

T.C.
RECEP TAYYİP ERDOĞAN ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI

YÜKSEK LİSANS

FARK KÜMELERİNİN VARLIK PROBLEMİ VE BRUCK RYSER
CHOWLA TEOREMİ

Safiye ÖZTÜRK

TEZ DANIŞMANI

Dr. Öğr. Üyesi Emek DEMİRCİ AKARSU

JÜRİ ÜYELERİ

Prof. Dr. Selçuk Han AYDIN

Dr. Öğr. Üyesi Mehmet Akif İNCE

RİZE-2020

Her Hakkı Saklıdır

T.C.
RECEP TAYYİP ERDOĞAN ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

**FARK KÜMELERİNİN VARLIK PROBLEMİ VE BRUCK RYSER CHOWLA
TEOREMİ**

Dr. Öğr. Üyesi Emek DEMİRCİ AKARSU danışmanlığında, Safiye ÖZTÜRK tarafından hazırlanan bu çalışma, Enstitü Yönetim Kurulu kararı ile oluşturulan jüri tarafından .../.../... tarihinde Matematik Anabilim Dalı'nda **YÜKSEK LİSANS** tezi olarak kabul edilmiştir.

Jüri Üyeleri	Unvanı, Adı Soyadı	İmza
Başkan	:	
Üye	:	
Üye	:	

Prof. Dr. Ferhat KALAYCI
ENSTİTÜ MÜDÜRÜ

ÖNSÖZ

Bu çalışmada Fark kümelerinin varlık problemi ve Bruck Ryser Chowla Teoremi ele alınmıştır.

Tez çalışmamda, planlanmasında, araştırılmasında yürütülmesinde ve oluşumunda bilgi ve tecrübelerinden yararlandığım yönlendirme ve bilgilendirmeleriyle çalışmamı şekillendiren sayın hocalarım Dr. Öğr. Üyesi Emek DEMİRCİ AKARSU'ya ve Dr. Öğr. Üyesi Rasim Volga OVALI' ya ayrıca maddi manevi eksiklerini esirgemeyen aileme teşekkürlerimi sunarım.

Safiye ÖZTÜRK

TEZ ETİK BEYANNAMESİ

Tarafımdan hazırlanan “Fark Kümelerinin Varlık Problemi ve Bruck Ryser Chowla Teoremi” başlıklı bu tezi, 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. 13/07/2020

Safiye ÖZTÜRK

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 KÜMELERİNİN VARLIK PROBLEMİ VE BRUCK RYSER CHOWLA TEOREMİ

Safiye ÖZTÜRK

Recep Tayyip Erdoğan Üniversitesi

Fen Bilimleri Enstitüsü

Matematik Anabilim Dalı

Yüksek Lisans Tezi

Danışmanı: Dr. Öğr. Üyesi Emek DEMİRCİ AKARSU

Tezin ilk bölümünde, fark kümelerinin tanımı, özellikleri, fark kümelerinin varlık problemi ve diğer zorunlu tanım ve teoremler verilmiştir. Daha sonra, fark kümelerini araştıran Bruck Ryser Chowla Teoremi uygulamaları mevcut literatür kullanılarak sunulmuştur. Çalışmanın ana bölümünde, Bruck Ryser Chowla Teoremi için koşulları sağlayan bir MATLAB kodu geliştirilmiştir. Tezin sonunda, bazı örnek çıktılarına sahip kaynak kodu ve test örneklerinin ayrıntılı analizi de verilmiştir.

2020, 65 sayfa

Anahtar Kelimeler: Fark Kümesi, Simetrik Dizayn, Bruck Ryser Chowla Teoremi

ABSTRACT

THE EXISTENCE PROBLEM OF DIFFERENCE SETS AND BRUCK RYSER CHOWLA THEORY

Safiye ÖZTÜRK

**Recep Tayyip Erdogan University
Graduate School of Natural and Applied Sciences
Department of Mathematics
Master Thesis
Supervisor: Assist. Prof. Dr. Emek DEMİRCİ AKARSU**

In the first part of thesis, the definition of difference sets, their properties, the existence problem of difference sets and the other required definitions and theorems are provided. Then, the applications for Bruck Ryser Chowla's Theorem which investigates of the difference sets are presented using the existing literature. In the main part of the study, a MATLAB code that provides the conditions for Bruck Ryser Chowla's Theorem is developed. At the end of the thesis, the source code with some sample outputs and detailed analysis of the test examples are also given.

2020, 65 pages

Keywords: Difference Sets, Symmetric Design, Bruck Ryser Chowla Theorem

İÇİNDEKİLER

ÖNSÖZ	I
TEZ ETİK BEYANNAMESİ.....	II
ÖZET	III
ABSTRACT	IV
ŞEKİLLER DİZİNİ	VI
TABLolar DİZİNİ.....	VII
SEMBOLLER ve KISALTMALAR DİZİNİ.....	IX
1. GENEL BİLGİLER	2
1.1. Giriş	2
1.2. Literatür Özeti.....	5
1.3. Temel Tanım ve Teoremler	8
1.4. Tekrarlanma Yapıları ve Dizaynlar	10
1.5. Fark Kümeleri	18
1.6. Ötelemeler	22
1.7. Fark Kümelerinde Varlık Problemi	25
1.8. Bruck Ryser Chowla Teoremi	26
1.8.1. v Tek Olduğunda BRC Teoreminin İspatı.....	35
1.9. Çarpanlar.....	37
1.10. Çarpan Teorisini Kullanarak Fark Kümesi Oluşturma	38
1.11. Fark Kümelerinin Varlığını Belirleyen Algoritma	43
2. YAPILAN ÇALIŞMALAR.....	45
2.1. Simetrik Dizaynın MATLAB Uygulaması	46
2.2. BRC Teoreminin MATLAB Uygulaması	47
2.4. Ana Program	49
2.5. Uygun Fark Kümesi Parametreleri İçin MATLAB Uygulaması.....	50
2.6. Lineer Diophant Denklem Çözümünün Matlab Uygulaması	52
3. BULGULAR.....	58
4. TARTIŞMA ve SONUÇLAR.....	59
5. ÖNERİLER.....	60
KAYNAKLAR	61
ÖZGEÇMİŞ.....	65

ŞEKİLLER DİZİNİ

Şekil 1. $(7,4,2)$ Parametrelî Simetrik Dizayn.....	15
Şekil 2. $n = 1, 2, 3$ için Projektif Düzlemler	27

TABLÖLAR DİZİNİ

Tablo 1. Simetrik dizayn olan fark kümelerinin uygun v , k , λ , n ve çarpan değerlerinin listesi	44
Tablo 2: Bazı (v, k, λ) parametreleri için ortalama çalışma süreleri.....	56
Tablo 3: Girilen v değerine karşılık bulunan olası fark kümesi sayıları için programın çalışma süresi.....	57
Tablo 4: Girilen (v, n, λ) parametrelerine karşılık lineer diophant denklemindeki (x, y, z) çözümlerinin kaç tane olduğunu veren örneklerin programdaki çalışma süreleri	57

SEMBOLLER ve KISALTMALAR DİZİNİ

$\mathbb{Z}$	Tam Sayıların Kümesi
G	Grup
D	Fark Kümesi
$\mathbb{N}$	Doğal Sayıların Kümesi
$\mathbb{Z}_p$	$(mod\ p)$ Tam Sayı Grubu
I	Birim Matris
$\emptyset$	Boş Küme
$\in$	Elemanıdır
Δ	Farkların Çoklu Kümesi
$G \oplus H$	Direkt Toplam
$\leq$	Küçük Eşittir
$\geq$	Büyük Eşittir
$\equiv$	Denktir
$\sim$	Etki
$\neq$	Eşit Değildir
$/$	Bölme
A^T	A'nın Transpozu
I_G	G'nin Birim Elemanı
$\notin$	Elemanı Değildir
$\subseteq$	Alt Küme Bağıntısı
$\cong$	Eşdeğerdir
λ	Farkların Tekrar Sayısı
$orb_G(x)$	x in G Kümesindeki Orbiti
$stab_G(x)$	x in G Kümesindeki Stabilizatörü
α	Otomorfizma
$\mathcal{P}$	Noktalar Kümesi
$\mathcal{B}$	Bloklar Kümesi
v	Bir G Grubunun eleman sayısı
k	Fark Kümesinin Eleman Sayısı

1. GENEL BİLGİLER

1.1. Giriş

Fark kümeleri ilk olarak James Singer'in 1938 tarihli 'A Theorem in Finite Projective Geometry and Applications to Number Theory' (Sonlu Projectif Geometride bir Teorem ve Sayı Teorisinde Bazı Uygulamalar) makalesinde ortaya çıkmıştır (Singer, 1938). Singer fark kümelerini tanımlamasına rağmen ana teoremi bir dizaynın otomorfizması ile ilgilidir. Bir grubun özel bir alt kümesi olan fark kümesi v , k , λ parametrelili simetrik dizayndır. Burada v parametresi grubun mertebesi, k parametresi fark kümesinin eleman sayısı ve λ parametresi ise fark kümesinden aldığımız birbirinden farklı iki elemanın farkının $(mod v)$ 'deki kalanları grubun etkisiz elemanından farklı elemanlarının tekrar sayısıdır. Her grubun fark kümesi olan uygun bir alt kümesi bulunabilir. Fark kümesinin parametreleri arasındaki ilişki incelendiğinde fark kümelerinin yeni bir parametresi olan n parametresi ortaya çıkmıştır. Bu n parametresi fark kümesinin mertebesi olarak adlandırılır. Fark kümelerinin tam anlamıyla sistematik olarak çalışılması Marshall Jr. Hall'ın çalışmalarıyla 1940'ların sonlarını bulmaktadır (Hall, 1947).

Bir fark kümesinin gerçekte ne olduğunu anlayabilmemiz için fark kümesinin nasıl oluşturulduğu bilgisine sahip olmamız gerekmektedir. Fark kümeleri ilk olarak değişmeli toplamsal gruplarda tanımlanmıştır. Bir grubun özel bir alt kümesi olan fark kümesi ancak simetrik dizayn olarak adlandırılan yapı şartlarını sağlarsa vardır.

Gerçek hayattaki problemlerde birçok uygulama alanına sahip fark kümeleri matematiğin soyut cebir, kombinatorik ve geometri alanlarını birleştirmeye çalışmaktadır. Kuzey Atlantik Antlaşması Örgütü NATO bu uygulamalardan bazılarını takip edebilmek için birçok NATO ülkesinden elektrik mühendisliği, bilgisayar bilimi ve matematik alanlarından uzmanları ve öğrencileri bir araya getirerek fark kümeleri ve diziler üzerine ileri çalışma enstitüsüne destek olmuştur (Pott vd., 1999).

Fark kümeleri yüksek enerjili optiklerde, iletişimde var olan sinyal gürültüsünün doğru yorumlanmasında, astronomik olayların görüntülenmesinde, hata düzeltme kodlarının oluşturulmasında, kuantum bilişimindeki süreçlerin kolaylaştırılmasında, kodlama ve deşifre etme gibi uygulama alanlarında

kullanılmaktadır.

Uzayın büyüklüğünü araştırmada fizikçiler Dünya atmosferinden kaçınmak için uydulara yerleştirilmiş teleskoplar kullanırlar. Sınırsız radyasyon atmosfere çarptığında rastgele yönlerde kırılır. Bu genellikle pırlıltı olarak adlandırılan bir olaya sebep olur. Bu pırlıltı Dünya’da görülen görüntüleri bulanıklaştırır. Dalgacıkların bir gölet yüzeyinde sahip olduğu benzer bir etkidir. Bu nedenle; pırlıltı yoksa teleskopların atmosfere yerleştirildiğinden emin olunur. Gezegenin yüzeyindeki teleskoplardan farklı olarak bilim adamları yüksek enerjili olaylarını görüntülemek ve görüntüleri aktarmak için merceklerin kullanımına güvenmemişlerdir ve sinyali doğru yorumlayabilmek için iyi otokorelasyon özelliklerine sahip fark kümeleri ile ikili diziler arasındaki ilişkiden yararlanılmıştır (Zhang vd., 1998).

Optiklerde de olduğu gibi, kodlama maskesini filtreden dedektöre giden verinin uygun bir ikili dizi olduğu düşünülebilir. Bu sinyal verilerde bir gürültü oranına sahip olacaktır. Görüntü yeniden oluşturulduğunda bilgisayarın uygun görüntüyü oluşturduğundan emin olması gerekmektedir. Bu gelen veriyi nesnenin olasılıksal bir modeli ile karşılaştırarak yapabilmektedir. Başka bir deyişle bilgisayarın sinyali ile ideal sinyal modeli arasındaki korelasyonu hesaplaması ve en yüksek korelasyona sahip olanı seçmesi gerekir. Bunun için bir fark kümesinin ötelemelerinden yararlanılır (Skinner, 1984).

Fark kümesinin yapısı fizikçilerin kaynaklarını doğrudan incelemek için özel dalga boylarındaki fotonları tespit etmek amacıyla özel filtreler oluşturmasını sağlar. Hastanelerde bulunan MR cihazları ve röntgen makinelerinde X-ışını kırınımı vardır. Hasta, radyasyon kaynağı ile radyasyona duyarlı dedektör arasına yerleştirilmelidir. Vücudun bölümleri radyasyonu soğurur, dedektörde gölgeler ve orijinal görüntüyü yeniden oluşturmak için bir kodlama işlemi yapar. Astrofiziksel görüntüleme amacıyla dedektör ile kaynak arasına maske yerleştirilir. Daha sonra bilgisayar maske vasıtasıyla geçen veriye bağlı olarak orijinal görüntüyü yeniden oluşturmayı denemektedir (Xie vd., 2013).

Fark kümelerinin yapıları verileri kodlamak ve kod çözmek için de kullanılmaktadır. Basit bir kod çözücünün ve bir fark kümesinin kodunun kullanılması çok etkili bir bellek koruma yöntemidir. Hata düzeltme kodu sadece bir sayı dizisini ifade eden algoritmadır. Öyle ki getirilen herhangi bir hata geri kalan sayılara göre tespit edilip düzeltilebilir.

Bir güneş tutulmasına asla doğrudan bakılmaması gerektiği bilinmektedir. Güneş tutulmasını dolaylı olarak görmeyi sağlayacak etkili yöntemler mevcuttur. Bunlardan bir tanesi birinin üzerinde küçük bir iğne deliği olan iki beyaz kağıdın kullanıldığı yaygın bir yöntemdir. Tutulmadan gelen ışık, içindeki delikten kağıda çarpar ve ikinci kağıt üzerine tutulmanın küçük bir görüntüsünü yansıtır. Bu sınırlı sayıda veriye izin verse de görüntü baş aşağı olsa bile elde edilen bir görüntü vardır ve bu iğne delikli kağıt maskenin en basit fikridir. Eğer kağıt üzerindeki delik çok küçükse resmin odaklı olduğu ancak çıkmakta olan sınırlı sayıda ışın nedeniyle parlak olmayabileceği fark edilmiştir. Eğer delik çok büyükse parlak bir görüntü elde edilir. Ama görüntü bulanık ve keskin değildir (Zand, 1995).

Bu tez çalışmasında, fark kümelerinin varlık problemi ve Bruck Ryser Chowla teoremi konusu için gerekli tanımlar, ilgili teoremler ve kümeyi tanımlayan parametrelerin özellikleri, gerekli teoremlerin ispatları varlık problemi ile ilgili genel bir literatür özeti bulunmaktadır. Fark kümelerinin simetrik dizayn ile ilişkisinden bahsedilerek Bruck Ryser Chowla Teoreminin şartlarını sağlayan ve sağlamayan örneklerle yer verilmiştir. Bu tezde, şartları sağlamayan örneklerin fark kümesi olmadıkları belirlenmiştir. Bruck Ryser Chowla teoremi tek yönlü bir gerektirme olduğundan gerektirmenin ikinci kısmının sağlanmaması birinci kısmı etkisiz hale getirir. Yani lineer diophant denkleminde bir çözümün olmaması o parametrelerle bir simetrik dizayn olamayacağını belirtmektedir. MATLAB programında yazılan simetrik dizayn kodu ile grubun fark kümesi olan özel alt kümelerini tarayarak uygun olanı seçmektedir. Ayrıca ana program kodu değer aralıkları verilen v , k ve λ parametrelerini sırasıyla simetrik dizayn ve BRC kodu ile birlikte fark kümelerinin bir listesini vermektedir. MATLAB programında yazılan bu kodların çalışma süreleri oldukça uzundur.

1.2. Literatür Özeti

Fark kümeleri ile ilgili Yabancı kaynaklarda birçok çalışma yapıldığı görülmektedir. İlk olarak sonlu geometrilere göre incelenen fark kümelerinin (Singer, 1938), simetrik dizaynlar, kodlama teorisi ve matematiğin diğer birçok alanıyla bağlantıları vardır. Fark kümelerinin sistematik çalışılması 1940'ların sonlarında Marshall Hall'ın çalışmalarına kadar gitmektedir (Hall, 1940).

Bose ve Nair (1939)'in çalışmasında blok dizaynlarının oluşturulmasının ilk sistematik metodu verilmiştir. (Levi, 1942) çalışmasında sonlu projektif ve afin geometri arasındaki yakın ilişki vurgulanmıştır. (Bruck ve Ryser, 1949), (Bose, 1949), ve (Schützenberger, 1949) çalışmalarında bu geometrileri çalışmak için denk matrisleri kullanmışlardır (Dembowski, 1997).

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 sonucu herhangi bir pozitif λ sayısına genişletmişlerdir. (Ryser, 1982) makalesinde teoremin daha basit bir çözümü verilmiştir. Sonrasında Ryser ve Chowla fark kümesi kabul edilen birçok örneğin fark kümesi olmadığını göstermiştir (Ryser ve Chowla, 1982).

Baumert (1971) çalışmasında $k \leq 100$ ile verilen devirli grupların fark kümeleri için parametrelerin tam bir listesini vermiştir. (Raghavara, 1971) çalışmasında blok dizaynının tanım ve özelliklerini vermiştir. Ayrıca simetrik dizaynının varlığını göstermiştir. (Kibler, 1978) makalesi $k < 20$ için devirli olmayan gruplardaki fark kümelerinin ilk geniş kapsamlı numaralandırmasını gerçekleştirmiştir. Fark kümelerinin $k < 20$ şartıyla bulunabilecek gruplar düşünülmüştür.

Simetrik dizaynların üçlü parametreleri hakkında birçok soru vardır. (Lander, 1983) çalışmasında her $\lambda > 1$ için çok fazla (v, k, λ) simetrik dizaynı bilindiğini göstermiştir. Lander yapmış olduğu çalışmada $k \leq 50$ ile olası değişmeli fark kümelerinin bir tablosunu vermiştir. (Kopilovich, 1989) bu aramayı $k < 100$ 'e kadar uzatmıştır. Bunlar $v \leq \lambda^2(\lambda + 2)$ şeklinde trivial olmayan simetrik dizaynlardır. λ bir asalın kuvveti olmak üzere (Lander, 1983)'e göre $v = \lambda^2(\lambda + 2)$ sınırına ulaşan bir simetrik dizayn vardır.

Balkanay (1986) değişmeli bir G grubundaki (v, k, λ) parametrelili fark kümelerinin yokluk kriteri olarak kullanılabilecek bir teorem ve ispatını vermiştir. (Aygör, 1987) hadamard matrisini (v, k, λ) parametrelili simetrik blok dizaynları ile özel olarak

oluşturulan hadamard dizaynını vererek yorumlamıştır. Bu çalışmanın sonucunda özel hadamard matris tipleri ve özellikleri incelenmiştir.

Lam, John, McCay, Swiercz ve Thiel (1989) makalesinde (Carter, 1970) çalışmalarının devamı olarak matematiksel akıl yürütme birleşimi ve bilgisayar aramasında onuncu mertebeden projektif uzayın bulunmadığını göstermişlerdir. (Cameron ve Lint, 1991) çalışmasında 12, 15, ve 18 mertebeli projektif uzayın bulunmadığını gösterilmiştir.

Assmus ve Key (1992)'e göre cebirsel kodlama teorisinin dizaynların analiz ve sınıflandırılmasındaki uygulamalarını incelenmiştir. (Demkowski, 1997) simetrik dizayn üzerine bilinen sonuçların bir listesini çalışmasında vermiştir.

Aygör (1994) doktora tezinde bir (v, k, λ) parametrelili simetrik blok dizaynının tekrarlanma matrisinin büzülmüş matrisi ile kodlar üretmiş ve bunların özelliklerini incelemiştir.

Delahaye (1996) çalışmasında hata düzeltme algoritmasının geliştirilmiş halini göstermiştir. Bu nedenle $(1057, 813, 34)$ devirli fark kümesi kodu teorideki 16 hata yerine 26 rastgele hatayı düzeltmeyi başarmıştır.

Lopez ve Sanchez (1997)'in makalesinde $k \leq 150$ ile değişmeli fark kümeleri için olası tüm parametrelere bakmıştır.

Ustamehmetoğlu (1999) çalışmasında k bir tek sayı olmak üzere (v, k, λ) simetrik dizaynının C kodu için C_1 alt kümesinde X sözcüğünün izafi ağırlığını, maksimum izafi ağırlık ve izafi ağırlık oranını tanımlayarak özelliklerini incelemiştir.

Türkiye'de projektif geometri üzerine yapılan çalışmalar incelendiğinde projektif geometri oluşturmadaki amacı perspektife uygun paralel doğruların sonsuz üzerinde kesiştiği bir geometri oluşturmak olarak belirlenmiştir. Bu doğrultuda Öklid düzlem geometrisi üzerindeki yeni noktalar eklenerek doğru tanımı içerisinde de küçük bir değişiklik yapılabilir. (Akpınar, 2005)'e göre 2, 3, 4, 5, 7 ve 8 mertebeli projektif düzlemlerin kuruluş metodlarının incelenerek bunların sonuçlarına karşılık 9. mertebeden bilinen dört farklı düzlemin nasıl elde edildiği araştırılmıştır. 10. mertebeden projektif düzlemin yokluğu hakkındaki bilgiler bir araya getirilmiş ve yorumlanmıştır. Bunun sonucunda projektif düzlemin mertebesinin büyümesi teorik olarak elle yapılan işlemlerde zorlaşma olduğundan yapılan araştırmalarla bilgisayar kullanılması zorunlu hale geldiği belirlenmiştir. Bu çalışmada en çok projektif düzleme genişletilebilen latin karelerden yararlanılmıştır.

Baskar ve Saravanan (2012) fark kümelerinin yapılarının verileri kodlamak ve deşifre etmek için kullanılabileceği ve aynı zamanda fark kümesi kodlarının bellek güvenliği üzerine kullanılması üzerinde çalışılmıştır. Son yıllarda (AbuGhneim, 2013; 2016) çalışmalarında 64 mertebeli tüm gruplar için neredeyse bütün numaralandırmaları bulunmuştur. Ve birkaç yazar 96 mertebeli gruplar için fark kümeleri bulmuşlardır (Golemac et al, 2005; 2007; AbuGhneim ve Smith, 2007).

Fark kümeleri çalışmasında alt yapı için gerekli tanım, teoremler ve ispatları (Taşçı, 2010), (Çevik, 2012), (Rosen vd., 2005), (Williams, 1937), (Bayraktar, 1988), (Ding, 2014), (Moore ve Pollatsek, 2013) kaynaklarında mevcuttur.

1.3. Temel Tanım ve Teoremler

Tanım 1.3.1 (*Grup*) G boş olmayan bir küme ve bu küme üzerinde bir ikili işlem $*$ olsun. Buna göre eğer aşağıdaki şartlar sağlanırsa $(G,*)$ cebirsel yapısına (ya da G kümesine $*$ işlemine göre) bir *grup* denir.

G1) Birleşme: Her $a, b, c \in G$ için $a * (b * c) = (a * b) * c$.

G2) Birim Eleman: Her $a \in G$ için $a * e = e * a = a$ şartını sağlayan $\exists e \in G$ mevcutsa e birim elemanı vardır.

G3) Ters Eleman: G kümesindeki her bir a için e , G 'nin birim elemanı olmak üzere $a * a' = a' * a = e$ olacak şekilde $\exists a' \in G$ vardır.

Tanım 1.3.2. (*Değişmeli Grup*) $(G,*)$ bir grup olmak üzere her $\forall a, b \in G$ için $a * b = b * a$ oluyorsa o zaman bu gruba *değişmeli grup* denir.

Tanım 1.3.3. (*Grubun Mertebesi*) G sonlu elemanlı bir küme ise $(G,*)$ grubuna bir sonlu grup, eleman sayısına da *grubun mertebesi* denir.

Tanım 1.3.4. (*Grup Homomorfizması*) $(G, \oplus)$ ve $(G', \odot)$ iki grup olmak üzere $f: G \rightarrow G'$ bir fonksiyon olsun.

- Eğer her $a, b \in G$ için $f(a \oplus b) = f(a) \odot f(b)$ oluyor ise o zaman f 'ye *grup homomorfizması* adı verilir.

Yukarıdaki tanımda $a \in G$ olmak üzere $f(a) \in G'$ olduğuna dikkat etmek gerekir. Farklı gözüken iki grup aynı temel yapıya sahip olabilir. Aşağıdaki tanım bununla ilgilidir.

Tanım 1.3.5. (*Grup İzomorfizması*) G ve G' bir grup olmak üzere $f: G \rightarrow G'$ fonksiyonu, aşağıdaki şartları sağlayacak şekilde mevcutsa G, G' ne *izomorftur* denir ve $G \cong G'$ şeklinde yazılır.

- Homomorfizma: Her $a, b \in G$ için $f(a \oplus b) = f(a) \odot f(b)$ dir.
- Birebirlik: Her $a, b \in G$ için $f(a) = f(b)$ ise $a = b$ dir.
- Örtelik: Her $g \in G'$ için $g = f(a)$ şeklinde yazılabilen en az bir $a \in G$ vardır.

Kısaca izomorfizma, homomorfik özelliğe sahip gruplar arasındaki birebir ve örten eşlemedir. Bu bizi, fark kümelerinin elde edilmesine katkıda bulunan özel bir

izomorfizma türü olan otomorfizmaya götürür.

Tanım 1.3.6. (*Grup Otomorfizması*) G bir grup olmak üzere grubun kendi üzerinde tanımlanan izomorfizmaya grup otomorfizması denir. Tüm otomorfizmaların grubu $Aut(G)$ ile gösterilir ve G nin otomorfizma grubu olarak adlandırılır (Bayraktar, 1988).

Grup yapısı tanımları verildiğine göre şimdi grup üzerinde yapılacak işlemleri tanımlayabiliriz.

Tanım 1.3.7. (*Etki*) Boştan farklı bir X kümesinin permütasyonlarının grubu G olmak üzere G grubu aslında X kümesi üzerinde tanımlanacak simetrik grubun bir alt grubu olup, X in tüm permütasyonlarının grubudur. Bu durumda her $g \in G$ ve her $x \in X$ için, $(g, x) \rightarrow g(x)$ kuralı altında tanımlanacak bir $G \times X \rightarrow X$ fonksiyonu aşağıdaki şartları sağlarsa G grubu X kümesi üzerine *soldan etki eder* denir. Ve $G \curvearrowright X$ şeklinde gösterilir.

- Her $g \in G$ ve her $x \in X$ için, gx elemanının bir anlamı vardır ve $gx \in X$ dir.
- Her $g_1, g_2 \in G$ ve her $x \in X$ için, $(g_1 g_2)x = g_1(g_2)x$ dir.
- Her $x \in X$ için $1_G x = x$ dir.

Tanım 1.3.8. (*Orbit-Yörünge*) Bir G grubu ve X kümesi için birim eleman ve birleşme özelliklerini sağlayan $F: G \times X \rightarrow X$ fonksiyonu varsa G 'nin X üzerine etki ettiği söylenmektedir.

- $\forall x \in X$ için $F(1_G, x) = x$ tir.
- $\forall g, h \in G$ ve $x \in X$ olmak üzere $F(gh, x) = F(g, F(h, x))$

$g \in G$ " $\sim$ " için $x_1 \sim x_2 \leftrightarrow F(g, x_1) = x_2$ ile X üzerinde bir *bağıntı* olarak tanımlanır. Eğer $x \in X$ ise o zaman x elemanının G grubuna göre *orbiti* $O(x) = \{gx \mid g \in G\}$ kümesidir ve $orb_G(x)$ ile gösterilir. Denklik sınıfları G nin X üzerindeki orbitleri olarak adlandırılır ve her orbit, x 'i içeren bir denklik sınıfıdır. Sabitleyici;

$$stab_G(x) = \{g \in G \mid F(g, x) = x\}$$

olarak tanımlanır (Çevik, 2012).

Teorem 1.3.1. G bir grup ve α , $\alpha(D) = D$ olacak şekilde D 'nin bir çarpanı olsun. O zaman D , G 'nin elemanlarının bir permütasyonu olarak α için orbitlerin birleşiminden oluşur (Çevik, 2012).

Sonradan göreceğimiz gibi fark kümeleri bir çok yoldan oluşturulabilir. Orbitlerin birleşimi bu yöntemlerden biridir.

1.4. Tekrarlanma Yapıları ve Dizaynlar

Tanım 1.4.1. (*Tekrarlanma yapısı*) $\mathcal{P}$ noktalar kümesi, $\mathcal{B}$ bloklar kümesi olmak üzere $\mathcal{P} \cap \mathcal{B} = \emptyset$ ve $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{B}$ olmak üzere $(\mathcal{P}, \mathcal{B}, \mathcal{I})$ üçlüsüne bir *tekrarlanma yapısı* denir. $p \in \mathcal{P}$ ve $B \in \mathcal{B}$ için $(p, B) \in \mathcal{I}$ ise p ve B 'nin *ilişkili* olduğu söylenir (Lander, 1983).

Aşağıda tekrarlanan yapı örneklerine yer verilmiştir.

Örnek 1.4.1. Öklid düzleminde, $\mathcal{P}$ yi noktalar kümesi ve $\mathcal{B}$ yi doğrular kümesi alabiliriz.

Örnek 1.4.2. $\mathcal{P} = \{1, 2, 3\}$ üç elemanlı noktalar kümesinin blok kümesi;

$\mathcal{B} = \{\{1\}, \{1, 2\}, \{1, 3\}, \{1, 2, 3\}\}$ olmak üzere 1 elemanı her dört blokta, 2 elemanı 2. ve 4. blokta ve 3 elemanı 3. ve 4. blokta bulunur.

Örnek 1.4.1. de noktalar ve bloklar sınırsız iken Örnek 1.4.2. de noktalar ve bloklar sınırlıdır. Örnek 1.4.1. de belirli bir düzende sınırsız nokta ve blok varken Örnek 1.4.2. de noktalar sınırlı bloklar düzensizdir. Bizim kullanacağımız kümeler sınırlı ve düzenli olan kümeler olacaktır.

Bir tekrarlanan yapıyı temsil etmek için matris gösterimi kullanılabilir. Bunun için aşağıdaki tanım kullanılacaktır.

Tanım 1.4.2. (*Tekrarlanma Matrisi*) $(\mathcal{P}, \mathcal{B}, \mathcal{I})$ tekrarlanma yapısında noktalar kümesi $\mathcal{P} = (p_1, p_2, \dots, p_v)$, bloklar kümesi $\mathcal{B} = (B_1, B_2, \dots, B_k)$ olsun. Burada $0 < i \leq v$ olmak üzere p_i noktaları ve $0 < j \leq k$ olmak üzere B_j blokları temsil etmek üzere *tekrarlanma matrisi* M , $m_{ij} \in M$ olmak üzere;

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

olarak tanımlanır.

Sonlu olan her tekrarlanma yapısı tekrarlanma matrisi ile temsil edilebilmektedir. Matrisin sütunları noktaları satırları ise blokları temsil etmektedir.

Örnek 1.4.3. Örnek 1.4.2. deki tekrarlanma matrisi aşağıdaki gibidir. Bu matriste sütunlar noktalardan ve satırlar bloklardan oluşmaktadır. $\mathcal{P} = \{1,2,3\}$ ve $\mathcal{B} = \{\{1\}, \{1,2\}, \{1,3\}, \{1,2,3\}\}$ olmak üzere tekrarlanma matrisi M ile gösterilirse;

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

olarak bulunur.

Tekrarlanma matrisleri sadece bir tekrarlanma yapısına ait olmayabilir. İki tekrarlanma yapısının aynı olup olmadığını kontrol etmek için bloklar veya noktaların sıralamaları değiştirilerek oluşan matris ile permütasyon matrisi çarpılabilir (Moore ve Pollatsek, 2013).

Tanım 1.4.3. (*İzomorf Tekrarlanma Yapıları*) $(\mathcal{P}, \mathcal{B}, \mathcal{I})$ ve $(\mathcal{P}', \mathcal{B}', \mathcal{I}')$ iki tekrarlanma yapısı olsun. Eğer $\mathcal{P}$ yi $\mathcal{P}'$ ne, $\mathcal{B}$ yi $\mathcal{B}'$ ne eşleyen birebir örten fonksiyon varsa bu yapılar *izomorf* olarak adlandırılır. İzomorfizma $(\mathcal{P}, \mathcal{B}, \mathcal{I})$ ve $(\mathcal{P}', \mathcal{B}', \mathcal{I}')$ yapısını korur (Lander, 1983).

Fark kümeleri ve dizaynlar bağlantılı olduğundan dizayn tanımları verilmektedir.

Tanım 1.4.4. (*Blok Dizaynı*) v tane noktanın oluşturduğu b tane blok için;

- Her blokta k tane farklı nokta vardır.
- Her nokta r farklı blokta vardır.
- Herhangi iki nokta çifti λ farklı blokta vardır.

şartlarını sağlayan yapıya *blok dizaynı* denir. Parametreleri arasındaki ilişki;

$$\begin{aligned} bk &= vr \\ r(k-1) &= \lambda(v-1) \end{aligned} \tag{1}$$

(1) eşitliği b, v, r, k, λ parametreleriyle sağlanır. Eğer b bloklarının sayısı v noktalarının sayısına eşitse dizaynın simetrik olduğu söylenir. $bk = vr$ eşitliğinde $k = r$ olduğunda bir simetrik dizayndır. Her fark kümesi, noktaları $\{0, 1, 2, \dots, v-1\}$, blokları $\{D, D+1, \dots, D+(v-1)\}$ olan bir simetrik blok dizaynı oluşturur (Baumert, 1971).

Örnek 1.4.4. Noktalar kümesi $\mathcal{P} = \{0, 1, 2, 3, 4, 5, 6\}$, $D = \{1, 2, 4\}$ ve bloklar kümesi;

$$B_1 = 0 + D = \{1, 2, 4\}$$

$$B_2 = 1 + D = \{2, 3, 5\}$$

$$B_3 = 2 + D = \{3, 4, 6\}$$

$$B_4 = 3 + D = \{0, 4, 5\}$$

$$B_5 = 4 + D = \{1, 5, 6\}$$

$$B_6 = 5 + D = \{0, 2, 6\}$$

$$B_7 = 6 + D = \{0, 1, 3\}$$

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

olmak üzere bu tekrarlanma yapısı $(7, 3, 1)$ dizaynını oluşturur.

Bazı trivial olmayan fark kümeleri;

$$D_1 = \{1, 2, 4\} \pmod{7},$$

$$D_2 = \{0, 3, 5, 6\} \pmod{7}$$

$$D_3 = \{0, 1, 3, 9\} \pmod{13}$$

$$D_4 = \{1, 4, 5, 6, 7, 9, 11, 16, 17\} \pmod{19}$$

şeklindedir.

Tanım 1.4.5. (Simetrik Dizayn) (v, k, λ) bir simetrik dizayn $(\mathcal{P}, \mathcal{B}, \mathcal{I})$ tekrarlanan yapı $0 < k < v$ olmak üzere aşağıdaki özellikler sağlanır. (Hall ve Ryser, 1951)

- v sayıda nokta vardır. $(|\mathcal{P}| = v)$
- v sayıda blok vardır. $(|\mathcal{B}| = v)$

- Her bir nokta k tane blokta bulunur.
- Her bir blok k tane nokta içerir.
- Herhangi iki blokta λ tane ortak nokta bulunur.
- Herhangi iki nokta λ blokta birlikte bulunur.

$\lambda = 0$ ve $\lambda = k - 1$ olan simetrik dizaynlar trivial (önemsiz) simetrik dizaynlar olarak adlandırılırlar.

Herhangi bir blok dizaynının A matrisi, 0 ve 1 den oluşan $v \times v$ boyutlu dizaynın tekrarlanma matrisi olarak adlandırılır. i . blokta j . eleman varsa $a_{ij} = 1$ yoksa $a_{ij} = 0$ alınarak matris oluşturulur. [i . blok $D + (i - 1)$ ve j . elemanı $(j - 1)$ dir.]

Örnek 1.4.4. ün tekrarlanma matrisi aşağıdaki gibidir.

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

Tanım 1.4.6. (*Simetrik Dizaynın Mertebesi*) $n = k - \lambda$ sayısına fark kümesinin mertebesi denir (Lander, 1983).

Tanım 1.4.7. (*Köşegen Matris*) $A = (a_{ij})_{n \times n}$ bir kare matris olmak üzere eğer $i \neq j$ için her zaman $a_{ij} = 0$ oluyorsa, bu taktirde A matrisine *köşegen matris* denir ve elemanları $diag(A)$ kümesiyle gösterilir.

Tanım 1.4.8. (*Denk Matris*) A ve B $n \times n$ tipinde iki matris olmak üzere, eğer $B = PAQ$ olacak şekilde P ve Q tersinir matrisleri varsa, o zaman A ve B matrislerine *denk matrisler* denir.

Tanım 1.4.9. (*Kongrüans matris*) A ve B $n \times n$ tipinde iki matris olmak üzere, eğer $B = Q^T A Q$ olacak şekilde Q tersinir matrisi varsa, o zaman A ve B matrislerine *kongrüans matrisler* denir. Kongrüans matrisler denk matrislerin özel bir halidir.

Tanım 1.4.10. (*Benzer Matris*) A ve B $n \times n$ tipinde iki matris olmak üzere, eğer $B = P^{-1}AP$ olacak şekilde tersinir bir P matrisi varsa, o zaman A ve B matrislerine *benzer matrisler* denir (Williams, 1937).

Tanım 1.4.11. (*Tekrarlanma Denklemi*) Bir simetrik dizaynın tekrarlanma matrisi A ise J , elemanlarının hepsi 1 olan uygun boyutlu bir kare matris ve J , uygun boyutlu birim matris olmak üzere $A^t A = (r - \lambda)J + \lambda J$ denklemine *tekrarlanma denklemi* denir. ($r = k$ olduğunda simetrik dizaynın tekrarlanma denklemi olur.)

Örnek 1.4.4. ün tekrarlanma denkleminde aşağıdaki matris elde edilir.

$$A^t A = (r - \lambda)J + \lambda J = \begin{bmatrix} 3 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 3 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 3 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 3 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 3 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 3 \end{bmatrix}$$

Yukarıdaki blok dizayn tanımından tekrarlanma matrisi ve denklemi arasındaki ilişki $A^t A = (r - \lambda)J + \lambda J$ dir. Burada J , v mertebeli birim matris ve J , aynı mertebeli tüm elemanları 1'den oluşan matristir. $A^t A$ ifadesinin determinanı;

$$\begin{aligned} |A^t A| &= [r + (v - 1)\lambda](r - \lambda)^{(v-1)} \\ &= [r + r(k - 1)](r - \lambda)^{(v-1)} \\ &= [k + k(k - 1)](k - \lambda)^{(v-1)} \\ &= k^2(k - \lambda)^{(v-1)} \neq 0 \end{aligned}$$

şeklindedir. Eğer blok dizaynı simetrikse (1) denklemi kullanılarak

$$|A^t A| = k^2(k - \lambda)^{v-1} \quad (2)$$

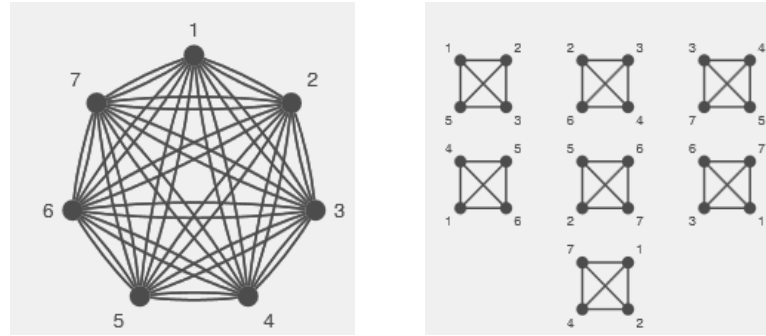
yazılır. A simetrik blok dizaynının tekrarlanma matrisi tekil değildir. Bunu kullanarak bir simetrik blok tasarımının tekrarlanma matrisinin normal olduğu gösterilebilir.

Yani $|A^t A| = |A|^2$ olduğundan;

$$A^t A = AA^t = (k - \lambda)I + \lambda J \quad (3)$$

(2) ve (3) denklemlerinden simetrik blok tasarımının sadece v çift, $n = k - \lambda$ bir tam kare olduğunda mevcut olacağı sonucuna varılmıştır (Moore ve Pollatsek, 2013).

Örnek 1.4.5. $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ kümesinin 4 elemanlı $D = \{1, 2, 3, 5\}$ alt kümesinin ötelemeleri alınarak oluşturulan bloklarıyla aşağıdaki gibi görülmektedir (Peifer, 2013).



Şekil 1. (7,4,2) Parametrelî Simetrik Dizayn (Peifer, 2013)

Bir blok dizaynının tekrarlanma matrisinin tanımı, farklı yazarlara ve hatta aynı yazarın farklı çalışmalarına göre değişmektedir. Bazıları yukarıda A^t tarafından belirlenen matrisin A yerine tekrarlanma matrisi olduğunu söylemektedir. Bu nedenle referansa başvururken kullanılan tekrarlanma matrisi dikkatlice kontrol edilmelidir.

Aşağıdaki teoremler fark kümelerinin parametreleri arasındaki ilişkileri, tekrarlanma matrisi ve tekrarlanma denklemleri ile ilgili bilgiler içermektedir.

Teorem 1.4.1. Bir D simetrik dizaynın v, k, λ parametreleri arasında $(v - 1)\lambda = k(k - 1)$ bağıntısı vardır. Bu bağıntıdan;

$$k^2 - \lambda v = k - \lambda,$$

$$(v - k)\lambda = (k - 1)(k - \lambda)$$

eşitlikleri elde edilir (Lander, 1983).

Teorem 1.4.2. Bir (v, k, λ) simetrik dizaynında v çift ise, n bir tam sayının karesine eşit olmak zorundadır (Schützenberger, 1949).

Özellik 1.4.1. Bir simetrik dizaynın tekrarlanma matrisi A ise, J elemanlarının hepsi 1 olan uygun boyutlu bir kare matris ve I uygun boyutlu birim matris olmak üzere,

- $AJ = JA = kI$
- $AA^T = A^T A = nI + \lambda J$
- $|\det A| = kn^{\frac{v-1}{2}}$

eşitlikleri mevcuttur (Lander, 1983).

Teorem 1.4.3. Bir simetrik dizaynın tekrarlanma matrisi A ise, J elemanlarının hepsi 1 olan uygun boyutlu bir kare matris ve I uygun boyutlu birim matris olmak üzere,

$$AA^T = A^T A = nI + \lambda J$$

dir (Ryser ve Bruck, 1949).

İspat: Özellik 1.4.1 deki $AA^T = nI + \lambda J$ eşitliğinden;

$$\begin{aligned} \det(AA^T) &= \det(nI + \lambda J) \\ &= \begin{bmatrix} n + \lambda & \lambda & \lambda & \dots & \lambda \\ \lambda & n + \lambda & \lambda & \dots & \lambda \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \lambda & \lambda & \lambda & \dots & n + \lambda \end{bmatrix} \end{aligned}$$

2., 3., ..., v . sütunlar 1. sütuna eklenirse;

$$= \begin{bmatrix} n + v\lambda & \lambda & \lambda & \dots & \lambda \\ n + v\lambda & n + \lambda & \lambda & \dots & \lambda \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ n + v\lambda & \lambda & \lambda & \dots & n + \lambda \end{bmatrix}$$

$$\begin{aligned}
&= (n + v\lambda) \begin{bmatrix} 1 & \lambda & \lambda & \dots & \lambda \\ 1 & n + \lambda & \lambda & \dots & \lambda \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & \lambda & \lambda & \dots & n + \lambda \end{bmatrix} \\
&= (n + v\lambda) \begin{bmatrix} 1 & \lambda & \lambda & \dots & \lambda \\ 0 & n & 0 & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \dots & n \end{bmatrix} \\
&= (n + v\lambda)n^{v-1}
\end{aligned}$$

bulunur. Yani;

$$\det(AA^T) = (n + v\lambda)n^{v-1}$$

dir. $n + v\lambda = k^2$ olduğundan

$$\det(AA^T) = A^2 = k^2 n^{v-1}$$

olur. Buradan $|detA| = kn^{\frac{v-1}{2}}$ bulunur.

Tanım 1.4.12 (*Simetrik Dizaynın Tekrarlanma matrisi*) Noktalar kümesi $\mathcal{P} = (p_1, p_2, \dots, p_v)$, bloklar kümesi $\mathcal{B} = (B_1, B_2, \dots, B_v)$ ve $i, j \in \{1, 2, \dots, v\}$ olmak üzere (v, k, λ) simetrik dizaynında;

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

şeklinde tanımlanan bir $M = [m_{ij}]_{v \times v}$ matrisine *simetrik dizaynın tekrarlanma matrisi* denir. M matrisi $(13, k, \lambda)$ simetrik dizaynının tekrarlanma matrisi olmak üzere aşağıdaki gibi ifade edilir (Hall ve Ryser, 1951; Lander, 1983).

$$MM^T = \begin{bmatrix} k & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda \\ \lambda & k & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda \\ \lambda & \lambda & k & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda \\ \lambda & \lambda & \lambda & k & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda \\ \lambda & \lambda & \lambda & \lambda & k & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda \\ \lambda & \lambda & \lambda & \lambda & \lambda & k & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda \\ \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & k & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda \\ \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & k & \lambda & \lambda & \lambda & \lambda & \lambda \\ \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & k & \lambda & \lambda & \lambda & \lambda \\ \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & k & \lambda & \lambda & \lambda \\ \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & k & \lambda & \lambda \\ \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & k & \lambda \\ \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & k \end{bmatrix}$$

1.5. Fark Kümeleri

Fark kümeleriyle ilgili incelemeye sonlu grup olan G dikkate alarak başlanmaktadır. G devirli grup ise $\mathbb{Z}_v = \{0, 1, 2, \dots, v-1\}$ ile temsil edilen toplamsal grubu kullanılmaktadır. Bir grubun alt kümesi olarak ayarlanan bir fark kümesini (Singer, 1939)'in tanımladığı gibi sonlu projektif geometriden üretilen küme olarak gösterebiliriz.

Tanım 1.5.1. (*Fark Kümesi*) v mertebeli $(G, +)$ grubunun $D = \{d_1, d_2, \dots, d_k\}$ boştan farklı alt kümesi ($\text{mod } v$) deki kalan sınıflarının k tane elemanı alındığında $d_i, d_j \in D, d_i \neq d_j$ ve $a \neq 0(\text{mod } v)$ olmak üzere;

$$d_i - d_j \equiv a(\text{mod } v)$$

kongüransı λ tane (d_i, d_j) çözümüne sahiptir. Buradaki D alt kümesine G grubunun (v, k, λ) parametrelili bir *fark kümesi* denir.

Fark kümelerini herhangi bir $*$ işlemi ile de tanımlayabiliriz. $|G| = v$ ve $(G, *)$ grubunun boştan farklı bir alt kümesi $|D| = k$ olsun. D kümesinden aldığımız birbirinden farklı iki elemanın

$$d_i * d_j^{-1} \equiv a(\text{mod } v)$$

şeklindeki elemanlarının oluşturduğu çoklu küme Δ , G 'nin etkisiz elemanından farklı

elemanlarının her birini tam λ kez içeriyorsa, D alt kümesine G 'nin (v, k, λ) parametrelerine sahip bir fark *kümesi* denir (Lander, 1983).

Fark kümelerinin uygulama sorularında işlem olarak toplama kullanılmıştır.

Örnek 1.5.1. $G = \mathbb{Z}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ olmak üzere $(G, +)$ grubunun on bir elemanı noktalar kümesi, $(\mathbb{Z}_{11}, +)$ grubunun fark kümesi $D = \{1, 3, 4, 5, 9\}$ kümesinin 11 adet ötelemesinden oluşturulsun. Yani $a \in G$ olmak üzere

$$B_1 = 0 + D = \{1, 3, 4, 5, 9\}$$

$$B_2 = 1 + D = \{2, 4, 5, 6, 10\}$$

$$B_3 = 2 + D = \{3, 5, 6, 7, 0\}$$

$$B_4 = 3 + D = \{4, 6, 7, 8, 1\}$$

$$B_5 = 4 + D = \{5, 7, 8, 9, 2\}$$

$$B_6 = 5 + D = \{6, 8, 9, 10, 3\}$$

$$B_7 = 6 + D = \{7, 9, 10, 0, 4\}$$

$$B_8 = 7 + D = \{8, 10, 0, 1, 5\}$$

$$B_9 = 8 + D = \{9, 0, 1, 2, 6\}$$

$$B_{10} = 9 + D = \{10, 1, 2, 3, 7\}$$

$$B_{11} = 10 + D = \{0, 2, 3, 4, 9\}$$

B kümesi bloklar kümesi olarak aşağıdaki gibidir.

$$B = \{\{0, 1, 2, 6, 9\}, \{0, 1, 5, 8, 10\}, \{0, 2, 3, 4, 8\}, \{0, 3, 5, 6, 7\}, \{0, 4, 7, 9, 10\}, \\ \{1, 2, 3, 7, 10\}, \{1, 3, 4, 5, 9\}, \{1, 4, 6, 7, 8\}, \{2, 4, 5, 6, 10\}, \{2, 5, 7, 8, 9\}, \{3, 6, 8, 9, 10\}\}$$

Bloklar kümesi incelendiğinde;

- 11 tane nokta vardır, $|G| = 11$.
- 11 tane blok vardır, $|B| = 11$.
- Her bir nokta 5 tane blokta bulunur.
- Her blokta 5 tane nokta bulunur.
- Herhangi iki blokta 2 tane ortak nokta bulunur.
- Herhangi iki nokta 2 blokta birlikte bulunur.

Dolayısıyla D kümesi, $(11, 5, 2)$ parametrelili bir simetrik dizayndır.

Teorem 1.5.1. D, G 'nin (v, k, λ) parametrelili bir fark kümesi olsun. Öyleyse v, k, λ parametreleri arasındaki ilişki;

- $k(k - 1) = \lambda(v - 1)$
- $n = k^2 - \lambda v$

dir (Lander, 1983).

İspat: D bir fark kümesi ise eleman sayısı k dır. D fark kümesinin her d_1, d_2 sıralı ikililerinin sayısı $k(k - 1)$ tanedir. Δ çoklu kümesinin eleman sayısı $d_1 - d_2$ farklarının sayısıdır. Yani $k(k - 1)$ tanedir. G 'nin boştan farklı $v - 1$ tane elemanı Δ çoklu kümesinde listelenen elemanlar arasında tam λ kez tekrar etmektedir. Yani $\lambda(v - 1)$ elde edilir. Bu iki ifade de $d_1 - d_2$ farklarının sayısını verir. Dolayısıyla;

$$k(k - 1) = \lambda(v - 1) \quad (4)$$

dir. (4) düzenlenirse;

$$k^2 - k = \lambda v - \lambda$$

$$k^2 - \lambda v = k - \lambda$$

$$k^2 - \lambda v = n$$

elde edilir. (n , fark kümesinin mertebesidir.)

Dizaynlar için önemli olan parametreler fark kümeleriyle doğrudan ilişkilidir. Bir fark kümesi genellikle üç parametre kullanılarak tanımlanır. Dördüncü parametre olarak fark kümesinin mertebesi sıklıkla tartışılmaktadır ve fark kümesinin en önemli parametresi olduğu düşünülmektedir. Fark kümesinin parametreleri aşağıdaki gibi ifade edilmektedir.

- $|G| = v$
- $|D| = k$
- λ sayısı G 'nin sıfırdan farklı elemanları için D 'deki iki elemanın farkı olarak temsil edilir.
- $n = k - \lambda$ fark kümesinin mertebesidir.

Fark kümesi tanımından fark kümesinin parametrelerinin birbiriyle ilişkili olduğu görülmektedir. Eğer D kümesi, G 'nin uygun bir alt kümesi ise, $0 < k \leq v$ ve

$\lambda < k$ olduğu açıktır. Dolayısıyla mertebenin her zaman pozitif olduğu söylenir.

Bir grubun fark kümesinin seçimi yapılırken özel şartlar altında uygun bir alt kümesi olması istenmektedir. Bu nedenle aşağıdaki (v, k, λ) simetrik dizaynları büyük ölçüde dikkate alınmamaktadır. Çünkü aşağıdaki alt kümeler bir grubun önemsiz alt kümeleridir ve her biri fark kümesidir.

$G = \{1, 2, \dots, v-1\}$ grubunun fark kümesi olan alt kümeleri;

- $D \neq \emptyset$,
- $D = \{0, 1, \dots, v-1\} = G$,
- $D = \{i\}$, $0 \leq i \leq v-1$,
- $i \in \{1, 2, \dots, v-2\}$ olmak üzere $D = \{0, 1, \dots, (i-1), (i+1), \dots, (v-1)\}$

şeklindedir.

Bu fark kümelerinin parametreleri;

- $(v, k, \lambda) = (v, 0, 0)$,
- $(v, k, \lambda) = (v, v, v)$,
- $(v, k, \lambda) = (v, 1, 0)$,
- $(v, k, \lambda) = (v, v-1, v-2)$

olarak bulunur (Moore ve Pollatsek, 2013).

Kuadratik rezidülerden yararlanarak da fark kümesi oluşturulabilmektedir. Aşağıdaki teoremden bir grubun tam karelerinin kümesiyle oluşturulabilecek fark kümesinden bahsedilmektedir.

Teorem 1.5.2. p tek asal sayı ve $D, \mathbb{Z}_p$ nin sıfırdan farklı tam karelerinin kümesi olsun. Eğer $D, \mathbb{Z}_p$ toplama grubunda bir fark kümesi ise $p \equiv 3(mod 4)$ tür (Lander, 1983).

İspat: Kabul edelim ki $D, \mathbb{Z}_p$ de bir fark kümesidir. $v = p$ olduğu bilinmektedir. $k = |D|$ olduğu gösterilmelidir. p asal olduğu için $\mathbb{Z}_p$ nin sıfırdan farklı $p-1$ tane elemanı ile $\mathbb{Z}_p^*$ çarpım grubu oluşturulabilir. Her bir elemanını elemanlarının karelerine gidecek şekilde oluşturulan çarpım grubu, D kümesi üzerinde bir homomorfizma oluşturacaktır. Çünkü p bir tek asal sayıdır, $x^2 = 1$ ise $x = \pm 1$ bu homomorfizmanın çekirdeğinin elemanıdır ve çekirdeğin eleman sayısı 2 dir. Bu durumda $\mathbb{Z}_p$ 'de sıfırdan farklı tam kare sayısı tam tamına $\frac{p-1}{2}$ tanedir. Dolayısıyla

$k = \frac{p-1}{2}$ dir. k değeri $k(k-1) = \lambda(v-1)$ denkleminde yerine yazılırsa;

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

elde edilir. Burada λ bir tam sayı olmak zorunda olduğundan $p \equiv 3(mod 4)$ olmalıdır.

Aşağıdaki iki teoremden toplamsal $\mathbb{Z}_p$ grubunun fark kümelerini bulmak için bir yöntemden bahsedilmiştir.

Teorem 1.5.3. x tek tamsayı olmak üzere $p = 4x^2 + 1$ formunda bir asal sayı ve $G = \mathbb{Z}_p$ olsun. O zaman G 'deki elemanların sıfır hariç tüm dördüncü kuvvetler kümesi olan D , bir fark kümesidir (Lehmer, 1953).

Teorem 1.5.4. x tek tamsayı olmak üzere $p = 4x^2 + 9$ formunda bir asal sayı ve $G = \mathbb{Z}_p$ olsun. O zaman G deki elemanların sıfır dahil tüm dördüncü kuvvetler kümesi olan D , bir fark kümesidir (Lehmer, 1953).

1.6. Ötelemeler

Bir G grubunda (v, k, λ) parametrelili fark kümesi $D = \{d_1, d_2, \dots, d_k\}$ varsa, bu orijinal fark kümesinin değerlerini grup elemanları ile öteleyerek yeni fark kümeleri tanımlanabilir. Yani bir gruba ait fark kümesi varsa diğer fark kümeleri, bu kümenin ötelemeleri yardımıyla bulunabilir.

Tanım 1.6.1. (Öteleme) Bir G grubunda (v, k, λ) parametrelili fark kümesi $D = \{d_1, d_2, \dots, d_k\}$ ve $s \in \mathbb{Z}$ bir tamsayı olsun.

$$D + s = \{d_1 + s, d_2 + s, \dots, d_k + s\}$$

kümesi $(mod v)$ de bir fark kümesidir. Bu orijinal fark kümesi D 'nin bir *ötelemesi* olarak adlandırılır (Lander, 1983).

Örnek 1.6.1. $\mathbb{Z}_7$ deki $D = \{1, 2, 4\}$ kümesinin $(7, 3, 1)$ parametrelili bir fark kümesi olduğu bilinmektedir. Bu küme ötelenerek başka fark kümeleri elde edilebilir.

- $1 + D = \{2, 3, 5\}$
- $4 + D = \{5, 6, 1\}$
- $10 + D = \{4, 5, 0\}$
- $16 + D = \{3, 4, 6\}$

şeklinde oluşturulan fark kümeleri parametreleri $(7, 3, 1)$ olan fark kümeleridir.

Aşağıdaki teoremden grubun elemanlarıyla uygun bir fark kümesinin ötelemeleri alınarak oluşturulabilecek fark kümesinden ve fark kümesi üzerinde tanımlanan otomorfizma ile oluşturulabilecek fark kümesinden bahsedilmektedir.

Teorem 1.6.1. $D \subseteq G$, (v, k, λ) parametreleriyle bir fark kümesi olsun.

- $g \in G$ olmak üzere $D + g$ ve $g + D$ kümelerinin ikisinin de parametreleri (v, k, λ) dır.
- a, G 'nin bir otomorfizması olduğu zaman $a(D)$, (v, k, λ) parametrelili bir fark kümesidir (Lander, 1983).

Tanım 1.6.2. (*Açınım-Development*) $D \subseteq G$, G grubunun bir fark kümesi olmak üzere, G 'nin elemanları tekrarlanan yapının noktalarını, D kümesinin elemanları ile G kümesinin elemanlarının ötelemeleri blokları oluşturuyorsa bu tekrarlanan yapıya D 'nin *açınımı* denir. $devD$ ile gösterilir (Lander, 1983).

Teorem 1.6.2. $D \subseteq G$ alt kümesi G grubunun (v, k, λ) parametrelili bir fark kümesi ise $devD$ bir simetrik dizayndır (Lander, 1983).

İspatı için (Moore ve Pollatsek, 2013) kaynağına bakılabilir.

Teorem 1.6.3. D ve D' , G grubunun iki fark kümesi olsun. $devD$ ve $devD'$ simetrik dizaynları birbirine izomorftur (Lander, 1983).

Tanım 1.6.3. (*Denk Fark Kümeleri*) (v, k, λ) parametrelerine sahip iki fark kümesi D_i ve D_j olsun. Eğer $D_i = a(D_j) + s$ olacak şekilde $s \in \mathbb{Z}$ ve $a \in \text{Aut}(G)$ bir otomorfizma ise D_i ve D_j denk fark kümeleridir denir (Lander, 1983).

Tanım 1.6.4. (*Tümleyen*) G grubunun iki fark kümesi D_1 ve D_2 olsun. Eğer;

$$D_1 \cup D_2 = \{0, 1, \dots, v-1\} = G$$

oluyorsa D_1 ve D_2 birbirinin *tümleyenidir* denir (Lander, 1983).

Eğer D_1 fark kümesinin parametreleri (v, k, λ) ise tümleyeni olan D_2 fark kümesinin parametreleri de hesaplanabilir. D_2 fark kümesinin parametreleri (v^*, k^*, λ^*) olmak üzere karşılık gelen eşitlikleri bulalım.

$$v^* = v, k^* = v - k \text{ ve } \lambda^* = \frac{k^*(k^*-1)}{(v^*-1)} \text{ olduğundan;}$$

$$\begin{aligned} \lambda^* &= \frac{(v-k)(v-k-1)}{(v-1)} \\ \lambda^* &= \frac{(v-k)(v-1)}{(v-1)} - \frac{(k(v-k)+k(1-1))}{(v-1)} \\ \lambda^* &= (v-k) - \frac{k(v-1)}{(v-1)} + \frac{k(k-1)}{(v-1)} \\ \lambda^* &= v - 2k + \lambda \end{aligned}$$

elde edilir. $n = k - \lambda$ olmak üzere $n^* = k^* - \lambda^*$ ifadesinin karşılığını bulalım.

$$\begin{aligned} n^* &= (v-k) - (v-2k-\lambda) \\ n^* &= k - \lambda \end{aligned}$$

olarak bulunur. Birbirinin tümleyeni olan kümelerde v ve n değerlerinin değişmediği görülür. D_1 ve D_2 fark kümeleri aynı G grubundan oluşturulmuştur. İki kümenin de v parametresinin aynı kalacağı açıktır. D_1 kümesinin mertebesi k ise D_2 tümleyeninin mertebesi $v - k$ dır. O halde tümleyenlerin λ değerleri birbirinden farklı olmak zorundadır. Bu nedenle tümleyen kümelerden birinin eleman sayısı $\frac{v}{2}$ değerinden büyük ise diğeri $\frac{v}{2}$ den küçük olmalıdır. D_1 kümesinin parametreleri (v, k, λ) , D_2 kümesinin parametreleri $(v, v - k, v - 2k + \lambda)$ şeklindedir (Moore ve Pollatsek, 2013).

Teorem 1.4.1. de (v^*, k^*, λ^*) yerine yazılırsa;

$$\begin{aligned}
 k^*(k^* - 1) &= \lambda^*(v - 1) \\
 (v - k)(v - k - 1) &= (v - 2k + \lambda)(v - 1) \\
 (v - k)(v - k - 1) &= (v - k - n)(v - 1) \\
 (v - k)(v - 1) - (v - k)k &= (v - k)(v - 1) - n(v - 1) \\
 n(v - 1) &= k(v - k) = kk^*
 \end{aligned}$$

elde edilir.

1.7. Fark Kümelerinde Varlık Problemi

Herhangi bir özel grup için bir fark kümesinin var olup olmadığı veya birden fazla eşit fark kümesi olup olmadığı nasıl belirlenir? Bir fark kümesinin var olması için gerekli şartlar nelerdir? Bu sorular tarafından belirlenen alanlar arasında önemli bir çakışma olmasına rağmen onları ayrı ayrı incelemek gerekmektedir. Bu bölüm öncelikli olarak fark kümelerinin varlığı için gerekli koşullarla ilgilenmektedir. (v, k, λ, n) parametreleri yardımıyla, fark kümelerinin var olma olasılığını analiz etmek için bazı araçlar kullanılacaktır.

Fark kümelerinde varlık problemi konusunda önemli ilerlemeler kaydedilmiştir. Bunlardan en önemlisi $k(k - 1) = \lambda(v - 1)$ veya $k^2 = \lambda v + n$ ilişkisidir. Bu genel varlık probleminin bir alt problemi olan $ebob(v, n) > 1$ ya da $ebob(k, v) > 1$ şartına uygun bir fark kümesinin var olma durumudur. Bunun varlığı 2003 yılına kadar ifade edilmemiştir. Bu makalede $ebob(v, n) > 1$ ve $ebob(v, n) = 1$ şartını sağlayan parametrelerle olası devirli fark kümelerinin bir tablosu verilmiştir (Baumert, 2003). Başka bir varlık problemi $\lambda = 1$ ile sonsuz sayıda düzlemsel fark kümesinin bulunduğunu belirtmektedir. Her $\lambda \geq 2$ için sınırlı sayıda fark kümesinin bulunduğu varsayılmıştır. Bu varsayım herhangi bir tek değer için ispatlanmamış olup aksi de ispatlanmamıştır. Aynı varsayım simetrik blok dizaynları için de açık bir problemdir (Baumert, 1971).

1.8. Bruck Ryser Chowla Teoremi

Bruck-Ryser-Chowla Teoremi belirli parametrelere sahip fark kümelerinin mevcut olup olmadığını kanıtlayan en önemli yöntemlerden biridir. Bruck Ryser Chowla teoremi (v, k, λ) simetrik dizaynının varlığı için v , k , λ parametrelerinde gerekli koşulları vermektedir. Bir fark kümesinin açılımı simetrik bir dizayn olduğundan bu teorem v mertebeli fark kümesinin parametrelerine sınırlamalar getirmektedir. Aynı zamanda lineer diophant denkleminin bir çözümünün varlığının simetrik bir dizaynın varlığı üzerinde nasıl etkisi olabileceğini de açıklamaktadır. Bruck Ryser Chowla teoremi yazarların ilk makalesinde $\lambda = 1$ için ispatlanmıştır. (Bruck ve Ryser, 1949) İkinci makalelerinde sonucu herhangi bir pozitif λ sayısı için genişletmişlerdir (Ryser ve Chowla, 1949;1950).

Tanım 1.8.1. (Projektif Uzay) N ve D elemanları sırasıyla noktalar ve doğrular olarak isimlendirilen ayrık iki küme ve $\circ$, N 'den D 'ye bir üzerinde olma bağıntısı ise $(N, D, \circ)$ sıralı üçlüsüne bir *geometrik yapı* denir. Aşağıdaki üç aksiyomu sağlayan bir $(N, D, \circ)$ geometrik yapısına bir *projektif düzlem* denir ve P ile gösterilir. N sonlu ise P projektif düzlemine *sonlu projektif düzlem* adı verilir (Kaya, 1992).

P1. Herhangi farklı iki noktadan bir tek doğru geçer.

P2. Herhangi iki doğrunun en az bir ortak noktası vardır.

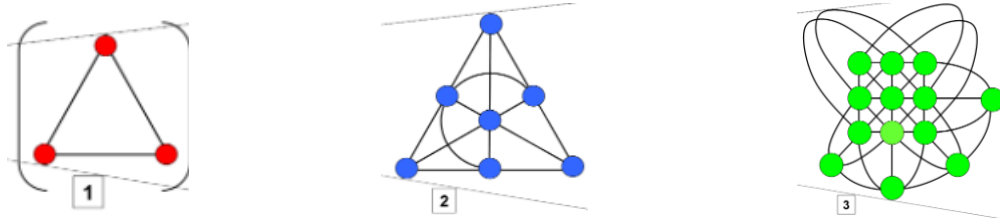
P3. Herhangi üçü doğrusal olmayan dört nokta vardır.

$P = (N, D, \circ)$ projektif düzlemin bir doğrusu üzerindeki nokta sayısının bir eksiğine P 'nin *mertebesi* denir. Sonlu bir projektif düzlemin mertebesi n ise toplam nokta ve doğrularının sayısı eşit ve $n^2 + n + 1$ dir. Projektif düzlemin en küçük mertebesi 2 dir ve bu projektif düzlem *Fano Düzlemi* olarak adlandırılır. $n \geq 2$ şartını sağlayan her tamsayı için projektif düzlemin varlığı kesin değildir. Tarry, mertebesi 6 olan 43 noktalı bir projektif düzlemin var olmadığını göstermiştir (Tarry, 1900).

Bilinen sonlu projektif düzlemlerin mertebeleri, p bir asal sayı ve r bir pozitif tam sayı olmak üzere p^r şeklindedir. Sonlu projektif düzlemlerin mertebelerinin yalnızca p^r şeklindeki sayılardan mı ibaret olduğu şimdiye kadar cevaplandırılmamış bir problemdir. Tahminler mertebesi p^r şeklinde olmayan bir projektif düzlemin varolamayacağı yönündedir. Hangi mertebeden projektif düzlemlerin var olduğu ve varsa bunların geometrik yapısının nasıl olacağı hala cevaplandırılmamış önemli bir sorudur.

Bu probleme kısmi olarak bir cevap Bruck Ryser tarafından verilmiştir. “ n , $n \equiv 1(mod4)$ ya da $n \equiv 2(mod4)$ özelliğinde bir tam sayı olsun. n negatif olmayan iki tam sayının kareleri toplamı olarak yazılamıyorsa mertebesi n olan bir projektif düzlem yoktur.” Bruck Ryser Chowla teoremine göre 6, 14, 21, 22, 30, 33, 38, 42, 46, 54, 57 gibi sonsuz çokluktaki sayıların hiçbirisi bir projektif düzlemin mertebesi değildir. Ayrıca 10, 12, 15, 18, 20, 24, 26, 28, 34, 35, 36, 40 gibi sonsuz çokluktaki sayıların herhangi biri için mertebesi bu sayı olan projektif düzlemin var olup olmadığı hala bilinmemektedir ve Bruck Ryser Chowla Teoremi de bu durumda kesin bir sonuç vermemektedir (Bennett,1995).

Tanım 1.8.2. (Projektif uzaylar) $(v, k, \lambda) = (n^2 + n + 1, n + 1, 1)$ parametrelili simetrik dizaynlardır. n parametresi projektif uzayın mertebesidir. BRC teoremi bir asalın kuvveti olmayan n mertebeli projektif uzaylarda varoluş sorusunu araştırmak için kullanılmaktadır. $n \equiv 1,2(mod4)$ olmak üzere bazı x, y için $n = x^2 + y^2$ dir. Aşağıdaki dizayn örnekleri $n=1$, $n=2$ ve $n=3$ mertebeli projektif düzlemleridir (Cameron, 1991).



Şekil 2. $n= 1, 2, 3$ için Projektif Düzlemler (Cameron, 1991)

Örnek 1.8.1. $k > 1$ bir asalın kuvveti olmadığı $\lambda = 1$ ile bir simetrik dizayn var mıdır?

Projektif düzlem bir tekrarlanma yapısıdır. Öyle ki;

- (i) Her bir farklı nokta çifti tam olarak bir doğruda bulunur.
- (ii) Her bir farklı doğru çifti ortak bir noktaya sahiptir.

Bir projektif uzayın sonlu tekrarlanma yapısı olması için gerek ve yeter şart $\lambda = 1$ ile bir simetrik dizayn olmasıdır. Dizaynın bir projektif düzlem olduğunu göstermek basittir. Projektif düzlem teorisi zengin ve karmaşıktır. $\lambda \geq 2$ olan simetrik dizaynlar hakkında nispeten az şey bilinmektedir.

Teorem 1.8.1. (*Bruck-Ryser-Chowla Teoremi, 1949;1950*) v mertebeli bir G grubunda (v, k, λ) bir simetrik dizayn olmak üzere;

- Eğer v çift ise n bir tam karedir.
- Eğer v tek ise $x^2 = ny^2 + (-1)^{(v-1)/2} \lambda z^2$ diophant denklemi x, y, z tamsayılarında sıfırdan farklı bir çözüme sahiptir.

Lineer diophant denklemi $v \equiv 3(mod 4)$ yada $v \equiv 1(mod 4)$ olduğu durumlarda aşağıdaki gibi yazılır.

$$x^2 = \begin{cases} \text{Eğer } v \equiv 3(mod 4) & ny^2 - \lambda z^2 \\ \text{Eğer } v \equiv 1(mod 4) & ny^2 + \lambda z^2 \end{cases} .$$

v 'nin çift sayı olduğu durumda ispat açıktır. v 'nin tek olma durumunu ispatlarken matrislerin denkliği kullanılmıştır.

İspata başlamadan önce bu teoremin farklı parametrelerle fark kümelerinin dışında nasıl kullanıldığına dair bazı örneklerle yer verilmiştir. Bu örneklerde ele alınan parametreler $k(k-1) = \lambda(v-1)$ temel testini karşılamaktadır.

Örnek 1.8.2. $(56, 11, 2)$ parametreleri incelenecek olursa; $v = 56$, $k = 11$ ve $\lambda = 2$ parametreleri $\lambda(v-1) = k(k-1)$ kriterini sağlamaktadır. Bruck Ryser Chowla teoremine göre $v = 56$ çift olduğundan simetrik dizaynın var olabilmesi için $n = k - \lambda$ nın bir tam kare olması gerekir. Burada $n = 11 - 2 = 9$ bir tam kare olduğundan $(56, 11, 2)$ parametrelerine sahip bir simetrik dizayn vardır ve bu nedenle bu parametrelere bağlı bir fark kümesi adayı vardır.

Örnek 1.8.3. $(76, 25, 8)$ parametrelerini ele alalım. v çift olduğunda n tam kare olmalıdır. $v = 76$, $k = 25$ ve $\lambda = 8$ parametreleri $\lambda(v-1) = k(k-1)$ şartını sağlar. Bruck Ryser Chowla teoremine göre $v = 76$ çift olduğundan simetrik dizaynın var olması için $n = k - \lambda$ bir tam kare olmalıdır. Ancak $n = 25 - 8 = 17$ bir tam kare olmadığından bu parametrelere bağlı bir simetrik dizaynın olmadığı söylenmektedir. Dolayısıyla $(76, 25, 8)$ parametreleriyle bir fark kümesi yoktur.

Örnek 1.8.4. $(49, 16, 5)$ parametrelerini ele alalım. $v = 49$ tek sayı, $n = 16 - 5 = 11$ olduğundan diophant denklemi;

$$x^2 = 11y^2 + (-1)^{\frac{49-1}{2}}5z^2 = 11y^2 + 5z^2$$

dir. $(x, y, z) = (4, 1, 1)$ sıfırdan farklı bir çözümdür. Bruck Ryser Chowla teoremi yardımıyla bu parametrelerle bir fark kümesinin var olabileceği söylenmektedir. Ancak Bruck Ryser Chowla teoreminin tanımı gereği $(49, 16, 5)$ parametreleri bir simetrik dizayn olmalıdır. Yani Bruck Ryser Chowla teoreminin çözüm üretmesi verilen üçlünün fark kümesi olmasını garanti etmemektedir (Moore ve Pollatsek, 2013).

Bir diophant denkleminin hiçbir çözümü olmadığını göstermek daha zordur. Şimdi Bruck Ryser Chowla teoreminin lineer diophant denklemine bir çözüm üretmediğinde bize yardımcı olacak Legendre teoremini tanımlayalım. Burada aRb 'nin anlamı $a, (mod\ b)$ de bir tam karedir.

Tanım 1.8.3. (*Kuadratik Rezidü*). a ve n , $(a, n) = 1$ ve $n > 0$ olacak şekilde tamsayılar olmak üzere $y^2 \equiv a(mod\ n)$ denkleminin bir çözümü varsa a 'ya $(mod\ n)$ de bir *kuadratik rezidü* denir (Williams, 1988).

Teorem 1.8.2. (*Legendre Teoremi*) a ve b sıfırdan farklı, en az biri pozitif tam kare olmayan eleman ve $d = ebob(a, b)$ olsun. Bu durumda; $x^2 = ay^2 + bz^2$ denkleminin sıfırdan farklı bir tamsayı çözümü olması için gerekli şartlar aşağıdaki gibidir.

- $a R b$: $a, (mod\ b)$ de tam karedir.
- $b R a$: $b, (mod\ a)$ da tam karedir.
- $-\left(\frac{ab}{d^2}\right) R d$: $-\left(\frac{ab}{d^2}\right), (mod\ d)$ de tam karedir.

(Legendre, 1785).

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

Aşağıdaki örnekte Legendre Teoreminin uygulama örneği verilmiştir.

Örnek 1.8.5. Eğer $n = 6$ mertebeli bir projektif uzay varsa $(v, k, \lambda) = (43, 7, 1)$ parametreleriyle bir simetrik dizayn olacaktır. Bruck Ryser Chowla teoremine göre böyle bir dizayn varsa $x^2 = 6y^2 - z^2$ diophant denkleminin sıfırdan farklı bir tamsayı çözümü olmalıdır. Legendre Teoremi bir çözüm için $-1 \pmod{6}$ da tam kare olması gerektiğini belirtir. Bu yüzden diophant denklemini sıfırdan farklı bir çözüme sahip değildir. Buradan 6 mertebeli projektif uzayın hiçbir dizaynının olmadığı söylenir (Moore ve Pollatsek, 2013).

1980’li yıllarda Bruck Ryser Chowla teoreminin tersinin doğru olabileceği düşünülmüştür. Yani (v, k, λ) parametreleri BRC şartlarını ve $k(k - 1) = \lambda(v - 1)$ ilişkisini sağlarsa o parametrelerle bir simetrik dizayn var mıdır sorusu sorulmuştur. 1989’da Clement Lam, John McCay, Stanley Swiercz ve Larry Thiel 1970’lerdeki Larry Carter’ın çalışmasına dayanarak 10 mertebeli projektif uzayın olmadığını ispatlamışlardır (Lam, 1989)

Şimdi Langrange teoreminin ispatında bize yardımcı olacak bir lemmayı inceleyeceğiz.

Lemma 1.8.3. p tek bir asal sayı olsun. m, x ve y tamsayı olmak üzere;

$$mp = x^2 + y^2 + 1 \quad ; \quad 1 \leq m < p$$

dir. (Moore ve Pollatsek, 2013)

İspat: x^2 ’nin $\pmod{p}$ ’ye göre değerlerinin kümesini $0 \leq x < \frac{p-1}{2}$ olarak düşünelim. Bu değerlerden ikisinin eşit olmadığını varsayalım. Bu nedenle bu küme $\frac{p+1}{2}$ farklı rezidü içerir. Şimdi $0 \leq y < \frac{p-1}{2}$ olacak şekilde $\pmod{p}$ ’ye göre $-y^2 - 1$ ’in tüm değerlerinin ikinci bir kümesini alalım. Yine $\frac{p+1}{2}$ farklı rezidü vardır. Çünkü $\pmod{p}$ ’nin farklı rezidüleri sadece p kadardır.

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

Herhangi bir x ve y için $x^2 + y^2 + 1 \equiv 0 \pmod{p}$ dir. Buradan en az bir $m \in \mathbb{Z}^+$ için

$$x^2+y^2 + 1 = mp$$

yazılır. Ayrıca $0 \leq x, y < \frac{p-1}{2}$ olduğundan;

$$x^2+y^2 + 1 = mp \leq \frac{(p-1)^2}{4} + \frac{(p-1)^2}{4} + 1 < p^2$$

dir. Dolayısıyla $1 \leq m < p$ için;

$$mp = x^2+y^2 + 1$$

elde edilir.

Teorem 1.8.4. (Lagrange Teoremi) Her pozitif tamsayı, dört tam karenin toplamı olarak yazılabilir (Lagrange, 1770).

İspat: İki tamsayının her biri dört tam karenin toplamı olarak yazılabilirse onların çarpımı şeklinde de yazılabilir. Bu yüzden her asal için sonucu ispatlamak yeterlidir. $p = 2$ asalı için $2 = 1^2 + 1^2 + 0^2 + 0^2$ yazılır. Şimdi p 'nin tek bir asal sayı olduğunu varsayalım. (Yani $p \neq 2$) Lemma 1.8.3.'ten $1 \leq m < p$ için $mp = x^2+y^2 + 1$ sağlayan bir m tamsayısı vardır. Bu, mp 'yi dört tam karenin toplamı olarak ifade edebileceğimizi gösterir.

$$mp = a^2+b^2 + c^2 + d^2 ; 1 \leq m < p \quad (5)$$

için m en küçük tamsayı seçilirse mp dört tam karenin toplamı olarak yazılır. $m = 1$ için gösterilir. $m > 1$ ve A, B, C, D tamsayıları;

$$a \equiv A, b \equiv B, c \equiv C, d \equiv D \pmod{m} ; \frac{-m}{2} \leq A, B, C, D \leq \frac{m}{2}$$

seçilirse $A^2 + B^2 + C^2 + D^2 \equiv 0 \pmod{m}$ yazılır. Buradan;

$$A^2 + B^2 + C^2 + D^2 = rm \quad (6)$$

olacak şekilde $r \in \mathbb{Z}^+$ tamsayısı vardır. Ayrıca $0 \leq A^2 + B^2 + C^2 + D^2 \leq 4\left(\frac{m}{2}\right)^2 = m^2$ dir. Yani $0 \leq r \leq m$ dir. Biz $0 < r < m$ olduğunu kabul etmiştik. Eğer $r = 0$ olursa A, B, C, D 'nin her biri sıfırdır. Ama bu her bir a, b, c, d 'nin m 'yi böldüğünü bu yüzden de $mp = a^2 + b^2 + c^2 + d^2$ 'ninde m^2 'yi böldüğü anlamına gelir. Dolayısıyla m böler p elde edilir. p asal ve $1 < m < p$ kabul ettiğimizden bu bir çelişkidir.

Tersine; $r = m$ ise A, B, C, D 'nin her biri $\frac{m}{2}$ olacaktır. Burada a, b, c, d 'nin herbirinin $\frac{m}{2}$ nin bir katı olduğu elde edilir. Çünkü $m^2, a^2 + b^2 + c^2 + d^2$ 'yi böler. Bu bir çelişkidir. (5) ve (6) denklemleri çarpılırsa;

$$(mp).(rm) = (a^2 + b^2 + c^2 + d^2)(A^2 + B^2 + C^2 + D^2) \quad (7)$$

elde edilir. Sağ taraftan dört tam karenin toplamı olarak yazılırsa;

$$\begin{aligned} rpm^2 &= (aA + bB + cC + dD)^2 + (aB - bA + cD - dC)^2 \\ &\quad + (aC - bD - cA + dB)^2 + (aD + bC - cB - dA)^2 \end{aligned} \quad (8)$$

elde edilir. (7) denkleminin sağ tarafındaki her bir terim en az bir u_j tamsayısı için $(u_j m)^2$ formundadır. (8) denkleminin her iki tarafı m^2 ile bölünürse rp dört tam karenin toplamı olarak kalır. $0 < r < m$ olup bu bir çelişkidir. Çünkü m , dört tam karenin toplamı olarak ifade edilebilen p 'nin en küçük tamsayı çarpanı olarak seçilmiştir. Bu nedenle $m = 1$ için $1.p = p$ dört tam karenin toplamı olarak ifade edilir. (İspat için (Rademacher ve Toeplitz, 1956) kaynağına bakılabilir.)

Köşegen matrislerin denkliğiyle ilgili aşağıdaki teoremin ispatında Lagrange teoreminin sonuçları kullanılacaktır.

Tanım 1.8.4. (Köşegenleştirme). A ve B elemanları $\mathbb{K}$ cisminden alınan aynı boyutlu kare matrisler olsun. Elemanları $\mathbb{K}$ cisminden alınan terslenebilen bir S matrisi için $S^T A S = B$ oluyorsa A, B ye dönüştüren matris S matrisidir (Moore ve Pollatsek, 2013).

Teorem 1.8.5. n bir pozitif bir tamsayı olmak üzere $\text{diag}(n, n, n, n) \cong \text{diag}(1, 1, 1, 1) = J_4$ tür (Moore ve Pollatsek, 2013).

İspat: S matrisi $J_4 \rightarrow nJ_4$ dönüştüren bir matris olmak üzere dört tam kareler teoremini kullanarak n dört tam sayının kareleri toplamı olarak,

$$n = a^2 + b^2 + c^2 + d^2$$

şeklinde yazılır. Matrisi oluşturmak için bu tamsayılar kullanılır.

$$S = \begin{bmatrix} a & b & c & d \\ b & -a & -d & c \\ c & d & -a & -b \\ d & -c & b & -a \end{bmatrix}$$

O halde $S^T J_4 S = nJ_4$ tür. S 'nin tersinin var olduğu, elemanlarının tam sayı olduğu ve aynı zamanda $\mathbb{Q}$ 'da oldukları unutulmamalıdır.

Bruck Ryser Chowla teoreminin ispatının devamı için matrislerin denkliği ile ilgili temel durumlara ihtiyacımız vardır.

Lemma 1.8.6. A matrisi $v \times v$ boyutlu bir matris olmak üzere B matrisi, en az bir $i \neq j$ için A matrisinin i .satırı ile j .sütunun yer değiştirmesi ve ya i .sütun ile j .sütunun yer değiştirmesiyle elde edilirse $A \cong B$ dir (Moore ve Pollatsek, 2013).

Lemma 1.8.7. A matrisi $v \times v$ boyutlu bir matris ve $c \in \mathbb{Q}$ olsun. B matrisi, A matrisinin en az bir $i \neq j$ için $c \times i$.satırı j .satıra eklenmesiyle ve ya $c \times i$. sütun, j . sütuna eklenmesiyle elde edilirse $A \cong B$ dir (Moore ve Pollatsek, 2013).

Lemma 1.8.8. Rasyonel elemanlı herhangi bir simetrik matris köşegen bir matrise denktir (Moore ve Pollatsek, 2013).

Lemma 1.8.9. A, B, C kare matrisler A ve B aynı boyutlu matrisler olmak üzere eğer $A \cong B$ ise $\begin{bmatrix} C & 0 \\ 0 & A \end{bmatrix} \cong \begin{bmatrix} C & 0 \\ 0 & B \end{bmatrix}$ dir (Williams, 1937).

Şimdi Bruck Ryser Chowla teoreminin, v 'nin tek olduğu durumun ispatında kullanacağımız aşağıdaki teoremi inceleyelim.

Teorem 1.8.10. (*Witt'in Sadeleştirme Teoremi, 1937*) A ve B matrisi $m \times m$ boyutlu terslenebilen matrisler ve $c \in \mathbb{Q}$ olsun. Eğer $A \cong B$ ise $\begin{bmatrix} c & 0 \\ 0 & A \end{bmatrix} \cong \begin{bmatrix} c & 0 \\ 0 & B \end{bmatrix}$ dir (Witt, 1937).

İspat: $(m+1) \times (m+1)$ boyutundaki matrislerin eşdeğer olduğunu ve A 'yı B 'ye dönüştüren rasyonel bir matrisin S olduğunu varsayalım. A ve B terslenebilen matrisler olduğundan S 'de terslenebilir olmalıdır.

$$W^T \cdot \begin{bmatrix} c & 0 \\ 0 & A \end{bmatrix} \cdot W = \begin{bmatrix} t & v^T \\ u & M^T \end{bmatrix} \begin{bmatrix} c & 0 \\ 0 & A \end{bmatrix} \begin{bmatrix} t & u^T \\ v & M \end{bmatrix} = \begin{bmatrix} c & 0 \\ v & B \end{bmatrix}$$

olacak şekilde $W = \begin{bmatrix} t & v^T \\ u & M^T \end{bmatrix}$ vardır. Matrislerin çarpımı ve karşılık gelen bloklara eşitlenmesi;

$$\begin{aligned} t^2c - v^TAv &= c \\ tcu^T + v^TAM &= 0 \\ tcu + M^TAv &= 0 \\ cuu^T + M^TAM &= B \end{aligned} \tag{9}$$

$d = \frac{1}{t+1} \neq 1 \neq 0$ sıfırdan farklı olmak üzere $S = M - dvu^T$ olsun. S^TAS olduğunu göstermeliyiz. İlk olarak;

$$\begin{aligned} S^TAS &= (M^T - duv^T)A(M - dvu^T) \\ &= M^TAM - dM^TAvu^T - duv^TAM + d^2uv^TAvu^T \end{aligned}$$

bulunur. Yukarıdaki (9) denklemleri kullanılırsa;

$$\begin{aligned} S^TAS &= M^TAM + cdtuu^T + cdtuu^T - d^2cu(t^2 - 1)u^T \\ &= M^TAM + cd[2t - d(t^2 - 1)]uu^T \end{aligned}$$

$$\begin{aligned}
&= M^T AM + cuu^T \\
&= B
\end{aligned}$$

elde edilir. Böylece $A \cong B$ gösterilmiş olur. İspat için (Moore ve Pollatsek, 2013) kaynağına bakılabilir.

1.8.1. v Tek Olduğunda BRC Teoreminin İspatı

İspat 1.8.1. Eğer v tek ve D , (v, k, λ) parametreleriyle bir simetrik dizayn ise;

$$x^2 = ny^2 + (-1)^{\frac{v-1}{2}} \lambda z^2$$

diophant denklemi sıfırdan farklı (x, y, z) tamsayı çözümüne sahiptir. (v, k, λ) simetrik dizaynının var olduğunu ve bu dizayn için $v \times v$ tekrarlanma matrisinin N olduğunu varsayalım. O zaman $N^T N = nI + \lambda J$ ile $(v+1) \times (v+1)$ boyutlu matris aşağıdaki gibi tanımlanır.

$$A = \begin{bmatrix} & & & 1 \\ & N & & \vdots \\ & & & 1 \\ 1 & \dots & 1 & k/\lambda \end{bmatrix}$$

$A^T D A = E$ olacak şekilde $D = \text{diag}[1, \dots, 1, -\lambda]$ ve $E = \text{diag}[n, \dots, n, -n/\lambda]$ regüler matrisleri var olduğundan $D \cong E$ dir.

1.DURUM: $v \equiv 1(mod 4)$ olduğu varsayılsa $\frac{v-1}{2}$ çifttir. Teorem 1.8.5. tekrar tekrar uygulanırsa E 'deki 1_s ile ns 'nin $(v-1)$ tanesi değiştirilirse elde edilen köşegen matris E 'ye denktir. Bu matrisler köşegen ve regüler matris olduğundan Witt'in sadeleştirme teoremini yeni matrisin ortak $(v-1)$ tane 1_s değerini sadeleştirmek için kullanabiliriz.

$$\begin{bmatrix} 1 & 0 \\ 0 & -\lambda \end{bmatrix} \cong \begin{bmatrix} n & 0 \\ 0 & -n/\lambda \end{bmatrix}$$

$M = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$ birinci matrisi ikinci matrise dönüştüren bir matris olsun.

$$M^T \begin{bmatrix} 1 & 0 \\ 0 & -\lambda \end{bmatrix} M = \begin{bmatrix} n & 0 \\ 0 & -n/\lambda \end{bmatrix}$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -\lambda \end{bmatrix} \begin{bmatrix} a & c \\ b & d \end{bmatrix} = \begin{bmatrix} n & 0 \\ 0 & -n/\lambda \end{bmatrix}$$

$a^2 - b^2\lambda = n$ elde edilir. Denklem $a^2 = b^2\lambda + n$ şeklinde düzenlenirse diophant denkleminin $(x, y, z) = (a, 1, b)$ basit olmayan bir çözümü bulunur.

2.DURUM: $v \equiv 3(mod 4)$ olduğu varsayılırsa $\frac{v-1}{2}$ tek olur. Önce $D \cong E$ olduğunu göstermeliyiz. Lemma 1.8.6. ve Lemma 1.8.9. kullanılarak $(v+2) \times (v+2)$ boyutlu matrisin elemanlarının $(v-1)$ tanesine n eklenirse;

$$diag[1, \dots, 1, n, -\lambda] \cong diag[n, \dots, n, n, -n/\lambda]$$

elde edilir. Teorem 1.8.5. kullanılarak ikinci matristeki 1_s ile ns 'nin $(v+1)$ tanesi değiştirilirse elde edilen köşegen matrisler birbirine denktir.

$$diag[1, \dots, 1, n, -\lambda] \cong diag[1, \dots, 1, 1, -n/\lambda]$$

Witt'in sadeleştirme teoreminden;

$$\begin{bmatrix} n & 0 \\ 0 & -\lambda \end{bmatrix} \cong \begin{bmatrix} 1 & 0 \\ 0 & -n/\lambda \end{bmatrix}$$

şeklinde yazılır. $M = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$ birinci matrisi ikinci matrise dönüştüren bir matris olsun.

$$M^T \begin{bmatrix} n & 0 \\ 0 & -\lambda \end{bmatrix} M = \begin{bmatrix} 1 & 0 \\ 0 & -n/\lambda \end{bmatrix}$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} n & 0 \\ 0 & -\lambda \end{bmatrix} \begin{bmatrix} a & c \\ b & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -n/\lambda \end{bmatrix}$$

Sonuç olarak $na^2 - \lambda b^2 = 1$ eşitliği elde edilir. Eşitlik düzenlenirse $na^2 - \lambda b^2 = 1^2$ diophant denkleminin $(x, y, z) = (1, a, b)$ olan sıfırdan farklı bir rasyonel çözümü olduğu gösterilmiş olur. İspat (Moore ve Pollatsek, 2013) kitabından alınmıştır.

1.9. Çarpanlar

Tanım 1.9.1. (*Çarpan*) D, G 'nin bir fark kümesi ve herhangi $x, y \in G$ için $\alpha: D \rightarrow aDb$ dönüşümü varsa G 'nin α otomorfizması D 'nin bir çarpanı olarak adlandırılır. Özel olarak $b = 1$ ise $\alpha(D) = xD$ olur. O halde α, D 'nin bir sol çarpanı olarak adlandırılır. Bu tanımdan eğer G değişmeliyse D kümesi de değişmeli olacağından her elemanı bir sol çarpan olacaktır (Hall, 1947).

G, v mertebeli değişmeli toplamsal bir grup t, v ile aralarında asal pozitif bir tamsayı olsun. G 'nin ϕ_t otomorfizması $\phi_t: a \rightarrow t \cdot a$ şeklinde tanımlanır. Eğer D, G 'de bir fark kümesi ise herhangi bir otomorfizması altındaki görüntüsü bir fark kümesidir. Çarpımsal gruplar için $\phi_t: a \rightarrow a^t$ şeklinde tanımlanan otomorfizma ile $\phi_t(D) = D^{(t)} = \{d^t \mid d \in D\}$ yazılır. Burada ϕ_t otomorfizması fark kümesini kendisine veya ötelemesine götürmektedir.

Tanım 1.9.2. (*Sayısal Çarpan*) G değişmeli bir grup, D 'de G kümesinin bir fark kümesi ve $(t, |G|) = 1$ şartını sağlayan bir t tam sayısı olsun. O halde bazı $h \in G$ için $\phi_t(D) = hD$ ise ϕ_t bir sayısal çarpandır (Hall, 1947).

Örnek 1.9.1. $D = \{2, 3, 5, 11\}$ kümesi $\mathbb{Z}_{13}$ 'te $(13, 4, 1)$ fark kümesi olsun. ϕ_3 dönüşümünü düşünürsek $\phi_3(D) = \phi_3(\{2, 3, 5, 11\}) = \{6, 9, 2, 7\}$ olur. Bu sayısal çarpan aslında D 'nin bir ötelemesidir. $4 \in \mathbb{Z}$ olmak üzere $\phi_3(D) = 4 + D$ olduğu görülmektedir. Bazı t çarpanları için $\phi_t(D) = D$ olduğunda ilginç bir durum oluşmaktadır.

Örnek 1.9.2. $D = \{0, 1, 3, 9\}$ kümesi $\mathbb{Z}_{13}$ ün $(13, 4, 1)$ parametrelili bir fark kümesi olmak üzere $\phi_3(D) = \phi_3(\{0, 1, 3, 9\}) = \{0, 3, 9, 1\} = D$ dir. Burada $\phi_3(D) = D$ olduğundan teoremden D, ϕ_3 'ün orbitlerinin bir birleşimidir.

Teorem 1.9.2. (Birinci Çarpan Teoremi) D , (v, k, λ) parametrelili deęişmeli bir fark kümesi p , n 'yi bölen ancak v 'yi bölmeyen bir asal sayı olsun. Eğer $p > \lambda$ ise o zaman p , D 'nin bir sayısal çarpanıdır (Hall, 1947). İspat için (Jungnickel, Dinitz ve Stinson, 1992) kaynaklarına bakılabilir.

Sonuç 1.9.1. Birinci çarpan teoremindeki varsayım olmadan $p > \lambda$ şartı sağlar. İspatı için (Hall, 1947) kaynağına bakılabilir.

Teorem 1.9.3. (İkinci Çarpan Teoremi) D , G kümesinin (v, k, λ) parametrelili deęişmeli bir fark kümesi ve $(m, v) = 1$ olacak şekilde n nin bir böleni $m > \lambda$ olsun.

O halde $t \in \mathbb{Z}$, $(t, v) = 1$ olmak üzere $\forall p - m$ asalı için $\exists f \in \mathbb{Z}, f \geq 0$ olmak üzere $t \equiv p^f \pmod{v^*}$ şartını sağlayan t , D nin bir sayısal çarpanıdır.

İspatı için (Beth, Jungnickel ve Lenz, 1999) makalesine bakılabilir.

Sonuç 1.9.2. D , G kümesinin (v, k, λ) parametrelili deęişmeli bir fark kümesi ve $\text{ebob}(p, v) = 1$ ile $n = k - \lambda$ nın p asalının bir kuvveti olduęu varsayılırsa o halde p , D için bir sayısal çarpanıdır. İspatı için (Jungnickel, 1992) kaynağına başvurulabilir.

1.10. Çarpan Teorisini Kullanarak Fark Kümesi Oluşturma

G bir grup ve α , $\alpha(D) = D$ olacak şekilde D fark kümesinin bir çarpanı olsun. O zaman D , G 'nin elemanlarının bir permütasyonu olarak α için orbitlerin birleşiminden oluşur. Bu teorem varoluş testinde kullanılabilir. v mertebeli bir grup verilmiş ise fark kümesini tanımlayabilecek olası parametre kümelerini bulmak için Tanım 1.6.4 kullanılır. Daha sonra herhangi bir çarpanın var olup olmadığını belirlemek için çarpan teoremleri kullanılır. Sonra fark kümelerinin orbitleri hesaplanır ve fark kümesinin boyutuna göre orbitlerden oluşturulup oluşturulamayacağı belirlenir. Bu adımlara uyulması orbitlerin bir fark kümesi oluşturmasını garanti etmeyecektir. Ancak orbitlerin birleşimi fark kümesinin boyutunu oluşturmazsa bu fark kümesinin bulunmamasını garanti edecektir.

Fark kümesi oluştururken çarpanlardan faydalanılabilir. Aşağıda örnek fark kümelerinin varlığını gösterirken çarpanın var olmasının fark kümesinin varlığını garanti etmede başarısız olduğunu gösterir.

Örnek 1.10.1. Mertebesi 79 olan bir grupta 79 asal sayı olup $\lambda = \frac{k(k-1)}{78}$ dan $k = 13$, $\lambda = 2$ olası fark kümesi $(79, 13, 2)$ parametreleri ile belirlenir. $n = k - \lambda = 13 - 2 = 11$ asal olup bir sayısal çarpandır. Ancak $\phi_{11}(G)$ 'nin orbitleri $[0]$ ve 39 elemanlı iki orbittir. Bu orbitlerin hiçbir birleşimi 13 elemanlı bir fark kümesi üretmeyecektir. Bu nedenle test bu parametrelerle bir fark kümesinin olmadığını kanıtlamaktadır. Yani çarpanın var olması fark kümesini garanti etmemektedir. $\phi_{11}(G)$ 'nin orbitlerinden bir tanesi aşağıdaki gibidir.

[1,2,4,5,8,9,10,11,13,16,18,19,20,21,22,23,25,26,31,32,36,38,40,42,44,45,46,49,50, 52,55,62,64,65,67,72,73,76]

İkinci Çarpan testi kullanılarak fark kümelerinin varlığı araştırılabilir. Ancak bu testin de geçemediği örnekler mevcuttur.

Örnek 1.10.2. G 'nin mertebesi 29 olsun. 29 bir asal sayı olduğundan $G \cong \mathbb{Z}_{29}$ alınır. Bir fark kümesinin olası parametrelerini bulmak için Tanım 1.6.4.'ü kullanabiliriz. Bu durumda $(29, 7, 1)$ parametreleri $n = k - \lambda = 7 - 1 = 6$ olduğunu verir. Bulunan n , bir asalın kuvveti olmadığı için ikinci çarpan testimiz başarısız olur.

Orbit (yörünge) tanımı kullanılarak fark kümelerinin varlığı araştırılabilmektedir. Teorem 1.9.1'den orbitlerin birleşimi kullanılarak fark kümeleri oluşturulabilir.

Örnek 1.10.3. Mertebesi 35 olan bir G grubunu düşünelim. 35 asal sayı olmadığından asal çarpanlarına ayrılır ve $\mathbb{Z}_{35} = \mathbb{Z}_7 \oplus \mathbb{Z}_5$ şeklinde yazılabilir. Şimdi bir fark kümesinin olası parametrelerini bulmak için Teorem 1.4.2. kullanılır. Bu durumda $(35, 17, 8)$ parametre kümesi fark kümesinin mertebesinin $n = k - \lambda = 17 - 8 = 9 = 3^2$ olduğunu verir. Dolayısıyla 3 bir sayısal çarpandır. ϕ_3 'ün orbitleri;

[0], [15, 10, 30, 20, 25, 5], [21, 28, 14, 7], [3, 9, 27, 11, 33, 29, 17, 16, 13, 4, 12, 1]
[6, 18, 19, 22, 31, 23, 34, 32, 26, 8, 24, 2]

dir. Bu orbitlerin boyutları 1, 4, 6, 12 dir. Bu nedenle parametreleri karşılayan orbitlerin birleşimi $1 + 4 + 12$ şeklindedir. Buradan olası fark kümeleri;

$$D_1 = \{0, 1, 3, 4, 7, 9, 11, 12, 13, 14, 16, 17, 21, 27, 28, 29, 33\}$$

$$D_2 = \{0, 2, 6, 7, 8, 14, 18, 19, 21, 22, 23, 24, 26, 28, 31, 32, 34\}$$

Ancak $(2,35) = 1$ olup $2D_1 = D_2$ olduğundan D_1 ve D_2 denk fark kümeleridir.

Örnek 1.10.4. $\mathbb{Z}_{21}$ in bir fark kümesini bulmak için çarpanları kullanalım. $v = 21$ ve k 'nın $1 < k < 11$ olduğuna dikkat ederek $k(k-1) = \lambda(v-1)$ eşitliğinden $k(k-1) = \lambda(20)$ elde edilir. Terimler düzenlenirse $\lambda = \frac{k(k-1)}{20}$ dir. Buradan $k(k-1)$ in 20 sayısının tamsayı katı olması gerektiği görülür. $k = 5$ bizim kriterimizi sağlar ve $\lambda = 1$ bulunur. O halde $(21, 5, 1)$ in bir fark kümesi olduğunu varsayalım. Şimdi orbitleri bulmak için bir t çarpanı seçmeliyiz. $(t, 21) = 1$ olduğundan $t = 2$ alınır. Şimdi ϕ_2 'nin bütün orbitlerini bulalım.

$$[\bar{0}]_2 = \{0\}$$

$$[\bar{1}]_2 = \{1, 2, 4, 8, 16, 11\}$$

$$[\bar{3}]_2 = \{3, 6, 12\}$$

$$[\bar{5}]_2 = \{5, 10, 20, 19, 17, 13\}$$

$$[\bar{7}]_2 = \{7, 14\}$$

$$[\bar{9}]_2 = \{9, 18, 15\}$$

$k = 5$ olacak şekilde kriterlere uygun iki fark kümesi $D_1 = [\bar{3}] \cup [\bar{7}] = \{3, 6, 12, 7, 14\}$ ve $D_2 = [\bar{9}] \cup [\bar{7}] = \{9, 18, 15, 7, 14\}$ dir. Şimdi $\phi_2(D) = D$ olduğunu göstermeliyiz.

$$\phi_2(D_1) = \phi_2(\{3, 6, 12, 7, 14\}) = \{6, 12, 3, 14, 7\} = D_1$$

$$\phi_2(D_2) = \phi_2(\{9, 18, 15, 7, 14\}) = \{18, 15, 9, 14, 7\} = D_2$$

D_1 ve D_2 kümeleri $\mathbb{Z}_{21}$ 'in iki fark küme adayıdır.

Örnek 1.10.5. Aşağıdaki fark kümeleri için 1'den farklı çarpan bulalım.

a) $D_1, \mathbb{Z}_{19}$ un kuadratik rezidüleri kümesi olsun.

b) $D_2, \mathbb{Z}_{23}$ ün kuadratik rezidüleri kümesi olsun.

Çözüm a) $\mathbb{Z}_{19}$ 'ün kuadratik rezidüleri $D_1 = \{1, 4, 5, 6, 7, 9, 11, 16, 17\}$ dir. $v = 19$ ve k değeri $\lambda = \frac{k(k-1)}{18}$ eşitliğinden $k = 9$ olarak bulunur. $k(k-1) = \lambda(v-1)$ denkleminde $\lambda = 4$ olarak bulunur. Dolayısıyla $n = k - \lambda = 9 - 4 = 5$ tir. 5 asal sayı ve $5 \nmid 19$ olduğundan 5, D_1 için bir sayısal çarpanıdır. (Birinci çarpan teoremine göre)

Çözüm b) $\mathbb{Z}_{23}$ 'ün kuadratik rezidülerinin kümesi $D_2 = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$ dir. $v = 23$ ve k değeri $\lambda = \frac{k(k-1)}{22}$ eşitliğinden 11 olarak bulunur. $k(k-1) = \lambda(v-1)$ eşitliğinden $\lambda = 5$ olarak bulunur. Dolayısıyla $n = k - \lambda = 11 - 5 = 6$ asal değildir. Ama çarpanlarından 3 asaldır. $3 \nmid 6$ ve $3 \nmid 23$ tür. Böylece birinci çarpan teoremine göre 3, D_2 'nin bir sayısal çarpanıdır.

Aşağıdaki teoremler çarpanlar ile otomorfizma ilişkisinden bahsetmektedir.

Teorem 1.10.1. G grubunun bir fark kümesi D ve α , D için bir sol çarpan olsun. O zaman α , $devD$ için bir otomorfizmadır (McFarland ve Rice, 1978).

Teorem 1.10.2. G , bir D fark kümesini oluşturan bir grup ve α , D için bir sol çarpan olsun. O zaman α , $devD$ deki bloklardan en az birine sabitlenir (McFarland ve Rice, 1978).

Eğer t , D kümesinin bir çarpanı ise o zaman bir fark kümesini bulmak için sadece ϕ_t nin orbitlerini bulmamız gerektiği söylenebilmektedir.

Örnek 1.10.6. $G = \mathbb{Z}_{67}$ olsun. $v = 67$ ve k değeri $\lambda = \frac{k(k-1)}{66}$ eşitliğinden $k = 12$, $k = 22$, $k = 33$ olarak bulunur. $k(k-1) = \lambda(v-1)$ eşitliğinden $\lambda = 2$, $\lambda = 7$ ve $\lambda = 16$ olarak bulunur. Potansiyel fark kümeleri $(67, 12, 2)$, $(67, 22, 7)$, ve $(67, 33, 16)$ dir. Bu parametrelere Bruck Ryser Chowla teoremi uygulandığında $v = 67 \equiv 3(mod 4)$ olduğundan lineer diophant denklemi $x^2 = ny^2 - \lambda z^2$ olarak bulunur.

Burada $n = k - \lambda = 33 - 16 = 17$ dir. $x^2 = 17y^2 - 16z^2$ lineer diophant denklemi için $(x, y, z) = (1, 1, 1)$ sıfırdan farklı bir çözümdür. Böylece olası fark kümesi parametreleri $(67, 33, 16)$ dir. Bu parametrelerle bir D 'nin var olduğunu kabul edelim. $n = k - \lambda = 33 - 16 = 17$ Sonuç 1.9.2'e göre $(17, 67) = 1$ olduğundan 17, D için bir sayısal çarpanıdır. Böylece Teorem 1.10.1 ve Teorem 1.10.2. ile G 'nin üzerindeki

orbitlerini tespit etmeliyiz.

$$\vartheta_0 = \{0\},$$

$$\vartheta_1 = \{1, 17, 21, 22, 39, 60, 15, 54, 47, 62, 49, 29, 24, 6, 35, 59, 65, 33, 25, 23, 56, 14, \\ 37, 26, 40, 10, 36, 9, 19, 55, 64, 16, 4\}$$

$$\vartheta_2 = \{2, 23, 42, 44, 11, 53, 30, 41, 27, 57, 31, 58, 48, 12, 3, 51, 63, 66, 50, 43, 45, 28, 7, 52, \\ 13, 20, 5, 18, 38, 43, 61, 32, 8\}$$

Orbitlerin uzunlukları olası fark kümesinin mertebesi ile aynıdır. Bu nedenle $v = 67$, $k = 33$ parametreleriyle iki fark kümesi yazılabilir. Bunlar; $D_1 = \vartheta_1$ ve $D_2 = \vartheta_2$ şeklindedir. Colbourn, $D_1 = \vartheta_1$ in $\mathbb{Z}_{67}$ ' nin $(67, 33, 16)$ parametrelili bir fark kümesi olduğunu göstermiştir (Colbourn, 2007).

1.11. Fark Kümelerinin Varlığını Belirleyen Algoritma

Verilen bu algoritma yardımıyla tekrarlanma yapısı parametrelerinin simetrik dizayn olup olmadığı belirlenmektedir. Simetrik dizayn olan tekrarlanma yapıları yani fark kümeleri belirlenmiş olacaktır.

- v mertebeli bir grup verilir.
 - v 'nin asal olup olmadığı test edilir.
 - Eğer v asal değilse, v 'nin asal çarpanları bulunur.
 - Olası fark kümelerinin (v, k, λ) parametreleri belirlenir. Bir fark kümesinin tümleyenleri kullanılarak yeni fark kümeleri belirlenebilir.
- $\lambda = \{1, 2, 3, \dots, (v - 2)\}$ olmak üzere;

$$k = \frac{1 + \sqrt{1 + 4\lambda(v - 1)}}{2}$$

- Özel bir parametre olan $n = k - \lambda$ hesaplanır.
- BRC testi kullanılır. (Gerekirse Legendre Teoremi kullanılır)
- n bir asalın kuvveti olacak şekilde $n = p^m$, $m \in \mathbb{Z}$ varsa p bulunur (Morrice, 2015).

Aşağıdaki tabloda simetrik dizayn olan fark kümelerinin uygun v , k , λ , n ve çarpan değerleri listelenmiştir (Baumert, 2004).

Tablo 1. Simetrik dizayn olan fark kümelerinin uygun v , k , λ , n ve çarpan değerlerinin listesi

v	k	λ	n	Çarpan
429	108	27	81	3
303	151	75	76	16
2585	153	9	144	2
616	165	44	121	11
407	175	75	100	2
4401	176	7	169	13
544	181	60	121	3
3949	189	9	180	3
1545	193	24	169	8
1380	197	28	169	2
1609	201	25	176	2
6271	210	7	203	29
1056	211	42	169	13
2233	217	21	196	16
6301	225	8	217	31
601	225	84	141	3
595	243	99	144	2
611	245	98	147	2
2057	257	32	225	3
2591	260	26	234	3
3181	265	22	243	3
1061	265	66	199	199
531	265	132	133	4
1615	270	45	225	4
2691	270	27	243	3
28325	292	3	289	2
591	295	147	148	16
10990	297	8	289	9

2. YAPILAN ÇALIŞMALAR

Bu çalışma da fark kümeleri ile ilgili genel tanım ve teoremler verilmiş ve fark kümelerinin varlığını araştıran Bruck Ryser Chowla teoreminin simetrik dizaynın varlığını araştırmadaki rolü incelenmiştir. Ayrıca bu çalışma da MATLAB program dilinde fark kümelerinin olmayanlarını eleyen bir kod çalışması yapılmıştır. Literatür taramasında birçok örnekle uygun parametrelili fark kümelerinin listesi oluşturulmuştur. (Lehmer, 1953)'in fark kümesi olarak kabul ettiği fakat (Bruck, Ryser ve Chowla, 1949)'nın uyguladığı yöntemle fark kümesi olmayan örnekler elenmiştir.

Fark kümesi olmayan dizayn örneklerini eleyen MATLAB program dilinde yazılmış Bruck Ryser Chowla teoreminin v parametresinin tek olduğu durumda sonuç veren kodunun bazı sonuçları listelenmiştir. Ana program kodunda $v = 60$ 'a kadar olan simetrik dizayn örnekleri elde edilmiştir. Küme parametrelerini araştıran koda grubun eleman sayısı girildiğinde $k(k - 1) = \lambda(v - 1)$ şartını sağlayan kaç tane (v, k, λ) olası fark kümesi olduğunu çıktı olarak vermektedir. Bruck Ryser Chowla teoreminin ikinci koşulunda yer alan lineer diophant denkleminin sıfırdan farklı çözümlerini istenen aralıkta listeleyen BRC lineer kodu yazılmıştır. Fark kümeleri belirli bir kurala göre dağılım göstermediğinden fark kümesi olan dizayn örneği bulmak oldukça zordur. Bizim yaptığımız çalışma da bir dizaynın fark kümesi olmadığını göstermenin daha kolay yöntemleri sunulmuştur.

2.1. Simetrik Dizaynın MATLAB Uygulaması

Bu başlık altında uygun parametrelili simetrik dizaynın oluşum aşamaları kod yardımıyla aktarılmıştır. Bu kod girilen (v, k, λ) değerleri ile uygun parametrelili bir simetrik dizaynın var olup olmadığını kontrol etmektedir. Eğer varsa 1 yoksa 0 sonucunu vermektedir.

```
%Adı Soyadı: Safiye Ozturk
%Ogrenci No: 172613012

% girdiler: v, G'nin eleman sayısı
% k, D'nin eleman sayısı

function g = simetrikdizayn(v,k,lam)
g = 0;
Z = 0:(v-1);
D = nchoosek(0:v,k);
[n_D,~]= size(D); %D matrisinin satır sayısı, Tüm D'leri tarıyoruz.
tic
for j=1:n_D
    Dk = D(j,:);%D'nin j. elemanını aldık. Bunu deneyeceğiz.
    %B dizilerini oluşturuyoruz.
    B = zeros(v,k); %initialization
    for i=1:v
        B(i,:) = Dk+(i-1);%öteleme işlemi
    end

    H = (B>=v) . *B-v; %
    H(H<0)=0; %Bu kısımda B vektörlerinin elemanlarından v'den
    %büyük olanlardan v çıkardık.
    B = (B<v) . *B + H ; %

    %A vektörünü oluşturalım
    A = zeros(v,v); %A matrisi tüm elemanları sıfır olan matris.
    for ii = 1:v
        for jj=1:v
            if ~isempty(find(Z(ii)==B(jj,:),1))
                A(jj,ii)=1;%B'nin içinde Z'nin elemanı varsa 1 yapıyoruz
            end
        end
    end
toc
    %%%%%%%%%

    if A'*A == lam*ones(v)+(k-lam)*eye(v)
        g = 1;
        return
    end

    %if Dk==[0 1 2]; disp(B);disp(A); disp(A'); disp(A'*A); end
    clear B A %A ve B yi temizledik, bir sonraki döngüde tekrar
    %oluşsun. Her ne kadar zeros ile initialize etsekte dursun burada
end
```

```

>>simetrikdizayn (7,3,1)    ans = 1
>>simetrikdizayn (11,5,2)   ans = 1
>>simetrikdizayn (13,4,1)   ans = 1
>>simetrikdizayn (15,7,3)   ans = 1
>>simetrikdizayn (19,9,4)   ans = 1
>>simetrikdizayn (21,5,1)   ans = 1
>>simetrikdizayn (23,11,5)  ans = 1
>>simetrikdizayn (31,6,1)   ans = 1
>>simetrikdizayn (31,15,7)  ans = 1
>>simetrikdizayn (35,17,8)  ans = 1
>>simetrikdizayn (37,9,2)   ans = 1
>>simetrikdizayn (43,21,10) ans = 1
>>simetrikdizayn (47,23,11) ans = 1
>>simetrikdizayn (59,29,14) ans = 1

```

2.2. BRC Teoreminin MATLAB Uygulaması

Bu kod BRC teoreminin ikinci şartının bir uygulamasıdır. Yani,

$x^2 = ny^2 + (-1)^{\frac{v-1}{2}} \lambda z^2$ denkleminin olası çözümlerini çalıştıracaktır. Bu uygulama y ve z değişkenleri için sadece 1 ile 1000 arasındaki tamsayı değerlerini kontrol edecektir. Yazılan üçlünün potansiyel fark kümesi olup olmadığını sonuç olarak gösterir. Eğer program 0 çıktısını verirse böyle bir dizayn yoktur denir. Ama 1 çıktısı çıkarsa simetrik dizayn olduğunu sağlamak gerekir.

```

%Adı Soyadı: Safiye Ozturk
%Ogrenci No: 172613012

function s = brc_tek(v,k,lam)
s = 0;
n = k-lam;
tic
for y= 1:1000
    for z= 1:1000
        x= sqrt((n*y^2)+((-1)^((v-1)/2))*lam*z^2);
        if floor(x)==x && x^2>0
            s = 1;
    end
end
toc
return
end
end
end

```


Aşağıdaki örnekler içerisinde Bruck Ryser Chowla teoreminin çözüm üretmediği dizayn olmayan örnekler de mevcuttur.

```
>> brc_tek (27,13,16)      ans = 0
>> brc_tek (34,12,4)      ans = 0
>> brc_tek (46,10,2)      ans = 0
>> brc_tek (92,14,2)      ans = 0
>> brc_tek (172,19,2)     ans = 0
>> brc_tek (115,19,4)     ans = 0
>> brc_tek (117,29,7)     ans = 0
>> brc_tek (119,59,7)     ans = 0
>> brc_tek (125,32,8)     ans = 0
>> brc_tek (67,12,2)      ans = 0
>> brc_tek (137,17,2)     ans = 0
>> brc_tek (103,18,3)     ans = 0
>> brc_tek (53,13,3)      ans = 0
>> brc_tek (43,15,5)      ans = 0
>> brc_tek (77,20,5)      ans = 0
>> brc_tek (157,40,10)    ans = 0
>> brc_tek (171,85,41)    ans = 0
>> brc_tek (173,44,11)    ans = 0
>> brc_tek (181,45,11)    ans = 0
>> brc_tek (185,24,3)     ans = 0
>> brc_tek (187,31,5)     ans = 0
>> brc_tek (193,129,82)   ans = 0
>> brc_tek (6271,210,7)   ans = 1
>> brc_tek (2591,260,26)  ans = 1
>> brc_tek (5167,288,16)  ans = 1
>> brc_tek (5167,820,130) ans = 0
>> brc_tek (5167,1107,237) ans = 0
>> brc_tek (5167,1477,422) ans = 0
>> brc_tek (5167,1764,602) ans = 0
>> brc_tek (5167,2296,1020) ans = 1
>> brc_tek (5167,2583,1291) ans = 1
```

2.4. Ana Program

Ana program öncelikle v , k , λ parametrelerinin uygun olup olmadığını ölçer. Daha sonra bu parametrelerle simetrik dizayn olup olmadığını kontrol eder ve verilen aralıkta uygun fark kümelerini listelemektedir. Birçok kombinasyon olacağından matlab programının sonuç verme süresi çok uzundur.

```
%Adı Soyadı: Safiye Ozturk
%Ogrenci No: 172613012

for v = 7:2:60
    for k = 3:1:v/2
        for lam = 1:(k-1)
            s = brc_tek(v,k,lam);
            tic
            if s == 1
                g = simetrikdizayn(v,k,lam);
                if g==1
                    fprintf('%i %i %i\n',v,k,lam)
                end
            end
        end
    end
end
end
```

Ana program kodunu çalıştırdığımızda v 'nin 60'a kadar olan değerlerini tarayarak uygun parametrelili simetrik dizaynların çıktısını aşağıdaki gibi vermektedir.

```
(v,k,lamda)=(7,3,1),(11,5,2),(13,4,1),(15,7,3),(19,9,4),(21,5,1),
(23,11,5),(31,6,1),(31,15,7),(35,17,8),(37,9,2),(43,21,10),(47,23,11),
(57,8,1),(59,29,14)
```

2.5. Uygun Fark Kümesi Parametreleri İçin MATLAB Uygulaması

Bu kod küme parametreleri arasındaki ilişki yardımıyla oluşturulabilecek olası fark kümelerinin sonuçlarını çıktı olarak vermektedir. Girilen bir v değeri karşılığında $k(k-1) = \lambda(v-1)$ şartını sağlayan olası (v, k, λ) parametrelili simetrik dizaynlarının sayısını vermektedir.

```
%Adı Soyadı: Safiye Ozturk
%Ogrenci No: 172613012

function kume_parametreleri(v)

% v G'nin mertebesi
% deger v'nin sınır değeri

if(mod(v,2)==0)
    deger = v/2;
else
    deger = (v-1)/2;
end
sayac=0;
% Burada k değerlerini 2'den başlatıyoruz. k,1 olduğunda lamda 0 olur.
for k=2:deger
    lam = (k*(k-1))/(v-1);
    if (mod(lam,1)==0)
        %Çıktıları fark kümesi parametreleri için adaydır.
        disp(sprintf('(v,k,l)=(%1.0f,%1.0f,%1.0f) parametrelerin
potansiyel kümesi.',v,k,lam))
        sayac=sayac+1;
    end
end
disp(sprintf('%1.0f potansiyel fark küme adayı vardır.',sayac))
end
```

Aşağıdaki çıktılar girilen v değeri ile $v(v-1) = \lambda(k-1)$ şartını sağlayan potansiyel üçlülerin sayısını vermektedir.

```
>> kume_parametreleri (6271)
(v,k,l)=(6271,210,7)      parametrelerin potansiyel kümesi.
(v,k,l)=(6271,286,13)     parametrelerin potansiyel kümesi.
(v,k,l)=(6271,495,39)     parametrelerin potansiyel kümesi.
(v,k,l)=(6271,760,92)     parametrelerin potansiyel kümesi.
(v,k,l)=(6271,1045,174)   parametrelerin potansiyel kümesi.
(v,k,l)=(6271,1255,251)   parametrelerin potansiyel kümesi.
(v,k,l)=(6271,1540,378)   parametrelerin potansiyel kümesi.
(v,k,l)=(6271,1596,406)   parametrelerin potansiyel kümesi.
```

```
(v,k,l)=(6271,1881,564) parametrelerin potansiyel kümesi.  
(v,k,l)=(6271,2091,697) parametrelerin potansiyel kümesi.  
(v,k,l)=(6271,2376,900) parametrelerin potansiyel kümesi.  
(v,k,l)=(6271,2641,1112) parametrelerin potansiyel kümesi.  
(v,k,l)=(6271,2850,1295) parametrelerin potansiyel kümesi.  
(v,k,l)=(6271,2926,1365) parametrelerin potansiyel kümesi.  
(v,k,l)=(6271,3135,1567) parametrelerin potansiyel kümesi.  
15 potansiyel fark küme adayı vardır.
```

```
>> kume_parametreleri (2591)  
(v,k,l)=(2591,260,26) parametrelerin potansiyel kümesi.  
(v,k,l)=(2591,371,53) parametrelerin potansiyel kümesi.  
(v,k,l)=(2591,630,153) parametrelerin potansiyel kümesi.  
(v,k,l)=(2591,666,171) parametrelerin potansiyel kümesi.  
(v,k,l)=(2591,925,330) parametrelerin potansiyel kümesi.  
(v,k,l)=(2591,1036,414) parametrelerin potansiyel kümesi.  
(v,k,l)=(2591,1295,647) parametrelerin potansiyel kümesi.  
7 potansiyel fark küme adayı vardır.
```

```
>> kume_parametreleri (15001)  
(v,k,l)=(15001, 625,26) parametreleri potansiyel fark kümesi.  
(v,k,l)=(15001, 5001,1667) parametreleri potansiyel fark kümesi.  
(v,k,l)=(15001, 5625,2109) parametreleri potansiyel fark kümesi  
3 potansiyel fark küme adayı vardır.
```

```
>> kume_parametreleri (5167)  
(v,k,l)=(5167, 288,16) parametreleri potansiyel fark kümesi.  
(v,k,l)=(5167, 820,130) parametreleri potansiyel fark kümesi.  
(v,k,l)=(5167,1107,237) parametreleri potansiyel fark kümesi.  
(v,k,l)=(5167, 1477,422) parametreleri potansiyel fark kümesi.  
(v,k,l)=(5167, 1764,602) parametreleri potansiyel fark kümesi.  
(v,k,l)=(5167, 2296,1020) parametreleri potansiyel fark kümesi.  
(v,k,l)=(5167, 2583,1291) parametreleri potansiyel fark kümesi.  
7 potansiyel fark küme adayı vardır.
```

2.6. Lineer Diophant Denklem Çözümünün Matlab Uygulaması

Bu kod BRC teoreminin lineer diophant denkleminde bulduğu çözüm üçlülerini listelemektedir. Ve girilen v , n ve λ değerlerini $x^2 = ny^2 + (-1)^{(v-1)/2}\lambda z^2$ lineer diophant denkleminde yerine koyarak (x,y,z) nin sıfırdan farklı çözümlerini yazdırır. Ayrıca kaç tane çözüm üretildiği de sonuç olarak yazılır.

```
%Adı Soyadı: Safiye Öztürk
%Numarası: 172613012
% BRC Teoreminde v nin tek olduğu durumda lineer diophant
denkleminin çözümünün var olup olmadığının incelenmesi
function BRC_lineer(v,n,l)
%girdiler:
% v parametresi , |G| nin mertebesi ve tek sayı olmalı
% n parametresi , k-1
% l, lambda değişkeni l=k(k-1)/v
if (mod(v,2)==0)
    error('verilen v degeri cifttir. BRC teoreminin birinci kosulu
saglar.')
end
devir=0;
for i=1:1000
    for j=1:1000
        x=sqrt((n*i^2)+(-1)^((v-1)/2)*(l*j^2));
        if ((x^2)>0 && mod(x,1)==0)
            disp(fprintf('(x,y,z)=(%1.0f,%1.0f,%1.0f)',x,i,j))
            devir=devir+1;
        end
    end
end
disp(fprintf(' Bu parametreler için %1.0f çözüm üçlüsü vardır',
devir))
end
```

Aşağıdaki çıktılar $\mathbb{Z}_{67}$ nin $\lambda = 2, n = 12$ parametreleriyle oluşturulmuş $(v, k, \lambda) = (67, 14, 2)$ olası bir fark kümesidir. Çok sayıda çözüm olduğu için (1817) çıktıların tamamı burada yayınlanmamıştır. $\mathbb{Z}_{67}$ kümesinin başka olası fark kümesi adayları için k ve λ değerleri test edilir.

```
>> BRC_lineer(67,12,2)
```

```
(x,y,z) = (2,1,2)
```

```
(x,y,z) = (4,2,4)
```

```
(x,y,z) = (10,3,2)
```

```
(x,y,z) = (6,3,6)
```

```
(x,y,z) = (8,4,8)
```

```
(x,y,z) = (10,5,10)
```

```
(x,y,z) = (20,6,4)
```

.....

```
(x,y,z) = (3310,993,662)
```

```
(x,y,z) = (3448,996,88)
```

```
(x,y,z) = (3320,996,664)
```

```
(x,y,z) = (3284,998,764)
```

```
(x,y,z) = (3330,999,666)
```

```
(x,y,z) = (3182,999,962)
```

Bu parametrelerle 1817 çözüm üçlüsü vardır.

$\mathbb{Z}_{67}$ 'nin simetrik dizayn olmayan bir üçlüsü aşağıdaki gibidir. Burada $v = 67, \lambda = 7, k = 22$ parametreleriyle olası bir fark kümesi olan $(v, k, \lambda) = (67, 22, 7)$ üçlüsünün bir fark kümesi olmadığı görülür.

```
>>BRC_lineer(67,15,7)
```

Bu parametrelerle 0 çözüm üçlüsü vardır.

Aşağıdaki çıktılar $\mathbb{Z}_{73}$ 'ün $\lambda = 1$, $n = 9$ parametreleriyle oluşturulmuş $(v, k, \lambda) = (73, 9, 1)$ olası bir fark kümesidir. Çok sayıda çözüm olduğu için (3038) çıktıların tamamı burada yayınlanmamıştır. $\mathbb{Z}_{73}$ kümesinin başka olası fark kümesi adayları için k ve λ değerleri test edilir.

```
>>BRC_lineer(73,8,1)
(x,y,z)=(273,91,91)
(x,y,z)=(387,91,289)
(x,y,z)=(663,91,611)
(x,y,z)=(276,92,92)
(x,y,z)=(414,92,322)
(x,y,z)=(561,92,497)
(x,y,z)=(759,92,713)
```

.....

```
(x,y,z)=(2988,996,996)
(x,y,z)=(2991,997,997)
(x,y,z)=(2994,998,998)
(x,y,z)=(2827,999,89)
(x,y,z)=(2997,999,999)
(x,y,z)=(2850,1000,350)
(x,y,z)=(3000,1000,1000)
```

Bu parametrelerle 3038 çözüm üçlüsü vardır.

Aşağıdaki çıktılar $\mathbb{Z}_{91}$ 'in $\lambda = 1$, $n = 9$ parametreleriyle oluşturulmuş $(v, k, \lambda) = (91, 10, 1)$ olası bir fark kümesidir. Çok sayıda çözüm olduğu için (919) çıktıların tamamı burada yayınlanmamıştır. $\mathbb{Z}_{91}$ kümesinin başka olası fark kümesi adayları için k ve λ değerleri test edilir.

```
>> BRC_lineer(91,9,1)
(x,y,z)=(12,5,9)
(x,y,z)=(9,5,12)
(x,y,z)=(24,10,18)
(x,y,z)=(18,10,24)
(x,y,z)=(36,13,15)
(x,y,z)=(15,13,36)
(x,y,z)=(36,15,27)
```

```
.....  
(x,y,z)=(2835,977,744)  
(x,y,z)=(2880,984,648)  
(x,y,z)=(2925,985,420)  
(x,y,z)=(2850,986,792)  
(x,y,z)=(2808,986,930)  
(x,y,z)=(2835,999,972)  
(x,y,z)=(2880,1000,840)  
Bu parametrelerle 919 çözüm üçlüsü vardır.
```

$\mathbb{Z}_{91}$ 'in simetrik dizayn olmayan bir üçlüsü aşağıdaki gibidir. Burada $v = 91$, $\lambda = 36$, $k = 14$ ve $n = 22$ parametreleriyle olası bir fark kümesi olan $(v, k, \lambda) = (91, 36, 14)$ üçlününün bir fark kümesi olmadığı görülür.

```
>> BRC_lineer(91,22,14)  
Bu parametrelerle 0 çözüm üçlüsü vardır.
```


Tablo 2: Bazı (v, k, λ) parametreleri için ortalama çalışma süreleri

(v, k, λ)	Fonksiyon	1&0	Programın Ortalama Çalışma Süresi
(7,3,1)	simetrikdizayn(v, k, lam)	1	0,14 saniye
(11,5,2)	simetrikdizayn (v, k, lam)	1	0,16 saniye
(13,4,1)	simetrikdizayn (v, k, lam)	1	0,35 saniye
(15,7,3)	simetrikdizayn (v, k, lam)	1	0,45 saniye
(19,9,4)	simetrikdizayn (v, k, lam)	1	0,74 saniye
(21,5,1)	simetrikdizayn (v, k, lam)	1	1,21 saniye
(23,11,5)	simetrikdizayn (v, k, lam)	1	1,77 saniye
(31,6,1)	simetrikdizayn (v, k, lam)	1	4,45 saniye
(43,15,5)	brc_tek (v, k, lam)	0	0,1 saniye
(53,13,3)	brc_tek(v, k, lam)	0	0,1 saniye
(67,12,2)	brc_tek (v, k, lam)	0	0,1 saniye
(77,20,5)	brc_tek (v, k, lam)	0	0,1 saniye
(103,18,3)	brc_tek (v, k, lam)	0	0,1 saniye
(115,19,4)	brc_tek (v, k, lam)	0	0,1 saniye
(117,29,7)	brc_tek (v, k, lam)	0	0,2 saniye
(119,59,7)	brc_tek(v, k, lam)	0	0,2 saniye
(125,32,8)	brc_tek(v, k, lam)	0	0,2 saniye
(137,17,2)	brc_tek(v, k, lam)	0	0,2 saniye
(157,40,10)	brc_tek(v, k, lam)	0	0,2 saniye
(171,85,41)	brc_tek(v, k, lam)	0	0,2 saniye
(173,44,11)	brc_tek(v, k, lam)	0	0,2 saniye
(181,45,11)	brc_tek(v, k, lam)	0	0,2 saniye
(185,24,3)	brc_tek(v, k, lam)	0	0,2 saniye
(187,31,5)	brc_tek(v, k, lam)	0	0,2 saniye
(193,129,82)	brc_tek(v, k, lam)	0	0,2 saniye
(2591,260,26)	brc_tek(v, k, lam)	1	0,3 saniye
(5167,288,16)	brc_tek(v, k, lam)	1	0,5 saniye
(5167,2296,1020)	brc_tek(v, k, lam)	1	0,5 saniye
(5167,2583,1291)	brc_tek(v, k, lam)	1	0,5 saniye
(5167,1477,422)	brc_tek(v, k, lam)	0	0,5 saniye
(5167,1764,602)	brc_tek(v, k, lam)	0	0,5 saniye

Tablo 3: Girilen v değerine karşılık bulunan olası fark kümesi sayıları için programın çalışma süresi

v	Fonksiyon	Fark küme sayısı	Programın Ortalama Çalışma Süresi
2591	kume_parametreleri(v)	7	0,17 saniye
5167	kume_parametreleri(v)	7	0,11 saniye
6271	kume_parametreleri(v)	15	0,65 saniye
15001	kume_parametreleri(v)	3	0,96 saniye

Tablo 4: Girilen (v, n, λ) parametrelerine karşılık lineer diophant denklemindeki (x, y, z) değişkenlerine göre çözümlerinin kaç tane olduğunu veren örneklerin programdaki çalışma süreleri

(v, n, λ)	Fonksiyon	Çözüm sayısı	Programın Ortalama Çalışma Süresi
(67,12,2)	BRC_lineer(v, n, l)	1817	0,22 saniye
(67,15,7)	BRC_lineer(v, n, l)	0	0,10 saniye
(73,8,1)	BRC_lineer(v, n, l)	3038	0,29 saniye
(91,9,1)	BRC_lineer(v, n, l)	919	0,15 saniye
(91,22,14)	BRC_lineer(v, n, l)	0	1,15 saniye

3. BULGULAR

Bu tez çalışmasında fark kümeleri konusu ile ilgili genel bir literatür özeti verilerek, fark kümelerinin varlık probleminde kullanılan BRC Teoreminden bahsedilmiştir.

Bruck Ryser Chowla Teoremi simetrik dizayn olan yapıların fark kümesi olup olmadığı ile ilgili kriterler vermektedir. Bruck Ryser Chowla Teoremini sağlayan her simetrik dizayn bir fark kümesidir. Ancak bu ifadenin tersi doğru değildir. Bu çalışmada MATLAB bilgisayar programına girilen v , k , λ değerlerine karşılık bir simetrik dizayn olup olmadığını kontrol eden ardından Bruck Ryser Chowla teoreminin kriterlerini uygulatan ve hepsini birlikte kontrol edip uygun parametrelili fark kümelerini listeleyen bir kod oluşturulmuştur.

4. TARTIŞMA ve SONUÇLAR

Bu tez çalışması için gerekli olan bilgiler mevcut literatürden faydalanılarak sunulmuştur. Fark kümeleri ile ilgili temel tanım ve teoremler, fark kümelerinin özellikleri, BRC Teoremi için önemli olan teoremler ve bir kısmının ispatları verilmiş, BRC Teoremini sağlayan ve sağlamayan örneklerle çalışma zenginleştirilmiştir.

Yapılan çalışmalar kısmında, verilen bir üçlü v, k, λ parametrelerinin ilk kriteri sağladıktan sonra simetrik dizayn olup olmadığını kontrol eden ve fark kümelerinin varlığını araştıran Bruck Ryser Chowla teoreminin kriterlerini sağlayan bilgisayar program dilinde yazılan kod parçaları sunulmuştur.

MATLAB program dilinde yazılan kodlar kullanılarak programa girilen herhangi v, k, λ üçlüsünün simetrik dizayn olup olmadığı, Bruck Ryser Chowla testini geçip geçmediği belirlenebilmektedir. Bu çalışma sonucunda simetrik dizayn olan, Bruck Ryser Chowla teoreminin ikinci koşulunu sağlayan ve sağlamayan örneklere ve Bruck Ryser Chowla teoreminin lineer diophant denkleminde ürettiği çözümleri çıktı olarak veren örneklere yer verilmiştir.

5. ÖNERİLER

Bruck Ryser Chowla teoremi diophant denkleminde bir çözümün varlığının simetrik dizaynın varlığı üzerindeki etkisini açıklamaktadır. Ancak bu yöntemler kullanılırken uygun parametrelili fark kümelerinin bulunması bilgisayar desteği olmadan kolay olmayabilir. Bu nedenle fark kümelerini araştıran farklı yöntem çeşitleri program dillerinde irdelenebilir. Orbit tanımı kullanılarak fark kümesi elde eden bir kod yazılabilir. Bruck Ryser Chowla teoreminin ikinci şartının uygulaması için daha basit yöntemler araştırılabilir. Çarpan teorisi kullanılarak Bruck Ryser Chowla testi gibi fark kümesi olmayan örnekleri eleyen bir kod yazılabilir. Matris çeşitlerinin simetrik dizayn olma üzerindeki etkisi araştırılabilir.

KAYNAKLAR

- AbuGhneim, O.A. and Smith, K.W. (2007). Nonabelian groups with $(96, 20, 4)$ difference sets. *Electronic Journal. Combinatorics*. 14(1): 8-17.
- Akpınar, A. (2005). On some projective planes of finite order, *Gazi University Journal of Science*, 18(2), 315-325. ISSN: 1303-9709.
- Assmus, E.F. and Key, J.D. (1992) Designs and their codes. Cambridge Universal Press, Cambridge.
- Baskar, S. and Saravanan, M. (2012). Error Detection and the Correction Enhanced Decoding of Difference Set Codes for Memory Application. *International Journal of Advanced Research in Computer and Communication Engineering*, 1(10), 816-820.
- Baumert, L.D. and Gordon, D.M. (2004). On the existence of cyclic difference sets with small parameters. *Fields Institute Communications*, 41, 61-68. ISSN: 1069-5265.
- Baumert, L.D. (1971). Cyclic Difference Sets. California Institute of Technology Pasadane, ISBN: 0-387-05368-9, 172 s., 1-9.
- Bayraktar, M. (1988). Soyut Cebir ve Sayılar Teorisi. Atatürk Üniversitesi Yayınları, Yayın No: 650, 275s, 87-98.
- Bayraktar, M. (1988). Soyut Cebir ve Sayılar Teorisi. Atatürk Üniversitesi Yayınları, Yayın No: 650, 275s, 121-126.
- Bennett, M.K. (1995). Affine and Projective Geometry. John Wiley & Sons, Inc, New York, 229 pp.
- Beth, T., Jungnickel, D. and Lenz, H. (1999). Design Theory. Cambridge University Press, 1120 s., 1-50.
- Bose, R.C. and Nair, K.R. (1939). Partially balanced incomplete block designs. *Sankhya: The Indian Journal of Statistics*, 4(3), 337-372.
- Bruck, R.H. and Ryser, H.J. (1949). The nonexistence of certain finite projective planes. *Canadian Journal of Mathematics*, 1(1), 88-93.
- Bruck, R.H. (1955). Difference sets in a finite group. *Transactions of the American Mathematical Society*, 78(2), 464-481. DOI: 10.2307/1993074.
- Cameron, P.J. And Lint J.H. (1991). Designs, Graps, Codes and their Links www.maa.org/programs/maa-awards/writing-awards/the-search-for-finite-projective-plane-of-order-10. Cambridge University Press.
- Carter, J.L. (1974). On the existence of a projective plane of order ten. 3rd education, Doctor of Philosophy Thesis, University of California, Berkeley.

- Chowla, S. and Ryser, H.J. (1950). Combinatorial problems. *Canadian Journal of Mathematics*, 2, 93-99.
- Colbourn, C.J. and Jeffrey H.D. (2007). Handbook of Combinatorial Designs. Boca Raton, FL: Chapman and Hall /Taylor and Francis.
- Çevik, A.S. (2012). Soyut Cebir Özel Konular. Nobel Akademik Yayıncılık, 235 s., 25-29.
- Delahaye, J.P. (1996). A difference set cyclic code (1057,813,34). *Annales Des Télécommunications*, 51(2), 19-26.
- Dembowski, P. (1997). Finite geometries. Mathematics Subject Classification (1991): 51E, Volume 44, ISBN-13: 978-3-540-61786-0.
- Ding, C. (2014). Codes from Difference Sets. Singapore: World Scientific, 341s., 67-75.
- Golemac, A., Vučićić, T. and Mandić, J. (2005). One (96,20,4) symmetric design and related nonabelian difference sets. *Designs, Codes Cryptography*, 37, 5-13.
- Hall Jr, M. (1947). Cyclic projective planes. *Duke mathematical Journal*, 14(4), 1079-1090.
- Hall, M. and Ryser, H.J. (1951). Cyclic incidence matrices. *Canadian Journal of Mathematics*, 3, 495-502.
- Hall, M. (1956). A survey of difference sets. *Proceedings of the American Mathematical Society*, 7(6), 975-986.
- Hall, M. (1959). The Theory of Groups. California Institute of Technology. Newyork. 434 pp, ISBN: 978-0-486-81690-6.
- Ireland, K. and Rosen, M. (1982). A Classical Introduction to Modern Number Theory. Springer-Verlag, 272-275.
- Jungnickel, D. (1992). Difference sets in Contemporary Design Theory: A Collection of Surveys. Wiley Interscience, 641 s, Dinitz, J.H. and Stinson, D.R. (B. ed), 241-365.
- Jungnickel, D. and Schmidt. B. (1997). Difference sets: An update. (Educations Hirschfeld, J.W.P., Magliveras, S.S. and Resmini, M.J.) Cambridge University Press, 89-112. DOI: <https://doi.org/10.1017/CBO9780511526114.010>
- Kaya, R. (1992). Projektif Geometri. Anadolu Üniversitesi Yayınları, No:551. Eskişehir, 465s, 112-114. ISBN: 978-9-754-92283-7.
- Kibler, R.E. (1978). A summary of noncyclic difference sets, $k < 20$. *Journal of Combinatorial Theory A*, 25(1), 62-67.

- Kopilovich, L.E. (1989). Difference sets in non-cyclic groups. *Cybernetics*, 25(2), 153-157.
- Lam, C.W., Thiel, L. Swiercz, S. McKay, J. (1983). The nonexistence of ovals in a projective plane of order 10. *Discrete Mathematics*, 45(2-3), 319-321.
- Lam, C.W., Thiel, L. and Swiercz, S. (1989). The nonexistence of finite projective planes of order 10. *Canadian Journal of Mathematics*, 41(6), 1117-1123.
- Lam, C.W. (1991). The search for a finite projective plane of order 10. Computer Science Department, Concordia University, *The American mathematical monthly*, 98(4), 305-318.
- Lander, E.S. (1983). Symmetric Designs. An Algebraic Approach. Volume 74 of London Mathematical Society, Lecture Note Series. Cambridge University.
- Lehmer, E. (1953). On residue difference sets. *Canadian Journal of Mathematics*, 5, 425-432.
- Levi, F.W. (1942). Groups in which the commutator operation satisfies certain algebraic conditions. *The Journal of the Indian Mathematical Society*, 6, 87-97.
- Lopez, A.V. and Sanchez, M.A.G. (1997). On the existence of abelian difference sets with $100 < k \leq 150$. *Journal of Mathematics and Computer Science*, 23, 97-112.
- McFarland, R.L. (1973). A family of difference sets in noncyclic groups. *Journal of Combinatorial Theory A*, 15(1), 1-10.
- McFarland, R.L. and Rice, B.F. (1978). Translates and multipliers of abelian difference sets. *Proceedings of American Mathematical Society*, 68, 375-379. ISSN: 0002-9939.
- Moore, E.H. and Pollatsek. H.S. (2013). Difference sets. American Mathematical Society, 298 s, 253-266.
- Morrice, R.T. (2015). Difference Sets- An investigation into the properties and criteria for existence.
- Peifer, D. (2013). Difference Set Transfers. *Northfield Undergraduate Mathematics Symposium*, 29 Ekim, 3-4.
- Pott, A., Kumar, P.V., Hellesteth, T. and Jungnickel, D. (1999). Difference Sets: Sequences and Their Correlation Properties. Kluwer Academic Publishers, cilt no:542, 448 s.
- Rademacher, H. and Toeplitz, O. (1956). The enjoyment of Math. Princeton Science Library. 7.Basım 1994.

- Ryser, H.J. (1982). The existence of symmetric block designs. *Journal of Combinatorial Theory A*, 32(1), 103-105.
- Rosen, K.H., Goddard, B. and O'Bryant, K. (2005). Elementary Number Theory and its Applications. Pearson/Addison Wesley, 5. Baskı, 721pp, 402-403.
- Schützenberger, M.P. (1949) A Nonexistence Theorem for Infinite family of symmetrical block designs. *Annals of Human Genetics*, 14(1), 286-287. DOI:10.1111/j.1469-1809.1947.tb02404.x.
- Siemons, J. (1989). Survey in Combinatorics. *Proceedings of the 12th British Combinatorial Conference*. Cambridge University Press, Cambridge.
- 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.
- Skinner, G.K. (1984). Imaging with coded aperture masks. *Nuclear Instruments and Methods in Physics Research*, 221(1), 33-40.
- Tarry, G. (1900). Le Probleme des 36 Officiers. *Compte Rendu de l'Association Française pour l'Avancement de Science Naturel*, 1, 122-123.
- Williams, G. (1937). Linear Algebra with Applications. Profesör Emeritus Stetson University, Deland, Florida, Ninth Edition, 316-317.
- Witt, E. (1937). Theorie der quadratischen Formen in beliebigen Körpern. *Journal für die reine und angewandte Mathematic*, 176, 31-44.
- 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.
- Zand, J. (1995). The MART-LIME High Energy Coded Aperture Teleskope. MART-LIME. SRON: Netherlands Institute for Space Research.
- 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*, Toronto, 8-14 Kasım, 1521-1524.

ÖZGEÇMİŞ

Safiye Öztürk 25.05.1992 tarihinde İspir’de doğdu. İlköğretimini 2005 yılında Erzurum/İspir’de Şehit Karabey Yıldırım İlköğretim Okulu’nda ve Ortaöğretimini 2009 yılında Erzurum/İspir’de İspir Lisesi’nde tamamladı. 2009 yılında başladığı lisans eğitimini 15.06.2013 tarihinde Atatürk Üniversitesi Fen Edebiyat Fakültesi Matematik Bölümü’nde tamamladı. Üniversite eğitimi sırasında Atatürk Üniversitesi’nden Pedagojik Formasyon Eğitimi Sertifikası aldı. 2017 yılında Recep Tayyip Erdoğan Üniversitesi Matematik Anabilim Dalı’nda başlayan tezli yüksek lisans öğrenimini halen devam ettirmektedir.