCİ AKARSU
TEZ JÜRİLERİ

PROF. DR. SELÇUK HAN AYDIN
DOÇ. DR. MÜCAHİDE NESİBE KESİCİOĞLU

YÜKSEK LİSANS TEZİ
MATEMATİK ANABİLİM DALI

RİZE- 2019
Her Hakkı Saklıdır

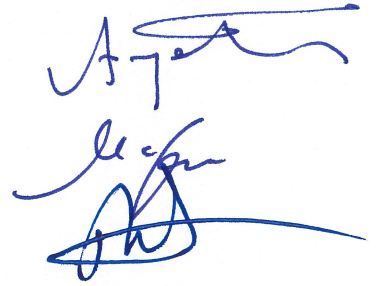
T.C.
RECEP TAYYİP ERDOĞAN ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

FARK KÜMELERİ VE İKİLİ DİZİ OLUŞTURMADAKİ UYGULAMALARI

Dr. Öğr. Üyesi Emek DEMİRCİ AKARSU danışmanlığında, Tuğba NAVDAR GÜNAY tarafından hazırlanan bu çalışma, Enstitü Yönetim Kurulu kararıyla oluşturulan jüri tarafından 24/05/2019 tarihinde Matematik Anabilim Dalı'nda **YÜKSEK LİSANS** tezi olarak kabul edilmiştir.

Jüri Üyeleri	Unvanı Adı Soyadı
Başkan	: Prof. Dr. Selçuk Han AYDIN
Üye	: Doç. Dr. Mücahide Nesibe KESİCİOĞLU
Üye	: Dr. Öğr. Üyesi Emek DEMİRCİ AKARSU

İmzası




Doç. Dr. Ferhat KALAYCI
FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ

ÖNSÖZ

Bu çalışma fark kümeleri ve ikili dizi oluşturmadaki uygulamalarını incelemek amacı ile Recep Tayyip Erdoğan Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı'nda yüksek lisans tezi olarak hazırlanmıştır.

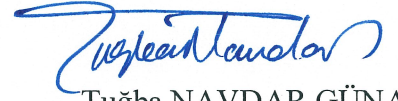
Tez çalışmasının planlanmasında, araştırılmasında, yürütülmesinde ve oluşumunda bilgi ve tecrübelerinden yararlandığım, yönlendirme ve bilgilendirmeleriyle çalışmayı şekillendiren sayın hocam Dr. Öğr. Üyesi Emek DEMİRCİ AKARSU'ya ve desteği ile tüm süreçte yanımda olan eşim Serkan GÜNAY'a teşekkürlerimi sunarım.

Hazırlanan bu Yüksek lisans tezi Recep Tayyip Erdoğan Üniversitesi Bilimsel Araştırma Projeleri Koordinasyon Birimi tarafından FYL-2018-960 nolu proje ile desteklenmiştir.

Tuğba NAVDAR GÜNAY

TEZ ETİK BEYANNAMESİ

Tarafımdan hazırlanan “Fark Kümeleri ve İkili Dizi Oluşturmadaki Uygulamaları” başlıklı bu tezin, Yükseköğretim Kurulu Bilimsel Araştırma ve Yayın Etiği Yönergesindeki hususlara uygun olarak hazırladığımı ve aksinin ortaya çıkması durumunda her türlü yasal işlemi kabul ettiğimi beyan ederim. 24/05/2019



Tuğba NAVDAR GÜNAY

***Uyarı:** Bu tezde kullanılan özgün ve/veya başka kaynaklardan sunulan içeriğin kaynak olarak kullanımı, 5846 sayılı Fikir ve Sanat Eserleri Kanunundaki hükümlere tabidir.*

ÖZET

FARK KÜMELERİ VE İKİLİ DİZİ OLUŞTURMADAKİ UYGULAMALARI

Tuğba NAVDAR GÜNAY

Recep Tayyip Erdoğan Üniversitesi

Fen Bilimleri Enstitüsü

Matematik Anabilim Dalı

Yüksek Lisans Tezi

Danışmanı: Dr. Öğr. Üyesi Emek DEMİRCİ AKARSU

Bu tez çalışmasında ilk olarak, fark kümelerinin genel tanımı, özellikleri, aileleri, fark kümelerinin varlık problemi ve fark kümelerinin ikili dizi oluşturmadaki bazı uygulamaları ile ilgili genel bilgiler mevcut literatürden faydalanılarak sunulmuştur. Sonrasında fark kümelerinin ikili dizi oluşturmadaki bir uygulaması olan kodlanmış maske oluşturmak için çalışmalar yapılmıştır. Kodlanmış maske oluşturmak için, bilgisayar programında yazılan kodlar yardımı ile uygun bir grup ve bu grup içerisindeki fark kümesi bulunmuştur. Son olarak bulunan bu fark kümesi kullanılarak bir kodlanmış maske oluşturulmuştur.

2019, 62 sayfa

Anahtar Kelimeler: Tekrarlanma Yapısı, Dizayn, Fark Kümesi, Kodlanmış Maske.

ABSTRACT

DIFFERENCE SETS AND THEIR APPLICATIONS ON THE BINARY SEQUENCES

Tuğba NAVDAR GÜNAY

**Recep Tayyip Erdogan University
Graduate School of Natural and Applied Sciences
Department of Mathematics**

Master Thesis

Supervisor : Asst. Prof. Dr. Emek DEMİRCİ AKARSU

In the study of this thesis, first of all, the general definition of difference sets, their properties, families, existence problems, some applications of constructing binary sequences, and relevant general information were presented by benefiting from the existence literature. Later on, the studies are made on a coding mask that is an application of difference sets for constructing binary sequences. To construct the coding mask, an appropriate group and a difference set in this group were found by using the constructed codes made by computer software program. Finally, by using this founded difference set, a coding mask was formed.

2019, 62 pages

Keywords: Incidence Structure, Design, Difference Set, Coding Mask.

İÇİNDEKİLER

ÖNSÖZ.....	I
TEZ ETİK BEYANNAMESİ.....	II
ÖZET.....	III
ABSTRACT.....	IV
İÇİNDEKİLER	V
ŞEKİLLER DİZİNİ.....	VII
TABLolar DİZİNİ	VIII
SEMBOLLER ve KISALTMALAR DİZİNİ	IX
1. GENEL BİLGİLER	1
1.1. Giriş.....	1
1.2. Literatür Özeti.....	2
1.3. Temel Kavramlar	5
1.3.1. Gruplar	5
1.3.2. Kuadratik Rezidüler	6
1.3.3. Tekrarlanma Yapıları ve Dizaynlar	7
1.4. Fark Kümeleri.....	13
1.4.1. Tanım	13
1.4.2. Hemen Hemen Fark Kümesi	17
1.4.3. Kısmi Fark Kümesi	18
1.4.4. Fark Kümelerinde Öteleme	19
1.4.5. Fark Kümelerinde Açınım (Development)	20
1.4.6. Fark Kümelerinde Denklik.....	21
1.4.7. Fark Kümelerinde Tümlen.....	21
1.4.8. Fark Kümelerinin Aileleri	22
1.5. Varlık Problemi ve Bruck-Ryser-Chowla Teoremi	27
1.6. Fark Kümelerinin Uygulamaları.....	29
1.6.1. İkili Diziler ve Korelasyon	30
1.6.2. Kodlanmış Maske İle Görüntüleme	34
2. YAPILAN ÇALIŞMALAR	40
2.1. İkiz Asal Fark Kümesi Oluşturma Teoreminin C++ Uygulaması.....	41
2.2. İkiz Asalları Bulmak İçin C# Kodları.....	44

2.3.	$\mathbb{Z}_{59} \oplus \mathbb{Z}_{61}$ Grubundaki Fark Kümesi.....	48
2.4.	$\mathbb{Z}_{59} \oplus \mathbb{Z}_{61}$ Grubundaki Fark Kümesi İçin Kodlanmış Maske Şablonu	54
3.	BULGULAR	56
4.	TARTIŞMA ve SONUÇLAR	57
5.	ÖNERİLER	58
	KAYNAKLAR	59
	ÖZGEÇMİŞ	62

ŞEKİLLER DİZİNİ

Şekil 1.	Farklı yollarla üçgen parçalarına ayrılmış iki beşgen	9
Şekil 2.	T_7 bloğunun gölgeli olduğu 4×4 formunda kareler dizaynı	11
Şekil 3.	Fano Düzlemi.....	15
Şekil 4.	Kodlanmış maske kullanarak görüntüleme için şema	35
Şekil 5.	$\mathbb{Z}_3 \oplus \mathbb{Z}_5$ ikiz asal grubundaki (15,7,3) parametrelili fark kümesi için oluşturulan bir şablon maske	36
Şekil 6.	$\mathbb{Z}_{11} \oplus \mathbb{Z}_{13}$ ikiz asal grubundaki (143,71,35) parametrelili fark kümesi için oluşturulan kodlanmış maske şablonu.....	37
Şekil 7.	Şekil 6 daki 1×1 tek şablon maske çoğaltılarak oluşturulan bir kodlanmış maske	37
Şekil 8.	İkiz asal fark kümesi oluşturma teoreminin C++ program dilinde kodları	42
Şekil 9.	C++ program dilinde yazılan kodlar kullanılarak $\mathbb{Z}_{11} \oplus \mathbb{Z}_{13}$ grubu için oluşturulan fark kümesi	44
Şekil 10.	C# program dilinde yazılan ikiz asalları bulma kodları	45
Şekil 11.	C# program dilinde yazılan kodlar kullanılarak 0–1000 aralığında bulunan ikiz asallar	46
Şekil 12.	$\mathbb{Z}_{59} \oplus \mathbb{Z}_{61}$ ikiz asal grubundaki fark kümesi kullanılarak oluşturulan kodlanmış maske şablonu	54
Şekil 13.	$\mathbb{Z}_{59} \oplus \mathbb{Z}_{61}$ ikiz asal grubundaki (3599,1799,899) parametrelili fark kümesi kullanılarak oluşturulan ayrıntılı kodlanmış maske şablonu	55

TABLÖLAR DİZİNİ

- Tablo 1.** $(\mathbb{Z}_{13}, +)$ grubundaki $D = \{0,1,3,9\}$ fark kümesi için çoklu küme tablosu..14
- Tablo 2.** $(\mathbb{Z}_{13}, +)$ grubundaki $D = \{1,3,4,9,10,12\}$ hemen hemen fark kümesi için oluşturulan çoklu küme tablosu18
- Tablo 3.** 0 - 1000 aralığındaki $\{p, q\}$ ikiz asalları için $\mathbb{Z}_p \oplus \mathbb{Z}_q$ ikiz asal grubundaki fark kümesinin parametreleri ve C++ programında yazılan kodların $\{p, q\}$ sayıları için ortalama fark kümesi oluşturma süresi.....47

SEMBOLLER ve KISALTMALAR DİZİNİ

$\mathbb{N}$	Doğal Sayıların Cümlesi
$\mathbb{Z}$	Tam Sayıların Cümlesi
$\mathbb{Z}_m$	mod m Tam Sayı Grubu
$\emptyset$	Boş Küme
$\subseteq$	Kümeler Arasındaki Alt Küme Bağlantısı
$\in$	Elemanıdır
$\notin$	Elemanı Değildir
$\mathbb{F}$	Cisim
1_G	G Grubunun Birim Elemanı
$GF(q)$	q Mertebeli Cisim, Galois Cismi
$G \oplus H$	Grupların Doğrudan Toplamı, $\{(a, b) a \in G, b \in H\}$
$\langle g \rangle$	g Tarafından Üretilen Grup
Δ	Birim Eleman Olmayan Farkların Çoklu Kümesi
$\text{dev}D$	D Fark Kümesinin Açınımı
$a\mathcal{R}b$	a , mod b de Bir Karedir
$\text{obeb}(a, b)$	a ile b nin En Büyük Ortak Bölünü
$\text{obeb}(a, b) = 1$	a ile b Aralarında Asaldır

1. GENEL BİLGİLER

1.1. Giriş

Genel olarak fark kümeleri alanı soyut cebir ve kombinatorik matematiğinin kesişiminde bulunur. Fark kümeleri çalışması bu alanlara ek olarak geometri, sayılar teorisi ve dizayn teorisinden araçlar kullanır. Fark kümesi bir grubun özel bir alt kümesi olup, bir grubun fark kümesi içermesi için simetrik dizayn olarak adlandırılan güzel bir yapıda etkin bir şekilde rol alması gerekir. Bu durumda bir fark kümesinin keşfedilmesi ilginç bir grup eylemi bulmakla eşdeğerdir.

Fark kümeleri fikri ilk olarak James Singer'ın 1938 tarihli "A Theorem in Finite Projective Geometry and Some Applications to Number Theory" makalesinde ortaya çıkmıştır. Birçok yazar fark kümelerini bu makaleye dayandırmaktadır. Singer (1938), bir fark kümesinin tanımını formüle etmesine rağmen ana teoremi bir dizaynın otomorfizması ile ilgilidir.

Fark kümelerinin sistematik olarak çalışılması Marshall Jr. Hall'ın 1940'ların sonlarındaki çalışmalarına kadar geri gider. Bu erken dönem makalelerinin tamamında kombinatorik, geometri ve cebir matematiği vardır. Konu geliştikçe cebirsel yöntemlerin kullanımı giderek artmaktadır.

Fark kümeleri matematiksel açıdan zengin olmakla birlikte gerçek hayattaki problemlerde de birçok uygulama alanı vardır. Fark kümeleri optik hizalama, iletişimde sinyal gürültüsü varlığı durumunda sinyallerin doğru yorumlanması, astronomik olayların görüntülenmesi, hata düzeltme kodlarının oluşturulması, kuantum bilişiminde süreçleri kolaylaştırmak, verileri kodlamak ve deşifre etmek gibi uygulama alanlarında kullanılmaktadır. Bu uygulamalardan optik hizalamada, iletişimde sinyal gürültüsünün varlığında sinyallerin doğru yorumlanmasında ve astronomik olayların görüntülenmesinde iyi otokorelasyon özelliklerine sahip fark kümeleri ve ikili diziler arasındaki ilişkiden yararlanır. Fark kümeleri aracılığıyla iyi otokorelasyon özelliklerine sahip ikili diziler oluşturulabilir. Diğer uygulamalarda kullanılan fark kümelerinin rolleri oldukça farklıdır.

Bu tez çalışmasında, fark kümeleri konusunun anlaşılabilmesi için gerekli temel kavramlar ve teoremler, fark kümelerinin tanımı, özellikleri, aileleri, fark kümelerine dair temel teoremler ve bunlardan bazılarının ispatları, bir fark kümesinin varlık problemi ile ilgili genel bir literatür özeti bulunmaktadır. Çalışmanın son kısmında ise fark kümelerinin ikili dizi oluşturmadaki uygulamalarından olan kodlanmış maske ile görüntüleme uygulamasında kullanmak için fark kümelerinin oluşturulmasına yönelik bilgisayar programlarında yazılmış kod parçaları bulunmaktadır. Bu kod parçaları kullanılarak bir fark kümesi oluşturulmuş ve oluşturulan fark kümesi için kodlanmış bir maske şablonu verilmiştir.

1.2. Literatür Özeti

Fark kümeleri fikri ilk olarak Singer (1938)'in makalesinde ortaya çıkmıştır. Singer bir fark kümesinin tanımını formüle etmesine rağmen ana teoremi bir dizaynın otomorfizması ile ilgilidir.

Fark kümeleri cebir ve kombinatoriklerin kesişiminde bulunur ve simetrik blok dizaynları için pratik ve etkili bir yapıcı yöntemle harekete geçirilir. (Singer, 1938), (Bose, 1939), (Bruck, 1955), (Hall, 1956) gibi pek çok makale bu konuyla açıkça ilgilidir. Bose (1939) tarafından dengeli tamamlanmamış blok dizaynlarının inşası üzerine iki "Modül Teoremi" geliştirilerek bunlar çeşitli dizayn aileleri oluşturmak için uygulanmış ve çeşitli inşa yöntemleri incelenmiştir.

Fark kümelerinin sistematik olarak çalışılması 1940'ların sonundaki (Hall, 1947) çalışmasına dayanmaktadır. Sonlu gruptaki fark kümeleri, Bruck (1955) tarafından bir makalede ayrıntılarıyla çalışılmıştır. Bruck (1955), Marshall Hall Jr.'ın bir fark kümesinin "çarpanı" kavramını gruptaki fark kümelerine genişletmiştir. İkinci olarak da Hall ve Ryser (1951)'in makalesindeki çarpanlar üzerine olan teoremi değişmeli gruplara kadar genişletmiştir. Hall daha sonra bir çalışmasında (Hall, 1956) teoreminin bir genellemesini almıştır. Menon (1960) tarafından yazılan makalede Hall (1956)'ın bu genel fark kümesi çarpanlarıyla ilgili teoremi değişmeli gruplara genişletilmiştir.

Lehmer (1953) tarafından rezidü fark kümeleri üzerinde çalışılmış olup bir mükemmel rezidü fark kümesinin (yani her farkın çoklu kümede bir kez görüldüğü rezidülerden oluşan fark kümesi) 2 modülo p nin tüm kuvvetlerini içerdiği ispat edilmiştir.

Baumert (1971) tarafından genel devirli fark kümeleri teorisinin oldukça kapsamlı bir araştırması verilmiştir. Sonlu gruplarda blok dizaynları ve fark kümelerinin daha genel konuları tanıtılsa da, bu konular devirli fark kümeleri için ortaya çıkan problemlere ışık tutmak için geliştirilmiştir.

Mcfarland (1973)'ın çalışmasında her asal q ve her pozitif s tamsayısı için parametreleri (v, k, λ) olan bazı devirli olmayan gruplardaki fark kümeleri için bir yapı verilmiştir.

Camion (1979) tarafından yapılan kısa bir çalışma, lineer projektif kodlar açısından fark kümeleri çalışmasının tamamını çerçevelemektedir ve bu konudaki (Ding, 2014) gibi kitapların tamamı o zamandan beri de yazılmıştır.

Bir fark kümesinin varlığı için simetrik bir dizaynın var olması gerekir. (Bruck ve Ryser, 1949) ve (Chowla ve Ryser 1950) çalışmalarında (v, k, λ) parametrelili simetrik dizaynların varlığı için Bruck-Ryser-Chowla Teoremi verilmiş ve ilk makalede yazarlar $\lambda = 1$ durumunda teoremi ispatlamışlardır. İkinci makalede ise sonucu herhangi bir λ pozitif tam sayısına genişletmişlerdir. Ryser (1982)'ın makalesinde teoremin çok daha basit bir ispatı verilmiştir. Sadece v nin tek sayı olduğu (v, k, λ) dizaynlarına değinilmektedir.

Lam vd. (1989) tarafından, 10 mertebeli projektif düzlemin yokluğu üzerine çalışılmış ve bunu takip eden süreçte yapılan bir başka çalışma (Lam, 1991), 10 mertebeli projektif düzlem sorununun evrimini ve bilgisayarların sorunu çözmek için nasıl kullanıldığını anlatan açıklayıcı bir makaledir.

Kibler (1978)'in makalesi $k < 20$ için devirli olmayan gruplardaki (v, k, λ) fark kümelerinin bir listesini içermektedir. Jungnickel (1992) tarafından modern dizayn

teorisinde fark kümeleri üzerine bir çalışma yapılmıştır. Ayrıca bu çalışmada da fark kümelerinin kullanışlı tabloları sunulmaktadır.

Beth vd. (1999) tarafından yapılan kapsamlı çalışma fark kümeleri konusundaki başlıca genel değerlendirme ve araştırmalardan biridir. Aynı yıl Pott ve yardımcı editörleri tarafından, fark kümelerinin daha özel alanlarının birçok değişik araştırmalarını bir araya toplayan bir kitap (Pott vd., 1999) yayınlanmıştır. (Jungnickel ve Pott, 1999) ve (Golomb, 1999) çalışmaları bu ciltte yayınlanan çalışmalardandır. Jungnickel ve Pott (1999) tarafından değişmeli durumlarda bulunan fark kümeleri teorisine giriş niteliğinde bir yaklaşım sunulmaktadır. Golomb (1999) tarafından ikili diziler ve onların korelasyon özellikleri ile fark kümeleri arasındaki ilişki verilmiştir ve bu konuda büyük ölçüde aydınlatıcı bir çalışmadır, ayrıca konu ile ilgili olarak MacWilliams ve Sloane (1976)'ın makalesi bulunmaktadır.

1999 sonrasında bu çalışma boyunca kullanılan ve fark kümeleri çalışmasına ilk ders kitabı tarzında girişlerden biri olarak hizmet veren Moore ve Pollatsek (2013)'in kitabı gibi diğer önemli eserler yayınlanmıştır. Moore ve Pollatsek (2013) tarafından yazılan kitapta fark kümelerinin yapısal özellikleri, fark kümelerinin aileleri, nasıl elde edildikleri, uygulama alanları, diğer alanlar ile ilişkileri ve matematiksel özellikleri ile ilgili uzman olmayanların da anlayabileceği şekilde kapsamlı bir çalışma sunulmuştur. Yakın zamanda yapılan tez çalışması (Trout, 2017) değişmeli gruplardaki fark kümeleri ve genellemeleri üzerine incelenebilecek ayrıntılı çalışmalardandır.

Fark kümelerinin bir çok alanda uygulaması bulunmakta olup bu konu üzerine birçok çalışma yapılmıştır. Godsil ve Roy (2009)'un makalesi kuantum bilişiminde fark kümelerinin kullanımı üzerine çalışma olup ayrıca eş açılı doğruların varlığını bir fark kümesinin varlığına bağlayan bir teorem içermektedir. Assmus ve Key (1992) tarafından cebirsel kodlama teorisinin dizaynların analiz ve sınıflandırılmasındaki uygulamaları detaylı olarak incelenmiştir. Baskar ve Saravanan (2012) tarafından fark kümelerinin yapılarının verileri kodlamak ve deşifre etmek için kullanılabileceği ve fark kümesi kodlarının bellek güvenliği için kullanılması üzerine çalışılmıştır. Ayrıca bu makalede fark kümesi kodlarının özelliklerinin, verilerin deşifreleme sürecini oldukça azaltmak için kullanılabileceği üzerine çalışmalar yapılmıştır. Fark kümeleri kozmoloji alanında

kullanılarak özel görüntüleme türlerinde büyük bir rol oynamıştır (Zhang vd., 1998). Özel görüntüleme türlerinde kullanımı üzerine (Skinner, 1984), (Skinner, 1988), (Zand, 1995) ve (Zand, 1996) çalışmaları örnek olarak gösterilebilir. Daha yakın zamanlarda, sinyal işleme (Xie vd., 2013) ile kuantum bilgisi ve hesaplama (Roetteler, 2016) için fark kümelerinin uygulamaları aktif araştırma alanları haline gelmiştir.

Fark kümeleri çalışmasının alt yapısı için gerekli olan cebir konuları, teoremler ve ispatları (Gallian, 2013), (Nicholson, 2012), (Rosen vd., 2005), (Ireland ve Rosen, 1982) kaynaklarında kapsamlı olarak mevcuttur.

1.3. Temel Kavramlar

1.3.1. Gruplar

Tanım 1.3.1. (*Grup*) G boş olmayan bir küme ve $*$ işlemi G de bir ikili işlem olsun. Verilen $*$ işleminin G de birleşme özelliği ve birim elemanı varsa ayrıca $*$ işlemine göre G deki her elemanın tersi varsa $(G,*)$ cebirsel yapısına grup denir.

Tanım 1.3.2. (*Değişmeli Grup*) Cebirsel yapı $(G,*)$ bir grup ve $\forall a, b \in G$ için $a * b = b * a$ değişme özelliği sağlanıyorsa gruba değişmeli grup veya abel grubu denir.

Tanım 1.3.3. (*Sonlu Grup*) G sonlu bir küme ise $(G,*)$ grubuna bir sonlu grup denir ve eleman sayısına da grubun mertebesi denir.

Tanım 1.3.4. (*Homomorfizma-İzomorfizma-Otomorfizma*) Cebirsel yapı olan $(G, \odot)$ ve $(G', \otimes)$ iki grup olmak üzere $f: G \rightarrow G'$ bir fonksiyon olsun. Eğer her $a, b \in G$ için; $f(a \odot b) = f(a) \otimes f(b)$ oluyorsa o zaman f ye *grup homomorfizması* adı verilir. Eğer f homomorfizması birebir ve örten ise bir *izomorfizma* adını alır. Ayrıca, eğer $G = G'$ ve f bir izomorfizma ise f ye bir *otomorfizma* denir.

Gruplar konusu ile ilgili daha fazla bilgi için (Gallian, 2013) ve (Nicholson, 2012) kaynaklarına bakılabilir.

1.3.2. Kuadratik Rezidüler

Fark kümelerinin uygulamaları üzerinde çalışılırken kullanılacak olan bazı fark kümeleri için kuadratik rezidüleme ihtiyacı duyulacaktır. Bu nedenle kuadratik rezidü kavramı için temel tanım ve teoremlerin verilmesi çalışma için faydalı olacaktır.

Tanım 1.3.5. (*Kuadratik Rezidü*) p bir tek asal ve a sayısı da $\text{obeb}(p, a) = 1$ olan bir tam sayı olsun. Eğer $x^2 \equiv a \pmod{p}$ kongrüansı çözülebilirse a ya p modülüne göre kuadratik rezidü (karesel kalan) denir, $x^2 \equiv a \pmod{p}$ kongrüansı çözülemez ise a ya p modülüne göre kuadratik olmayan rezidü denir.

Lemma 1.3.6. p bir tek asal ve a da p ile bölünemeyen bir tamsayı olmak üzere, $x^2 \equiv a \pmod{p}$ kongrüansı ya çözümsüzdür ya da p modülüne göre birbirlerine kongrüent olmayan iki çözümü vardır.

İspat: $x^2 \equiv a \pmod{p}$ kongrüansının $x = x_0$ gibi bir çözüme sahip olduğu varsayalım. $x = -x_0$ diğer çözümdür. Gerçekten $(-x_0)^2 = x_0^2 \equiv a \pmod{p}$ olup $-x_0$ bir çözümdür. $x_0 \not\equiv -x_0 \pmod{p}$ dir. Eğer $x_0 \equiv -x_0 \pmod{p}$ olsaydı $2x_0 \equiv 0 \pmod{p}$ olup, $p|x_0$ olurdu. Halbuki p tek asal $p \nmid a$ olup $x_0^2 \equiv a \pmod{p}$ ve $p \nmid x_0$ dir. İki tane çözüm olmadığını göstermek için de $x^2 \equiv a \pmod{p}$ nin $x = x_0$ ve $x = x_1$ gibi iki çözümü olduğu kabul edilsin. O zaman $x_0^2 \equiv x_1^2 \equiv a \pmod{p}$ ve $x_0^2 - x_1^2 = (x_0 + x_1)(x_0 - x_1) \equiv 0 \pmod{p}$ olup, ya $p|(x_0 + x_1)$ ya da $p|(x_0 - x_1)$ dir. Bunlardan da ya $x_1 \equiv -x_0 \pmod{p}$ ya da $x_1 \equiv x_0 \pmod{p}$ olur ki bu da bize sadece iki tane birbirlerine kongrüent olmayan çözüm olduğunu verir. (Rosen vd., 2005)

Teorem 1.3.7. p bir tek asal olmak üzere p nin kuadratik rezidüleri ile kuadratik olmayan rezidüleri sayısı birbirine eşit olup her biri $(p - 1)/2$ tanedir.

İspat: $1, 2, \dots, p - 1$ sayıları arasında p nin bütün kuadratik rezidüleri bulunmak istenirse bu sayıların karelerinin p modülüne göre en küçük pozitif kalanları bulunmalıdır. $p - 1$ tane kare hesaplanacağından ve her bir $x^2 \equiv a \pmod{p}$ kongrüansı ya çözümsüz ya da iki çözümlü olacağından $1, 2, \dots, p - 1$ sayıları arasında tam $(p - 1)/2$ tane p nin kuadratik rezidüsü olmalıdır. Geriye kalan $(p - 1)/2$ tane

$p - 1$ den küçük pozitif tam sayı da p nin kuadratik olmayan rezidüleridir. (Rosen vd., 2005)

Kuadratik rezidüler ile ilgili daha fazla bilgi için (Rosen vd., 2005) kaynağına bakılabilir.

1.3.3. Tekrarlanma Yapıları ve Dizaynlar

Tanım 1.3.8. (*Tekrarlanma Yapısı*) Bir tekrarlanma yapısı olan $\mathcal{D}$, $(\mathcal{P}, \mathcal{B}, \mathcal{I})$ sıralı üçlüsünden meydana gelir. Burada $\mathcal{P}$, p noktalarının kümesi; $\mathcal{B}$, $\mathcal{P}$ kümesindeki noktalardan oluşan B bloklarının kümesi; $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{B}$, $\mathcal{P}$ ile $\mathcal{B}$ arasındaki tekrarlanma ilişkisidir.

Eğer (p, B) , $\mathcal{I}$ tekrarlanma ilişkisi içerisinde ise p ve B nin çakıştığı söylenir. Bir blok diğer bir blok ile aynı nokta kümesine sahipse “tekrarlanır” denir. Bir tekrarlanma yapısında tekrarlanan bloklar yoksa basit tekrarlanma yapısı olarak bilinirler. Çalışılacak olan tekrarlanma yapıları basittir, bu yüzden bir blok nokta kümesi olarak görülebilir. p noktası B bloğu ile ilişkili ise $p \in B$ olur. $\mathcal{P}$ nin alt kümesi olarak tanımlanan bloklarla oluşturulan tekrarlanma yapısı basitçe $(\mathcal{P}, \mathcal{B})$ olarak yazılır. Tekrarlanma yapısı kavramı için şu örnekler verilebilir.

Örnek 1.3.9. Öklid düzleminde, $\mathcal{P}$ düzlemdeki noktalar kümesi ve $\mathcal{B}$ düzlemdeki doğrular kümesinden oluşur.

Örnek 1.3.10. $\mathcal{P} = \{a, b, c\}$ kümesi üç kişiden oluşan bir komiteyi temsil etsin ve $\mathcal{B} = \{\{a\}, \{a, b\}, \{a, c\}, \{a, b, c\}\}$ kümesi de bu kişilerden oluşan dört komiteyi temsil etsin. a kişisi dört komitenin hepsinde, b kişisi 2. ve 4. komitede, c kişisi ise 3. ve 4. komitede yer almaktadır.

Örnek 1.3.9 da bulunan nokta ve blokların kümesi sonsuzdur. Örnek 1.3.10 da ise nokta ve bloklar sonludur. Örnek 1.3.9 da herhangi iki nokta bir doğruyu belirlediğinden, herhangi iki noktanın sadece 1 doğru üzerinde birlikte bulunabileceği düzenlilik koşuluna sahiptir. Örnek 1.3.10 ise böyle bir düzenlilik koşuluna sahip değildir, bloklar bile farklı

büyükklüktedir. Bu çalışmada incelenecek olan tekrarlanma yapıları sonludur.

Bir tekrarlanma yapısını temsil etmek için matris gösterimi de kullanılabilir. Bu gösterim için aşağıdaki tanım kullanılacaktır.

Tanım 1.3.11. (Tekrarlanma Matrisi) $\mathcal{D} - (\mathcal{P}, \mathcal{B}, \mathcal{I})$ tekrarlanma yapısında $\mathcal{P}$ nin mertebesi $|\mathcal{P}| = v$ ve $\mathcal{B}$ nin mertebesi $|\mathcal{B}| = u$ olsun. Burada p_i , $0 < i \leq v$ olmak üzere noktaları ve B_j , $0 < j \leq u$ olmak üzere blokları temsil etsin. Bu durumda tekrarlanma matrisi olan M , $m_{ij} \in M$ olmak üzere;

$$m_{ij} = \begin{cases} 1 & \text{eğer } p_i \in B_j \text{ ise,} \\ 0 & \text{aksi durumda.} \end{cases}$$

olarak tanımlanır.

Her sonlu tekrarlanma yapısı tekrarlanma matrisi ile temsil edilebilir, burada sütunlar noktaları ve satırlar blokları temsil eder.

Örnek 1.3.12. Örnek 1.3.10 daki tekrarlanma yapısının tekrarlanma matrisi ile ifade edilişi, $\mathcal{P} = \{a, b, c\}$ ve $\mathcal{B} = \{\{a\}, \{a, b\}, \{a, c\}, \{a, b, c\}\}$ olmak üzere;

$$M = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

bulunur.

Bir tekrarlanma matrisi, sadece bir tekrarlanma yapısını temsil etmek için bir yol değildir. Bazen matris çarpımı, tekrarlanma yapısını incelemek için bir araç sağlar. Örneğin, iki tekrarlanma yapısının esas olarak aynı olup olmadığını kontrol etmek için bloklar veya noktalar yeniden sıralanarak tekrarlanma matrisi permütasyon matrisi ile çarpılabilir. (Moore ve Pollatsek, 2013)

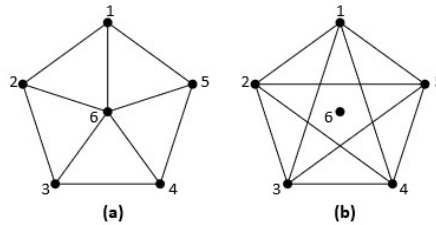
Gruplarda olduğu gibi tekrarlanma yapıları da karşılaştırılabilir. Bu karşılaştırma için izomorf tekrarlanma yapıları tanımı verilecektir.

Tanım 1.3.13. (*İzomorf Tekrarlanma Yapıları*) İki basit tekrarlanma yapısı $(\mathcal{P}, \mathcal{B}, \mathcal{I})$ ve $(\mathcal{P}', \mathcal{B}', \mathcal{I}')$ olmak üzere, $\mathcal{P}$ yi $\mathcal{P}'$ ne, $\mathcal{B}$ yi $\mathcal{B}'$ ne eşleyen bire-bir fonksiyon varsa bu tekrarlanma yapıları izomorfiktir.

Fark kümeleri konusu çoğunlukla özel bir dizayn ile ilişkili olduğundan dizaynlar ile ilgili temel bilgiler çalışma için faydalı olacaktır.

Tanım 1.3.14. (*t-Dizayn*) t negatif olmayan bir tamsayı olmak üzere, (v, k, λ) parametrelili bir t -dizaynı $\mathcal{D}=(\mathcal{P}, \mathcal{B})$ tekrarlanma yapısıdır. Burada $\mathcal{P}$, v büyüklüğünde noktalar kümesini ve $\mathcal{B}$, bloklar adı verilen $\mathcal{P}$ nin k elemanlı alt kümelerinden oluşan bir kümeyi ifade eder. Öyle ki $\lambda \geq 1$ olmak üzere, $\mathcal{P}$ nin t elemanlı her bir alt kümesi bu bloklarda tam olarak λ kez bulunur.

Örnek 1.3.15. 2 - (6,3,2) dizayn örneği incelenecektir. Merkezinde bir tepe noktası bulunan beşgen üzerindeki bloklar iki şekilde ayrılarak sunulacaktır. Şekil 1 deki köşe noktaları ve merkezi ilk altı doğal sayı ile saat yönünün tersine doğru numaralandırılmış olan iki beşgen ele alınırsa, (a) beşgeninde ağırlık merkezini tepe noktası olarak almış olan beş tane üçgen ve (b) beşgeninde bir kenarı beşgenin çevresi üzerinde bulunan beş tane ikizkenar üçgen vardır. (a) ve (b) beşgenlerinde bulunan bu üçgenlerin her biri üç elemanlı bloklardır ve bu bloklarda bulunan her nokta çifti tam olarak iki üçgende görülür.



Şekil 1. Farklı yollarla üçgen parçalarına ayrılmış iki beşgen.

2 - (6,3,2) dizaynının blok kümesi bu iki beşgende bulunan bloklar kümesinin birleşiminden oluşur.

(a) daki bloklar:

$$[162], [263], [364], [465], [561]$$

(b) deki bloklar:

$$[134], [245], [315], [421], [523]$$

2-(6,3,2) dizaynındaki bloklar:

$$[162], [263], [364], [465], [561], [134], [245], [315], [421], [523]$$

olarak bulunur. 2-(6,3,2) dizaynındaki bloklar esasında, ilk altı doğal sayı kullanılarak kolayca ortaya çıkarılan dizaynın doğasını gizler. (Bu örnek (Trout, 2017) tez çalışmasından alınmıştır.)

Özet olarak bir t -(v, k, λ) dizaynı için parametreler aşağıdaki gibidir.

v : noktaların sayısı,

b : blokların sayısı,

k : her blokta bulunan nokta sayısı,

r : noktalar kümesinden herhangi bir noktanın bulunduğu blok sayısı,

λ : verilen herhangi bir nokta çiftinin bulunduğu blok sayısı.

Teorem 1.3.16. Eğer $\mathcal{D}$ bir 2-dizaynı ise, $r(k - 1) = \lambda(v - 1)$.

İspat: x , dizaynın noktalar kümesinden alınan herhangi bir nokta olmak üzere, $x \neq y$ olacak şekilde (x, y) çiftleri iki şekilde sayılarak ispat yapılacaktır. Noktalar kümesinde x ten farklı $v - 1$ tane nokta vardır ve $t = 2$ olduğundan bu (x, y) çifti λ tane blokta birlikte bulunmalıdır. Bununla birlikte x noktasının bulunduğu blok sayısı r tanedir. x ile bir çift oluşturan $k - 1$ tane başka nokta vardır. O halde iki taraf da sayılacak olursa, $r(k - 1) = \lambda(v - 1)$ olacaktır.

Teorem 1.3.17. Bir t -(v, k, λ) dizaynı için, $vr = bk$ eşitliği mevcuttur.

İspat: $x \in B$ olmak üzere (x, B) ve $(\mathcal{P}, \mathcal{B})$ çiftleri ele alınsın. Burada v tane nokta vardır ve her biri r tane blokta bulunmalıdır. Diğer taraftan b tane blok var ve her biri k tane nokta içeriyor. İki taraflı sayım sonucu, $vr = bk$ olur.

Tanım 1.3.18. (*Simetrik Dizayn*) Simetrik (v, k, λ) -dizaynı $0 < k < v$ olmak üzere aşağıda verilen koşullar ile birlikte bir $(\mathcal{P}, \mathcal{B}, \mathcal{I})$ tekrarlanma yapısıdır.

- i) $|\mathcal{P}| = v$.
- ii) $|\mathcal{B}| = v$.
- iii) Her bir nokta k tane blokta bulunur.
- iv) Her blokta k tane nokta bulunur.
- v) Her nokta çifti λ blokta bulunur.
- vi) Her blok çifti λ noktada çıkarılır.

$\lambda = 0$ veya $\lambda = k - 1$ olan dizaynlar trivial (önemsiz) simetrik dizaynlar olarak adlandırılırlar. $n = k - \lambda$ değeri simetrik dizaynın mertebesi olarak adlandırılır.

Örnek 1.3.19. Şekil 2 de verilen 1×1 tipinde küçük karelerden oluşan 4×4 tipinde bir tablo düşünölsün.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Şekil 2. T_7 bloğunun gölgeli olduđu 4×4 formunda kareler dizaynı.

Tablo üzerinde bulunan 16 farklı kare dizaynın noktalarını oluşturur. T_j blođu j noktası hariç j noktasının bulunduđu tüm satır ve tüm sütundaki noktalardan oluşur. Böylece her blok 6 adet kare içerir. Örneğin Şekil 2 de gösterilen kareleri yazacak olursak T_7 blođu 3,5,6,8,11,15 sayılarından oluşur. Benzer şekilde $j \in \{1,2,\dots,16\}$ olmak üzere tüm T_j

blokları bulunabilir. Bu bloklar verilen kurala göre oluşturulduklarında şu şekildedirler:

$$\begin{array}{ll}
T_1 = \{2,3,4,5,9,13\} & T_9 = \{10,11,12,1,5,13\} \\
T_2 = \{1,3,4,6,10,14\} & T_{10} = \{9,11,12,2,6,14\} \\
T_3 = \{1,2,4,7,11,15\} & T_{11} = \{9,10,12,3,7,15\} \\
T_4 = \{1,2,3,8,12,16\} & T_{12} = \{9,10,11,4,8,16\} \\
T_5 = \{6,7,8,1,9,13\} & T_{13} = \{14,15,16,1,5,9\} \\
T_6 = \{5,7,8,2,10,14\} & T_{14} = \{13,15,16,2,6,10\} \\
T_7 = \{5,6,8,3,11,15\} & T_{15} = \{13,14,16,3,7,11\} \\
T_8 = \{5,6,7,4,12,16\} & T_{16} = \{13,14,15,4,8,12\}
\end{array}$$

Sonuç olarak oluşturulan tüm bloklar incelenirse bu yapı formu $(16,6,2)$ simetrik dizaynıdır. (Moore ve Pollatsek, 2013)

Örnek 1.3.15 te gösterilen 2-dizaynı bir simetrik dizayn değildir çünkü nokta ve blok kümeleri farklı büyüklüktedirler.

Simetrik dizaynlarda $b = v$ olduğundan Teorem 1.3.17 den $r = k$ yazılır. Bu durumda simetrik dizaynlarda $r = k$ olduğu için Teorem 1.3.16 yerine aşağıdaki teorem yazılır. Bu teorem aynı zamanda simetrik bir dizaynın parametreleri arasındaki ilişkiyi verir.

Teorem 1.3.20. Simetrik (v, k, λ) -dizaynı için, $(v - 1)\lambda = k(k - 1)$.

İspat: Teoremin ispatı, Teorem 1.3.16 nın ispatı ile aynı şekilde yapılmaktadır.

Tekrarlanma yapıları ve dizaynlar ile ilgili daha fazla bilgi için (Bose, 1939), (Hall ve Ryser, 1951), (Beth vd., 1999), (Jungnickel, 1992) çalışmalarına bakılabilir.

1.4. Fark Kümeleri

1.4.1. Tanım

Bu kısımda sonlu gruplar üzerinde çalışılacaktır. Eğer G , v mertebeli sonlu bir grup ise genellikle G , modülo v toplama işlemi altındaki tam sayılar grubu $\mathbb{Z}_v = \{1, 2, \dots, v-1\}$ olarak tanımlanacaktır.

Tanım 1.4.1. (*Fark Kümesi*) v mertebeli bir G grubunun k elemanlı bir alt kümesi D olsun. $d_i, d_j \in D$ olmak üzere $d_i * d_j^{-1}$ şeklindeki elemanların oluşturduğu çoklu küme Δ , G nin birim elemanından farklı elemanlarının her birini tam λ kez içeriyorsa, bu D alt kümesine, G grubu içindeki bir (v, k, λ) parametrelili fark kümesi denir.

Fark kümesi oluştururken kullanılan gruplar genellikle toplamsal gruplar olduğundan tanım şu şekilde verilebilir: G sonlu bir grup ve $|G| = v$ olsun. $\emptyset \neq D \subseteq G$ ve eleman sayısı $|D| = k$ olmak üzere, $D = \{d_1, d_2, \dots, d_k\}$ olan modülo v deki kalan sınıflarının k tane elemanından oluşsun. $d_i, d_j \in D$, $d_i \neq d_j$ ve $\alpha \in G$, $\alpha \neq 1_G \pmod{v}$ olmak üzere;

$$d_i - d_j \equiv \alpha \pmod{v}$$

kongrüansı tam olarak λ tane (d_i, d_j) çözüm çiftini içerir. Burada çoklu küme Δ :

$$\Delta = \{d_i - d_j \mid d_i, d_j \in D, d_i \neq d_j\}.$$

Bu yapıdaki (v, k, λ) parametre sistemi, $D \subseteq G$ fark kümesini verecektir. G grubu çarpımsal bir grup ise fark kümesi kongrüansı:

$$d_i d_j^{-1} \equiv \alpha \pmod{v}$$

tam olarak λ tane (d_i, d_j) çözüm çiftini içerir. Burada çoklu küme Δ :

$$\Delta = \{d_i d_j^{-1} \mid d_i, d_j \in D, d_i \neq d_j\}.$$

Örnek 1.4.2. $(\mathbb{Z}_{13}, +)$ grubunda $D = \{0,1,3,9\}$ kümesi $(13,4,1)$ parametrelili fark kümesidir. D nin G de bir fark kümesi olup olmadığını kontrol etmek için çalışmayı bir tabloda düzenlemek uygun olur. D kümesindeki elemanların farklarından oluşan çoklu küme tablosu Δ , Tablo 1 de verilmiştir.

Tablo 1. $(\mathbb{Z}_{13}, +)$ grubundaki $D = \{0,1,3,9\}$ fark kümesi için çoklu küme tablosu.

–	0	1	3	9
0	$0-0 \equiv 0 \pmod{13}$	$0-1 \equiv 12 \pmod{13}$	$0-3 \equiv 10 \pmod{13}$	$0-9 \equiv 4 \pmod{13}$
1	$1-0 \equiv 1 \pmod{13}$	$1-1 \equiv 0 \pmod{13}$	$1-3 \equiv 11 \pmod{13}$	$1-9 \equiv 5 \pmod{13}$
3	$3-0 \equiv 3 \pmod{13}$	$3-1 \equiv 2 \pmod{13}$	$3-3 \equiv 0 \pmod{13}$	$3-9 \equiv 7 \pmod{13}$
9	$9-0 \equiv 9 \pmod{13}$	$9-1 \equiv 8 \pmod{13}$	$9-3 \equiv 6 \pmod{13}$	$9-9 \equiv 0 \pmod{13}$

Tablo 1 deki çoklu kümeyi oluşturan farklar modülo 13 te değerlendirilmiştir. $\mathbb{Z}_{13}$ ün birim elmanı $\{0\}$ hariç tüm elemanları, D alt kümesindeki elemanların farklarının alınması ile oluşturulan Δ çoklu kümesinde bir kez temsil edilmiş olup D kümesi $(13,4,1)$ parametrelili fark kümesidir.

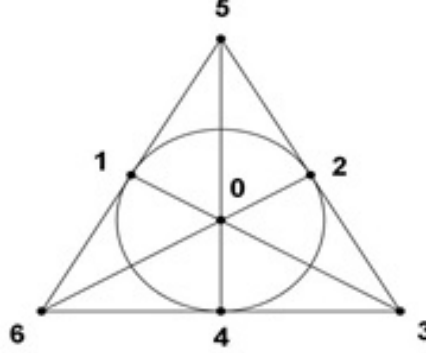
Örnek 1.4.3. $G = \mathbb{Z}_7 = \{0,1,2,3,4,5,6\}$ olmak üzere $(G, +)$ grubunun yedi elemanı noktalar kümesi olarak belirlensin. Bloklar kümesi ise $(\mathbb{Z}_7, +)$ grubunun fark kümesi olan $D = \{1,2,4\}$ kümesinin yedi adet ötelemesinden oluşsun. Yani, $a \in G$ olmak üzere $(a + D) = \{a + 1, a + 2, a + 4\}$ kümesi bloklar kümesi L olarak ele alınsın.

$$L = \{\{1,2,4\}, \{2,3,5\}, \{3,4,6\}, \{4,5,0\}, \{5,6,1\}, \{6,0,2\}, \{0,1,3\}\}$$

G grubu ve bu grubun D fark kümesinin ötelemelerinden oluşan L bloklar kümesi incelendiğinde;

- i) 7 tane nokta vardır, $|G| = 7$.
- ii) 7 tane blok vardır, $|L| = 7$.
- iii) Her bir nokta 3 tane blokta bulunur.
- iv) Her blokta 3 tane nokta bulunur.

- v) Herhangi iki blokta 1 tane ortak nokta bulunur.
- vi) Herhangi iki nokta 1 blokta birlikte bulunur.



Şekil 3. Fano Düzlemi: P noktalar kümesi ve L doğrular kümesi olmak üzere $|P| = 7$ ve $|L| = 7$ olan, her noktasının ve her doğrusunun derecesi 3 olan $S = (P, L)$ lineer uzayı.

Şekil 3 te blokların çoğu doğru olarak temsil edilir, $\{2,4,1\}$ bloğu daire ile temsil edilir. Bloklar doğrular olarak düşünülürse yedi tane doğru vardır, herhangi iki doğru bir ortak nokta bulundurur, her doğru üç noktadan oluşur, her nokta üç doğruya aittir, herhangi iki nokta yalnızca bir doğru üzerinde bulunur. Bu yapı aynı zamanda $(7,3,1)$ simetrik dizaynını oluşturur. Bu örnek (Moore ve Pollatsek, 2013) kaynağından uyarlanmıştır.

Dizaynlarda olduğu gibi, önemli parametreler fark kümeleri ile de ilişkilidir. Bu parametreleri belirtmek için aşağıdaki harfler kullanılır:

- $v = |G|$,
- $k = |D|$,
- λ , G deki birim eleman dışındaki elemanların D deki elemanların farkları olarak tekrarlanma sayısı,
- $n = k - \lambda$ ise fark kümesinin mertebesi olarak bilinir.

Bu parametreler ile birlikte D , (v, k, λ) -fark kümesidir. Fark kümesi tanımının bir sonucu olarak fark kümesinin parametrelerinin birbiri ile ilişkili olduğu görülür. Eğer D kümesi G nin uygun bir alt kümesi ise $0 < k < v$ olduğu açıktır. Ayrıca $\lambda < k$ ve dolayısıyla mertebenin daima pozitif bir sayı olduğu söylenebilir.

Teorem 1.4.4. $D \subset G$ olmak üzere, D bir (v, k, λ) -fark kümesi olsun. Bu durumda parametreler arasında $k(k - 1) = \lambda(v - 1)$ ilişkisi vardır. O zaman, $n = k^2 - \lambda v$ dir.

İspat: Bu teoremin ispatı iki taraflı sayım yapılarak yapılacaktır. Varsayalım ki G toplamsal bir gruptur. Çoklu küme Δ nın tanımı:

$$\Delta = \{d_i - d_j \mid d_i, d_j \in D, d_i \neq d_j\}.$$

Burada $k(k - 1)$ tane birim eleman olmayan fark mevcuttur, bu yüzden $|\Delta| = k(k - 1)$. Aynı zamanda D bir fark kümesi olduğu için G nin birim elemandan farklı $v - 1$ tane elemanı Δ çoklu kümesinde λ kez bulunmalıdır, bu nedenle $|\Delta| = \lambda(v - 1)$. İki taraflı içermelere bakılırsa $k(k - 1) = \lambda(v - 1)$ olur. Ayrıca $n = k^2 - \lambda v$ olduğu biliniyor. Aynı zamanda fark kümesinin parametreleri arasındaki bağıntı $k(k - 1) = \lambda(v - 1)$ olduğundan $k^2 - k = \lambda v - \lambda$ bulunur ve buradan $k^2 - \lambda v = k - \lambda$ ise $n = k^2 - \lambda v$ sonucuna ulaşılır.

Dikkat çekmeye değer ancak çok önemli olmayan birkaç fark kümesi vardır. Tanıma geri dönülürse, D nin G nin uygun bir alt kümesi olduğundan emin olunmalıdır. Dolayısıyla, aşağıdakiler büyük ölçüde göz ardı edilir. Grubunun fark kümesi olan alt kümelerine bakılırsa ilk akla gelenler:

- i) $D = \emptyset$,
- ii) $D = \{0, 1, \dots, v - 1\} = G$,
- iii) $D = \{i\}$, $0 \leq i \leq v - 1$,
- iv) $i \in \{1, 2, \dots, v - 2\}$ olmak üzere $D = \{0, 1, \dots, i - 1, i + 1, \dots, v - 1\}$.

Bu kümelerin parametreleri incelenecek olursa:

- i) $(v, k, \lambda) = (v, 0, 0)$,
- ii) $(v, k, \lambda) = (v, v, v)$,
- iii) $(v, k, \lambda) = (v, 1, 0)$,
- iv) $(v, k, \lambda) = (v, v - 1, v - 2)$.

1.4.2. Hemen Hemen Fark Kümesi

$(G, +)$, v mertebeli toplama işlemi altında bir grup ve D , G nin k elemanlı bir alt kümesi olsun. G deki elemanların t kadarı D nin elemanlarının farkları tarafından λ kez temsil edilirken G nin t tane elemanı ve birim elemanı hariç geriye kalan elemanları ($v - 1 - t$ tane elemanı) $\lambda + 1$ kez temsil edilir. Bu durumda D , (v, k, λ, t) parametrelili hemen hemen fark kümesidir.

Fark kümelerinin parametreleri arasındaki bağıntı kullanılarak, hemen hemen fark kümesi için, $k(k - 1) = \lambda t + (\lambda + 1)(v - 1 - t) = (\lambda + 1)(v - 1) - t$ denklemi yazılır.

Örnek 1.4.5. $(\mathbb{Z}_{13}, +)$ grubu için $D = \{1, 3, 4, 9, 10, 12\}$ alt kümesi $(13, 6, 2, 6)$ parametrelili hemen hemen fark kümesidir. D kümesinin hemen hemen fark kümesi olabilmesi için kümedeki elemanların farkları ile oluşturulan Δ çoklu kümesinde birim eleman $\{0\}$ hariç, $\mathbb{Z}_{13}$ kümesindeki t tane eleman λ kez ve $v - 1 - t$ tane eleman $\lambda + 1$ kez temsil edilmelidir. Bu durumu inceleyebilmek için Δ çoklu kümesini tablo şeklinde yazmak faydalı olacaktır. Verilen grup toplama işlemi altında bir grup olduğu için Δ çoklu kümesi oluşturulurken D kümesindeki elemanların farkları alınacaktır. Alınan bu fark sonuçları modülo 13 te değerlendirilerek yazılacaktır. Tablo oluşturulduktan sonra λ ve t değerleri ortaya çıkar ve verilen kümenin hemen hemen fark kümesi olup olmadığı sonucuna varılır. Bu çoklu küme Tablo 2 de verilmiştir.

Tablo 2 incelendiğinde $D = \{1, 3, 4, 9, 10, 12\}$ kümesinin elemanlarının farkları tarafından $\mathbb{Z}_{13}$ ün $t = 6$ tane elemanı olan 1, 3, 4, 9, 10, 12 sayıları $\lambda = 2$ kez ve $13 - 6 - 1 = 6$ adet elemanı olan 2, 5, 6, 7, 8, 11 sayıları $\lambda + 1 = 3$ kez temsil edilmiştir. Bu nedenden dolayı $D = \{1, 3, 4, 9, 10, 12\}$ alt kümesi $(13, 6, 2, 6)$ parametrelili hemen hemen fark kümesidir.

Tablo 2. $(\mathbb{Z}_{13}, +)$ grubundaki $D = \{1,3,4,9,10,12\}$ hemen hemen fark kümesi için oluşturulan çoklu küme tablosu.

$s \in \mathbb{Z}_{13}/\{0\}$	$\lambda = 2$ Değeri İçin Farklar	$\lambda + 1 = 3$ Değeri İçin Farklar
1	$(4 - 3), (10 - 9)$	-
2	$(1 - 12), (3 - 1)$	$(12 - 10)$
3	$(4 - 1), (12 - 9)$	-
4	$(1 - 10), (3 - 12)$	-
5	$(1 - 9), (4 - 12)$	$(9 - 4)$
6	$(3 - 10), (9 - 3)$	$(10 - 4)$
7	$(3 - 9), (4 - 10)$	$(10 - 3)$
8	$(4 - 9), (9 - 1)$	$(12 - 4)$
9	$(10 - 1), (12 - 3)$	-
10	$(1 - 4), (9 - 12)$	-
11	$(1 - 3), (10 - 12)$	$(12 - 1)$
12	$(3 - 4), (9 - 10)$	-

1.4.3. Kısmi Fark Kümesi

G , v mertebeli toplama işlemi altında bir grup ve D , G nin k elemanlı bir alt kümesi olsun. G nin birim elemanı dışındaki her bir elemanı D nin elemanlarının farklarından oluşan çoklu kümede λ kez temsil edilirken G nin birim eleman ve D den farklı elemanları çoklu kümede μ kez temsil edilir. Bu şartlar altında $D-(v, k, \lambda, \mu)$ kısmi fark kümesidir.

Eğer $\mu = \lambda$ olursa D bir fark kümesi, $\mu = \lambda + 1$ olursa D bir hemen hemen fark kümesi olur.

Örnek 1.4.6. $(\mathbb{Z}_5, +)$ grubu için $D = \{1,4\}$ alt kümesi $(5,2,0,1)$ parametrelili bir kısmi fark kümesidir. Burada $\mathbb{Z}_5$ in D kümesinden ve birim elemandan farklı elemanları $\mathbb{Z}_5/(D \cup \{0\}) = \{2,3\}$, $1 - 4 \equiv 2(\text{mod } 5)$ ve $4 - 1 \equiv 3(\text{mod } 5)$ olarak D alt kümesinin elemanlarının farkı tarafından 1 kez temsil edilmiştir. $\mathbb{Z}_5$ in diğer elemanları 0 kez temsil edildiğinden $\lambda = 0$ ve $\mu = 1$ olup $D-(5,2,0,1)$ kısmi fark kümesidir.

1.4.4. Fark Kümelerinde Öteleme

Bir gruba ait fark kümesi biliniyorsa diğer fark kümeleri bu kümenin ötelemeleri ile elde edilebilir. Bir G grubunda (v, k, λ) parametrelili fark kümesi verilmiş olsun, bu orijinal fark kümesinin elemanlarını grubun elemanları ile öteleyerek yeni fark kümeleri tanımlanabilir.

Tanım 1.4.7. (Öteleme) $D = \{d_1, d_2, \dots, d_k\}$ elemanlarından oluşan bir (v, k, λ) parametrelili fark kümesi ve $s \in \mathbb{Z}$ bir tam sayı olsun. $D + s = \{d_1 + s, d_2 + s, \dots, d_k + s\}$ kümesi modülo v de bir fark kümesidir. Bu fark kümesine orijinal fark kümesi D nin ötelemesi denir.

Bu tanım toplamsal bir grup üzerinden yapılmış olup, eğer grup çarpımsal bir grup ise $Ds = \{d_1s, d_2s, \dots, d_k s\}$ kümesi modülo v de bir fark kümesi ve D nin bir ötelemesi olacaktır.

Örnek 1.4.8. Örnek 1.4.2 den, $\mathbb{Z}_{13}$ deki $D = \{0, 1, 3, 9\}$ kümesinin $(13, 4, 1)$ -fark kümesi olduğu biliniyor. Bu küme ötelenerek başka fark kümeleri elde edilebilir.

- i) $3 + D = \{3, 4, 6, 12\}$
- ii) $5 + D = \{5, 6, 8, 1\}$
- iii) $9 + D = \{9, 10, 12, 5\}$
- iv) $12 + D = \{12, 0, 2, 8\}$

Teorem 1.4.9. D , G değişmeli grubundaki (v, k, λ) -fark kümesi olsun. Bu durumda;

- i) $g \in G$ için gD ve Dg nin her ikisi de (v, k, λ) -fark kümesidir.
- ii) α , G nin bir otomorfizması olsun. O halde, $\alpha(D) = \{\alpha(d) | d \in D\}$, (v, k, λ) -fark kümesidir.

İspat: i) $D \subset G$ ve G bir grup olduğu için $g \in G$ ve $h \in D$ için h yi g ile çarpmak h yi $hg \in G$ ile eşleştirecektir. D bir fark kümesi olduğu için $hg \in G$, D nin elemanları tarafından çarpma işlemine göre tam olarak λ kez temsil edilmelidir. $hd_1, hd_2 \in D$ olmak üzere $hg = (hd_1)(hd_2)^{-1}$ olmalıdır. G değişmeli bir grup olduğu için $(hd_1)(hd_2)^{-1} = d_1d_2^{-1}$ olur. Yani G nin elemanları Dg deki elemanlar tarafından tam

olarak λ kez temsil edilmiş olur. O halde Dg , (v, k, λ) -fark kümesidir. gD için de aynı işlemler yapılarak ispatlanır.

ii) $g, h \in G$ ve $d_1, d_2 \in D$ olmak üzere, D bir fark kümesi olduğundan $gh \in G$ tam olarak λ kez $gh = d_1 d_2^{-1}$ şeklinde yazılır. α , G nin bir otomorfizması olduğu için $\alpha(gh) = \alpha(d_1 d_2^{-1})$ ve $\alpha(gh) = \alpha(d_1) \alpha(d_2)^{-1}$. Buradan $\alpha(gh) \in G$ ve $\alpha(d_1), \alpha(d_2) \in \alpha(D)$ olduğundan $\alpha(D)$, (v, k, λ) -fark kümesidir.

Teorem 1.4.9 çarpımsal bir grup üzerinde yazılmış olup, eğer grup toplamsal ise i maddesinde $g + D$ ve $D + g$ yazılacak ve ii maddesi aynı kalacaktır. İspatı ise aynı şekilde sadece işlem değişikliği ile yapılacaktır.

1.4.5. Fark Kümelerinde Açınım (Development)

G bir grup ve D , G nin (v, k, λ) parametrelili bir fark kümesi olmak üzere bu sistem bir tekrarlanan yapı olarak düşünülebilir. G grubunun elemanları noktalar ve $\forall g \in G$ için D nin $D + g$ ötelemeleri bu yapının blokları olarak alınabilir. Bu dizaynın parametreleri de D fark kümesinin parametreleri ile aynı olacaktır. Aslında aynı parametrelere sahip görünimleri farklı fark kümeleridir.

Tanım 1.4.10. (*Açınım*) $D \subset G$ alt kümesi G grubunun bir fark kümesi olmak üzere, tekrarlanan bir yapının noktalarını G nin elemanları, bloklarını ise D nin G kümesinin elemanları ile ötelemeleri oluşturuyorsa bu tekrarlanan yapıya D nin açınımı denir ve $\text{dev}D$ ile gösterilir.

Teorem 1.4.11. $D \subset G$, (v, k, λ) -fark kümesi olsun. O halde $\text{dev}D$, simetrik (v, k, λ) dizaynıdır.

İspat: Teoremin ispatı için (Moore ve Pollatsek, 2013) kaynağına bakılabilir.

1.4.6. Fark Kümelerinde Denklik

Tanım 1.4.12. (*Denklik*) D_1 ve D_2 , G grubundaki iki fark kümesi olsun. Eğer bazı $g \in G$ ve G nin bir α otomorfizması için $D_2 = g\alpha(D_1)$ oluyorsa D_1 ve D_2 fark kümeleri denktir denir. (Eğer grup toplamsal bir grup ise bu koşul $D_2 = g + \alpha(D_1)$ olarak yazılır.)

Tanımdaki g ve α nın kendi gruplarının birim elemanları olabileceğine dikkat edilmelidir. Aslında, herhangi bir fark kümesi açıkça kendisine denktir. Şimdi daha kullanışlı bir örnek sunulacaktır.

Örnek 1.4.13. Kibler (1978)'e göre $G = \langle a, b | a^4 = b^4 = 1, ab = ba \rangle$ değişmeli grubundaki $(16, 6, 2)$ parametrelili fark kümesi $D_1 = \{1, a, a^2, b, b^3, a^3b^2\}$ dir. G nin bir α otomorfizması $\alpha(a) = b$ ve $\alpha(b) = ab$ olarak tanımlanabilir. Bu durumda G deki bir fark kümesi olan $ab\alpha(D_1) = \{ab, ab^2, ab^3, a^2b^2, 1, a^3b^2\} = D_2$ fark kümesi ile D_1 denktir.

1.4.7. Fark Kümelerinde Tümleyen

Tanım 1.4.14. (*Tümleyen*) D_1 ve D_2 , v mertebeli bir $G = \{0, 1, \dots, v-1\}$ grubunun iki fark kümesi olsun. $D_1 \cup D_2 = \{0, 1, \dots, v-1\} = G$ ise D_1 ve D_2 birbirlerinin tümleyeni olarak adlandırılır.

Eğer D_1 fark kümesinin parametreleri (v, k, λ) ise tümleyeni olan D_2 fark kümesinin parametreleri kolayca hesaplanabilir. D_2 fark kümesinin parametreleri (v', k', λ') olsun. D_2 fark kümesi de G grubundan alındığı için, $v' = v$ ve $k' = v - k$ olur. Bulunan bu değerler Teorem 1.4.4 te bulunan $k(k-1) = \lambda(v-1)$ denkleminde λ' için yazılırsa,

$$\lambda' = \frac{k'(k'-1)}{(v'-1)} = \frac{(v-k)(v-k-1)}{(v-1)} = v - 2k + \lambda$$

bulunur. Bu durumda $(v', k', \lambda') = (v, v - k, v - 2k + \lambda)$ olur.

D_1 fark kümesinin mertebesi olan n aynı zamanda D_2 fark kümesinin de mertebesidir. Yani birbirini tümleyen fark kümelerinin mertebeleri aynıdır. D_1 fark kümesinin mertebesi n ve bunun tümleyeni olan D_2 fark kümesinin mertebesi n' olsun. Bir fark kümesinin parametreleri arasındaki bağıntıdan $n = k - \lambda$ olduğu biliniyor. Bu durumda, $n' = k' - \lambda' = v - k - (v - 2k + \lambda) = k - \lambda$ olduğundan $n' = n$ bulunur.

Birbirinin tümleyeni olan iki fark kümesinin eleman sayıları k ve k' parametreleri $v/2$ değerinden büyük veya küçük olmalıdır. Eğer bu parametrelerden biri $v/2$ olursa diğeri de $v/2$ olacaktır ve bu kümelerin mertebeleri de eşit olduğundan bu λ parametrelerinin de eşit olması anlamına gelir. Ancak birbirini tümleyen iki kümenin λ parametreleri birbirinden farklıdır, o halde tümleyen kümelerden birinin eleman sayısı mutlaka $v/2$ den küçük diğeri ise $v/2$ den büyük olmalıdır.

1.4.8. Fark Kümelerinin Aileleri

Diğer cebirsel yapıların çoğu gibi, fark kümeleri de sınıflandırılabilir. Fark kümelerinin sınıflandırılması aileler aracılığıyla yapılır. Çeşitli sonsuz fark kümesi ailesinin var olduğu bilinmektedir. Bu kısımda fark kümelerinin bazı aileleri tanıtılacak olup örnekler ve teoremler verilecektir.

Tanıtılacak olan ilk aile $p \equiv 3(\text{mod } 4)$ olduğunda $\mathbb{Z}_p$ deki sıfırdan farklı karelerden yani kuadratik rezidülerden oluşan ailedir. Teorem 1.4.15 bu örneğin sonlu cisim $GF(q)$ üzerinde sıfır olmayan karelere genelleştirilebileceğini göstermektedir. Burada elemanların sayısı q , bir asalın kuvvetidir. Teorem 1.4.15 teki fark kümelerine genellikle *Paley fark kümeleri* denir.

Teorem 1.4.15. q bir asalın kuvveti, $q \equiv 3(\text{mod } 4)$ ve G , sonlu cisim $GF(q)$ nun toplamsal grubu olmak üzere D , $GF(q)$ daki sıfırdan farklı karelerin bir kümesi olsun. Bu durumda D , $(q, (q-1)/2, (q-3)/4)$ parametreleriyle bir fark kümesidir.

İspat: Teoremin ispatı için (Moore ve Pollatsek, 2013) kaynağına bakılabilir.

Tanıtılacak olan ikinci aile bu çalışmanın kapsamı için önemli bir aile olan *ikiz asal fark kümesi* ailesidir. Bu fark kümeleri, astronomik olayların görüntülenmesinde kullanılan kodlanmış maskelerin oluşturulması için kullanılan türlerden biridir. İkiz asallar, aralarındaki fark 2 olan asallardır. En küçük ikiz asal $\{3,5\}$ çiftidir. $\mathbb{Z}_3 \oplus \mathbb{Z}_5$ toplamsal grubu en küçük ikiz asal fark kümesinin bulunduğu gruptur. Teorem 1.4.16, p ve $p + 2$ nin asal sayı olması durumunda $G = \mathbb{Z}_p \oplus \mathbb{Z}_{p+2}$ deki fark kümelerinin oluşturulmasına yönelik genel bir prosedürü açıklar.

Teorem 1.4.16. p ve $p + 2$ asal sayı olmak üzere $G = \mathbb{Z}_p \oplus \mathbb{Z}_{p+2}$ olsun. D kümesi, $(a, b) \in G$ ikililerinden oluşan G nin bir alt kümesi olmak üzere;

- i) $D_1 = \{(a, b) | a \in \mathbb{Z}_p, b = 0\}$
- ii) $D_2 = \{(a, b) | a \text{ ve } b \text{ alındıkları cisimde sıfırdan farklı kare olan sayılar}\}$
- iii) $D_3 = \{(a, b) | a \text{ ve } b \text{ alındıkları cisimde kare olmayan sayılar}\}$

Bu şartlar ile oluşturulan $D = D_1 \cup D_2 \cup D_3$ bir fark kümesidir ve $|D| = |D_1| + |D_2| + |D_3|$.

İspat: Teoremin ispatı için (Moore ve Pollatsek, 2013) kaynağına bakılabilir.

İkiz asal grupları ile oluşturulan fark kümelerinin (v, k, λ) parametreleri oluşturulma şekillerinden faydalanılarak bulunabilir. Şöyle ki, p ve $p + 2$ asal sayı olmak üzere $G = \mathbb{Z}_p \oplus \mathbb{Z}_{p+2}$ olsun. Bu grubun eleman sayısı $|G| = v = p(p + 2) = p^2 + 2p$ olacaktır. Fark kümesi D nin eleman sayısı olan k değerini bulmak için Teorem 1.4.16 da oluşturulan D_1, D_2, D_3 kümelerinin eleman sayılarını bularak toplamak gerekir çünkü fark kümesi D , bu üç kümenin bileşiminden oluşmaktadır ve bu kümeler ayrık olduğundan doğrudan eleman sayıları toplamaları fark kümesinin eleman sayısını verecektir. İlk oluşturulan küme olan D_1 kümesi $a \in \mathbb{Z}_p$ ve $b = 0$ olmak üzere (a, b) ikililerinden oluşmaktadır. Bu kümedeki (a, b) ikililerinin sayısı $|D_1| = (p)(1) = p$ tanedir. D_2 kümesi $\mathbb{Z}_p$ ve $\mathbb{Z}_{p+2}$ deki kare olan sayılar tarafından oluşturulan (a, b) ikililerinden oluşmaktadır. $\mathbb{Z}_p$ ve $\mathbb{Z}_{p+2}$ de kare olan sayılar p ve $p + 2$ asal sayı olduğu için bu kümelerdeki kuadratik rezidüler anlamına gelir. Teorem 1.3.7 den $\mathbb{Z}_p$ deki kuadratik rezidü sayısı $(p - 1)/2$ ve $\mathbb{Z}_{p+2}$ deki kuadratik rezidü sayısı $(p + 2 - 1)/2 = (p + 1)/2$ tanedir. O halde bu iki kümeden alınan kuadratik rezidülerin (a, b)

ikililerinden oluşturulan D_2 kümesinin eleman sayısı:

$$|D_2| = \left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right) = \frac{p^2-1}{4}$$

olacaktır. Aynı şekilde D_3 kümesi oluşturulurken $\mathbb{Z}_p$ ve $\mathbb{Z}_{p+2}$ de kare olmayan sayılar p ve $p+2$ asal sayı olduğu için bu kümelerdeki kuadratik rezidü olmayan elemanlar anlamına gelir. Teorem 1.3.7 den bir kümedeki kuadratik rezidü sayısı ile kuadratik rezidü olmayan eleman sayısının birbirine eşit olduğu biliniyor. O halde bu kümelerdeki kuadratik olmayan rezidülerin (a, b) ikililerinden oluşturulan D_3 kümesinin eleman sayısı:

$$|D_3| = \left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right) = \frac{p^2-1}{4}$$

bulunacaktır. Bu durumda fark kümesi D nin eleman sayısı:

$$k = |D_1| + |D_2| + |D_3| = p + \left(\frac{p^2-1}{4}\right) + \left(\frac{p^2-1}{4}\right) = \frac{p^2+2p-1}{2}$$

olur. Elde olan v ve k değeri ile fark kümelerinin parametreleri arasındaki bağıntı olan $k(k-1) = \lambda(v-1)$ denklemi kullanılarak λ değeri hesaplanabilir:

$$\lambda = \frac{k(k-1)}{(v-1)} = \frac{\left(\frac{p^2+2p-1}{2}\right)\left(\frac{p^2+2p-1}{2}-1\right)}{(p^2+2p-1)} = \frac{p^2+2p-3}{4}$$

Sonuç olarak, ikiz asal grupları kullanılarak oluşturulan fark kümesinin parametreleri,

$$(v, k, \lambda) = \left(p^2+2p, \frac{p^2+2p-1}{2}, \frac{p^2+2p-3}{4}\right)$$

bulunur.

Örnek 1.4.17. $G = \mathbb{Z}_3 \oplus \mathbb{Z}_5$ olmak üzere G grubu kullanılarak ikiz asal fark kümesi inşa edilebilir. Burada ikiz asal fark kümesi teoremini kullanmak için öncelikle $\mathbb{Z}_3$ ve $\mathbb{Z}_5$ in kuadratik ve kuadratik olmayan rezidüleri bulunmalıdır.

$\mathbb{Z}_3 = \{0,1,2\}$ ün kuadratik rezidüsü $\{1\}$ kuadratik olmayan rezidüsü $\{2\}$.

$\mathbb{Z}_5 = \{0,1,2,3,4\}$ in kuadratik rezidüleri $\{1,4\}$ kuadratik olmayan rezidüleri $\{2,3\}$.

Teorem 1.4.16 kullanılarak;

i) $D_1 = \{(0,0), (1,0), (2,0)\}$

ii) $D_2 = \{(1,1), (1,4)\}$

iii) $D_3 = \{(2,2), (2,3)\}$

kümeleri oluşturulur. O zaman G grubundaki ikiz asal fark kümesi:

$$D = D_1 \cup D_2 \cup D_3 = \{(0,0), (1,0), (2,0), (1,1), (1,4), (2,2), (2,3)\}.$$

Bu ikiz asal fark kümesinin parametreleri ise $(15, 7, 3)$ olarak bulunur.

Örnek 1.4.18. $G = \mathbb{Z}_5 \oplus \mathbb{Z}_7$ olmak üzere G grubu kullanılarak ikiz asal fark kümesi inşa edilebilir. Burada ikiz asal fark kümesi teoremini kullanmak için öncelikle $\mathbb{Z}_5$ ve $\mathbb{Z}_7$ nin kuadratik ve kuadratik olmayan rezidüleri bulunmalıdır.

$\mathbb{Z}_5 = \{0,1,2,3,4\}$ in kuadratik rezidüleri $\{1,4\}$ kuadratik olmayan rezidüleri $\{2,3\}$.

$\mathbb{Z}_7 = \{0,1,2,3,4,5,6\}$ nin kuadratik rezidüleri $\{1,2,4\}$ kuadratik olmayan rezidüleri $\{3,5,6\}$.

Teorem 1.4.16 kullanılarak,

i) $D_1 = \{(0,0), (1,0), (2,0), (3,0), (4,0)\}$

ii) $D_2 = \{(1,1), (1,2), (1,4), (4,1), (4,2), (4,4)\}$

iii) $D_3 = \{(2,3), (2,5), (2,6), (3,3), (3,5), (3,6)\}$

kümeleri oluşturulur. O zaman G grubundaki ikiz asal fark kümesi $D = D_1 \cup D_2 \cup D_3$ olduğundan,

$$D = \{(0,0), (1,0), (2,0), (3,0), (4,0), (1,1), (1,2), (1,4), (4,1), (4,2), (4,4), (2,3), (2,5), (2,6), (3,3), (3,5), (3,6)\}.$$

Bu ikiz asal fark kümesinin parametreleri ise $(35, 17, 8)$ olarak bulunur.

Bazı $\mathbb{Z}_p$ gruplarındaki elemanların dördüncü kuvvetleri kullanılarak iki farklı fark kümesi ailesi, Teorem 1.4.19 ve Teorem 1.4.20 kullanılarak oluşturulabilir.

Teorem 1.4.19. $p = 4x^2 + 1$ formunda bir asal sayı olmak üzere, x tek tamsayı ve $G = \mathbb{Z}_p$ olsun. O zaman G deki elemanların sıfır hariç tüm dördüncü kuvvetleri kümesi olan D bir fark kümesidir.

İspat: Teoremin ispatı için (Lehmer, 1953) kaynağına bakılabilir.

Teorem 1.4.20. $p = 4x^2 + 9$ formunda bir asal sayı olmak üzere, x tek tam sayı ve $G = \mathbb{Z}_p$ olsun. O zaman G deki elemanların sıfır dahil tüm dördüncü kuvvetleri kümesi olan D bir fark kümesidir.

İspat: Teoremin ispatı için (Lehmer, 1953) kaynağına bakılabilir.

Bu çalışma için önemli olan bir diğer aile Hadamard fark kümeleri ailesidir. Sonrasında birkaç aileden kısaca bahsedilecektir.

Hadamard fark kümesi ailesi, $t \in \mathbb{Z}^+$ olmak üzere mertebesi $v = 4t - 1$ olan devirli değişmeli gruplar üzerinde tanımlanmıştır. $t \in \{0, 1, \dots, v - 1\}$ olmak üzere $(v, k, \lambda) = (4t - 1, 2t - 1, t - 1)$ parametrelerine sahip fark kümeleridir.

Singer fark kümesi ailesi, Singer (1938)'ın makalesinde keşfettiği devirli fark kümeleri ailesi olarak bilinir. Devirli gruplar üzerinde tanımlıdır. Singer fark kümelerinin parametreleri:

$$v = \frac{q^{m+1} - 1}{q - 1}, \quad k = \frac{q^m - 1}{q - 1}, \quad \lambda = \frac{q^{m-1} - 1}{q - 1}$$

şeklindedir. Bu parametrelerde q herhangi bir asal sayı ve $m > 1$ dir.

McFarland fark kümesi ailesi, McFarland (1973)'ın makalesinde, devirli ve değişmeli olmayan gruplar üzerinde tanımlanmıştır. Bu makalede McFarland aşağıda sunulan parametrelerle fark kümeleri oluşturmuştur:

$$v = q^{s+1} \left(\frac{q^{s+1} - 1}{q - 1} + 1 \right), \quad k = q^s \left(\frac{q^{s+1} - 1}{q - 1} \right), \quad \lambda = q^s \left(\frac{q^s - 1}{q - 1} \right)$$

q bir asal sayı olmak üzere $\mathbb{F} = GF(q)$ cismi üzerinde $s + 1$ boyutlu V vektör uzayı ile bir fark kümesi yaratılır, burada s pozitif tamsayıdır. (McFarland, 1973)

1.5. Varlık Problemi ve Bruck-Ryser-Chowla Teoremi

Bruck-Ryser-Chowla (BRC) Teoremi, fark kümelerinin belirli parametreler ile var olamayacağını kanıtlamanın en önemli araçlarından biridir. BRC Teoremi (v, k, λ) parametrelili simetrik dizaynın varlığı için (v, k, λ) parametreleri ve buna bağlı olarak belirlenen mertebe olan n değeri üzerinde gerekli olan koşulları verir. Teorem 1.4.11 den bilindiği üzere bir fark kümesinin açılımı fark kümesi ile aynı parametrelere sahip simetrik bir dizayndır, dolayısıyla bu teorem v mertebeli bir G grubundan alınan fark kümesinin (v, k, λ) parametrelerine kısıtlamalar getirir. Fark kümelerinin varlık problemi için BRC Teoremi kullanılırken lineer cebir ve sayılar teorisinden faydalanılır. Bir fark kümesinin varlığı için önce parametrelerin $k(k - 1) = \lambda(v - 1)$ denklemini sağlaması gerekir, sonrasında varlık için BRC Teoremi kullanılır.

Teorem 1.5.1. (*Bruck-Ryser-Chowla Teoremi*) Varsayalım ki v mertebeli bir G grubunda (v, k, λ) -simetrik dizaynı vardır. O zaman:

- i) Eğer v çift tamsayı ise $n = k - \lambda$ bir tamkaredir.
- ii) Eğer v tek tamsayı ise $x^2 = ny^2 + (-1)^{(v-1)/2} \lambda z^2$ diophant denkleminin x, y, z tamsayılarında sıfırdan farklı bir çözümü vardır.

İspat: Teoremin ispatı için (Ryser, 1982) kaynağına bakılabilir.

Örnek 1.5.2. $(22,7,2)$ parametreleri incelenecek olursa; $k(k-1) = \lambda(v-1)$ şartını bu parametreler sağlar. BRC Teoremi'ne göre $v = 22$ çift sayı olduğundan simetrik dizaynın varlığı için $n = k - \lambda$ bir tamkare olmalıdır, ancak $n = 7 - 2 = 5$ bir tamkare olmadığı için $(22,7,2)$ parametreleri ile bir simetrik dizayn yoktur ve bu nedenle bu parametrelere sahip bir fark kümesi yoktur.

Örnek 1.5.3. $(49,16,5)$ parametreleri incelenecek olursa; fark kümesinin varlığı veya bu parametrelere sahip simetrik bir dizayn için, 49 tek sayı olduğundan, $x^2 = 11y^2 + 5z^2$ denkleminin sıfırdan farklı bir tamsayı çözümüne sahip olması gerekir. Böyle bir çözüm $(x, y, z) = (4, 1, 1)$ tarafından sağlanır bu nedenle BRC Teoremi bu parametrelere sahip bir fark kümesi bulunması olasılığını ekarte edemez.

Örnek 1.5.3 te bulunan diophant denklemi için sıfır olmayan bir çözümün bulunması nispeten kolaydır. Ancak bir diophant denkleminin sıfır olmayan bir çözümünün olmadığını göstermek daha zordur. Çözümlerin varlığının tespiti için Legendre Teoremi tanımlanacaktır. Teoremde bulunan $s \mathcal{R} t$ sembolü, s nin modülo $|t|$ de bir kare olduğu anlamına gelir.

Teorem 1.5.4. (*Legendre Teoremi, 1785*) a ve b sıfırdan farklı, en az biri tamkare olmayan tamsayı ve $d = \text{ebob}(a, b)$ olsun. Bu durumda aşağıdaki koşullar sağlanıyorsa $x^2 = ay^2 + bz^2$ denkleminin sıfırdan farklı bir çözümü vardır.

- i) $a \mathcal{R} b$,
- ii) $b \mathcal{R} a$,
- iii) $-(ab/d^2) \mathcal{R} d$.

İspat: Teoremin ispatı için (Ireland ve Rosen, 1982) kaynağına bakılabilir.

Örnek 1.5.5. $(43,15,5)$ parametreleri incelenecek olursa; bu parametreler ile bir fark kümesinin var olabilmesi için BRC Teoremi'ne göre $v = 43$ tek sayı olduğu için $x^2 = 10y^2 - 5z^2$ diophant denkleminin sıfırdan farklı bir çözümü bulunmalıdır. Legendre Teoremi kullanılarak çözümün varlığı kontrol edilebilir. Bu denklemde $a = 10$, $b = -5$ ve $d = \text{obeb}(10, -5) = 5$. Burada $-(ab/d^2) = 2$ sayısı modülo 5 için bir kare değildir. Bu nedenle $x^2 = 10y^2 - 5z^2$ denklemi için sıfırdan farklı bir çözüm yoktur. $(43,15,5)$

parametreleri ile simetrik bir dizaynın olmadığı ve bu nedenle bu parametrelerle herhangi bir fark kümesi olmadığı sonucuna varılır.

Örnek 1.5.6. $n = 10$ mertebeli projektif bir düzlem varsa, $(n^2 + n + 1, n + 1, 1) = (111, 11, 1)$ parametreleri ile simetrik bir dizayn var olmalıdır. Lam tarafından 1989'da 10 mertebeli bir projektif düzlemin mevcut olmadığı kanıtlanmıştır (Lam vd., 1989; Lam, 1991). Bununla birlikte, $(111, 11, 1)$ parametreleri BRC testini geçer. Şöyle ki $v = 111$ tek ve $x^2 = 10y^2 - z^2$ diophant denklemi $(x, y, z) = (1, 1, 3)$ noktalarında bir çözüme sahiptir. Bu yüzden, BRC teoremi, 10 mertebeli bir projektif düzlemin varlığını dışlamaz. Ancak, 10 mertebeli projektif bir düzlem olmadığı için, bu örnek BRC testini geçmenin simetrik bir dizaynın varlığını garanti etmek için yeterli olmadığını gösterir.

Konu ile ilgili daha fazla bilgi için (Bruck ve Ryser, 1949), (Chowla ve Ryser 1950), (Ryser, 1982) kaynaklarına bakılabilir.

1.6. Fark Kümelerinin Uygulamaları

Fark kümeleri, sayılar teorisi, kombinatorik, grup teorisi ve dizayn teorisinin kesişim noktası olduğundan, fark kümelerinin birçok alanda uygulaması bulunur. En sık olarak, optik hizalama, iletişimde sinyal gürültüsünün varlığı durumunda sinyallerin doğru yorumlanması, astronomik olayların görüntülenmesi, hata düzeltme kodlarının oluşturulması, kuantum bilişiminde süreçlerin kolaylaştırılması ile verilerin kodlanması ve deşifre edilmesi gibi uygulama alanlarında kullanılmaktadır. Bahsedilen uygulama alanlarından optik hizalamada, iletişimde sinyal gürültüsü varlığında sinyallerin doğru yorumlanmasında ve astronomik olayların görüntülenmesinde iyi otokorelasyon özelliklerine sahip devirli fark kümeleri ve ikili diziler arasındaki ilişkiden yararlanılır. Fark kümeleri aracılığıyla iyi otokorelasyon özelliklerine sahip ikili diziler oluşturulabilir. Diğer uygulamalarda kullanılan fark kümelerinin rolleri oldukça farklıdır.

1.6.1. İkili Diziler ve Korelasyon

v periyotlu bir ikili dizi $\mathbf{a} = (a_0, a_1, \dots, a_{v-1})$, bir v çoklusudur. a_j değişkenlerinin tamamı $\{-1, +1\}$ kümesinden ya da $\{0, 1\}$ kümesinden seçilir. Periyot kelimesinin kullanılması, $\mathbf{a}$ sonlu dizisinin tekrarlayarak sonsuz bir periyodik diziye genişlemesi nedeniyledir.

İncelenecek olan ilk uygulama olan “sinyal gürültüsünün varlığı durumunda sinyallerin doğru yorumlanması” için her sinyalin, ± 1 girişli v periyotlu ikili dizi olduğu bir sinyal kaynağı ele alınsın. Bu sinyallerin, gürültülü (parazitli) bir kanal üzerinden iletildiği varsayılınsın. Gönderilen sinyal verileri bir sinyal gürültü oranına sahip olacaktır, yani veri iletilirken problem çıkacaktır. Sinyal alındığında, alıcı doğru sinyalin alındığından emin olmak zorundadır. Alıcı gelen sinyalleri, sinyalin ideal modeli ile karşılaştırarak bunu yapabilir. Başka bir deyişle alıcı alınan sinyallerin her biri ile ideal sinyal modeli arasındaki korelasyonu hesaplayarak ve bu korelasyonlar arasından en yüksek değere sahip olanını seçerek bunu yapabilir.

Tanım 1.6.1. (Korelasyon) $a_j, b_j \in \{0, 1\}$ veya $a_j, b_j \in \{-1, +1\}$ olmak üzere $\mathbf{a} = (a_0, a_1, \dots, a_{v-1})$ ve $\mathbf{b} = (b_0, b_1, \dots, b_{v-1})$, v periyotlu iki tane ikili dizi olsun. Bu durumda $C(\mathbf{a}, \mathbf{b})$ korelasyonu, şu şekilde tanımlanır:

$$C(\mathbf{a}, \mathbf{b}) = \frac{1}{v} \sum_{j=0}^{v-1} a_j b_j.$$

Temel olarak $a_j, b_j \in \{-1, +1\}$ kullanılırsa $C(\mathbf{a}, \mathbf{b}) = (A - D)/(A + D)$ olacaktır. Burada A , $\mathbf{a}$ ve $\mathbf{b}$ nin aynı yönde olduğu pozisyonları, D ise zıt yönde olduğu pozisyonları temsil eder. Bu durum $\mathbb{R}^v$ vektör uzayında standart korelasyon ile iyi bir şekilde ilişkilidir:

- Tüm $\mathbf{a}$ ve $\mathbf{b}$ ler için, $-1 \leq C(\mathbf{a}, \mathbf{b}) \leq 1$.
- Eğer $\mathbf{a}=\mathbf{b}$ ise, $C(\mathbf{a}, \mathbf{b}) = 1$.
- Eğer $\mathbf{a}$ ve $\mathbf{b}$ her pozisyonunda zıt yönlü ise, $C(\mathbf{a}, \mathbf{b}) = -1$.
- Eğer v çift ve $\mathbf{a}$ ile $\mathbf{b}$ pozisyonların tam yarısında aynı yönlü ise $C(\mathbf{a}, \mathbf{b}) = 0$.

Örnek 1.6.2. $\mathbf{a} = (1, 1, -1, 1, -1)$ ve $\mathbf{b} = (-1, 1, -1, 1, 1)$ olmak üzere $\mathbf{a}$ ile $\mathbf{b}$ arasındaki korelasyon;

$$C(\mathbf{a}, \mathbf{b}) = \frac{A - D}{A + D} = \frac{3 - 2}{3 + 2} = \frac{1}{5}$$

bulunur.

Özel bir $D \subseteq \mathbb{Z}_v = \{0, 1, \dots, v-1\}$ fark kümesi ile bir $\mathbf{a} = (a_0, a_1, \dots, a_{v-1})$ ikili dizisi tanımlanabilir. $a_j \in \{-1, +1\}$ kullanılarak bu ikili dizi tanımlanırken $j \in D$ ise $a_j = 1$ ve $j \notin D$ ise $a_j = -1$ değerini alır.

Şimdi kaynak sinyali $\mathbf{a} = (a_0, a_1, \dots, a_{v-1})$ ve kopya sinyali (yani $\mathbf{a}$ nın devirli ötelemeleri) $t \in \{1, 2, \dots, v-1\}$ için $\mathbf{a}_t = (a_t, a_{t+1}, \dots, a_{t+v-1})$ tanımlanabilir. Buradaki $\{t, t+1, \dots, t+v-1\}$ değerleri modülo v de yorumlanır.

D nin birbirinden farklı v tane ötelemesi dev D nin bloklarıdır, bu nedenle $\mathbf{a}_t$ devirli ötelemelerinin de birbirinden farklı olduğu sonucu ortaya çıkar.

Örnek 1.6.3. $(\mathbb{Z}_{13}, +)$ grubundaki $(13, 4, 1)$ parametrelili $D = \{0, 1, 3, 9\}$ fark kümesi ikili bir dizi olarak ifade edilebilir. Bu fark kümesi $\mathbf{a}$ ikili dizisi ile aşağıdaki şekilde tanımlanır:

$$\begin{aligned} \mathbf{a} &= (a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, a_{12}) \\ &= (1, 1, -1, 1, -1, -1, -1, -1, -1, 1, -1, -1, -1). \end{aligned}$$

Fark kümelerinin ikili diziler kullanılarak ifade edilmesinin altında bir neden vardır. Bu nedeni açıklamak için, bir ikili dizi ve onun ötelemeleri arasındaki korelasyon için bir sonraki tanımlama yapılacaktır.

Tanım 1.6.4. (Periyodik Otokorelasyon Fonksiyonu) $\mathbf{a} = (a_0, a_1, \dots, a_{v-1})$ v periyotlu bir ikili dizi olsun. $\mathbf{a}$ nın periyodik otokorelasyon fonksiyonu $C_{\mathbf{a}}(t)$, $t \in \{0, 1, 2, \dots, v-1\}$ olmak üzere şu şekilde tanımlanır:

$$C_{\mathbf{a}}(t) = \frac{1}{v} \sum_{j=0}^{v-1} a_j a_{j+t}$$

$t \neq 0$ için $C_{\mathbf{a}}(t)$ nin bu değerleri *tepe noktası dışındaki korelasyonlar* olarak tanımlanır.

Örnek 1.6.5. $G = \mathbb{Z}_{13}$ grubundaki $(13, 4, 1)$ parametrelili $D = \{0, 1, 3, 9\}$ fark kümesinin ikili dizisi kullanılarak $t = 2$ ötelemesine denk gelen dizi arasındaki periyodik otokorelasyon hesaplanabilir. $D = \{0, 1, 3, 9\}$ fark kümesine karşılık gelen ikili dizi $\mathbf{a} = \mathbf{a}_0 = (1, 1, -1, 1, -1, -1, -1, -1, -1, 1, -1, -1, -1)$ olur ve bu dizinin $t = 2$ ötelemesine denk gelen dizi $\mathbf{a}_2 = (-1, 1, -1, -1, -1, -1, -1, 1, -1, -1, -1, 1, 1)$ olacaktır. Bu $\mathbf{a}$ dizisinin $t = 2$ ötelemesi için periyodik otokorelasyonu:

$$\begin{aligned} C_{\mathbf{a}}(t) &= \frac{1}{v} \sum_{j=0}^{v-1} a_j a_{j+t} = \frac{1}{13} [-1 + 1 + 1 - 1 + 1 + 1 + 1 - 1 + 1 - 1 + 1 - 1 - 1] \\ &= \frac{1}{13} \end{aligned}$$

Periyodik otokorelasyon, bir fark kümesinin ikili dizisi ile fark kümesinin ötelemeleri tarafından oluşturulan ikili dizileri kıyaslamak için kullanışlı bir yöntem verir.

$$C_{\mathbf{a}}(0) = \frac{1}{v} \sum_{j=0}^{v-1} a_j a_j = \frac{1}{v} v = 1$$

bunlardan biridir. Burada orijinal fark kümesinin ikili dizisinin $t = 0$ ötelemesi (kendisi) ile otokorelasyonu 1 dir, yani tam uyumluluk söz konusudur. Fark kümelerinin kullanımı konusuna giriş yapılırken bahsedilen iletişim örneğine tekrar dönülecek olursa, orijinal sinyal verisi orijinal fark kümesinin ikili dizisidir, kopya sinyaller ise fark kümesi ikili dizisinin ötelemeleridir. $C_{\mathbf{a}}(0) = 1$ olduğundan, sinyalin kendisi ile olan otokorelasyonu

1 olacaktır. Bu orijinal kaynağı ve kopyalarını ayırt etmeye olanak sağlar.

Ötelenmiş ikili diziler özellikle, tepe noktası dışındaki korelasyonların mutlak büyüklüklerinin hepsi küçük ya da sıfıra yakın olduğunda, sinyal kaynakları olarak daha faydalıdır.

Teorem 1.6.6. $v \leq 2$ ve $0 < k < v$ olmak üzere v ve k tam sayıları seçilsin. a_j girişleri $\{-1, +1\}$ kümesinden olmak üzere $\mathbf{a}$, v periyotlu bir ikili dizi ve bu dizide tam olarak k tane giriş $+1$ değerine eşit olsun. Varsayalım ki $0 < t < v$ için $C_{\mathbf{a}}(0) = b$ ve $C_{\mathbf{a}}(t) = c$ olacak şekilde iki sayı b ve c olsun. $D = \{j \in \mathbb{Z}_v \mid a_j = +1\}$ olsun. O zaman D bir (v, k, λ) parametrelili fark kümesidir, $b = 1$ ve $n = k - \lambda$ için $c = (v - 4n)/v$ dir. Dahası her devirli fark kümesi bu şekilde ortaya çıkar.

İspat: Teoremin ispatı için (Jungnickel ve Pott, 1999) kaynağına bakılabilir.

Teorem 1.6.6 ayrıca a_j girişleri $\{0,1\}$ kümesinden olan diziler için de geçerlidir, ancak bu durumda b ve c değerleri farklı olacaktır.

Devirli fark kümelerinden elde edilen ikili diziler birçok güzel özelliğe sahiptir. $p \equiv 3 \pmod{4}$ için $\mathbb{Z}_p$ de sıfır olmayan karelerden gelen dizilerin $+1$ değerine eşit $(v-1)/2$ tane girişi ve -1 değerine eşit $(v+1)/2$ tane girişi vardır. Neredeyse eşit olan $+1$ ve -1 lerin dengesi, ikili dizileri rastgele dizilere benzer kılar. “Sözde rastgele (pseudo-random)” dizisi için başka bir özellik istenir, bir alt dizinin bilinmesi tam dizi hakkında çok az bilgi verir. Özellikle, $v = 2^m - 1$ ise, m uzunluğundaki $2^m - 1$ tane ardışık alt dizilerinin hepsinin farklı olması istenir.

Örnek 1.6.7. $\{1,2,4\} \subset \mathbb{Z}_7$ fark kümesi göz önüne alınsın. Bu fark kümesi $(-1, +1, +1, -1, +1, -1, -1)$ dizisini verir. $v = 7 = 2^3 - 1$ ve bu dizinin uzunluğu 3 olan 7 alt dizisi şunlardır: $(-1, +1, +1)$, $(+1, +1, -1)$, $(+1, -1, +1)$, $(-1, +1, -1)$, $(+1, -1, -1)$, $(-1, -1, -1)$, $(-1, -1, +1)$. Bu üçlülerin hepsi farklıdır.

İkili diziler ve korelasyon başlığı altında verilen bilgiler ağırlıklı olarak (Golomb, 1999) kaynağına dayanmaktadır. (Golomb, 1999) kaynağında konu ile ilgili kapsamlı bilgiler mevcuttur. Ayrıca konu ile ilgili olan (MacWilliams ve Sloane, 1976) makalesine bakılabilir.

1.6.2. Kodlanmış Maske İle Görüntüleme

Tanım 1.6.8. (*Kodlanmış Maske*) Kodlanmış maskeler veya kodlu açıklık maskeleri çeşitli ışık dalga boylarına opak olan ızgaralar veya ağırlardır. Bu dalga boyları genellikle X ışınları ve gama ışınları gibi yüksek enerjili radyasyonlardır. Kodlanmış bir maske ile ışık bilinen bir düzende bloke edilerek, kodlanmış bir gölge bir dedektör düzlemi üzerine dökülür.

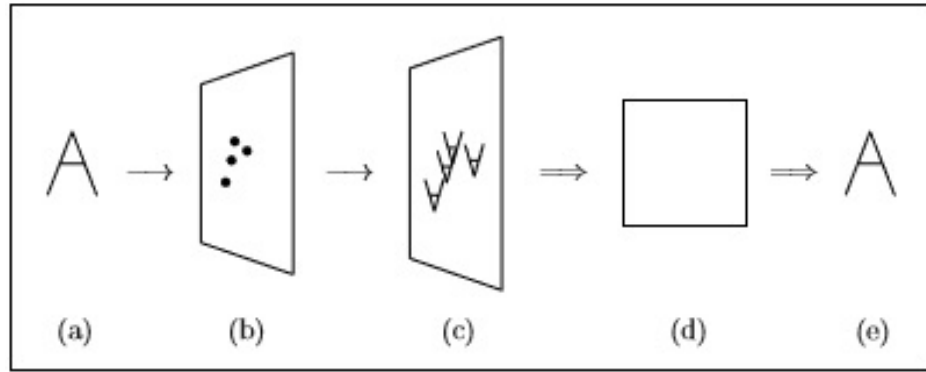
Gökbilimciler yüksek enerjili radyasyonları incelerken, radyasyonun dünya atmosferi tarafından engellenmesini önlemek için uydulara monte edilen aletler ile inceleme yaparlar. Gezegenin yüzeyindeki teleskopların aksine, bilim insanları yüksek enerjili olayları izlemek ve görüntülerini (uzak galaksilerden gelen gama ışını patlamaları gibi) iletmek için sıradan mercek kullanımına güvenemezler. Bunun yerine röntgen çekimindeki gibi, hastanın bir radyasyon kaynağı ve radyasyona duyarlı bir dedektör arasına konumlandırıldığı X ışınları ile tıbbi görüntülemenin elde edilmesine benzer bir yol kullanırlar. Bu yöntemde vücudun X ışınlarını emen kısmı dedektöre gölge düşürür ve radyologlar bu gölge görüntüsünü insan vücudu ile ilgili çıkarımlar yapmak için yorumlarlar.

Astronomik araştırmalardaki görüntüleme için bu durum kaynak ile dedektör arasına radyasyonu emen bir maske koymaktır. Sonrasında bilgisayar kaynağın görüntüsünü yeniden oluşturmak için, maske aracılığıyla dedektöre gelen verileri kullanır.

En basit maske iğne deliği kamera gibi tek bir deliğe sahiptir. Bu maskenin kullanımında nesnenin ters çevrilmiş bir görüntüsü elde edilir. Delik ne kadar küçük olursa görüntü o kadar net olur. Bununla birlikte delik çok küçük olursa sadece birkaç tane yüksek enerjili ışın geçecektir. Daha da kötüsü uzak bir kaynaktan gelen ve delikten

geçen ışınların sayısı, kozmik ışınların ürettiği arka plandaki gürültüye (parazite) nazaran çok küçük olacaktır. Bilim ve mühendislik dilinde “sinyal gürültü oranı” çok düşüktür. Çok fazla arka plan gürültüsü olduğunda aranan görüntü belirlenemez. Bu nedenle bilim insanları tek delikli bir maske kullanmazlar.

Açık bir çözüm çok delikli bir maske kullanmaktır, fakat bu durumda da her delik kendi görüntüsünü oluşturacağı için dedektör üzerinde çakışan çoklu görüntüler oluşacaktır. Eğer maskedeki delikler doğru konumlandırılırsa (kodlanırsa), böylece kaynağın tek bir net görüntüsü dedektördeki çoklu görüntüler arasından seçilebilir. Şekil 4 te yüksek enerjili radyasyonların sinyal kaynağı için kodlanmış maske cihazının kullanımının nasıl olduğu şematik olarak gösterilmektedir.



Şekil 4. Kodlanmış maske kullanarak görüntüleme için şema. (a) görüntü kaynağı, (b) filtre (buradaki noktalar delikler), (c) filtreden gelen görüntü, (d) görüntüyü yeniden oluşturmak için kullanılan yazılım, (e) yeniden oluşturulmuş görüntü (Moore ve Pollatsek, 2013).

Kullanılacak olan maskenin iyi kodlanmış olması için, maske tarafından dökülen gölgenin değiştirilmiş herhangi bir versiyonu ile aralarında zayıf bir eşleme olmalıdır. Yani kodlanmış maske, ötelenmiş kendi versiyonları ile düşük korelasyonlu bir delik düzenine sahip olmalıdır. Bu durum fark kümelerinden tanıdık gelebilir. O halde devirli fark kümeleri kullanılarak kodlanmış maske oluşturulması mümkün olabilir. Ancak bir doğrudaki delikler dizisinden dikdörtgen biçimli delikler dizisi oluşturulmalı ve gerekli olan otokorelasyon özellikleri korunmalıdır.

Bu şekilde bir kodlanmış bir maske oluşturmak için fark kümesi kullanmanın bir yöntemi $\mathbb{Z}_p \oplus \mathbb{Z}_{p+2}$ deki ikiz asal fark kümesini kullanmaktır. Teorem 1.4.16 yı

kullanarak bir fark kümesi oluşturulabilir ve bu fark kümesinin ikili dizisi oluşturulurken dizinin girişleri olan a_j elemanları $\{-1, +1\}$ kümesinden seçilir. Örnek 1.4.17 de bulunan fark kümesi için bir kodlanmış maske oluşturulabilir. Şekil 5 bu tür bir maskeyi göstermektedir.

(0,0)	(0,1)	(0,2)	(0,3)	(0,4)
(1,0)	(1,1)	(1,2)	(1,3)	(1,4)
(2,0)	(2,1)	(2,2)	(2,3)	(2,4)

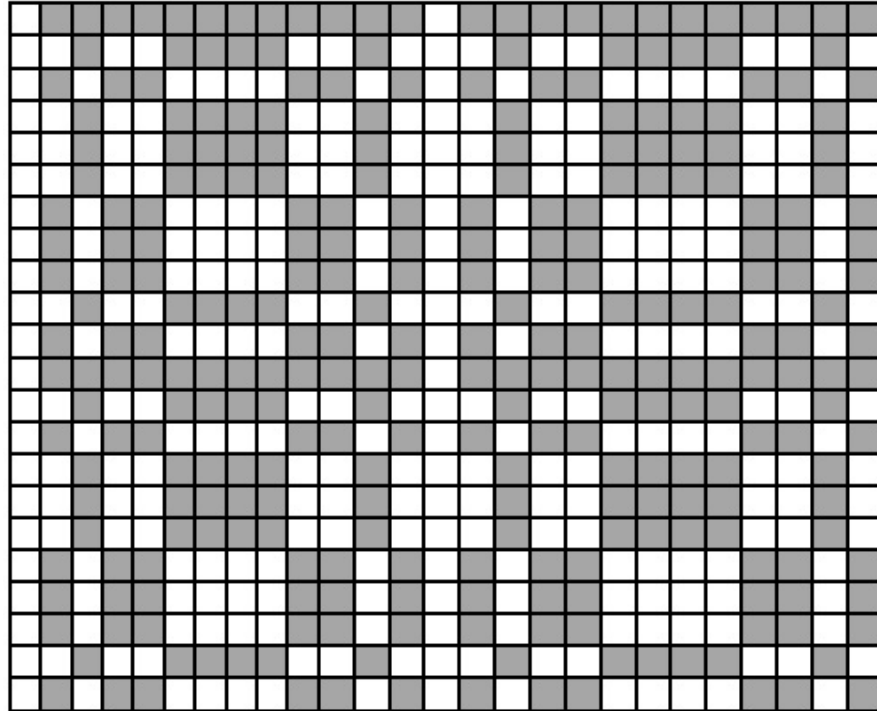
Şekil 5. $\mathbb{Z}_3 \oplus \mathbb{Z}_5$ ikiz asal grubundaki $(15,7,3)$ parametrelili fark kümesi için oluşturulan bir şablon maske. Beyaz bölge $+1$ değerini, gri bölge -1 değerini belirtir.

Şekil 5 te $\mathbb{Z}_3 \oplus \mathbb{Z}_5$ in elemanları dikdörtgen bir dizinde düzenlenmiştir. Satırlar $\mathbb{Z}_3$ ün elemanları tarafından, sütunlar ise $\mathbb{Z}_5$ in elemanları tarafından dizin oluşturur. Şekil 5 te fark kümesinde bulunmayan elemanlar gölgelidir. Diziyi bir hücre tarafından yatay olarak ötelemek her elemana $(1,0)$ eklemek, aynı şekilde dikey olarak kaydırmanın her elemana $(0,1)$ eklemek olduğu görülebilir. Böylece istenen otokorelasyon özelliği korunabilir.

Gerçekçi bir şekilde iyi bir kodlama maskesi oluşturmak için ikiz asalların daha büyük bir kümesi gereklidir. Bir maske, yeterli ışık sızması için genellikle tam bir filtre formu ile çok küçük oluşturulur. Daha sonra bu orijinal maske kopyalanarak çoğaltılır ve orijinal 1×1 maske şablon olarak kullanılarak bir $n \times n$ ağı oluşturmak için yan yana ve alt alta yerleştirilir. Şekil 6 da $\mathbb{Z}_{11} \oplus \mathbb{Z}_{13}$ ikiz asal grubundaki $(143,71,35)$ parametrelili fark kümesi kullanılarak oluşturulmuş olan 1×1 maske şablonu görülebilir. Şekil 7 de ise bu tek maske şablonu kullanılarak bir kodlanmış maske oluşturan 4×4 maskesi görülebilir.

(0,0)	(0,1)	(0,2)	(0,3)	(0,4)	(0,5)	(0,6)	(0,7)	(0,8)	(0,9)	(0,10)	(0,11)	(0,12)
(1,0)	(1,1)	(1,2)	(1,3)	(1,4)	(1,5)	(1,6)	(1,7)	(1,8)	(1,9)	(1,10)	(1,11)	(1,12)
(2,0)	(2,1)	(2,2)	(2,3)	(2,4)	(2,5)	(2,6)	(2,7)	(2,8)	(2,9)	(2,10)	(2,11)	(2,12)
(3,0)	(3,1)	(3,2)	(3,3)	(3,4)	(3,5)	(3,6)	(3,7)	(3,8)	(3,9)	(3,10)	(3,11)	(3,12)
(4,0)	(4,1)	(4,2)	(4,3)	(4,4)	(4,5)	(4,6)	(4,7)	(4,8)	(4,9)	(4,10)	(4,11)	(4,12)
(5,0)	(5,1)	(5,2)	(5,3)	(5,4)	(5,5)	(5,6)	(5,7)	(5,8)	(5,9)	(5,10)	(5,11)	(5,12)
(6,0)	(6,1)	(6,2)	(6,3)	(6,4)	(6,5)	(6,6)	(6,7)	(6,8)	(6,9)	(6,10)	(6,11)	(6,12)
(7,0)	(7,1)	(7,2)	(7,3)	(7,4)	(7,5)	(7,6)	(7,7)	(7,8)	(7,9)	(7,10)	(7,11)	(7,12)
(8,0)	(8,1)	(8,2)	(8,3)	(8,4)	(8,5)	(8,6)	(8,7)	(8,8)	(8,9)	(8,10)	(8,11)	(8,12)
(9,0)	(9,1)	(9,2)	(9,3)	(9,4)	(9,5)	(9,6)	(9,7)	(9,8)	(9,9)	(9,10)	(9,11)	(9,12)
(10,0)	(10,1)	(10,2)	(10,3)	(10,4)	(10,5)	(10,6)	(10,7)	(10,8)	(10,9)	(10,10)	(10,11)	(10,12)

Şekil 6. $\mathbb{Z}_{11} \oplus \mathbb{Z}_{13}$ ikiz asal grubundaki (143,71,35) parametrelili fark kümesi için oluşturulan kodlanmış maske şablonu.



Şekil 7. Şekil 6 daki 1×1 tek şablon maske çoğaltılarak oluşturulan bir kodlanmış maske.

Astrofizikçi Zand (1996), doğru kodlama maskesini ararken iki temel özellik belirtir. Bu özellikler:

- i) Maske şablonunun otokorelasyon fonksiyonu bir delta fonksiyonu olmalıdır,
- ii) Kodlanmış bir gökyüzü kaynağının sinyal-gürültü oranı optimum olmalıdır.

Bir fark kümesinin otokorelasyon özelliği kullanılarak sinyal-gürültü oranı en uygun hale gelir.

Baumert (1971), D fark kümesini ikili bir dizi $\mathbf{a} = (a_0, a_1, \dots, a_{v-1})$ ile ifade etmek için $a_i \in \{0,1\}$ olarak seçmiş ve bu şekilde oluşan ikili diziyi, D fark kümesinin *karakteristik fonksiyonu* ya da *tekrarlanma vektörü* olarak adlandırmıştır. Oluşturulan ikili dizi için $R_a(t)$ otokorelasyon fonksiyonunu, $i + t$ değeri modülo v de değerlendirilmek üzere;

$$R_a(t) = \sum_{i=0}^{v-1} a_i a_{i+t} = \begin{cases} k & t \equiv 0 \pmod{v} \text{ ise,} \\ \lambda = \frac{k(k-1)}{v-1} & t \not\equiv 0 \pmod{v} \text{ ise.} \end{cases}$$

olarak tanımlamıştır. $P_a(t)$ periyodik otokorelasyon fonksiyonunu (normalleştirilmiş otokorelasyon fonksiyonu) ise;

$$P_a(t) = \frac{1}{v} R_a(t)$$

şeklinde tanımlamıştır. Kodlanmış maske ile görüntüleme sürecinde k değeri sinyali ve λ değeri arka plan seviyesini belirler. Zand (1996) tarafından verilen doğru maske şablonu tasarlanması için gerekli kriterlerden ikinci kritere göre sinyal-gürültü oranı optimum olmalıydı. Yukarıdaki korelasyon tanımından görülebileceği gibi bu şartın sağlanması için k ile λ arasında mümkün olduğu kadar büyük bir fark olmalıdır.

Baumert (1971), bazı $t \in \mathbb{Z}$ değerleri için $v = 4t - 1$, $k = 2t - 1$ ve $\lambda = t - 1$ olduğunda k ile λ arasında maksimum fark olacağını göstermiştir. Bu özel değerlere sahip olan fark kümelerinin Hadamard fark kümesi olarak adlandırıldığı biliniyor. Bu parametrelere sahip fark kümeleri üç temel türle sınıflandırılabilir. Bu türler:

- i) Kuadratik rezidü fark kümeleri; v asaldır.
- ii) İkiz asal fark kümeleri; p ve $p + 2$ asal sayıları için $v = p(p + 2)$.
- iii) Pseudo-gürültü fark kümeleri; $m \in \mathbb{Z}$ için $v = 2^m - 1$.

Bu üç maddede belirtilen bir türe ait olan fark kümesi, aynı zamanda başka bir türe de ait olabilir.

Örnek 1.6.9. $(\mathbb{Z}_{71} \oplus \mathbb{Z}_{73})$ ikiz asal grubundaki (5183,2591,1295) parametrelili fark kümesi ele alınsın. $(v, k, \lambda) = (5183, 2591, 1295)$ parametreleri incelendiğinde $t = 1296$ değeri için $(5183, 2591, 1295) = (4t - 1, 2t - 1, t - 1)$ olduğu görülür. Böylece bu ikiz asal fark kümesi türünün, bir Hadamard fark kümesi olduğu anlaşılır.

Konu ile ilgili daha fazla bilgi için (Skinner, 1984), (Skinner, 1988), (Zand, 1995), (Zand, 1996), (Zhang vd., 1998) çalışmalarına bakılabilir.

Fark kümelerinin diğer uygulama alanlarından olan hata düzeltme kodları için (Assmus ve Key, 1992) ile (Beth vd., 1999) çalışmalarına, verilerin kodlanması ve deşifrelenmesi için (Baskar ve Saravanan, 2012) makalesine, kuantum bilişimindeki uygulaması için Godsil ve Roy (2009)'un makalesine bakılabilir.

2. YAPILAN ÇALIŞMALAR

Fark kümelerinin ikili dizi oluşturmadaki uygulamalarından olan, astronomik olayların görüntülenmesi için kodlanmış bir maske oluşturulması gerekmektedir. Kodlanmış maskeyi oluşturmak için bir yöntem, ikiz asal fark kümesi oluşturma teoremini kullanarak fark kümesi inşa etmektir. Ancak oluşturulacak olan kodlanmış maskenin astronomik olayların görüntülenmesinde kullanılabilmesi için büyük bir fark kümesi bulmak gerekmektedir. Gereken büyüklükteki fark kümelerini bilgisayar desteği olmadan bulmak zordur, bu nedenle bu fark kümelerini bulabilmek için bilgisayar programında yazılan kodlar kullanılmış ve fark kümesi oluşturan öğeler tespit edilmiştir.

Fark kümesi oluşturan öğeler tespit edilirken, $\mathbb{Z}_p \oplus \mathbb{Z}_{p+2}$ grubunu oluşturan ikiz asallar p ve $p + 2$ kullanılmaktadır. Ancak yazılan program kodlarında ikiz asallar doğrulanmamaktadır, yani kodları çalıştırırken ikiz asal çiftlerinden birincisi olan p yerine başka herhangi bir sayı girildiğinde program kendini sonlandırmaktadır. Bu nedenle öncelikle ikiz asalların doğru tespit edilmesi gerekir. Kullanılacak olan ikiz asalları bulmak için C# programında yazılan kodlar kullanılmıştır. Burada bulunan ikiz asallar C++ programındaki kodlar için kullanılarak bir fark kümesi inşa edilmiştir.

İstenilen büyüklükte fark kümesi inşa edildikten sonra fark kümesinde bulunan ikililer beyaz alanda ve fark kümesinde bulunmayan ikililer gölgeli alanda olmak üzere kodlanmış bir maske şablonu oluşturulmuştur.

Uydu teleskoplarında kullanılan en yaygın fark kümelerinden ikisi, $\mathbb{Z}_{41} \oplus \mathbb{Z}_{43}$ grubundaki (5183,2591,1295) parametrelili fark kümesi ve $\mathbb{Z}_{71} \oplus \mathbb{Z}_{73}$ grubundaki (1763,881,440) parametrelili fark kümesidir. Bu fark kümelerinin her ikisi de yeterince büyük 1x1 şablon maske üretmektedir. Çalışma için $\mathbb{Z}_{59} \oplus \mathbb{Z}_{61}$ ikiz asal grubundaki fark kümesi bulunarak, bu fark kümesinin oluşturduğu kodlanmış maske şablonu görselleştirilmiştir.

Not: Çalışmada C++ ve C# programlarında yazılmış olan kodlar sunulurken daha anlaşılabilir ve kullanışlı olması için, kodların ve program çıktılarının kullanılan programdaki ekran görüntüleri alınarak sunulmuştur.

2.1. İkiz Asal Fark Kümesi Oluşturma Teoreminin C++ Uygulaması

Bu başlık altında Şekil 8 ve devamında sunulan kodlar, kullanıcıdan $\mathbb{Z}_p \oplus \mathbb{Z}_{p+2}$ ikiz asal grubunu oluşturan kümelerden ilki olan $\mathbb{Z}_p$ nin eleman sayısı olan p asal sayısını tek bir girdi olarak isteyecektir. Sonrasında $p + 2$ asalını kendisi tespit ederek, Teorem 1.4.16 da belirtilen D_1, D_2, D_3 kümelerini bulacak ve en sonunda bulunan kümelerin bileşkelerini alarak $\mathbb{Z}_p \oplus \mathbb{Z}_{p+2}$ grubundaki D fark kümesini oluşturacaktır. Bu kodlar, seçilen ilk giriş olan p nin asallık kontrolünü yapmaz ve oluşturulan ikinci $p + 2$ sayısını da kontrol etmez. Bu nedenle ikiz asalları en başta belirleyerek giriş yapılmalıdır. Yapılan denemeler sonucunda, ikiz asal sisteminin bir parçası olmayan girilen her değer hata vermiş ve uygulamanın kapanmasına neden olmuştur.

```

1 // NTL:Sayılar Teorisi için kullanılan bir kütüphanedir.
2 // Paketler ve readme dosyaları http://www.shoup.net/ntl/ adresinde bulunabilir.
3 // Burada sunulan kod, NTL 6.2.1 ile yazılmıştır.
4 #include <locale.h>
5 #include <ctime>
6 #include "stdafx.h"
7 #include <stdio.h>
8 #include <NTL/ZZ.h>
9 #include <NTL/vector.h>
10 int main()
11 {
12     // Programın, Türkçe harf karakterlerini desteklemesini sağlar.
13     setlocale(LC_ALL, "Turkish");
14     // Girilen her değer için programın çalışma süresinin hesaplanmasını sağlar.
15     clock_t başlangıç = clock(), bitiş;
16     NTL_CLIENT
17     // Kullanılacak olan asalları başlatır.
18     ZZ p_asal, q_asal;
19     cout << "İkiz Asallardan Birincisini Giriniz:\n";
20     cin >> p_asal;
21     cout << "\n";
22     q_asal = p_asal + 2;
23     cout << "Z_" << p_asal << "xZ_" << q_asal <<
24         " İkiz Asal Grubu İçin Oluşturulan Fark Kümesi Aşağıda Listelenmiştir.";
25     cout << "\n";
26     // modülo p ve modülo q da kuadratik rezidü ve kuadratik olmayan rezidü
27     // değerlerini elde etmek için vektörler oluşturulur.
28     Vec<ZZ> p_asal_kuadr, p_asal_nkuadr, q_asal_kuadr, q_asal_nkuadr;
29     // Teorem 1.3.7 den, kuadratik rezidü ve kuadratik olmayan rezidü sayısı
30     // kullanılarak vektör kümelerinin uzunlukları tanımlanır.
31     long p_uzunluk = conv<long>(p_asal - 1) / 2;
32     long q_uzunluk = conv<long>(q_asal - 1) / 2;
33     // Vektörler kümesi, kuadratik rezidüleri ve kuadratik olmayan rezidüleri
34     // elde etmek için uygun uzunluklarda olacak şekilde ayarlanır.
35     p_asal_kuadr.SetLength(p_uzunluk);
36     p_asal_nkuadr.SetLength(p_uzunluk);
37     q_asal_kuadr.SetLength(q_uzunluk);
38     q_asal_nkuadr.SetLength(q_uzunluk);
39     int p_ddeki_kuadr = 0;
40     int q_ddeki_kuadr = 0;
41     int p_ddeki_nkuadr = 0;
42     int q_ddeki_nkuadr = 0;
43     ZZ değişken;
44     // p_asal_kuadr ve p_asal_kuadrn kümelerinin her ikisi de doldurulur.
45     for (int i = 1; i < p_asal; i++)
46     {
47         değişken = i;
48         if (Jacobi(değişken, p_asal) == 1)
49         {
50             p_asal_kuadr[p_ddeki_kuadr] = i;
51             p_ddeki_kuadr++;
52         }
53         else
54         {

```

Şekil 8. İkiz asal fark kümesi oluşturma teoreminin C++ program dilindeki kodları.

```

55     p_asal_nkuadr[p_ddeki_nkuadr] = i;
56     p_ddeki_nkuadr++;
57 }
58 }
59 // q_asal_kuadr ve q_asal_kuadr kümelerinin her ikisi de doldurulur.
60 for (int j = 1; j < q_asal; j++)
61 {
62     deęişken = j;
63     if (Jacobi(deęişken, q_asal) == 1)
64     {
65         q_asal_kuadr[q_ddeki_kuadr] = j;
66         q_ddeki_kuadr++;
67     }
68
69     else
70     {
71         q_asal_nkuadr[q_ddeki_nkuadr] = j;
72         q_ddeki_nkuadr++;
73     }
74 }
75 // Teorem 1.4.16 dan, grup  $Z_p \times Z_q$  formunda olduęundan D_1 kümesi için (a,b)
76 // ikilileri oluşturulur. Burada a deęeri  $Z_p$  kümesinin elemanı ve b=0 olacak.
77 cout << "{";
78 for (int k = 0; k < p_asal; k++)
79 {
80     cout << "(" << k << ",0)";
81 }
82 // Teorem 1.4.16 dan, grup  $Z_p \times Z_q$  formunda olduęundan D_2 kümesi için (a,b)
83 // ikilileri oluşturulur. Burada a,  $Z_p$  kümesinin kuadratik rezidüsü; b,  $Z_q$ 
84 // kümesinin kuadratik rezidüsü.
85 for (int k = 0; k < p_uzunluk; k++)
86 {
87     for (int l = 0; l < q_uzunluk; l++)
88     {
89         cout << "(" << p_asal_kuadr[k] << "," << q_asal_kuadr[l] << ")";
90     }
91 }
92 // Teorem 1.4.16 dan, grup  $Z_p \times Z_q$  formunda olduęundan D_3 kümesi için (a,b)
93 // ikilileri oluşturulur. Burada a,  $Z_p$  kümesinin kuadratik olmayan rezidüsü;
94 // b,  $Z_q$  kümesinin kuadratik olmayan rezidüsü.
95 for (int k = 0; k < p_uzunluk; k++)
96 {
97     for (int l = 0; l < q_uzunluk; l++)
98     {
99         cout << "(" << p_asal_nkuadr[k] << "," << q_asal_nkuadr[l] << ")";
100     }
101 }
102 cout << "}\n" << "\n";
103 bitiş = clock();
104 cout << (float)(bitiş - başlangıç) / CLOCKS_PER_SEC;
105 system("pause");
106 return 0;
107 }

```

Şekil 8 (devam). İkiz asal fark kümesi oluşturma teoreminin C++ program dilindeki kodları.

Program, Şekil 8 ve devamında verilen kodlar ile çalıştırıldığında ikiz asal sistemindeki ilk sayının girilmesini isteyecektir. Örneğin $\mathbb{Z}_{11} \oplus \mathbb{Z}_{13}$ grubundaki D fark kümesi için kodlar çalıştırılırsa program, grubu oluşturan ikiz asallardan ilki olan 11 sayısının girilmesini isteyecektir ve sonuçta Şekil 9 da verilen $\mathbb{Z}_{11} \oplus \mathbb{Z}_{13}$ grubundaki bir fark kümesini oluşturacaktır.

```
İkiz Asallardan Birincisini Giriniz:
11
Z_11xZ_13 İkiz Asal Grubu İçin Oluşturulan Fark Kümesi Aşağıda Listelenmiştir.
{(0,0)(1,0)(2,0)(3,0)(4,0)(5,0)(6,0)(7,0)(8,0)(9,0)(10,0)(1,1)(1,3)(1,4)(1,9)(
1,10)(1,12)(3,1)(3,3)(3,4)(3,9)(3,10)(3,12)(4,1)(4,3)(4,4)(4,9)(4,10)(4,12)(5,
1)(5,3)(5,4)(5,9)(5,10)(5,12)(9,1)(9,3)(9,4)(9,9)(9,10)(9,12)(2,2)(2,5)(2,6)(2
,7)(2,8)(2,11)(6,2)(6,5)(6,6)(6,7)(6,8)(6,11)(7,2)(7,5)(7,6)(7,7)(7,8)(7,11)(8
,2)(8,5)(8,6)(8,7)(8,8)(8,11)(10,2)(10,5)(10,6)(10,7)(10,8)(10,11)}
```

Şekil 9. C++ program dilinde yazılan kodlar kullanılarak $\mathbb{Z}_{11} \oplus \mathbb{Z}_{13}$ grubu için oluşturulan fark kümesi.

2.2. İkiz Asalları Bulmak için C# Kodları

Bu başlık altında Şekil 10 da verilen kodlar, belirtilen değer ile 0 aralığındaki ikiz asalların bulunması için kullanılmaktadır. Kodlar çalıştırıldığında kullanıcıdan tek bir giriş isteyecektir. Sonrasında girilen sayı ile 0 aralığındaki tüm ikiz asalları listeleyecektir.

```

1 using System;
2 using System.Collections.Generic;
3 using System.Linq;
4 using System.Text;
5 class Program
6 {
7     static void Main(string[] args)
8     {
9         int girilenSayi = 0;
10        Console.WriteLine("İkiz Asal İçin Üst Limit Giriniz: ");
11        girilenSayi = Convert.ToInt32(Console.ReadLine());
12        int[] Array_OfPrimes = GetPrimesUpto(girilenSayi);
13        Console.WriteLine("İkiz Asallar");
14        for (int i = 0; i < Array_OfPrimes.Length - 1; i++)
15        {
16            int FirstInt = Array_OfPrimes[i];
17            if (Array_OfPrimes.Contains(FirstInt + 2))
18            {
19                Console.WriteLine("{0} + {1} = {2}", FirstInt, (FirstInt + 2).ToString(), (FirstInt + 2));
20            }
21        }
22        Console.ReadKey();
23    }
24    private static int[] GetPrimesUpto(int maxNum)
25    {
26        List<int> primeNums = new List<int>();
27        if (maxNum != 0)
28        {
29            Array ArrValues = Array.CreateInstance(typeof(int),
30                new int[] { maxNum - 1 }, new int[] { 2 });
31            for (int chkPrime = ArrValues.GetLowerBound(0); chkPrime <= (int)Math.Ceiling
32                (Math.Sqrt(ArrValues.GetUpperBound(0))); chkPrime++)
33            {
34                if ((int)ArrValues.GetValue(chkPrime) == 1) continue;
35                {
36                    for (int multiplier = chkPrime; multiplier <= maxNum / 2; multiplier++)
37                    {
38                        if (chkPrime * multiplier <= maxNum)
39                        {
40                            ArrValues.SetValue(1, chkPrime * multiplier);
41                        }
42                    }
43                }
44            }
45            for (int chkPrime = ArrValues.GetLowerBound(0);
46                chkPrime <= ArrValues.GetUpperBound(0); chkPrime++)
47            {
48                if ((int)ArrValues.GetValue(chkPrime) == 0)
49                {
50                    primeNums.Add(chkPrime);
51                }
52            }
53        }
54        return primeNums.ToArray();
55    }
56 }
57 }

```

Şekil 10. C# program dilinde girilen değer ile 0 arasındaki ikiz asalları bulma kodları.

0 – 1000 aralığındaki ikiz asalların listelenmesi için program çalıştırıldığında ikiz asallar için üst limit olarak 1000 yazılır ve Şekil 11 de verilen ikiz asallar elde edilir.

```
ikiz Asal İçin Üst Limit Giriniz: 1000
İkiz Asallar
{3,5}{5,7}{11,13}{17,19}{29,31}{41,43}{59,61}{71,73}{101,103}{107,109}{
137,139}{149,151}{179,181}{191,193}{197,199}{227,229}{239,241}{269,271}
{281,283}{311,313}{347,349}{419,421}{431,433}{461,463}{521,523}{569,571}
{599,601}{617,619}{641,643}{659,661}{809,811}{821,823}{827,829}{857,85
9}{881,883}
```

Şekil 11. C# program dilinde yazılan kodlar kullanılarak 0 – 1000 aralığında bulunan ikiz asallar.

C# programındaki kodlar sayesinde 0 – 1000 aralığında listelenen $\{p, q\}$ ikiz asalları ile oluşturulan $\mathbb{Z}_p \oplus \mathbb{Z}_q$ grubundaki ikiz asal fark kümesini bulmak için C++ programındaki kodlar çalıştırıldığında çok kısa süreler içerisinde fark kümeleri listelenebilmektedir. Belirtilen aralıktaki ikiz asalların oluşturduğu grupların fark kümeleri için (v, k, λ) ve n parametreleri hesaplanmış olup, bu parametrelere sahip ikiz asal fark kümelerinin oluşturulması için programın çalışma süresi yaklaşık olarak Tablo 3 te sunulmuştur. Bilgisayar üzerinde çalıştırılan komutların çalışma süresi bilgisayarın durumuna (çalışan işlem sayısı, cpu kullanımı, ram kullanımı, cpu hızı vb.) bağlı olarak değişmektedir. Bundan dolayı komutların çalışma süreleri “Big O Notation” olarak adlandırılan bir yöntem ile bulunarak değerlendirilmektedir. Tablo 3 te sunulan süreler yaklaşık olarak verilmiştir.

Tablo 3. 0-1000 aralığındaki $\{p, q\}$ ikiz asalları için $\mathbb{Z}_p \oplus \mathbb{Z}_q$ ikiz asal grubundaki fark kümesinin parametreleri ve C++ programında yazılan kodların $\{p, q\}$ sayıları için ortalama fark kümesi oluşturma süresi.

p	q	(v, k, λ)	n	Programın Ortalama Çalışma Süresi
3	5	(15, 7, 3)	4	2 saniye
5	7	(35, 17, 8)	9	2 saniye
11	13	(143, 71, 35)	36	2 saniye
17	19	(323, 161, 80)	81	2 saniye
29	31	(899, 449, 224)	225	4 saniye
41	43	(1763, 881, 440)	441	4 saniye
59	61	(3599, 1799, 899)	900	6 saniye
71	73	(5183, 2591, 1295)	1296	7 saniye
101	103	(10403, 5201, 2600)	2601	12 saniye
107	109	(11663, 5831, 2915)	2916	14 saniye
137	139	(19043, 9521, 4760)	4761	22 saniye
149	151	(22499, 11249, 5624)	5625	26 saniye
179	181	(32399, 16199, 8099)	8100	31 saniye
191	193	(36863, 18431, 9215)	9216	37 saniye
197	199	(39203, 19601, 9800)	9801	45 saniye
227	229	(51983, 25991, 12995)	12996	59 saniye
239	241	(57599, 28799, 14399)	14400	69 saniye
269	271	(72899, 36449, 18224)	18225	86 saniye
281	283	(79523, 39761, 19880)	19881	95 saniye
311	313	(97343, 48671, 24335)	24336	116 saniye
347	349	(121103, 60551, 30275)	30276	152 saniye
419	421	(176399, 88199, 44099)	44100	207 saniye
431	433	(186623, 93311, 46655)	46656	239 saniye
461	463	(213443, 106721, 53360)	53361	243 saniye
521	523	(272483, 136241, 68120)	68121	292 saniye
569	571	(324899, 162449, 81224)	81225	356 saniye
599	601	(359999, 179999, 89999)	90000	358 saniye
617	619	(381923, 190961, 95480)	95481	376 saniye
641	643	(412163, 206081, 103040)	103041	394 saniye
659	661	(435599, 217799, 108899)	108900	414 saniye
809	811	(656099, 328049, 164024)	164025	635 saniye
821	823	(675683, 337841, 168920)	168921	665 saniye
827	829	(685583, 342791, 171395)	171396	678 saniye
857	859	(736163, 368081, 184040)	184041	710 saniye
881	883	(777923, 388961, 194480)	194481	785 saniye

2.3. $\mathbb{Z}_{59} \oplus \mathbb{Z}_{61}$ Grubundaki Fark Kümesi

Aşağıda, $\mathbb{Z}_{59} \oplus \mathbb{Z}_{61}$ ikiz asal grubundaki (3599,1799,899) parametrelili Hadamard fark kümesi sunulmuştur. Bu fark kümesi, ikiz asal fark kümesi oluşturma teoreminin C++ uygulaması kullanılarak oluşturulmuştur.

{(0,0), (1,0), (2,0), (3,0), (4,0), (5,0), (6,0), (7,0), (8,0), (9,0), (10,0), (11,0), (12,0), (13,0), (14,0), (15,0), (16,0), (17,0), (18,0), (19,0), (20,0), (21,0), (22,0), (23,0), (24,0), (25,0), (26,0), (27,0), (28,0), (29,0), (30,0), (31,0), (32,0), (33,0), (34,0), (35,0), (36,0), (37,0), (38,0), (39,0), (40,0), (41,0), (42,0), (43,0), (44,0), (45,0), (46,0), (47,0), (48,0), (49,0), (50,0), (51,0), (52,0), (53,0), (54,0), (55,0), (56,0), (57,0), (58,0), (1,1), (1,3), (1,4), (1,5), (1,9), (1,12), (1,13), (1,14), (1,15), (1,16), (1,19), (1,20), (1,22), (1,25), (1,27), (1,34), (1,36), (1,39), (1,41), (1,42), (1,45), (1,46), (1,47), (1,48), (1,49), (1,52), (1,56), (1,57), (1,58), (1,60), (3,1), (3,3), (3,4), (3,5), (3,9), (3,12), (3,13), (3,14), (3,15), (3,16), (3,19), (3,20), (3,22), (3,25), (3,27), (3,34), (3,36), (3,39), (3,41), (3,42), (3,45), (3,46), (3,47), (3,48), (3,49), (3,52), (3,56), (3,57), (3,58), (3,60), (4,1), (4,3), (4,4), (4,5), (4,9), (4,12), (4,13), (4,14), (4,15), (4,16), (4,19), (4,20), (4,22), (4,25), (4,27), (4,34), (4,36), (4,39), (4,41), (4,42), (4,45), (4,46), (4,47), (4,48), (4,49), (4,52), (4,56), (4,57), (4,58), (4,60), (5,1), (5,3), (5,4), (5,5), (5,9), (5,12), (5,13), (5,14), (5,15), (5,16), (5,19), (5,20), (5,22), (5,25), (5,27), (5,34), (5,36), (5,39), (5,41), (5,42), (5,45), (5,46), (5,47), (5,48), (5,49), (5,52), (5,56), (5,57), (5,58), (5,60), (7,1), (7,3), (7,4), (7,5), (7,9), (7,12), (7,13), (7,14), (7,15), (7,16), (7,19), (7,20), (7,22), (7,25), (7,27), (7,34), (7,36), (7,39), (7,41), (7,42), (7,45), (7,46), (7,47), (7,48), (7,49), (7,52), (7,56), (7,57), (7,58), (7,60), (9,1), (9,3), (9,4), (9,5), (9,9), (9,12), (9,13), (9,14), (9,15), (9,16), (9,19), (9,20), (9,22), (9,25), (9,27), (9,34), (9,36), (9,39), (9,41), (9,42), (9,45), (9,46), (9,47), (9,48), (9,49), (9,52), (9,56), (9,57), (9,58), (9,60), (12,1), (12,3), (12,4), (12,5), (12,9), (12,12), (12,13), (12,14), (12,15), (12,16), (12,19), (12,20), (12,22), (12,25), (12,27), (12,34), (12,36), (12,39), (12,41), (12,42), (12,45), (12,46), (12,47), (12,48), (12,49), (12,52), (12,56), (12,57), (12,58), (12,60), (15,1), (15,3), (15,4), (15,5), (15,9), (15,12), (15,13), (15,14), (15,15), (15,16), (15,19), (15,20), (15,22), (15,25), (15,27), (15,34), (15,36), (15,39), (15,41), (15,42), (15,45), (15,46), (15,47), (15,48), (15,49), (15,52), (15,56), (15,57), (15,58), (15,60), (16,1), (16,3), (16,4), (16,5), (16,9), (16,12), (16,13), (16,14), (16,15), (16,16), (16,19), (16,20), (16,22), (16,25), (16,27), (16,34), (16,36), (16,39), (16,41), (16,42),

(16,45), (16,46), (16,47), (16,48), (16,49), (16,52), (16,56), (16,57), (16,58), (16,60),
 (17,1), (17,3), (17,4), (17,5), (17,9), (17,12), (17,13), (17,14), (17,15), (17,16), (17,19),
 (17,20), (17,22), (17,25), (17,27), (17,34), (17,36), (17,39), (17,41), (17,42), (17,45),
 (17,46), (17,47), (17,48), (17,49), (17,52), (17,56), (17,57), (17,58), (17,60), (19,1),
 (19,3), (19,4), (19,5), (19,9), (19,12), (19,13), (19,14), (19,15), (19,16), (19,19), (19,20),
 (19,22), (19,25), (19,27), (19,34), (19,36), (19,39), (19,41), (19,42), (19,45), (19,46),
 (19,47), (19,48), (19,49), (19,52), (19,56), (19,57), (19,58), (19,60), (20,1), (20,3), (20,4),
 (20,5), (20,9), (20,12), (20,13), (20,14), (20,15), (20,16), (20,19), (20,20), (20,22),
 (20,25), (20,27), (20,34), (20,36), (20,39), (20,41), (20,42), (20,45), (20,46), (20,47),
 (20,48), (20,49), (20,52), (20,56), (20,57), (20,58), (20,60), (21,1), (21,3), (21,4), (21,5),
 (21,9), (21,12), (21,13), (21,14), (21,15), (21,16), (21,19), (21,20), (21,22), (21,25),
 (21,27), (21,34), (21,36), (21,39), (21,41), (21,42), (21,45), (21,46), (21,47), (21,48),
 (21,49), (21,52), (21,56), (21,57), (21,58), (21,60), (22,1), (22,3), (22,4), (22,5), (22,9),
 (22,12), (22,13), (22,14), (22,15), (22,16), (22,19), (22,20), (22,22), (22,25), (22,27),
 (22,34), (22,36), (22,39), (22,41), (22,42), (22,45), (22,46), (22,47), (22,48), (22,49),
 (22,52), (22,56), (22,57), (22,58), (22,60), (25,1), (25,3), (25,4), (25,5), (25,9), (25,12),
 (25,13), (25,14), (25,15), (25,16), (25,19), (25,20), (25,22), (25,25), (25,27), (25,34),
 (25,36), (25,39), (25,41), (25,42), (25,45), (25,46), (25,47), (25,48), (25,49), (25,52),
 (25,56), (25,57), (25,58), (25,60), (26,1), (26,3), (26,4), (26,5), (26,9), (26,12), (26,13),
 (26,14), (26,15), (26,16), (26,19), (26,20), (26,22), (26,25), (26,27), (26,34), (26,36),
 (26,39), (26,41), (26,42), (26,45), (26,46), (26,47), (26,48), (26,49), (26,52), (26,56),
 (26,57), (26,58), (26,60), (27,1), (27,3), (27,4), (27,5), (27,9), (27,12), (27,13), (27,14),
 (27,15), (27,16), (27,19), (27,20), (27,22), (27,25), (27,27), (27,34), (27,36), (27,39),
 (27,41), (27,42), (27,45), (27,46), (27,47), (27,48), (27,49), (27,52), (27,56), (27,57),
 (27,58), (27,60), (28,1), (28,3), (28,4), (28,5), (28,9), (28,12), (28,13), (28,14), (28,15),
 (28,16), (28,19), (28,20), (28,22), (28,25), (28,27), (28,34), (28,36), (28,39), (28,41),
 (28,42), (28,45), (28,46), (28,47), (28,48), (28,49), (28,52), (28,56), (28,57), (28,58),
 (28,60), (29,1), (29,3), (29,4), (29,5), (29,9), (29,12), (29,13), (29,14), (29,15), (29,16),
 (29,19), (29,20), (29,22), (29,25), (29,27), (29,34), (29,36), (29,39), (29,41), (29,42),
 (29,45), (29,46), (29,47), (29,48), (29,49), (29,52), (29,56), (29,57), (29,58), (29,60),
 (35,1), (35,3), (35,4), (35,5), (35,9), (35,12), (35,13), (35,14), (35,15), (35,16), (35,19),
 (35,20), (35,22), (35,25), (35,27), (35,34), (35,36), (35,39), (35,41), (35,42), (35,45),
 (35,46), (35,47), (35,48), (35,49), (35,52), (35,56), (35,57), (35,58), (35,60), (36,1),

(36,3), (36,4), (36,5), (36,9), (36,12), (36,13), (36,14), (36,15), (36,16), (36,19), (36,20),
 (36,22), (36,25), (36,27), (36,34), (36,36), (36,39), (36,41), (36,42), (36,45), (36,46),
 (36,47), (36,48), (36,49), (36,52), (36,56), (36,57), (36,58), (36,60), (41,1), (41,3), (41,4),
 (41,5), (41,9), (41,12), (41,13), (41,14), (41,15), (41,16), (41,19), (41,20), (41,22),
 (41,25), (41,27), (41,34), (41,36), (41,39), (41,41), (41,42), (41,45), (41,46), (41,47),
 (41,48), (41,49), (41,52), (41,56), (41,57), (41,58), (41,60), (45,1), (45,3), (45,4), (45,5),
 (45,9), (45,12), (45,13), (45,14), (45,15), (45,16), (45,19), (45,20), (45,22), (45,25),
 (45,27), (45,34), (45,36), (45,39), (45,41), (45,42), (45,45), (45,46), (45,47), (45,48),
 (45,49), (45,52), (45,56), (45,57), (45,58), (45,60), (46,1), (46,3), (46,4), (46,5), (46,9),
 (46,12), (46,13), (46,14), (46,15), (46,16), (46,19), (46,20), (46,22), (46,25), (46,27),
 (46,34), (46,36), (46,39), (46,41), (46,42), (46,45), (46,46), (46,47), (46,48), (46,49),
 (46,52), (46,56), (46,57), (46,58), (46,60), (48,1), (48,3), (48,4), (48,5), (48,9), (48,12),
 (48,13), (48,14), (48,15), (48,16), (48,19), (48,20), (48,22), (48,25), (48,27), (48,34),
 (48,36), (48,39), (48,41), (48,42), (48,45), (48,46), (48,47), (48,48), (48,49), (48,52),
 (48,56), (48,57), (48,58), (48,60), (49,1), (49,3), (49,4), (49,5), (49,9), (49,12), (49,13),
 (49,14), (49,15), (49,16), (49,19), (49,20), (49,22), (49,25), (49,27), (49,34), (49,36),
 (49,39), (49,41), (49,42), (49,45), (49,46), (49,47), (49,48), (49,49), (49,52), (49,56),
 (49,57), (49,58), (49,60), (51,1), (51,3), (51,4), (51,5), (51,9), (51,12), (51,13), (51,14),
 (51,15), (51,16), (51,19), (51,20), (51,22), (51,25), (51,27), (51,34), (51,36), (51,39),
 (51,41), (51,42), (51,45), (51,46), (51,47), (51,48), (51,49), (51,52), (51,56), (51,57),
 (51,58), (51,60), (53,1), (53,3), (53,4), (53,5), (53,9), (53,12), (53,13), (53,14), (53,15),
 (53,16), (53,19), (53,20), (53,22), (53,25), (53,27), (53,34), (53,36), (53,39), (53,41),
 (53,42), (53,45), (53,46), (53,47), (53,48), (53,49), (53,52), (53,56), (53,57), (53,58),
 (53,60), (57,1), (57,3), (57,4), (57,5), (57,9), (57,12), (57,13), (57,14), (57,15), (57,16),
 (57,19), (57,20), (57,22), (57,25), (57,27), (57,34), (57,36), (57,39), (57,41), (57,42),
 (57,45), (57,46), (57,47), (57,48), (57,49), (57,52), (57,56), (57,57), (57,58), (57,60),
 (2,2), (2,6), (2,7), (2,8), (2,10), (2,11), (2,17), (2,18), (2,21), (2,23), (2,24), (2,26), (2,28),
 (2,29), (2,30), (2,31), (2,32), (2,33), (2,35), (2,37), (2,38), (2,40), (2,43), (2,44), (2,50),
 (2,51), (2,53), (2,54), (2,55), (2,59), (6,2), (6,6), (6,7), (6,8), (6,10), (6,11), (6,17), (6,18),
 (6,21), (6,23), (6,24), (6,26), (6,28), (6,29), (6,30), (6,31), (6,32), (6,33), (6,35), (6,37),
 (6,38), (6,40), (6,43), (6,44), (6,50), (6,51), (6,53), (6,54), (6,55), (6,59), (8,2), (8,6), (8,7),
 (8,8), (8,10), (8,11), (8,17), (8,18), (8,21), (8,23), (8,24), (8,26), (8,28), (8,29), (8,30),
 (8,31), (8,32), (8,33), (8,35), (8,37), (8,38), (8,40), (8,43), (8,44), (8,50), (8,51), (8,53),

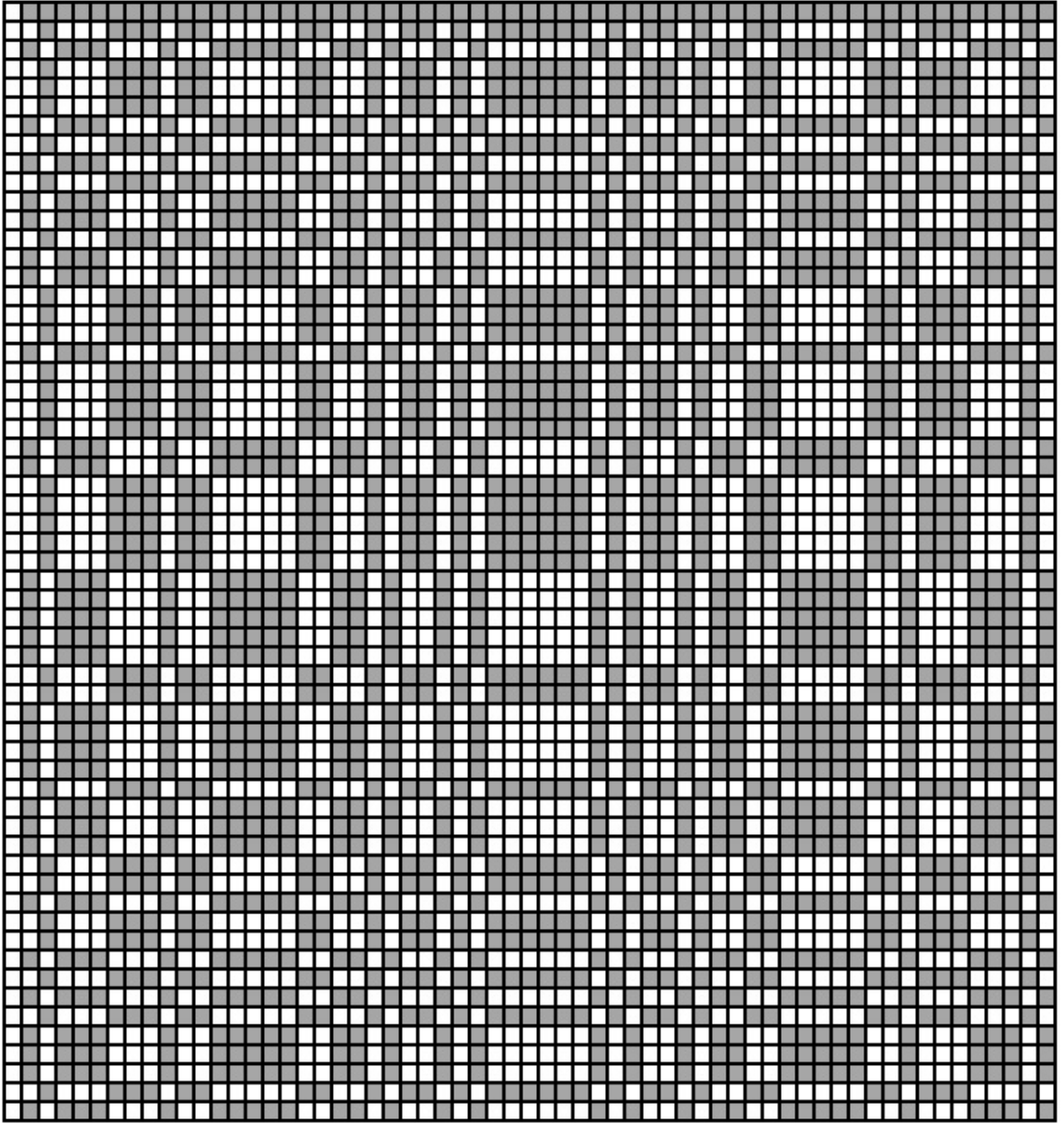
(8,54), (8,55), (8,59), (10,2), (10,6), (10,7), (10,8), (10,10), (10,11), (10,17), (10,18),
 (10,21), (10,23), (10,24), (10,26), (10,28), (10,29), (10,30), (10,31), (10,32), (10,33),
 (10,35), (10,37), (10,38), (10,40), (10,43), (10,44), (10,50), (10,51), (10,53), (10,54),
 (10,55), (10,59), (11,2), (11,6), (11,7), (11,8), (11,10), (11,11), (11,17), (11,18), (11,21),
 (11,23), (11,24), (11,26), (11,28), (11,29), (11,30), (11,31), (11,32), (11,33), (11,35),
 (11,37), (11,38), (11,40), (11,43), (11,44), (11,50), (11,51), (11,53), (11,54), (11,55),
 (11,59), (13,2), (13,6), (13,7), (13,8), (13,10), (13,11), (13,17), (13,18), (13,21), (13,23),
 (13,24), (13,26), (13,28), (13,29), (13,30), (13,31), (13,32), (13,33), (13,35), (13,37),
 (13,38), (13,40), (13,43), (13,44), (13,50), (13,51), (13,53), (13,54), (13,55), (13,59),
 (14,2), (14,6), (14,7), (14,8), (14,10), (14,11), (14,17), (14,18), (14,21), (14,23), (14,24),
 (14,26), (14,28), (14,29), (14,30), (14,31), (14,32), (14,33), (14,35), (14,37), (14,38),
 (14,40), (14,43), (14,44), (14,50), (14,51), (14,53), (14,54), (14,55), (14,59), (18,2),
 (18,6), (18,7), (18,8), (18,10), (18,11), (18,17), (18,18), (18,21), (18,23), (18,24), (18,26),
 (18,28), (18,29), (18,30), (18,31), (18,32), (18,33), (18,35), (18,37), (18,38), (18,40),
 (18,43), (18,44), (18,50), (18,51), (18,53), (18,54), (18,55), (18,59), (23,2), (23,6), (23,7),
 (23,8), (23,10), (23,11), (23,17), (23,18), (23,21), (23,23), (23,24), (23,26), (23,28),
 (23,29), (23,30), (23,31), (23,32), (23,33), (23,35), (23,37), (23,38), (23,40), (23,43),
 (23,44), (23,50), (23,51), (23,53), (23,54), (23,55), (23,59), (24,2), (24,6), (24,7), (24,8),
 (24,10), (24,11), (24,17), (24,18), (24,21), (24,23), (24,24), (24,26), (24,28), (24,29),
 (24,30), (24,31), (24,32), (24,33), (24,35), (24,37), (24,38), (24,40), (24,43), (24,44),
 (24,50), (24,51), (24,53), (24,54), (24,55), (24,59), (30,2), (30,6), (30,7), (30,8), (30,10),
 (30,11), (30,17), (30,18), (30,21), (30,23), (30,24), (30,26), (30,28), (30,29), (30,30),
 (30,31), (30,32), (30,33), (30,35), (30,37), (30,38), (30,40), (30,43), (30,44), (30,50),
 (30,51), (30,53), (30,54), (30,55), (30,59), (31,2), (31,6), (31,7), (31,8), (31,10), (31,11),
 (31,17), (31,18), (31,21), (31,23), (31,24), (31,26), (31,28), (31,29), (31,30), (31,31),
 (31,32), (31,33), (31,35), (31,37), (31,38), (31,40), (31,43), (31,44), (31,50), (31,51),
 (31,53), (31,54), (31,55), (31,59), (32,2), (32,6), (32,7), (32,8), (32,10), (32,11), (32,17),
 (32,18), (32,21), (32,23), (32,24), (32,26), (32,28), (32,29), (32,30), (32,31), (32,32),
 (32,33), (32,35), (32,37), (32,38), (32,40), (32,43), (32,44), (32,50), (32,51), (32,53),
 (32,54), (32,55), (32,59), (33,2), (33,6), (33,7), (33,8), (33,10), (33,11), (33,17), (33,18),
 (33,21), (33,23), (33,24), (33,26), (33,28), (33,29), (33,30), (33,31), (33,32), (33,33),
 (33,35), (33,37), (33,38), (33,40), (33,43), (33,44), (33,50), (33,51), (33,53), (33,54),
 (33,55), (33,59), (34,2), (34,6), (34,7), (34,8), (34,10), (34,11), (34,17), (34,18), (34,21),

(34,23), (34,24), (34,26), (34,28), (34,29), (34,30), (34,31), (34,32), (34,33), (34,35),
 (34,37), (34,38), (34,40), (34,43), (34,44), (34,50), (34,51), (34,53), (34,54), (34,55),
 (34,59), (37,2), (37,6), (37,7), (37,8), (37,10), (37,11), (37,17), (37,18), (37,21), (37,23),
 (37,24), (37,26), (37,28), (37,29), (37,30), (37,31), (37,32), (37,33), (37,35), (37,37),
 (37,38), (37,40), (37,43), (37,44), (37,50), (37,51), (37,53), (37,54), (37,55), (37,59),
 (38,2), (38,6), (38,7), (38,8), (38,10), (38,11), (38,17), (38,18), (38,21), (38,23), (38,24),
 (38,26), (38,28), (38,29), (38,30), (38,31), (38,32), (38,33), (38,35), (38,37), (38,38),
 (38,40), (38,43), (38,44), (38,50), (38,51), (38,53), (38,54), (38,55), (38,59), (39,2),
 (39,6), (39,7), (39,8), (39,10), (39,11), (39,17), (39,18), (39,21), (39,23), (39,24), (39,26),
 (39,28), (39,29), (39,30), (39,31), (39,32), (39,33), (39,35), (39,37), (39,38), (39,40),
 (39,43), (39,44), (39,50), (39,51), (39,53), (39,54), (39,55), (39,59), (40,2), (40,6), (40,7),
 (40,8), (40,10), (40,11), (40,17), (40,18), (40,21), (40,23), (40,24), (40,26), (40,28),
 (40,29), (40,30), (40,31), (40,32), (40,33), (40,35), (40,37), (40,38), (40,40), (40,43),
 (40,44), (40,50), (40,51), (40,53), (40,54), (40,55), (40,59), (42,2), (42,6), (42,7), (42,8),
 (42,10), (42,11), (42,17), (42,18), (42,21), (42,23), (42,24), (42,26), (42,28), (42,29),
 (42,30), (42,31), (42,32), (42,33), (42,35), (42,37), (42,38), (42,40), (42,43), (42,44),
 (42,50), (42,51), (42,53), (42,54), (42,55), (42,59), (43,2), (43,6), (43,7), (43,8), (43,10),
 (43,11), (43,17), (43,18), (43,21), (43,23), (43,24), (43,26), (43,28), (43,29), (43,30),
 (43,31), (43,32), (43,33), (43,35), (43,37), (43,38), (43,40), (43,43), (43,44), (43,50),
 (43,51), (43,53), (43,54), (43,55), (43,59), (44,2), (44,6), (44,7), (44,8), (44,10), (44,11),
 (44,17), (44,18), (44,21), (44,23), (44,24), (44,26), (44,28), (44,29), (44,30), (44,31),
 (44,32), (44,33), (44,35), (44,37), (44,38), (44,40), (44,43), (44,44), (44,50), (44,51),
 (44,53), (44,54), (44,55), (44,59), (47,2), (47,6), (47,7), (47,8), (47,10), (47,11), (47,17),
 (47,18), (47,21), (47,23), (47,24), (47,26), (47,28), (47,29), (47,30), (47,31), (47,32),
 (47,33), (47,35), (47,37), (47,38), (47,40), (47,43), (47,44), (47,50), (47,51), (47,53),
 (47,54), (47,55), (47,59), (50,2), (50,6), (50,7), (50,8), (50,10), (50,11), (50,17), (50,18),
 (50,21), (50,23), (50,24), (50,26), (50,28), (50,29), (50,30), (50,31), (50,32), (50,33),
 (50,35), (50,37), (50,38), (50,40), (50,43), (50,44), (50,50), (50,51), (50,53), (50,54),
 (50,55), (50,59), (52,2), (52,6), (52,7), (52,8), (52,10), (52,11), (52,17), (52,18), (52,21),
 (52,23), (52,24), (52,26), (52,28), (52,29), (52,30), (52,31), (52,32), (52,33), (52,35),
 (52,37), (52,38), (52,40), (52,43), (52,44), (52,50), (52,51), (52,53), (52,54), (52,55),
 (52,59), (54,2), (54,6), (54,7), (54,8), (54,10), (54,11), (54,17), (54,18), (54,21), (54,23),
 (54,24), (54,26), (54,28), (54,29), (54,30), (54,31), (54,32), (54,33), (54,35), (54,37),

(54,38), (54,40), (54,43), (54,44), (54,50), (54,51), (54,53), (54,54), (54,55), (54,59),
 (55,2), (55,6), (55,7), (55,8), (55,10), (55,11), (55,17), (55,18), (55,21), (55,23), (55,24),
 (55,26), (55,28), (55,29), (55,30), (55,31), (55,32), (55,33), (55,35), (55,37), (55,38),
 (55,40), (55,43), (55,44), (55,50), (55,51), (55,53), (55,54), (55,55), (55,59), (56,2),
 (56,6), (56,7), (56,8), (56,10), (56,11), (56,17), (56,18), (56,21), (56,23), (56,24), (56,26),
 (56,28), (56,29), (56,30), (56,31), (56,32), (56,33), (56,35), (56,37), (56,38), (56,40),
 (56,43), (56,44), (56,50), (56,51), (56,53), (56,54), (56,55), (56,59), (58,2), (58,6), (58,7),
 (58,8), (58,10), (58,11), (58,17), (58,18), (58,21), (58,23), (58,24), (58,26), (58,28),
 (58,29), (58,30), (58,31), (58,32), (58,33), (58,35), (58,37), (58,38), (58,40), (58,43),
 (58,44), (58,50), (58,51), (58,53), (58,54), (58,55), (58,59)}

2.4. $\mathbb{Z}_{59} \oplus \mathbb{Z}_{61}$ Grubundaki Fark Kümesi İçin Kodlanmış Maske Şablonu

İkiz asal fark kümesi oluşturma teoreminin C++ uygulamasındaki kodları ile bulunan $\mathbb{Z}_{59} \oplus \mathbb{Z}_{61}$ grubundaki fark kümesi kullanılarak oluşturulan kodlanmış maske şablonu Şekil 12 de gösterilmiştir. Ayrıca bu kodlanmış maske şablonunun içeriğindeki bazı ikililerin bilgi amaçlı gösterildiği detaylı kodlanmış maske şablonu Şekil 13 te sunulmuştur.



Şekil 12. $\mathbb{Z}_{59} \oplus \mathbb{Z}_{61}$ ikiz asal grubundaki fark kümesi kullanılarak oluşturulan kodlanmış maske şablonu.

3. BULGULAR

Bu tez çalışmasında fark kümeleri konusu ile ilgili genel bir literatür özeti verilerek, fark kümelerinin ikili dizi oluşturmadaki uygulamalarından olan, astronomik olayların görüntülenmesi uygulamasında kullanılan kodlanmış maske oluşturulmasına yönelik çalışmalar yapılmıştır.

Kodlanmış maske oluşturmak için öncelikle uygun bir grup ve bu grup içerisindeki fark kümesini bulmak gerekmektedir. Bunun için gerekli olan fark kümesini bulmanın bir yolu ikiz asal gruplarını kullanmaktır. İkiz asal bir gruba sahip olmak için ikiz asalların tespit edilmesi gerekir. Bu nedenle C# bilgisayar programında yazılmış olan kodlardan faydalanılarak belirli bir aralık için ikiz asallar listelenmiştir. Bu ikiz asallar içerisinde keyfi $\{59,61\}$ ikilisi seçilerek $\mathbb{Z}_{59} \oplus \mathbb{Z}_{61}$ grubu oluşturulmuştur. Oluşturulan ikiz asal grubunun içerisinde gömülü olan fark kümesini bulmak için ikiz asal fark kümesi teoreminden faydalanılmıştır. Ancak seçilen grup büyük olduğu için içerisindeki fark kümesini bulma sürecinde, ikiz asal fark kümesi teoreminin C++ bilgisayar programında yazılmış olan kodları kullanılmıştır. Programdaki kodların çalıştırılması neticesinde $\mathbb{Z}_{59} \oplus \mathbb{Z}_{61}$ grubu içerisindeki fark kümesi bulunmuştur.

Bulunan bu fark kümesi kullanılarak, astronomik olayların görüntülenmesi uygulamasında kullanılanlara benzer bir kodlanmış maske şablonu oluşturulmuştur.

4. TARTIŞMA ve SONUÇLAR

Tez çalışmasında öncelikle çalışma için gerekli olan bilgiler mevcut literatürden faydalanılarak sunulmuştur. Bu bilgiler içerisinde fark kümeleri ile ilgili temel kavramlar, fark kümelerinin özellikleri, aileleri, çalışma için önemli olan teoremler ve bazılarının ispatları verilmiş olup, fark kümelerinin uygulama alanlarına dair bilgiler sunulmuştur. Fark kümelerinin ikili dizi oluşturmadaki uygulamalarından olan kodlanmış maske oluşturulmasına yönelik ayrıntılı bir çalışma yapılmıştır.

Yapılan çalışmalar kısmında, fark kümelerinin ikili dizi oluşturmadaki uygulamalarından olan astronomik olayların görüntülenmesi için kullanılan kodlanmış maske oluşturulmasına yönelik olarak, öncelikle belirli aralıklardaki ikiz asalların bulunması ve bu ikiz asallar ile oluşturulan gruplar içerisindeki fark kümelerinin belirlenmesi için bilgisayar program dillerinde yazılan kod parçaları sunulmuştur.

C# program dilinde yazılan kodlar kullanılarak belirli aralıklardaki ikiz asallar listelenebilmektedir. Bu ikiz asallar içerisinde keyfi seçilen {59,61} ikiz asalları kullanılarak oluşturulan grup içerisindeki fark kümesi, C++ program dilinde yazılan kodlar sayesinde elde edilmiştir. Bulunan fark kümesi ile belirli kurallar çerçevesinde bir kodlanmış maske şablonu oluşturulmuştur.

5. ÖNERİLER

Fark kümeleri konusu oldukça kapsamlı olup birçok alanda uygulamaları bulunmaktadır. Bu uygulama alanlarının her biri için çok detaylı çalışmalar yapılması gerekmektedir. Fark kümelerinin uygulamalarda kullanılabilmesi için öncelikle grup içerisinde gömülü olan fark kümesinin bulunması gerekir. Bir grup içerisindeki fark kümesini bulmak için birçok yöntem mevcuttur. Ancak bu yöntemler kullanılırken fark kümelerinin bilgisayar desteği olmadan bulunması her zaman kolay olmayabilir. Bu nedenle bilgisayar program dillerinde, fark kümelerinin bulunmasına yönelik yöntemlere uygun kod parçaları yazılabilir. Ayrıca verilen (v, k, λ) parametreleri ile bir fark kümesi bulunup bulunmadığı üzerine kodlar yazılabilir.

KAYNAKLAR

- Assmus, E.F. and Key, J.D., 1992.** Designs and Their Codes. Cambridge University Press, ISBN: 0-521-45839-0, 343 s., 132-138.
- Baskar, S. and Saravanan, M., 2012.** Error detection and correction enhanced decoding of differenceset codes for memory application. International Journal of Advanced Research in Computer and Communication Engineering, 1(10), 816-820. DOI: 10.17148/IJARCCE
- Baumert, L.D., 1971.** Cyclic difference sets. Springer, cilt no:182, ISBN: 978-3540053682, 172 s., 1-9.
- Beth, T., Jungnickel, D. and Lenz, H., 1999.** Design theory. Cambridge University Press, cilt no:1, ISBN: 0-521-44432-2, 1120 s., 1-50.
- Bose, R.C., 1939.** On the construction of balanced incomplete block designs. Annals of Eugenics, 9(4), 353-399. DOI: 10.1111/j.1469-1809.1939.tb02219.x
- Bruck, R.H. and Ryser, H.J., 1949.** The nonexistence of certain finite projective planes. Canadian Journal of Mathematics, 1(1), 88-93. DOI: 10.4153/CJM-1949-009-2
- Bruck, R.H., 1955.** Difference sets in a finite group. Transactions of the American Mathematical Society, 78(2), 464-481. DOI: 10.2307/1993074
- Camion, P., 1979.** Difference sets in elementary abelian groups. Presses de l'Université de Montréal., cilt no:66.
- Chowla, S. and Ryser, H.J., 1950.** Combinatorial problems. Canadian Journal of Mathematics, 2, 93-99. DOI: 10.4153/CJM-1950-009-8
- Ding, C., 2014.** Codes from difference sets. World Scientific, ISBN: 978-9814619356, 341 s., 67-75.
- Gallian, J.A., 2013.** Contemporary abstract algebra. Nelson Education, yayın no:1, 9. baskı, ISBN: 978-1-305-65796-0, 631 s., 31-65.
- Godsil, C. and Roy, A., 2009.** Equiangular lines, mutually unbiased bases, and spin models. European Journal of Combinatorics, 30(1), 246-262. DOI: 10.1016/j.ejc.2008.01.002
- Golomb, S.W., 1999.** Construction of signals with favorable correlation properties. In Difference Sets, Sequences and Their Correlation Properties. Kluwer Academic Publishers, cilt no:542, ISBN13: 978-94-011-4459-9, 448 s., 159-194.
- Hall Jr, M., 1947.** Cyclic projective planes. Duke Mathematical Journal, 14(4), 1079-1090. DOI: 10.1215/S0012-7094-47-01482-8

- Hall, M. and Ryser, H.J., 1951.** Cyclic incidence matrices. Canadian Journal of Mathematics, 3, 495-502. DOI: 10.4153/CJM-1951-050-8
- Hall, M., 1956.** A survey of difference sets. Proceedings of the American Mathematical Society, 7(6), 975-986. DOI: 10.2307/2033024
- Ireland, K. and Rosen, M., 1982.** A classical introduction to modern number theory. Springer Verlag, cilt no:84, 2. baskı, ISBN 13: 978-1-4757-1779-2, 354 s., 272-275.
- Jungnickel, D., 1992.** Difference Sets in Contemporary Design Theory: A Collection of Surveys. Wiley Interscience, ISBN: 0-471-53141-3, 641 s., Dinitz, J.H. and Stinson, D.R.(B. Ed.), 241-365.
- Jungnickel, D. and Pott, A., 1999.** Differences Sets: An Introduction in Difference Sets, Sequences and Their Correlation Properties. Kluwer Academic Publishers, cilt no:542, ISBN13: 978-94-011-4459-9, 448 s., 259-295.
- Kibler, R.E., 1978.** A summary of noncyclic difference sets, $k < 20$. Journal of Combinatorial Theory A, 25(1), 62-67. DOI: 10.1016/0097-3165(78)90031-6
- Lam, C.W., Thiel, L. and Swiercz, S., 1989.** The non-existence of finite projective planes of order 10. Canadian Journal of Mathematics, 41(6), 1117-1123. DOI: 10.4153/CJM-1989-049-4
- Lam, C.W., 1991.** The search for a finite projective plane of order 10. The American mathematical monthly, 98(4), 305-318. DOI: 10.1080/00029890.1991.12000759
- Lehmer, E., 1953.** On residue difference sets. Canadian Journal of Mathematics, 5, 425-432. DOI: 10.4153/CJM-1953-047-3
- MacWilliams, F.J. and Sloane, N.J., 1976.** Pseudo-random sequences and arrays. Proceedings of the IEEE, 64(12), 1715-1729. DOI: 10.1109/PROC.1976.10411
- McFarland, R.L., 1973.** A family of difference sets in non-cyclic groups. Journal of Combinatorial Theory A, 15(1), 1-10. DOI: 10.1016/0097-3165(73)90031-9
- Menon, P.K., 1960.** Difference sets in abelian groups. Proceedings of the American Mathematical Society, 11(3), 368-376. DOI: 10.2307/2034778
- Moore, E.H. and Pollatsek, H.S., 2013.** Difference Sets. American Mathematical Society, cilt no:67, ISBN: 978-0-8218-9176-6, 298 s., 253-266.
- Nicholson, W.K., 2012.** Introduction to abstract algebra. John Wiley and Sons, 4. baskı, ISBN: 978-1-118-13535-8, 560 s.
- Pott, A., Kumar, P.V., Helleseht, T. and Jungnickel, D.(Eds.), 1999.** Difference Sets, Sequences and Their Correlation Properties. Kluwer Academic Publishers, cilt no:542, ISBN13: 978-94-011-4459-9, 448 s.

- Roetteler, M., 2016.** Quantum algorithms for abelian difference sets and applications to dihedral hidden subgroups. 11th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2016), Leibniz International Proceedings in Informatics (LIPIcs), 61, 8:1–8:16. DOI: 10.4230/LIPIcs.TQC.2016.8
- Rosen, K.H., Goddard, B. and O’Bryant, K., 2005.** Elementary number theory and its applications. Pearson/Addison Wesley, 5. Baskı, ISBN: 0-321-26314-6, 721 s., 402-403.
- Ryser, H.J., 1982.** The existence of symmetric block designs. Journal of Combinatorial Theory A, 32(1), 103-105. DOI: 10.1016/0097-3165(82)90068-1
- Singer, J., 1938.** A theorem in finite projective geometry and some applications to number theory. Transactions of the American Mathematical Society, 43(3), 377-385. DOI: 10.2307/1990067
- Skinner, G.K., 1984.** Imaging with coded-aperture masks. Nuclear Instruments and Methods in Physics Research, 221(1), 33-40. DOI: 10.1016/0167-5087(84)90174-1
- Skinner, G.K., 1988.** X-ray imaging with coded masks. Scientific American, 259(2), 84-89. DOI: 10.1038/scientificamerican0888-84
- Trout, G.M., 2017.** Difference Sets in Abelian Groups and Their Generalizations. Doktora Tezi. Delaware Üniversitesi, Matematik Bilimi Bölümü, Newark, Amerika Birleşik Devletleri, 95 s.
- Xie, Y., Yuan, J. and Malaney, R., 2013.** Quantum stabilizer codes from difference sets. 2013 IEEE International Symposium on Information Theory, İstanbul, 7-12 Temmuz, 524-528. DOI: 10.1109/ISIT.2013.6620281
- Zand, J., 1995.** The MART-LIME High Energy Coded Aperture Telescope. MART-LIME. SRON:Netherlands Institute for Space Research.
- Zand, J., 1996.** Coded Aperture Camera Imaging Concept [EB/OL]. NASA-Goddard Space Flight Center.
- Zhang, L., Horn, B.K.P. and Lanza, R.C., 1998.** Pattern design and imaging methods in 3-D coded aperture techniques. 1998 IEEE Nuclear Science Symposium Conference Record, 1998 IEEE Nuclear Science Symposium and Medical Imaging Conference (Cat. No. 98CH36255), Toronto, 8-14 Kasım, 1521-1524. DOI: 10.1109/NSSMIC.1998.773833

ÖZGEÇMİŞ

Tuğba NAVDAR GÜNAY, 05/03/1991 tarihinde Borçka’da doğdu. İlköğretimini 2004 yılında Borçka ilçesinde Atatürk İlköğretim Okulu’nda ve ortaöğretimini 2007 yılında Borçka ilçesinde Şehit Savaş Gedik Lisesi’nde tamamladı. 03/09/2007 tarihinde başladığı lisans eğitimini 25/12/2010 tarihinde Atatürk Üniversitesi Fen Edebiyat Fakültesi Matematik Bölümü’nde tamamladı. 2017 yılında Recep Tayyip Erdoğan Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı’nda başladığı yüksek lisans öğrenimini halen devam ettirmektedir. Artvin Çoruh Üniversitesi kurumunda bilgisayar işletmeni olarak 2013 yılı itibariyle görev yapmaktadır. Tuğba NAVDAR GÜNAY, evli olup Artvin’de yaşamaktadır.