



**T.C.
RECEP TAYYİP ERDOĞAN ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI**

**DÖNGÜSEL SINIFLARDAN FARK KÜMESİ ELDE ETME
(Yüksek Lisans Tezi)**

Yasin YILMAZ

**Danışman
Dr. Öğrt. Üyesi Emek DEMİRCİ AKARSU**

**RİZE
2022**

KABUL VE ONAY

Recep Tayyip Erdoğan Üniversitesi, Lisans Eğitim Enstitüsü, Matematik Anabilim Dalında Dr. Öğrt. Üyesi Emek DEMİRCİ AKARSU danışmanlığında Yasin YILMAZ tarafından hazırlanan “Döngüsel Sayılardan Fark Kümesi Elde Etme” adlı bu tez çalışması 04/07/2022 tarihinden yapılan savunma sınavı sonucunda oy birliği ile başarılı bulunarak jürimiz tarafından **Yüksek Lisans Tezi** olarak kabul edilmiştir.

Jüri Üyeleri	Unvanı, Adı SOYADI	İmza
Başkan	: Dr. Öğrt. Üyesi Emek DEMİRCİ AKARSU	
Üye	: Prof. Dr. Selçuk Han AYDIN	
Üye	: Dr. Öğrt. Üyesi Tuğçem PARTAL	

ETİK BEYAN

Matematik Yüksek Lisans Programından mezun olmak üzere teslim ettiğim “Döngüsel Sayılardan Elde Edilen Fark Kümeleri” adlı tezim, bilim ve araştırma etiği prensiplerine riayet edilerek tarafımdan yazılmıştır.

Tez çalışmamda, başka kaynaklardan aktarılan bütün bilgi ve alıntılar, Enstitünüz Tez Yazım Kılavuzuna uygun olarak açıkça gösterilmiştir. Kaynağı gösterilenler dışında kalan bütün bilgiler uygun araştırma yöntemi kullanılarak tarafımdan edinilmiş ve esere bu şekilde yansıtılmıştır. Şahsıma ait olmayan hiçbir bilgi, kasıt veya kusurlar, şahsıma aitmiş gibi gösterilmemiştir. İnternet kaynakları dâhil, sahibine/kaynağına atıf yapılmaksızın hiçbir bilgi kullanılmamıştır. Aksinin ortaya çıkması halinde doğacak bütün hukuki, idari, akademik ve etik sorumluluk tarafıma ait olacaktır. Eserin tesliminden sonra herhangi bir zamanda, bilim etiğine aykırılık tespit edilmesi ve eserimle ilgili intihal veya intihal şeklinde anlaşılabacak bir durumun ortaya çıkması halinde; Üniversiteniz ve eğitim kadronuzun hiçbir şekilde sorumlu tutulmayacağını hür irademle kabul, beyan ve taahhüt ederim.

04/07/2022

Yasin YILMAZ

ÖN SÖZ

Bu çalışma döngüsel sınıflardan elde edilen fark kümeleri ve uygulamalarını incelemek amacıyla Recep Tayyip Erdoğan Üniversitesi Lisansüstü Eğitim Enstitüsü Matematik Anabilim dalında yüksek lisans tezi olarak hazırlanmıştır.

Tez çalışmasında, planmasında, araştırılmasında, yürütülmesinde ve oluşumunda bilgi ve tecrübelerinden yaralandığım yönlendirme ve bilgilendirmeleriyle çalışmaları şekillendiren sayın hocalarım Dr. Öğr. Üyesi Emek DEMİRCİ AKARSU'ya ve Arş. Gör. Dr. Ali KÖSEOĞLU'ya teşekkürlerimi sunarım.

Yasin YILMAZ

04/07/2022

İÇİNDEKİLER

KABUL VE ONAY.....	I
ETİK BEYAN.....	II
ÖN SÖZ.....	III
İÇİNDEKİLER	IV
TÜRKÇE ÖZET.....	VI
ABSTRACT.....	VII
KISALTMALAR.....	VIII
TABLolar LİSTESİ	IX
ŞEKİLLER LİSTESİ	X
GİRİŞ	1
1. Genel Bilgiler.....	3
1.1 Literatür Taraması.....	3
1.2 Temel Kavramlar.....	5
1.2.1. İlkel Kökler ve İndeksler.....	5
1.2.2. Gruplar.....	8
1.2.3. Halkalar ve Cisimler.....	9
1.2.4. Tekrarlanma Yapıları ve Dizaynlar.....	10
1.3. Döngüsel Sayılar.....	13
1.3.1. 2. Mertebeden Döngüsel Sayılar.....	14
1.3.2. 3. Mertebeden Döngüsel Sayılar.....	15
1.3.3. 4. Mertebeden Döngüsel Sayılar.....	18
1.4. Döngüsel Sınıflar.....	23
1.5. Fark Kümeleri.....	24
1.6. Döngüsel Sınıflar İle Elde Edilen Fark Kümeleri ve Hemen Hemen Fark Kümeleri.....	34
2. YAPILAN ÇALIŞMALAR.....	40
2.1 Rezidülerden Elde Edilen Fark Kümeleri İçin MATLAB Uygulaması....	41
2.2 İlkel Kök Elde Eden MATLAB Uygulaması.....	43
2.3 C_0^2 Döngüsel Sınıfıyla Elde Edilen Fark Kümelerinin MATLAB Uygulaması.....	45

2.4	C_4^2 Döngüsel Sınıfıyla Elde Edilen Fark Kümelerinin MATLAB Uygulaması.....	47
2.5.	$C_4^2 \cup \{0\}$ Döngüsel Sınıfıyla Elde Edilen Fark Kümelerinin MATLAB Uygulaması.....	48
2.6.	C_8^2 Döngüsel Sınıfıyla Elde Edilen Fark Kümelerinin MATLAB Uygulaması.....	52
2.7.	$C_0^6 \cup C_1^6 \cup C_3^6$ Döngüsel Sınıfıyla Elde Edilen Fark Kümelerinin MATLAB Uygulaması.....	55
2.8.	BULGULAR.....	58
3.	TARTIŞMA VE SONUÇLAR.....	59
3.1	ÖNERMELER.....	60
	KAYNAKÇA.....	61

Recep Tayyip Erdoğan Üniversitesi Lisansüstü Eğitim Enstitüsü

Anabilim Dalı : Matematik

Tez Türü : Yüksek Lisans

Danışman : Dr. Öğr. Üyesi Emek DEMİRCİ AKARSU

Yazan : Yasin YILMAZ

Yıl : 2022

Sayfa : 74

ÖZET

DÖNGÜSEL SINIFLARDAN FARK KÜMESİ ÜRETME

Tezin ilk bölümünde döngüsel sayıların tanımı, özellikleri, 1. mertebeden, 2. mertebeden, 3. mertebeden ve 4. mertebeden döngüsel sayılar ve döngüsel sınıflar verilmiştir. Ayrıca fark kümelerinin tanımı ve özellikleri verilmiş olup döngüsel sınıflar ile fark kümeleri arasındaki ilişki incelenmiştir. Çalışmanın temel bölümünde ise özel döngüsel sınıflardan elde edilen fark kümelerinin elde edilmesine yönelik MATLAB programlama diliyle kod çalışması yapılmıştır. Kaynak kodlar tezin son bölümünde verilmiştir.

Anahtar Kelimeler: Döngüsel Sayılar, Döngüsel Sınıflar, Fark Kümeleri, Kısmi Fark Kümeleri

Recep Tayyip Erdogan University Institute of Graduate Studies

Department : Mathematics
Thesis Type : Master Thesis
Supervisor : Assist. Prof. Dr. Emek DEMİRCİ AKARSU
Author : Yasin YILMAZ
Year : 2022
Pages : 74

ABSTRACT

DIFFERENCE SETS CONTRUCTION FROM CYCLOTOMY CLASSES

In the first part of the thesis, the definition of cyclotomic numbers, their properties, 1st order, 2nd order, 3rd order and 4th order cyclotomic numbers and cyclotomic classes are given. In addition the definition and properties of difference sets are given and the relationship between cyclotomic classes and difference sets investigated. In the basic part of the study, a coding study was conducted by the MATLAB programming language for obtaining the difference sets acquired from the particular cyclotomic classes. Source codes are given in the last part of the thesis.

Keywords: Cyclotomic Numbers, Cyclotomic Classes, Difference Sets, Almost Difference Set

KISALTMALAR

$\mathbb{P}$	: Asal sayılar kümesi
$\subset$	: Alt küme
$(a, b)_{ebob}$	: a ve b sayılarının en büyük ortak böleni
Δ	: Birim eleman olmayan farkların çoklu kümesi
$\geq$	: Büyüktür veya eşittir
$\emptyset$	: Boş küme
$\equiv$	: Denktir
$devD$	: D fark kümesinin açılımı
$\mathbb{N}$	: Doğal sayılar kümesi
$\notin$	: Elemanı değildir
$\in$	: Elemanıdır
$\leq$	: Küçüktür veya eşittir
$GF(q)$	: Mertebesi q olan cisim (Galois Field)
$\mathbb{Z}_m$	: Mod m kalan sınıfı kümesi
$\mathbb{R}$	: Reel(Gerçel) sayılar kümesi
$\mathbb{Z}$	: Tam sayılar kümesi
$\langle g \rangle$	: Üreteni g olan grup
V	: Vektör uzayı

TABLolar LİSTESİ

Tablo 1. $(\mathbb{Z}_{11}, \oplus)$ grubunda $D = \{1, 3, 4, 5, 9\}$ fark kümesi için çoklu küme tablosu.....	24
Tablo 2. $(\mathbb{Z}_{11}, \oplus)$ grubunda $D = \{0, 1, 5, 8, 10\}$ fark kümesi için çoklu küme tablosu.....	26
Tablo 3. $(\mathbb{Z}_{17}, \oplus)$ grubunda $D = \{1, 2, 4, 8, 9, 13, 15, 16\}$ fark kümesi için çoklu küme tablosu.....	30
Tablo 4. $(\mathbb{Z}_{13}, \oplus)$ grubunda $D = \{1, 3, 4, 9, 10, 12\}$ fark kümesi için çoklu küme tablosu.....	32
Tablo 5. $q \equiv 9 \pmod{16}$ olduğunda 8.mertebedeki döngüsel sayıların ilişkileri....	35
Tablo 6. $q \equiv 9 \pmod{16}$ iken 8. mertebeden döngüsel sayılar.....	36
Tablo 7. $(\mathbb{Z}_9, \oplus)$ grubunda $D = \{1, 2, 4, 5\}$ fark kümesi için çoklu küme tablosu.....	38
Tablo 8. Kuadratik Rezidü Programın Çalışma Süreleri.....	42
Tablo 9. Bazı Sonlu Cisimlerin Üreteçleri Bulduran Programın Çalışma Süreleri...	43
Tablo 10. C_0^2 Sınıfından Elde Edilen Fark Kümesi Programının Çalışma Süreleri....	46
Tablo 11. C_4^2 Sınıfından Elde Edilen Fark Kümesi Programının Çalışma Süreleri ...	49
Tablo 12. $C_4^2 \cup \{0\}$ Sınıfından Elde Edilen Fark Kümesi İçin Programının Çalışma Süreleri.....	51
Tablo 13. C_8^2 Sınıfından ve $C_0^6 \cup C_1^6 \cup C_3^6$ Sınıfından Elde Edilen Fark Kümesi Programının Çalışma Süreleri.....	55

ŞEKİLLER LİSTESİ

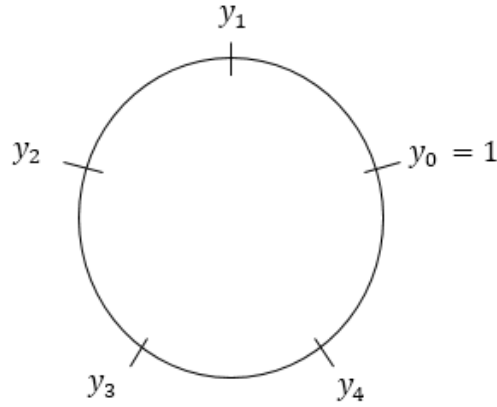
Şekil 1. $x^5 - 1 = 0$ denkleminin köklerinin birim çember üzerindeki gösterimi.....	2
Şekil 2. $(25, 8, 2)$ parametrelili bir simetrik dizayn.....	12
Şekil 3. Kuadratik Rezidülerden Elde Edilen Fark Kümeleri için MATLAB Uygulaması.....	41
Şekil 4. İlkel Kök Elde Eden MATLAB Uygulaması.....	43
Şekil 5. C_0^2 Döngüsel Sınıf ile Elde Edilen Fark Kümesi İçin Uygun Parametrelerin MATLAB Uygulaması.....	45
Şekil 6. C_0^2 Döngüsel Sınıf ile Elde Edilen Fark Kümesinin MATLAB Uygulaması..	45
Şekil 7. C_4^2 Döngüsel Sınıflar İçin Uygun Parametreleri Bulduran MATLAB Uygulaması.....	48
Şekil 8. C_4^2 Döngüsel Sınıf ile Elde Edilen Fark Kümesinin MATLAB Uygulaması..	48
Şekil 9. $C_4^2 \cup \{0\}$ Döngüsel Sınıf ile Elde Edilen Fark Kümesi İçin Uygun Parametrelerin MATLAB Uygulaması.....	51
Şekil 10. $C_4^2 \cup \{0\}$ Döngüsel Sınıf ile Elde Edilen Fark Kümesinin MATLAB Uygulaması.....	51
Şekil 11. C_8^2 Döngüsel Sınıf İçin Uygun Parametreleri Bulduran MATLAB Uygulaması.....	53
Şekil 12. C_8^2 Döngüsel Sınıfları ile Elde Edilen Fark Kümesinin MATLAB Uygulaması.....	54
Şekil 13. $C_0^6 \cup C_1^6 \cup C_3^6$ Döngüsel Sınıf ile Elde Edilen Fark Kümesinin MATLAB Uygulaması.....	56

GİRİŞ

Döngü (Cyclotomy) teorisi Öklid zamanında $n = 2^s, 3 \cdot 2^s, 5 \cdot 2^s, 15 \cdot 2^s$ kenarlı düzgün çokgenler üzerinde s 'nin tüm değerleri için inşa edilebileceği ileri sürülmüştür. Ancak 18.yy'da Carl Friedrich Gauss, pusula ve cetvel yapımında farklı birimden ölçekler elde edebilmek için döngü teorisini sistematize eden ilk kişi olmuştur. Gauss burada $n = 2^{2^k} + 1$ formunda olan Fermat asal sayıları için $2^s \cdot n$ kenarlı düzgün çokgenler ile bu ölçeklerin elde edilebileceğini ispat etmiştir. 1935 yılında ise mertebesi $e \leq 6$ olan döngüsel sayılar üzerinde Gauss Periyotlarını ve Jacobi toplamalarını kullanarak çalışmalar yapmıştır. Daha sonrasında ise Hall, Storer, Whiteman, Parnami, Katre ve Rajwade bu Jacobi toplamalarını ve Gauss periyotlarını kullanarak daha yüksek mertebeden döngüsel sayıların geliştirilmesinde katkıda bulunmuştur.

Simetrik dizaynın özel bir hali olan fark kümeleri kavramı ilk olarak 1938 yılında James Singer tarafından “Sonlu Projektif Geometride bir Teorem ve Sayılar Teorisinde Bazı Uygulamalar” makalesinde yayımlanmıştır. Daha sonrasında 1940 yılında Marshall Jr. Hall fark kümeleri üzerinde çalışmalarda bulunmuştur. İyi bir otokorelasyon özelliğine sahip olan fark kümesi üzerinde yapılan çalışmalar sonucu olarak çeşitleri olan fark kümeleri aileleri, hemen hemen fark kümesi, kısmi fark kümesi, vb. dallara bölünmüş olup bir çok uygulama alanına kodlama ve şifreleme, astronomik olayların yorumlanması, entegre edilebilir bir yapıda olduğundan günümüze kadar bir çok bilim insanının ilgi kaynağı olmuştur.

Geometrik şekiller üzerine inşa edilmiş olan döngü teorisinin aritmetik ile ilişkisi zaman içerisinde artmış olup ve n kenarlı bir çokgende n sayısının asal olması durumunda $\mathbb{Z}_n$ kalan sınıfı ile ilginç ilişkilere kaynaklık etmiştir. Örneğin; $n = 5$ olması durumunda döngü teoremi şu şekilde ifade edilebilir. $x^5 - 1 = 0$ cebirsel ifadesinin kökleri $y_0, y_1, y_2, y_3, y_4, y_5$ olsun. Buradaki temel amaç şekil üzerinde de görüleceği üzere koordinat düzleminde birim çemberin çevresini 5 eşit yaya bölüp cebirsel ifadenin köklerinin karşılık geldiği koordinatlarını ilkel kökler yardımıyla indisler ile ifade edilmesidir.



Şekil 1. $x^5 - 1 = 0$ denkleminin köklerinin birim çember üzerindeki gösterimi

Hemen hemen fark kümelerinin kriptografi ve kodlama teorisinde ilginç uygulamaları vardır. Hemen hemen fark kümelerinin bilinen ailelerini çok yönlü bir şekilde ele alarak bazı fark kümeleri ile bazı hemen hemen fark kümeleri arasında ilişkiler kurulur ve hemen hemen fark kümelerinin bazı ailelerinin sayısal çarpan grubunu belirlenebilir. Ayrıca, hemen hemen fark kümelerinden oluşan altı yeni sınıf ve optimal otokorelasyona sahip dört adet periyot ($\text{mod } 4$) ikili dizisi sınıfı oluşturulabilir. Başka bir deyişle iki sınıf görelî fark kümesi ve dört bölünebilir fark kümesi elde edilmiş olur. Ayrıca, Jungnickel'e (1982) bağılı bir sonucun, optimal otokorelasyon ile $4l$ periyodundaki hemen hemen fark kümelerini ve dizilerini oluşturmak için kullanılabileceğini belirtilmektedir (K. T. Arasu, 2001).

Hemen hemen fark kümelerine dayalı inceltme teknikleri, düşük mod yan lob seviyelerine sahip MIMO radar döngüsel dizilerini tasarlamak için sunulmuştur. Standart hemen hemen fark kümeleri yaklaşımı, verici ve alıcı dizilerin eleman konumlarını analitik olarak belirlemeye ve MIMO sanal dizilerinin radyasyon modeli yan loblarının üst sınırını tahmin etmeye olanak sağlar. Hemen hemen fark kümesi tabanlı MIMO dizilerinin en yüksek yan lob performanslarının, aynı zamanda daha geniş dizi konfigürasyonları setinde elde edilebilen, döngüsel fark kümeleri tabanlı MIMO dizilerinininkilerle karşılaştırılabilir olduğu ortaya çıkmıştır. Tamamen hemen hemen fark kümesi tabanlı metodolojinin esneklik ve yan lob performansları açısından sınırlamalarının üstesinden gelmek için gelişmiş hemen hemen fark kümesi fark kümesi tabanlı bir genetik algoritma prosedürde önerilmiştir. Temsili sayısal

sonular, nerilen hemen hemen fark kmesi yaklařımlarının zelliklerini ve performanslarını gstermek ve diğerk benzer tasarım metodolojilerine kıyasla etkinliklerini ve verimliliğini doğrulamak iin gsterilmiřtir. (Jian Dong, 2013)

Bu tez alıřmasında dngsel sayılar, fark kmeleri, fark kmesinin eřitleri ve dngsel sayılardan elde edilen fark kmelerini ieren tanım, teorem ve bu yapıların zellikleri iermektedir. Ayrıca kuadratik rezidülerden elde edilen fark kmeleri, C_0^2 dngsel sınıfları, C_4^2 dngsel sınıfları, $C_4^2 \cup \{0\}$ dngsel sınıfları, C_8^2 dngsel sınıfları ve $C_0^6 \cup C_1^6 \cup C_3^6$ dngsel sınıflarından elde edilen dngsel sınıflar zerinden farklı parametrelere sahip fark kmelerinin MATLAB uygulamalarını iermektedir.

1. Genel Bilgiler

1.1.Literatr zeti

Dngsel sayıların temellerini oluřturan okgenlerin blnmesinin temelleri ilk olarak M..300'lerde klid zamanında atıldıđı grlmřtir (klid'in Elemanları, Sinan SERTZ). İřlevseliğini uzun yıllar sonra pusula ve harita yapımında kazanan dngsel sayılar (Johann Carl Friedrich Gauss, 1798) matematiğinin sayılar teoresi, kombinatorik, vb. alanıyla baėlantısı olmasından dolayı zerinde birok alıřmalar yapılmasına olanak saėlamıřtır. İlk olarak ikinci mertebeden dngsel sayıları elde eden Gauss, nc mertebeden dngsel sayılarda kendi ismini vermiř olduđu Gauss tipi iřaret belirsizliğı ile karřılařmıřtır. İřaret belirsizliğinin kaldırılmasına ynelik alıřmalar Hall ve Storer (1940) tarafından yapılmıřtır.

Gauss ve Jacobi toplamaları kullanılarak (Whiteman, 1935) bu iřaret belirsizliğı ortadan kaldırmıřtır. Aynı dnemde Dickson Waring problemi adında ıkartmıř olduđu makalesinde ilk 5 mertebeden dngsel sayıları yayınlamıřtır (Dickson, 1935).

7. mertebeden ve 11. mertebeden dngsel sayıları (Leonard P.A. ve Williams K. S. 1974) elde etmiřtir. 14. mertebeden dngsel sayıları (Muskat J.B., 1966) elde etmiřtir. 15. mertebeden dngsel sayılar (Nicholas Buck, Lones Smith, Blair K. Spearman ve Kenneth S. Williams, 1987) tarafından elde edilmiřtir. 16. mertebeden dngsel sayılar (Ronald J. Evans ve Jay Roderick, 1979) tarafından elde edilmiřtir.

1982 yılında ise Panami ve arkadaşları 5. mertebeden döngüsel sayılar için bir asal sayının kuvveti mertebesinde olan cisimler üzerinde genelleştirmeler yapmıştır.

Katre ve Rajwade 1985 yılında yayınlamış olduğu makalesinde $n = 2l$ formundan olan n mertebeli döngüsel sayılar için işaret belirsizliğine yönelik genel bir çalışma yapmışlardır.

Devendra Shirolkar ve S. A. Katre, Jacobi toplamaları ve l^2 mertebeli döngüsel sayılara yönelik çalışmalar yapmıştır.

En son 24. mertebeden döngüsel sayı (Evans, 1980) elde edilmiş olup merite artıkça elde edilen Diophant denklemler daha komplike hale geldiğinden yüksek mertebeden döngüsel sayıların elde edilmesi daha güç bir hale gelmiştir.

Fark kümesinin var olabilmesi için o yapının esasında bir simetrik dizayn olaması gerekir. Bu simetrik dizayn varlığı üzerinde ise Bruck ve Ryser (v, k, λ) parametrelili simetrik dizayn için Bruck Ryser Chowla Teoremi kanıtlamıştır (Chowla ve Ryser, 1950). İlk olarak $\lambda = 1$ için verilmiş olan bu teorem daha sonrasında λ sayısının pozitif olması durumu için genelleştirilmiştir (Ryser ve Chowla, 1982).

Simetrik dizaynın özelleştirilmesi olan fark kümesi kavramı ilk olarak Sonlu Projektif Geometride Bir Teorem ve Sayılar Teorisinde Bazı Uygulamalar (Singer, 1938) adlı makalede yer almıştır. Fark kümelerinin sistematik çalışılması 1940'ların sonlarında Marshall Hall'ın çalışmalarına kadar gitmektedir (Hall, 1940).

E. Lehmer (1953) bir cisim üzerinde kuadratik rezidülerin oluşturmuş olduğu sınıfın fark kümesi olduğunu ispatlamıştır. Bu çalışmaların üzerine rezidü olmayan sınıflar üzerinde fark kümesi ailesi olduğunu (R.L. McFarland, 1973) makalesinde göstermiştir. Buna benzer fark kümeleri aileleri Emily. H. Moore'nin Fark Kümeleri, Cebir, Kombinasyon ve Geometri kitabında ele alınmıştır. Ayrıca konu üzerinde daha anlaşılabilir olması açısından fark kümeleri üzerinde derleme çalışması niteliğinde (Trout, 2017) olan tez çalışması yapılmıştır.

Fark kümesi birçok uygulamada, çalışma alanında yer almış bir yapıdır. Roy ve Godsil 2009'da yayınlamış olduğu makalesinde fark kümelerin kuantum bilişiminde kullanılacağında bahsetmiştir. Ayrıca Assmus ve Key (1992) cebirsel kodlama üzerinde dizaynın analiz uygulamalarını incelemiştir.

Kerdock ve Preparata kodlarının biçimsel ikiliğinin açıklaması, son birkaç yılda uygulamalı cebir alanında göze çarpan sonuçlardan biridir. Bu sonuç, $\mathbb{Z}_4$ üzerinde korelasyon özellikleri en iyi ikili dizilerden daha iyi olan büyük dört fazlı dizi setlerinin keşfi ile ilgilidir. Ayrıca, dizilerin korelasyon özellikleri, (döngüsel) gruplardaki belirli kümelerin fark kümelerinin özellikleriyle yakından ilişkilidir.

1.2. Temel Kavramlar

Bu bölümde dizayn adını verdiğimiz yapıya özel bir şekilde etki ederek bu yapı üzerinde fark kümesi, hemen hemen fark kümesi, kısmi fark kümesi, fark kümelerileri aileleri vb. yapılar elde edilir. Genel olarak fark kümesi, hemen hemen fark kümesi vb. yapılar için özel olarak sonlu ve toplamsal gruplar kullanılmaktadır.

Diğer taraftan döngüsel sayıların yapılarını inceleyebilmek için ise sayılar teorisinden bazı temel kavramlara (İlkel kök, indeks kavramı, kuadratik rezidü, vb.) ve bunlara istinaden fark kümesi ve hemen hemen fark kümesi elde edebilmek için kullanacağımız döngüsel sayıların özel bir birleşiminden oluşan döngüsel sınıflar içinse cisim yapısına ihtiyaç duyacağız.

1.3.1 İlkel (Primitif) Kökler ve İndeksler

Tanım 1.3.1. Her $m > 0$ tam sayını, m 'yi geçmeyen ve m ile aralarında asal olan tam sayıların sayısına eşleyen fonksiyona Euler φ – fonksiyonu adı verilir ve m 'nin Euler fonksiyonu $\varphi(m)$ ile gösterilir.

Tanım 1.3.2. $m, t \in \mathbb{Z}$ ve $(m, t)_{\text{ebob}} = 1$ olsun. Bu takdirde $t^k \equiv 1 \pmod{m}$ kongüransını sağlayan en küçük pozitif k tam sayısına a 'nın modülüne göre mertebesi denir ve $o_m(a)$ notasyonu ile gösterilir. $o_m(a) = \varphi(a)$ ise bu durumda a 'ya m modülüne göre ilkel kök denir.

Tanım 1.3.3. m modülüne göre g bir ilkel kök ve b tam sayı olmak üzere $(b, t)_{\text{ebob}} = 1$ olsun. Bu takdirde $b \equiv g^j \pmod{m}$, $1 \leq j \leq \varphi(m)$ şartını sağlayan j tamsayısına b 'nin g tabanına göre indeksi denir ve $\text{ind}_g b = j$ ile gösterilir.

Teorem 1.3.1. g, m modülüne göre bir ilkel kök olsun. Bu taktirde,

$$g^u \equiv a \pmod{m} \Leftrightarrow \text{ind}_g a \pmod{\varphi(m)}$$

İspat. $g^u \equiv a \pmod{m}$ olsun.

$$g^u \equiv a \equiv g^{\text{ind}_g a} \pmod{m}$$

yazılabilir. Buradan ise,

$$u \equiv \text{ind}_g a \pmod{\varphi(m)}$$

bulunur. Tersine $u \equiv \text{ind}_g a \pmod{\varphi(m)}$ ise uygun bir $v \in \mathbb{Z}$ için

$$u = \text{ind}_g a + v \cdot \varphi(m)$$

yazabiliriz. Şu halde,

$$g^u \equiv g^{\text{ind}_g a + v \cdot \varphi(m)} \equiv g^{\text{ind}_g a} (g^{\varphi(m)})^v \equiv g^{\text{ind}_g a} \equiv a \pmod{m}$$

elde edilir.

Teorem 1.3.2. m modülüne göre g ilkel kök, n pozitif tamsayı ve $(m, a)_{\text{ebob}} = (m, b)_{\text{ebob}} = 1$ olsun. Bu taktirde aşağıdaki ifadeler sağlanır.

$$(i) \text{ind}_g a \cdot b \equiv \text{ind}_g a + \text{ind}_g b \pmod{\varphi(m)}$$

$$(ii) \text{ind}_g a^n \equiv n \cdot \text{ind}_g a \pmod{\varphi(m)}$$

İspat. (i) $\text{ind}_g a = u$ ve $\text{ind}_g b = v$ diyelim. İndeks tanımına göre $g^u \equiv a \pmod{m}$ ve $g^v \equiv b \pmod{m}$ diyebiliriz. $a \cdot b \equiv g^u \cdot g^v \equiv g^{\text{ind}_g a + \text{ind}_g b} \pmod{m}$ bir önceki teoremden $\text{ind}_g a \cdot b \equiv \text{ind}_g a + \text{ind}_g b \pmod{\varphi(m)}$ olarak bulunup istenen elde edilir. (ii) ispatı (i) den açık görülebilir.

Örnek 1.3.1. $m = 10$ için $\varphi(10)$ nun değerini bulalım.

$$(10, 1)_{\text{ebob}} = (10, 3)_{\text{ebob}} = (10, 7)_{\text{ebob}} = (10, 9)_{\text{ebob}} = 1$$

olup 10'dan küçük 10 ile arasında asal olan 4 sayı mevcuttur. O halde $\varphi(10) = 4$ bulunur.

Teorem 1.3.3. $\varphi(1) = 1$ ve $n > 1$ pozitif bir tamsayı olmak üzere

$$\varphi(n) = n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

dir. Burada çarpım n tamsayısının bütün p asal bölenlerin üzerinden alınmaktadır. Bu halde n tamsayısının kanonik formu $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ ise

$$\varphi(n) = n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right)$$

olur. Burada $p_1, p_2, \dots, p_k \in \mathbb{P}$ ve $\alpha_1, \alpha_2, \dots, \alpha_k \in \mathbb{N}$ dir.

Sonuç 1.3.1. $p \in \mathbb{P}$ olmak üzere, $\varphi(p) = p - 1$ olur.

Örnek 1.3.2. $m = 19$ için $\varphi(19)$ değerini bulalım.

19 bir asal sayı olduğundan $\varphi(19) = 19 - 1 = 18$ elde edilir.

Örnek 1.3.3. $m = 100$ için $\varphi(100)$ ün değerini bulalım.

$100 = 2^2 5^2$ şeklinde kanonik formda yazılacak olursa

$$\varphi(100) = 100 \cdot \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 40$$

bulunur. Yani 100'den küçük 100 ile aralarında asal olan 40 tamsayı mevcuttur.

Teorem 1.3.4. p asal sayı olmak üzere, p moduna göre $\varphi(\varphi(p))$ tane ilkel kök vardır.

Örnek 1.3.4. $p = 101$ asal sayı için ilkel kök sayısını bulalım.

$p = 101$ sayısının ilkel kök sayısı Teorem 1.3. ten $\varphi(\varphi(101))$ tanedir.

$\varphi(101) = 101 - 1 = 100$ elde edilir. $\varphi(\varphi(101)) = \varphi(100) = 40$ olup $p = 101$ sayısının 40 tane ilkel kökü vardır.

Tanım 1.3.4. p tek asal sayı ve $(p, a)_{\text{ebob}} = 1$ olacak şekilde $a \in \mathbb{Z}$ olsun. Eğer $x^2 \equiv a \pmod{p}$ kongrüansının çözümü mevcutsa a 'ya p modülüne göre kuadratik rezidü eğer çözüm yoksa kuadratik olmayan rezidü denir.

Teorem 1.3.5. p tek asal sayı olmak üzere p 'nin kuadratik rezidülerinin sayısı $(p - 1)/2$ tanedir.

İspat. $1, 2, 3, \dots, p - 1$ sayıları arasından p 'nin tüm kuadratik rezidülerini bulmak için bu sayıların karelerinin p modülüne göre en küçük pozitif kalanları bulunmalıdır. $p - 1$ tane kare hesaplanacağından ve her $x^2 \equiv a \pmod{p}$ kongrüansı ya çözümsüz ya da iki çözümlü olacağından $1, 2, 3, \dots, p - 1$ sayıları arasında $(p - 1)/2$ tane p 'nin kuadratik rezidüsü olmalıdır.

1.3.2 Gruplar

Tanım 1.3.5. G boş olmayan bir küme ve $*$ işlemi G de bir ikili işlem olsun. Verilen $*$ işleminin G de birleşme özelliği ve birim elemanı varsa ayrıca $*$ işlemine göre G deki her elemanın tersi varsa $(G, *)$ cebirsel yapısına grup denir.

Tanım 1.3.6. $(G, *)$ bir grup ve $\forall a, b \in G$ için $a * b = b * a$ değişme özelliği sağlıyorsa G grubuna değişmeli grup veya abel grup denir.

Tanım 1.3.7. G sonlu bir küme ise $(G, *)$ grubuna sonlu grup denir ve eleman sayısına da grubun mertebesi denir. $|G|$ ile gösterilir.

Tanım 1.3.8. $(G, *)$ ve (H, Δ) gruplar olsun. Eğer;

(i) $H \subseteq G$

(ii) $\forall a, b \in H$ için $a \Delta b = a * b$ ise

o zaman H ye G nin bir alt grubu denir ve $H \leq G$ şeklinde gösterilir.

Tanım 1.3.9. G bir grup ve $\emptyset \neq A \subseteq G$ olsun. Bu durumda

$$\langle A \rangle = \{a_1 a_2 a_3 \dots a_n : \forall 1 \leq i \leq n \text{ için } a_i \in A \text{ veya } a_i^{-1} \in A\}$$

kümesine A tarafından üretilen küme adı verilir.

Teorem 1.3.6. G bir grup, $\emptyset \neq A \subseteq G$ olsun. Bu durumda $\langle A \rangle \leq G$ dir. Bu alt gruba A tarafından üretilen alt grup adı verilir.

Tanım 1.3.10. G bir grup ve $a_1, a_2, \dots, a_n \in G$ olsun. Eğer $G = \langle a_1, a_2, \dots, a_n \rangle$ ise o zaman $a_1, a_2, \dots, a_n$ elemanına G nin üreteçleri denir.

Teorem 1.3.7. G bir grup ve $a \in G$ olsun. Eğer

$$H = \{a^n : n \in \mathbb{Z}\}$$

ise o zaman H kümesi G nin bir alt grubudur.

Tanım 1.3.11. G bir grup ve $a \in G$ olsun. G nin $H := \{a^n : n \in \mathbb{Z}\}$ alt gruplarına G nin a tarafından üretilen devirli alt grubu denir ve $\langle a \rangle$ şeklinde gösterilir. Özel olarak $G = \langle a \rangle$ olacak şekilde $a \in G$ varsa o zaman G ye a tarafından üretilen devirli grup denir.

Tanım 1.3.12. G bir grup ve $a \in G$ olsun. Eğer $G = \langle a \rangle$ ise o zaman a ya G nin bir üretici denir.

1.3.3 Halka ve Cisimler

Tanım 1.3.13. $(R, +)$ bir değişmeli bir grup ve R üzerinden çarpma $\cdot$ işlemi tanımlı olsun. Eğer;

- (i) R de $\cdot$ işlemi birleşme özelliğine sahip,
 - (ii) R de $\cdot$ işlemi $+$ üzerine soldan ve sağdan dağılma özelliğine sahip,
- ise $(R, +, \cdot)$ üçlüsüne bir halka denir.

Tanım 1.3.14. $(R, +, \cdot)$ bir halka olsun. Her $x \in R$ için $e \cdot x = x \cdot e = x$ olacak biçimde $e \in R$ varsa e ye R halkasının birimi denir ve R ye bir birimli halka adı verilir.

Tanım 1.3.15. $(R, +, \cdot)$ bir halka olsun. Her $x, y \in R$ için $x \cdot y = y \cdot x$ ise R ye bir değişmeli halka denir.

Tanım 1.3.16. F birimli, değişmeli bir halka ve $1_F \neq 0_F$ olsun. Eğer F çarpma işlemi altında değişmeli bir grup ise F ye bir cisim denir. Başka bir deyişle komutatif (değişmeli) bölme halkasına cisim denir.

Tanım 1.3.17. $(R, +, \cdot)$ bir cisim ve $g \in R$ olsun. $R = \langle g \rangle$ oluyorsa g elemanına R cisminin üretici denir.

1.3.4 Tekrarlanma Yapıları ve Dizaynlar

Bu bölümde dizayn yapısını ele alacağız. Burada t -dizaynları, simetrik dizaynlar ve bu dizayndan elde edilen fark kümeleriyle ilgili bağıntılar inceleyeceğiz.

Dizayn teorisi, kombinatorial bir alan olmak ile birlikte istatistik ve istatistiksel bağıntıları irdelemek amaçlı karşımıza çıkmış olan bir teoridir. Üzerinde yapılan çalışmalar sonucunda geometri, kodlama teorisi, grup teorisi ve fark kümeleride dahil olmak üzere matematiğin bir çok alanında yer almıştır.

Tanım 1.3.18. (*Tekrarlanma Yapısı*) $\mathcal{P}$ noktalar kümesi, $\mathcal{B}$ ise $\mathcal{P}$ noktalar kümesi üzerinden elde edilen bloklar kümesi olsun. $\mathcal{P} \cap \mathcal{B} = \emptyset$ ve $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{B}$ bağıntısı ile oluşan $(\mathcal{P}, \mathcal{B}, \mathcal{I})$ sıralı üçlüsüne tekrarlanma yapısı denir. Ayrıca $\mathcal{I}$ bağıntısında yer alan her sıralı ikili için ilişkilidir denir (Lander,1953).

Örnek 1.3.5. $(\mathbb{Z}_n, +)$ grubunu ele alalım. $\mathcal{P} = \{\bar{1}, \bar{2}, \dots, \overline{n-1}\}$ noktalar kümesi ve $\mathcal{B}$ ise bu elemanların denklik sınıflarında oluşsun. $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{B}$ bağıntısı ile birlikte $(\mathcal{P}, \mathcal{B}, \mathcal{I})$ sıralı üçlüsü bir tekrarlanma yapısına örnek teşkil eder.

Tanım 1.3.19. (*Tekrarlanma Matrisi*) $\mathcal{P} = \{p_1, p_2, \dots, p_u\}$ noktalardan oluşan bir küme, $\mathcal{B} = \{b_1, b_2, \dots, b_v\}$ bloklar kümesi ve $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{B}$ bağıntısı ile $(\mathcal{P}, \mathcal{B}, \mathcal{I})$ tekrarlanma yapısı olmak üzere;

$$m_{ij} = \begin{cases} 1, & p_i \in \mathcal{B}_j \\ 0, & \text{diğer durumlarda} \end{cases}$$

şeklinde tanımlanan $M = [m_{ij}]_{u \times v}$ matrisine tekrarlanma matrisi denir (Lander,1953).

Örnek 1.3.6. Bir dizayn örneğinin tekrarlanma matrisi $\mathcal{P} = \{1, 2, 3, 4, 5\}$ noktalar kümesi ve $\mathcal{B} = \{\{1, 2\} \{1, 3, 4\} \{2, 3, 4, 5\} \{1, 2, 3, 4, 5\}\}$ bloklar kümesinden oluşan tekrarlanma yapısını ele alalım. Bu tekrarlanma yapısının matrisi,

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

şeklinde oluşur. Örnek üzerinden de görüleceği üzere $\mathcal{P}$ noktalar kümesi sütunları, $\mathcal{B}$ bloklar kümesi satırları temsil etmektedir.

Tanım 1.3.20. (*t-dizayn*) t pozitif bir tamsayı, $\mathcal{P} = \{p_1, p_2, \dots, p_v\}$ mertebesi v olan noktalar kümesi ve $\mathcal{B}$ ise $\mathcal{P}$ kümesinin k elemanlı alt kümelerinden oluşan bloklar kümesi olsun. Burada $\lambda \geq 1$ olmak üzere $\mathcal{P}$ nin t elemanlı her bir alt kümesi bu bloklarda tam olarak λ kez bulunuyor ise bu tekrarlanma yapısına (v, k, λ) parametrelili bir t - dizayn adı verilir (Baumert, 1971).

Örnek 1.3.7. $\mathbb{Z}_2$ sonlu cismi üzerinde $(\mathbb{Z}_2)^4$ olarak tanımlanan 4 - boyutlu vektör uzayını ele alalım. Burada $\mathcal{P}$ kümesi uzayda yer alan $\vec{0}$ vektör hariç tüm vektörlerin kümesi, $\mathcal{B}$ ise $x + y + z = 0$ koşulunu sağlayan bloklar kümesi olsun. Bu taktirde $(x, y, z \in (\mathbb{Z}_2)^4)$ yapısı bir 2 - dizayn oluşturur.

Tanım 1.3.21. (*Simetrik Dizayn*) (v, k, λ) parametrelili bir dizayn ve $0 \leq k < v$ olsun.

- (i) v sayıda nokta mevcuttur.
- (ii) v sayıda blok mevcuttur.
- (iii) Her bir nokta k tane blokta bulunur.
- (iv) Her bir blokta k tane nokta bulunur.
- (v) Herhangi bir blokta λ tane ortak nokta bulunur.
- (vi) Herhangi iki nokta λ blokta birlikte yer alır.

Bu aksiyomları sağlayan yapıya simetrik dizayn adı verilir (Hall ve Ryser, 1951).

Örnek 1.3.8. 5×5 boyutunda 25 kareden oluşan bir yapıyı ele alalım. Bu yapının içinde yer alan her bir kare noktalar kümesini, karenin kendisi hariç olmak üzere satırında ve sütununda yer alan kareler ise bloklar kümesini oluştursun.

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

Şekil 2. $(25, 8, 2)$ parametrelili bir simetrik dizayn

Yukarıda yer alan tabloda $\mathcal{B}_{10}$ bloğunu gösterilmiştir. Şekilde görülebileceği üzere her bir blokta 8 kare yer alır. Bu noktalar ver bloklardan kümesinde oluşan yapı tanım gereği $(25, 8, 2)$ parametrelili bir simetrik dizayn oluşturur.

1.4. Döngüsel Sayılar (Cyclotomic Numbers)

Cyclotomy kelimesi “Daire bölünmesi” anlamına gelir ve birim dairenin çevresini eşit uzunlukta yayların verilen n sayısına eşit şekilde bölme işlemini sonucunda elde edilen köklerin indisler ile ifade edilmesidir.

Tanım 1.4.1. (*Döngüsel Sayılar*) $p \in \mathbb{P}$ ve $\alpha \in \mathbb{N}$ olmak üzere $q = p^\alpha = e \cdot f + 1$ formunda bir asal sayının kuvveti ve g ise $(\text{mod } q)$ için bir ilkel kök olsun.

$0 \leq s, t \leq e$ olacak biçimde s, t tam sayıları için e mertebeli $(s, t)_e$ döngüsel sayısı $1 \leq n \leq e - 2$ aralığında bulunan ve aşağıdaki koşulu sağlayan n tam sayıdır.

$$\text{ind}_g n \equiv s \pmod{e} \text{ ve } \text{ind}_g(n + 1) \equiv t \pmod{e}$$

Burada yola çıkarak döngüsel sayılar benzer bir şekilde (a, b) çifti olarak ifade edilebilir.

$$1 + g^{e.a+s} \equiv g^{e.b+t} \pmod{p}$$

Burada $0 \leq a, b \leq f - 1$ aralığında yer alır (Thomas Storer, 1967).

Teorem 1.4.1. e mertebeli döngüsel sayılar için $(s, t)_e = (e - s, s - t)_e$ eşitliği sağlanır (Thomas Storer, 1967).

Teorem 1.4.2. e mertebeli döngüsel sayılar için aşağıdaki ifade sağlanır (Thomas Storer, 1967).

$$(s, t)_e = \begin{cases} (t, s)_e & , \quad \text{eğer } f \equiv 0 \pmod{2} \\ \left(t + \frac{e}{2}, s + \frac{e}{2}\right)_e & , \quad \text{eğer } f \not\equiv 0 \pmod{2}. \end{cases}$$

Teorem 1.4.3. e mertebeli döngüsel sayılar için aşağıdaki ifade sağlanır (Thomas Storer, 1967).

$$\sum_{t=0}^{e-1} (s, t)_e = \begin{cases} f - 1, & [f \text{ çift} \wedge s \equiv 0 \pmod{e}] \vee [f \text{ tek} \wedge s \equiv \frac{e}{2} \pmod{e}] \\ f, & \text{diğer durumlarda.} \end{cases}$$

Teorem 1.4.4. e mertebeli döngüsel sayılar için aşağıdaki ifade sağlanır (Thomas Storer, 1967).

$$\sum_{s=0}^{e-1} (s, t)_e = \begin{cases} f - 1; & t \equiv 0 \pmod{e} \\ f & ; t \not\equiv 0 \pmod{e}. \end{cases}$$

Teorem 1.4.5. (2. Mertebeden Döngüsel Sayılar) $p = 2f + 1$ formunda bir asal olsun. Bu takdirde;

$$4(0, 0)_2 = p - 4 - (-1)^f$$

$$4(0, 1)_2 = p - (-1)^f$$

$$4(1, 0)_2 = 4(1, 1)_2 = p - 2 + (-1)^f$$

sağlanır (Dickson, 1935).

İspat. $f \equiv 0 \pmod{2}$ olduğu durumda, Teorem 1.4.1. ve Teorem 1.4.2.'den

$$(0,0)_2 = A$$

$$(0,1)_2 = (1,0)_2 = (1,1)_2 = B.$$

2. mertebeden döngüsel matrisin aşağıdaki forma sahip olduğu görülür

$$\begin{matrix} & 0 & 1 \\ 0 & A & B \\ 1 & B & B \end{matrix}$$

A ve B 'nin Teorem 1.4.3. lineer bağıntısı elde edilir

$$A + B = f - 1$$

$$2B = f.$$

Dolayısıyla bu durumda,

$$4(0,0)_2 = 4A = 2f - 4 = p - 5,$$

$$4(0,1)_2 = 4(1,0)_2 = 4(1,1)_2 = 4B = 2f = p - 1$$

olarak bulunur. Şimdi f' in tek olduğu durumu ele alalım.

$f \not\equiv 0 \pmod{2}$ olduğu durumda, Teorem 1.4.1 ve Teorem 1.4.2.'ye göre

$$(0,0)_2 = (1,0)_2 = (1,1)_2 = A$$

$$(0,1)_2 = B$$

bulunur. Buna göre 2. mertebeden döngüsel matrisin aşağıdaki forma sahip olduğu görülür

$$\begin{matrix} & 0 & 1 \\ 0 & A & B \\ 1 & A & A \end{matrix}.$$

A ve B 'nin Teorem 1.4.3'ten aşağıdaki lineer bağıntısı elde edilir

$$A + B = f$$

$$2A = f - 1.$$

Dolayısıyla bu durumda,

$$4(0,0)_2 = 4(1,0)_2 = 4(1,1)_2 = 4A = 2f - 2 = p - 3$$

$$4(0,1)_2 = 4B = 2f + 2 = p + 1$$

olarak bulunup istenen elde edilir.

1.4.6. 3. Mertebeden Döngüsel Sayılar

$p = 3f + 1$ formunda bir asal ve $(mod p)$ 'nin ilkel kökü g olsun. Bu takdirde Teorem 1.4.1 ve Teorem 1.4.2'den

$$\begin{aligned}(0, 0)_2 &= A \\ (0, 1)_2 &= (1, 0)_2 = (2, 2)_2 = B \\ (0, 2)_2 &= (2, 0)_2 = (1, 1)_2 = C \\ (1, 2)_2 &= (2, 1)_2 = D\end{aligned}$$

bulunur. 3. mertebeden döngüsel matrisin aşağıdaki forma sahip olduğu görülür

$$\begin{matrix} & 0 & 1 & 2 \\ \begin{matrix} 0 \\ 1 \\ 2 \end{matrix} & \begin{bmatrix} A & B & C \\ B & C & D \\ C & D & B \end{bmatrix} \end{matrix}.$$

A, B, C ve D 'nin Teorem 1.4.3 lineer bağıntısı elde edilir

$$\begin{cases} A + B + C = f - 1 \\ B + C + B = f. \end{cases} \quad (1)$$

A, B, C ve D 'nin Teorem 1.4.3'ten lineer bağıntısı elde edilir. Böylece, 3.dereceden döngüsel sayıları belirlemek için A, B, C ve D arasındaki iki doğrusal ilişki daha gereklidir. Gauss'un,

$$1 + g^{3(u_1)} + g^{3(u_2)-1} + g^{3(u_3)+2} \equiv 0 \pmod{p} \quad (2)$$

denkleminin çözümlerine N dersek N sayısını iki farklı şekilde sayarak iki doğrusal ilişkiyi nasıl elde edilebileceği gösterilir.

İlk olarak;

$$\begin{aligned} N &= \sum_{\substack{u_1, u_2, u_3=0 \\ 1 + g^{3u_1} + g^{3u_2+1} + g^{3u_3+2} \equiv 0 \pmod{p}}}^{f-1} 1 \\ &= \sum_{h=0}^2 \sum_{v=0}^{f-1} \left(\sum_{\substack{u_1=0 \\ 1 + g^{3u_1} \equiv g^{3v+h} \pmod{p}}}^{f-1} 1 \right) \left(\sum_{\substack{u_2, u_3=0 \\ g^{3v+h} + g^{3u_2+1} + g^{3u_3+2} \equiv 0 \pmod{p}}}^{f-1} 1 \right) \end{aligned}$$

$$\begin{aligned}
&= \sum_{h=0}^2 \left(\sum_{v=0}^{f-1} 1 \right) \left(\sum_{u_2, u_3=0}^{f-1} 1 \right) \\
&\quad \left(1 + g^{3u_1} \equiv g^{3v+h} \right) \left(1 + g^{3u_2+1-h} + g^{3u_3+2-h} \equiv 0 \pmod{p} \right) \\
&= \sum_{h=0}^2 (0, h)(1-h, 2-h)
\end{aligned}$$

$$= AD + B^2 + C^2.$$

İkinci olarak;

$$\begin{aligned}
N &= \sum_{\substack{u_1, u_2, u_3=0 \\ 1 + g^{3u_1} + g^{3u_2+1} + g^{3u_3+2} \equiv 0 \pmod{p}}}^{f-1} 1 \\
&= \sum_{h=0}^2 \sum_{v=0}^{f-1} \left(\sum_{u_2=0}^{f-1} 1 \right) \left(\sum_{u_3=0}^{f-1} 1 \right) \\
&\quad \left(1 + g^{3u_2+1} \equiv g^{3v+h} \pmod{p} \right) \left(g^{3v+h} + g^{3u_1} + g^{3u_3+2} \equiv 0 \pmod{p} \right) \\
N &= BC + CD + BD.
\end{aligned}$$

N için iki ifadeyi eşitleyerek aşağıdaki denklem elde edilir

$$AD + B^2 + C^2 = BC + CD + BD \quad (3)$$

şimdi (2)'den

$$A = D - 1 \quad (4)$$

elde edilir. Denklem (4)'ü (3)'te yerine yazılacak olursa,

$$D = B^2 + C^2 + D^2 - BC - BD - CD, \quad (5)$$

(2) ve (5)'ten

$$\begin{aligned}
4p &= 12f + 4 = 12(B + C + D) + 4 = 36D + 12(B + C) - 24D + 4 \\
&= 36(B^2 + C^2 + D^2 - BC - BD - CD) + 12(B + C) - 24D + 4 \\
4p &= (-3B - 3C + 6D - 2)^2 + 3(3B - 3C)^2
\end{aligned}$$

denklemini elde edilir. Denklemde görüldüğü üzere $4p$ 'nin ikinci dereceden denklemi A, B, C ve D 'yi içeren iki ek doğrusal ilişkiyi verir.

$$\begin{cases} -3B - 3C + 6D - 2 = r_3 \\ 3B - 3C = s_3 \end{cases} \quad (6)$$

burada r_3 ve s_3 tam sayıları

$$4p = r_3^2 + 3s_3^2, r_3 \equiv 1 \pmod{3}, s_3 \equiv 0 \pmod{3} \quad (7)$$

formundadır. 4 doğrusal denklemin A, B, C, D için (2) ve (6)'da çözülmesi sonucunda,

$$\begin{cases} 9A = p + r_3 - 8 \\ 18B = 2p - r_3 + 3s_3 - 4 \\ 18C = 2p - r_3 + 3s_3 - 4 \\ 9D = p + r_3 + 1. \end{cases}$$

İyi bilinir ki r_3 için tek çözüm bulunur fakat s_3 'te işaret belirsizliği mevcuttur. Burada r_3 ilkel kök olan g 'ye bağımlı değildir sadece p 'ye bağımlıdır. Şimdi aşağıdaki kongrüansı sağlayan s_3 için tek çözüm olduğunu gösterelim.

$$3s_3 \equiv (g^{(p-1)/3} - g^{2(p-1)/3})r_3 \pmod{p}.$$

Bu bağıntı için aşağıdaki toplamı dikkate alırsak,

$$\sum = \sum_{x=1}^{p-1} (1 + x^3)^{(p-1)/3}$$

$\pmod{p}$ için toplamını iki farklı şekilde yapılır. $w \equiv g^{(p-1)/3} \equiv g^f \pmod{p}$ kongrüansının çözümleri böylece, $w^3 \equiv 1 \pmod{p}$, $w \not\equiv 1 \pmod{p}$, $1 + w + w^2 \equiv 0 \pmod{p}$, $(w - w^2)^2 \equiv -3 \pmod{p}$ şekilde bulunur.

İlk olarak, 3. mertebeden ki döngüsel sayılar için elde edilen formülleri kullanılarak,

$$\begin{aligned} \sum &\equiv \sum_{u=0}^{3f-1} (1 + g^{3u})^f \equiv 3 \sum_{u=0}^{3f-1} (1 + g^{3u})^f \equiv 3 \sum_{\substack{u=0 \\ u \neq f/2}}^{3f-1} (1 + g^{3u})^f \\ &\equiv 3 \sum_{h=0}^2 \sum_{v=0}^{f-1} \sum_{\substack{u=0 \\ 1+g^{3u} \equiv g^{3v+h} \pmod{p}}}^{f-1} (1 + g^{3u})^f \\ &\equiv 3 \sum_{h=0}^2 g^{hf} \sum_{\substack{u=0 \\ 1+g^{3u} \equiv g^{3v+h} \pmod{p}}}^3 1 \equiv 3 \sum_{h=0}^2 w^h(0, h)_3 \\ &\equiv \frac{1}{6} ((2p + 2r_3 - 16) + w(2p - r_3 + 3s_3 - 4) + w^2(2p - r_3 - 3s_3 - 4)) \\ &\equiv \frac{1}{2} (r_3 + s_3(w - w^2)) - 2. \end{aligned}$$

İkinci olarak da binom teoremi kullanılarak, $\pmod{p}$ bulunur,

$$\sum \equiv \sum_{x=1}^{p-1} \sum_{n=0}^{(p-1)/3} \binom{(p-1)/3}{n} x^{3n} \equiv \sum_{n=0}^{(p-1)/3} \binom{(p-1)/3}{n} \sum_{x=1}^{p-1} x^{3n}$$

$$\equiv \sum_{\substack{n=0 \\ p-1 \mid 3}}^{(p-1)/3} \binom{(p-1)/3}{n} = -2.$$

$\text{mod } p$ 'ye göre bulunan iki ispatı bir araya getirerek, aşağıdaki denklem görülür.

$$r_3 + s_3(w - w^2) \equiv 0 \pmod{p}.$$

Bu kongrüansı $(w - w^2)$ ile çarparak;

$$3s_3 \equiv (w - w^2)r_3 \pmod{p}$$

elde edilir. Böylece s_3 için işaret belirsizliği ortadan kaldırılır.

Teorem 1.4.6. (3. Mertebeden Döngüsel Sayılar) $p = 3f + 1$ formunda bir asal ve $(\text{mod } p)$ 'nin ilkel kökü g olsun,

$$\begin{cases} 4p \equiv r_3^2 + 3s_3^2 \equiv 1 \pmod{3}, & s_3 \equiv 0 \pmod{3} \\ 3s_3 \equiv (g^{(p-1)/3} - g^{2(p-1)/3})r_3 \pmod{p}. \end{cases} \quad (8)$$

Yukarıdaki kongrüansta tek çözüme sahip olan r_3 ve s_3 tam sayıları için

$$\begin{cases} 9A = p + r_3 - 8 \\ 18B = 2p - r_3 + 3s_3 - 4 \\ 18C = 2p - r_3 + 3s_3 - 4 \\ 9D = p + r_3 + 1 \end{cases} \quad (9)$$

doğrusal denklemlerin sağlandığı üstteki bölümde ispatlanmıştır (Dickson, 1935).

1.4.7. 4. Mertebeden Döngüsel Sayılar

$p = 4f + 1$ formunda bir asal ve $(\text{mod } p)$ 'nin ilkel kökü g olsun. Bu takdirde

Teorem 1.4.1 ve Teorem 1.4.2'ye göre f 'nin tek ve çift olması durumunda

4.dereceden döngüsel sayıların matrisi aşağıdaki gibidir;

$$\begin{array}{cc} f \text{ çift ise} & f \text{ tek ise} \\ \begin{array}{c} 0 \quad 1 \quad 2 \quad 3 \\ \begin{bmatrix} A & B & C & D \\ B & D & E & E \\ C & E & C & E \\ D & E & E & B \end{bmatrix} \end{array} & \begin{array}{c} 0 \quad 1 \quad 2 \quad 3 \\ \begin{bmatrix} A & B & C & D \\ E & E & D & B \\ A & E & A & E \\ E & D & B & E \end{bmatrix} \end{array} \end{array} \quad (1)$$

A, B, C, D ve E 'nin Teorem 1.4.3'ten lineer bağıntısı elde edilir;

$$\begin{array}{ll}
f \text{ çift ise} & f \text{ tek ise} \\
\left\{ \begin{array}{l} A + B + C + D = f - 1 \\ B + D + 2E = f \\ 2C + 2E = f \end{array} \right. & \left\{ \begin{array}{l} A + B + C + D = f \\ B + D + 2E = f \\ 2A + 2E = f - 1. \end{array} \right.
\end{array} \quad (2)$$

Burada 4. mertebeden döngüsel sayıyı belirlemek için A, B, C, D ve E 'yi içeren ikiden daha fazla lineer denkleme ihtiyaç duyulur. Bunun için aşağıdaki kongrüans denklemi

$$1 + g^{4u_1} + g^{4u_2} + g^{4u_3} \equiv 0 \pmod{p}, 0 \leq u_1, u_2, u_3 \leq f - 1$$

$k = 3$ olduğu gibi iki farklı şekilde sayarsak aşağıdaki ikinci dereceden denklemler elde edilir

$$\begin{cases} AE + B^2 + CD + DE = BC + DE + CE + E^2, & \text{eğer } f \text{ çift ise} \\ AE + BD + BC + DE = AE + E^2 + AD + BE, & \text{eğer } f \text{ tek ise.} \end{cases} \quad (3)$$

Bu noktada f 'nin tek ve f 'nin çift olduğu durumları ayrı ayrı inceleyelim.

f çift olsun. (3)'den,

$$0 = AE + B^2 + CD - BC - CE - E^2 \quad (4)$$

eşitliği sağlanır. Şimdi (2)'den elde edilen denklemlerden A bulunacak olursa;

$$A = -C + 2E - 1.$$

Bu denklemi (4)'te yerine yazılırsa;

$$0 = (C - E)^2 + B^2 + CD - BC - C^2 - E. \quad (5)$$

Tekrar (2)'den C 'yi elde edilirse;

$$C = (B + D)/2.$$

O halde

$$B^2 + CD - BC - C^2 = (B - D)^2/4$$

buradan aşağıdaki denklem elde edilir

$$0 = 4(C - E)^2 + (B - D)^2 - 4E. \quad (6)$$

Ayrıca (2)'den

$$4E = f - 2(C - E)$$

böylece (6) yeniden yazılabilir.

$$f = 4(C - E)^2 + 2(C - E) + (B - D)^2$$

burada her iki tarafı 4 ile çarpar ve 1 eklenirse;

$$p = 4f + 1 = (4(C - E) + 1)^2 + (2B - 2D)^2$$

bu bize gerekli olan iki doğrusal ilişkiyi verir;

$$\begin{cases} 4(C - E) + 1 = -a_4 \\ 2B - 2D = b_4. \end{cases} \quad (7)$$

Buradan ise,

$$p = a_4^2 + b_4^2, \quad a_4 \equiv -1 \pmod{4} \quad (8)$$

(2) ve (7) denklemlerinde A, B, C, D ve E için aşağıdaki çözümleri elde edilir

$$16A = p + 6a_4 - 11,$$

$$16B = p - 2a_4 + 4b_4 - 3$$

$$16C = p - 2a_4 - 3$$

$$16D = p - 2a_4 - 4b_4 - 3$$

$$16E = p + 2a_4 + 1.$$

iyi bilinir ki a_4 için tek çözüm bulunur fakat b_4 'te işaret belirsizliği mevcuttur. Bölümün sonunda nasıl tek çözüme sahip olduğu görülür. Şimdi f 'in tek olduğu durumu ele alalım.

f tek olsun. (3)'den

$$0 = E^2 + AD + BE - BD - BC - DE$$

şimdi (2)'den $A + C = 2E$ elde ediyoruz. Böylece C yi elimine edilirse;

$$0 = E^2 + AD + AB - BD - BE - DE. \quad (9)$$

Ayrıca (2)'den $B + D = 1 + 2A$ olduğu görüldü. Böylece;

$$\begin{cases} 2B = 1 + 2A + (B - D) \\ 2D = 1 + 2A - (B - D). \end{cases} \quad (10)$$

(9)' 4 ile çarpılıp (10)'da $2B$ ve $2D$ yer değiştirilirse;

$$0 = 4E^2 - 4E - 1 - 8AE + 4A^2 + (B - D)^2$$

buradan aşağıdaki denklem elde edilir.

$$4E + 1 = (B - D)^2 + 4(A - E)^2.$$

Dolayısıyla (7)'den

$$\begin{aligned} p &= 4f + 1 = 4(2A + 2E + 1) + 1 = 4(4E + 1) + 8(A - E) + 1 \\ &= 4(B - D)^2 + 16(A - E)^2 + 8(A - E) + 1 = (4(A - E) + 1)^2 + (2B - 2D)^2 \end{aligned}$$

bulunur. O halde

$$\begin{cases} 4(A - E) + 1 = a_4 \\ 2B - 2D = b_4 \end{cases} \quad (11)$$

burada D, E, a_4 ve b_4 parametreleri cinsinden yazılırsa p 'nin formu

$$p = a_4^2 + b_4^2, \quad a_4 \equiv 1 \pmod{4} \quad (12)$$

şeklinde yazılır. (2) ve (11) denklemlerinde A, B, C, D ve E için aşağıdaki çözümleri elde edilir;

$$16A = p + 2a_4 - 7,$$

$$16B = p + 2a_4 + 4b_4 + 1$$

$$16C = p - 6a_4 + 1$$

$$16D = p + 2a_4 - 4b_4 + 1$$

$$16E = p - 2a_4 - 3.$$

Şimdi f 'in tek ve f 'in çift olduğu durumlarda kongrüanslarda ortaya çıkan b_4 'te ki işaret belirsizliğini ortadan kaldırılacaktır

$$b_4 \equiv g^{(p-1)/4} a_4 \pmod{4}$$

işaret belirsizliğini kaldırmak için Gauss toplamı argümanına benzer bir şekilde ele alarak yapılacak olursa;

$$\sum := \sum_{x=1}^{p-1} (1 + x^4)^{p-1/4}$$

burada $w \equiv g^{(p-1)/4} \pmod{p}$ dersek $w^2 \equiv -1 \pmod{p}$, $w^3 \equiv -w \pmod{p}$ ve $w^4 \equiv 1 \pmod{p}$ kongrüanslarını elde edilir.

Şimdi ilk olarak $\sum$ içinde $x, (1 \leq x \leq p-1)$ ile $g^u, (0 \leq u \leq p-2)$ yer değişikliği yapılırsa,

$$\sum \equiv 2a_4 + 2b_4 - 2 \pmod{p}.$$

İkinci olarak ise binom teoremini $\sum$ içinde $(1 + x^4)^{p-1/4}$ 'e uygulayıp toplam sırasını değiştirerek aşağıdaki ifadeyi elde edilir,

$$\sum \equiv -2 \pmod{p}.$$

$\sum \equiv \pmod{p}$ 'in yukarıda bulunan iki sonuç karşılaştırılırsa;

$$a_4 + b_4 w \equiv 0 \pmod{p}$$

elde edilir. Buradan ise;

$$b_4 \equiv a_4 w \pmod{p}$$

bulunur. Öyle ki b_4 için işaret belirsizliği ortadan kaldırılmış olur. Özetle, bu bize aşağıdaki teoremi verir.

Teorem 1.4.6. (4. Mertebeden Döngüsel Sayılar) $p = 4f + 1$ formundan bir asal sayı ve $(\text{mod } p)$ nin bir ilkel kökü g olsun. $f \equiv 0 \pmod{2}$ olması durumunda 4. mertebeden döngüsel sayı aşağıdaki doğrusal denklemleri şeklinde ifade edilir;

$$\begin{aligned} 16A &= p + 6a_4 - 11, \\ 16B &= p - 2a_4 + 4b_4 - 3 \\ 16C &= p - 2a_4 - 3 \\ 16D &= p - 2a_4 - 4b_4 - 3 \\ 16E &= p + 2a_4 + 1. \end{aligned}$$

Eğer $f \equiv 1 \pmod{2}$ ise;

$$\begin{aligned} 16A &= p + 2a_4 - 7, \\ 16B &= p + 2a_4 + 4b_4 + 1 \\ 16C &= p - 6a_4 + 1 \\ 16D &= p + 2a_4 - 4b_4 + 1 \\ 16E &= p - 2a_4 - 3 \end{aligned}$$

ile elde edilen ifadeler için;

$$p = a_4^2 + b_4^2, a_4 \equiv -\left(\frac{2}{p}\right) \pmod{4}, b_4 \equiv g^{\frac{p-1}{4}} a_4 \pmod{p}$$

koşulları altında tek türlü yazılabilen a_4 ve b_4 tam sayıları için doğrusal denklemlerin ispatı üst bölümde verilmiştir (Dickson, 1935).

Örnek 1.4.1. 4. mertebeden döngüsel sayılar için $p = 17$ ve $(\text{mod } 17)$ için ilkel kök olan $g = 3$ sayısını ele alalım. Açıkça görülür ki $a_4 = -1$ ve $b_4 = \pm 4$ olur. Böylece $g^{(p-1)/4} a_4 \equiv 3^4 \equiv -4 \pmod{17}$ olup $b_4 \equiv (-1)(-4) \equiv 4 \pmod{17}$ tam sayısını elde edilir,

$$(0,0)_4 = 0, (0,1)_4 = 2, (0,2)_4 = 1, (0,3)_4 = 0, (1,2)_4 = 1$$

$(\text{mod } 4)$ kalan sınıfı için kolayca görülür.

$$\begin{aligned} \text{ind}_3 1 &\equiv 0, \text{ind}_3 2 \equiv 2, \text{ind}_3 3 \equiv 1, \text{ind}_3 4 \equiv 0, \text{ind}_3 5 \equiv 1, \text{ind}_3 6 \equiv 3, \text{ind}_3 7 \equiv 3 \\ \text{ind}_3 8 &\equiv 2, \text{ind}_3 9 \equiv 2, \text{ind}_3 10 \equiv 3, \text{ind}_3 11 \equiv 3, \text{ind}_3 12 \equiv 1, \text{ind}_3 13 \equiv 0 \\ \text{ind}_3 14 &\equiv 1, \text{ind}_3 15 \equiv 2, \text{ind}_3 16 \equiv 0. \end{aligned}$$

Örnek 1.4.2. 5.Mertebeden döngüsel sayılarının matrisini bulalım.

$p = 5f + 1$ formunda bir asal sayı olsun. Burada e tek tam sayı olduğunda f çift sayı olmalıdır. Aksi durumda p çift sayı olup asal sayı olması durumu ile çelişir.

$$(0, 0)_5 = A, (0, 1)_5 = B, (0, 2)_5 = C, (0, 3)_5 = D, (0, 4)_5 = E, (1, 2)_5 = F \\ (1, 3)_5 = G$$

olarak kabul edilirse, Teorem 1.4.1 ve Teorem 1.4.2'den,

$$(0, 0)_5 = A$$

$$(0, 1)_5 = (1, 0)_5 = (4, 4)_5 = B$$

$$(0, 2)_5 = (2, 0)_5 = (3, 3)_5 = C$$

$$(0, 3)_5 = (3, 0)_5 = (2, 2)_5 = D$$

$$(0, 4)_5 = (4, 0)_5 = (1, 1)_5 = E$$

$$(1, 2)_5 = (2, 1)_5 = (3, 4)_5 = (4, 3)_5 = (4, 1)_5 = (1, 4)_5 = F$$

$$(1, 3)_5 = (3, 1)_5 = (2, 3)_5 = (3, 2)_5 = (4, 2)_5 = (2, 4)_5 = G$$

döngüsel sayılar elde edilir. Şimdi bunlar matriste yerine yazılırsa;

$$\begin{array}{c} 0 \quad 1 \quad 2 \quad 3 \quad 4 \\ \begin{array}{c} 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \left[\begin{array}{ccccc} A & B & C & D & E \\ B & E & F & G & A \\ C & F & A & G & B \\ D & G & G & A & C \\ E & A & B & C & D \end{array} \right] \end{array}$$

$e = 5$ için döngüsel sayılar matrisi elde edilmiş olur.

1.5 Döngüsel Sınıflar (Cyclotomic Classes)

Tanım 1.5.1. $p \in \mathbb{P}$ ve $\alpha \in \mathbb{N}$ olmak üzere $q = p^\alpha = ef + 1$ formunda bir asal sayının kuvveti ve $g, GF(q)$ cisminin bir ilkel kök olsun.

$$C_i^e = g^i < g^e > = \{ g^{e \cdot s + i} \mid 0 \leq s \leq f - 1 \}$$

bu cosetlere $GF(q)$ cismi üzerinde e mertebeli döngüsel (cyclotomy) sınıf denir.

Ayrıca $0 \leq i, j \leq e - 1$ tam sayıları için,

$$(i, j)_e = |(C_i + 1) \cap C_j|$$

olarak tanımlanır (Thomas Storer, 1967).

Teorem 1.5.1. $p \in \mathbb{P}$ ve $\alpha \in \mathbb{N}$ olmak üzere $q = p^\alpha = ef + 1$ formunda bir asal sayının kuvveti ve g ise $GF(q)$ cisminin bir ilkel kök olsun. Bu takdirde;

$$GF(q)/\{0\} = \bigcup_{i=0}^{e-1} C_i^e$$

$GF(q)$ kümesinin elemanları döngüsel (cyclotomy) sınıfların birleşimi olarak ifade edilebilir (Thomas Storer, 1967).

1.6 Fark Kümeleri

Tanım 1.6.1. (*Fark Kümesi*) $(G, *)$ yapısı mertebesi v olan bir sonlu grup ve D, G 'nin k elemanlı bir alt kümesi olsun. $d_i, d_j \in D$ olmak üzere $d_i * d_j^{-1}$ şeklindeki elemanların oluşturduğu çoklu Δ , G 'nin birim elemanı hariç diğer tüm elemanlarını λ kez ihtiva ediyorsa D kümesine, G grubu içindeki bir (v, k, λ) – parametrelili fark kümesi denir.

İlk kısımda da bahsettiğimiz gibi fark kümelerinde genel olarak toplamsal grupları ele alacağımız için tanımını toplamsal gruba göre dizayn edilebilir (Lander, 1953).

$(G, +)$ mertebesi v olan sonlu toplamsal bir grup ve D ise G 'nin k elemanlı bir alt kümesi olmak üzere D üzerinde tanımlanan çoklu kümesi $i, j \in \{1, 2, 3, \dots, v-1\}$ ve $i \neq j$ sayıları için;

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

şeklinde ifade edilebilir. Burada Δ çoklu kümesi G grubunun birim elemanı yani 0_R elemanı hariç diğer tüm elemanlarını λ kez içeriyorsa D kümesine (v, k, λ) – fark kümesi denir (Moore ve Pollatsek, 2013).

Örnek 1.6.1. $(\mathbb{Z}_{11}, \oplus)$ grubunda $D = \{1, 3, 4, 5, 9\}$ alt kümesinin fark kümesi olduğunu gösterelim.

Eleman sayısı az olan gruplarda fark kümesi olup olmadığını incelerken kolaylık sağlaması amacıyla tablo üzerinde inceleyeceğiz. Şimdi Δ çoklu kümesi için bir tablo oluşturalım.

Tablo 1. $(\mathbb{Z}_{11}, \oplus)$ grubunda $D = \{1, 3, 4, 5, 9\}$ fark kümesi için çoklu küme tablosu.

$\mathbb{Z}_{11}/\{0\}$	$\lambda = 2$	
1	5 – 4	4 – 3
2	5 – 3	3 – 1
3	4 – 1	1 – 9
4	9 – 5	5 – 1
5	9 – 4	3 – 9
6	9 – 3	4 – 9
7	5 – 9	1 – 5
8	9 – 1	1 – 4
9	1 – 3	3 – 5
10	4 – 5	3 – 4

Tabloda görüldüğü üzere Δ kümesi $(\mathbb{Z}_{11}, \oplus)$ grubundaki birim eleman haricinde diğer elemanları $\lambda = 2$ kez içerdiğinden D kümesi bir $(11, 5, 2) -$ fark kümesidir.

Tanım 1.6.2. (*Fark Fonksiyonu*) $(G, +)$ mertebesi v olan bir değişmeli grup ve D , G 'nin $(v, k, \lambda) -$ fark kümesi olsun. Bu takdirde fark fonksiyonu şu şekilde tanımlanır,

$$d_D(x) = |(D + x) \cap D| = \lambda$$

burada $x \in G/0_G$ 'dir (Cunsheng Ding, 2014).

Yukarıdaki örnekte $(\mathbb{Z}_{11}, \oplus)$ grubunda $D = \{1, 3, 4, 5, 9\}$ alt kümesinin fark kümesi olduğunu görmüştük. Şimdi fark fonksiyonun bir örneğine bu fark kümesi üzerinde bakalım. Keyfi bir $x \in G/0_G$ alalım, örneğin $x = 2$ olsun.

$$\begin{aligned}
 d_D(2) &= |(D + 2) \cap D| \\
 &= |(\{1, 3, 4, 5, 9\} + 2) \cap \{1, 3, 4, 5, 9\}| \\
 &= |\{0, 3, 5, 6, 7\} \cap \{1, 3, 4, 5, 9\}| \\
 &= |\{3, 5\}| = 2
 \end{aligned}$$

olup $d_D(2) = 2 = \lambda$ eşitliği görülür. Diğer $x \in G/0_G$ içinde $d_D(x) = 2$ eşit olduğu açıkça görülebilir (Moore ve Pollatsek, 2013).

Teorem 1.6.1. $(G, *)$ mertebesi v olan bir değişmeli grup ve D ise G 'nin $(v, k, \lambda) -$ fark kümesi olsun. Bu durumda;

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

eşitliği her zaman sağlanır (Moore ve Pollatsek, 2013).

İspat. D , G grubunun bir (v, k, λ) parametrelili bir fark kümesi olsun. Bu takdirde Δ çoklu kümesinde D 'nin k tane elemanı mevcut olduğundan $d_i, d_j \in D$ ve $d_i \neq d_j$ olmak üzere $d_i * d_j^{-1}$ şeklinde $k(k - 1)$ tane eleman bulunabileceğinden Δ çoklu kümesinin eleman sayısı $k(k - 1)$ olarak bulunur. Diğer taraftan D fark kümesi olduğundan G grubunun birim elemanı hariç diğer $(v - 1)$ tane elemanını λ kez içerecektir. Bu yüzden D 'nin Δ çoklu kümesinin eleman sayısı $(v - 1)\lambda$ olacaktır. Böylece istenen eşitlik elde edilmiş olur.

Burada bilmemiz gerek şey; bu teorem fark kümesi olması durumunda her zaman doğrudur. Fakat bu teoremin varlığı her zaman o yapının bize fark kümesi olduğunu göstermez. Örneğin; $(111, 11, 1)$ – parametrelili bir projektif uzayında bu teoremi sağlanmasına rağmen bir fark kümesi teşkil etmez.

Fark kümelerinde öteleme; herhangi bir fark kümesinde grubun biriminden farklı seçeceğimiz eleman ile fark kümesinin elemanlarını işleme koyduğumuzda oluşacak olan yeni kümesinde fark kümesiyle aynı parametrelere sahip bir fark kümesi olduğu görülebilir (Moore ve Pollatsek, 2013).

Tanım 1.6.3. (Öteleme) $(G, +)$ grubunda D bir k elemanlı bir (v, k, λ) parametrelili bir fark kümesi ve $g \in G$ olsun. $g + D = \{g + d_1, g + d_2, g + d_3, \dots, g + d_k\}$ kümesi de bir (v, k, λ) parametrelili bir fark kümesidir. Bu oluşan fark kümesine D 'nin g ile ötelemesi denir.

Burada $g \in G$ olduğundan dolayı G grubunun birim elemanı haricinde $v - 1$ tane olup D fark kümesinin toplamda $v - 1$ tane ötelemesi mevcut olup D fark kümesi ile aynı parametrelere sahip olur (Lander, 1983).

Örnek 1.6.3. $(\mathbb{Z}_{11}, \oplus)$ grubunda $D = \{1, 3, 4, 5, 9\}$ alt kümesinin fark kümesi olduğu örnekten biliniyor. Şimdi ise bu fark kümesinin bir ötelemesini ele alalım. Örneğin; $g = 7$ için bakalım. $g = 7$ için ötelemesi $7 + D = \{7 + 1, 7 + 3, 7 + 4, 7 + 5, 7 + 9\} = \{0, 1, 5, 8, 10\}$ olur. Şimdi $7 + D$ kümesinin fark kümesi olduğunu tablo yöntemiyle gösterelim.

Tablo 2. $(\mathbb{Z}_{11}, \oplus)$ grubunda $D = \{0, 1, 5, 8, 10\}$ fark kümesi için çoklu küme tablosu.

$\mathbb{Z}_{11}/\{0\}$	$\lambda = 2$	
1	$1 - 0$	$4 - 3$
2	$10 - 8$	$1 - 10$
3	$8 - 5$	$0 - 8$
4	$5 - 1$	$1 - 8$
5	$10 - 5$	$5 - 0$
6	$5 - 10$	$0 - 5$
7	$8 - 1$	$1 - 5$
8	$8 - 0$	$5 - 8$
9	$10 - 1$	$8 - 10$
10	$0 - 1$	$10 - 0$

Tabloda görüldüğü üzere D 'nin ötelemesi olan $7 + D$ kümesi de yine bir $(11, 5, 2)$ parametrelili bir fark kümesidir.

Tanım 1.6.4. (*Açınım*) $(G, +)$ değişmeli grubunda $D \subset G$ bir fark kümesi olsun. Burada tekrarlanan yapının noktaları G kümesinin elemanları, bloklarını ise D fark kümesinin bütün ötelemeleri tarafından oluşuyorsa bu tekrarlanan yapıya D 'nin açınımı denir ve $\text{dev}D$ ile gösterilir (Lander, 1983).

Örnek 1.6.4. $(\mathbb{Z}_7, +)$ grubu ve fark kümesi olan $D = \{1, 2, 4\}$ alt kümesini ele alalım. $(\mathbb{Z}_7, +)$ grubunda $D = \{1, 2, 4\}$ alt kümesinin bir fark kümesi olduğu kolayca gösterilebilir. Şimdi burada tekrarlanan yapının noktalarını $\mathbb{Z}_7$ kümesinin elemanları ve $\forall a \in \mathbb{Z}_7$ için $a + D$ fark kümelerini de bu yapının blokları olarak kabul edelim. Yani bloklar kümesini $\mathcal{B}$ ile gösterirsek;

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

şeklinde oluşur. $\mathcal{B}$ kümesinden oluşan bu yapı D fark kümesinin bütün ötelemelerini içerdiğinden bir açınım teşkil eder.

Tanım 1.6.5. (*Tümleyen*) D_1 ve D_2 mertebesi v olan bir G grubunun ayırık iki farklı fark kümesi olsun. $D_1 \cup D_2 = G$ oluyorsa bu D_1 ve D_2 fark kümeleri birbirlerinin

tümleyeni olarak adlandırılır ve $D_1 = D_2^c$ veya $D_2 = D_1^c$ şeklinde gösterilir (Lander, 1953).

Burada D_1 ve D_2 fark kümelerinin parametreleri arasında ilişki vardır. D_1 fark kümesinin parametrelerini (v, k, λ) olarak kabul edersek tümleyeni olan D_2 fark kümesinin parametrelerini D_1 fark kümesinin parametrelerin cinsinden yazabiliriz. Kabul edelim ki D_2 fark kümesinin parametreleri (v', k', λ') olsun. D_2, G grubundan bir fark kümesi olduğundan $v' = v$ olur. Diğer taraftan $D_1 \cup D_2 = G$ ve D_1 fark kümesinin mertebesi k olduğundan $k' = v - k$ olduğu görülür. Teorem 1.6.1 bulunan $k(k-1) = \lambda(v-1)$ denklemi λ' için uyarlırsak,

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

olarak bulunur. O halde,

$$(v', k', \lambda') = (v, v-k, v-2k+\lambda).$$

Teorem 1.6.2. (Paley Fark Kümeleri) $p \in \mathbb{P}$ ve $m \in \mathbb{N}$ olmak üzere $p^m \equiv 3 \pmod{4}$ olacak şekilde bir asalın kuvveti ve $D, G = GF(p^m)$ cisminin toplam grubunda kuadratik rezidülerin sınıfı olsun. Bu durumda $D, \left(q, \frac{q-1}{2}, \frac{q-3}{4}\right)$ parametreleriyle bir fark kümesidir (Moore ve Pollatsek, 2013).

Örnek 1.6.5. (Fano Uzayı) $(\mathbb{Z}_7, +)$ grubunda $D = \{1, 2, 4\}$ alt kümesi bir $(7, 3, 1)$ parametrelili fark kümesi olduğunu biliyoruz. Bu fark kümesi bir Paley fark kümesidir. Çünkü $q = 7$ bir asal olup $(7, (7-1)/2, (7-3)/4) = (7, 3, 1)$ fark kümesidir.

Teorem 1.6.3. $p \in \mathbb{P}$ ve x tek tam sayı olmak üzere $p = 4x^2 + 1$ formunda bir asal sayı ve $G = \mathbb{Z}_p$ olsun. O halde G 'deki sıfırdan farklı tüm elemanların dördüncü kuvvetlerinin kümesi bir fark kümesidir (Lehmer, 1953).

Örnek 1.6.6. $x = 3$ olmak üzere $p = 4 \cdot 3^2 + 1 = 37$ formunda bir asal sayı olup $\mathbb{Z}_{37}$ grubunda 4. kuvvetlerinin oluşturduğu $D = \{1, 2, 7, 9, 10, 12, 16, 26, 33, 34\}$ sınıfı $(37, 9, 2)$ parametrelili bir fark kümesidir.

Teorem 1.6.4. $p \in \mathbb{P}$ ve x tek tam sayı olmak üzere $p = 4x^2 + 9$ formunda bir asal sayı ve $G = \mathbb{Z}_p$ olsun. O halde G 'deki tüm elemanların dördüncü kuvvetlerinin kümesi bir fark kümesidir (Lehmer, 1953).

Örnek 1.6.7. $x = 1$ olmak üzere $p = 4 \cdot 1^4 + 9 = 13$ formunda bir asal sayı olup $\mathbb{Z}_{13}$ grunuda dördüncü kuvvetlerin oluşturduğu $D = \{0, 1, 3, 9\}$ sınıfı $(13, 4, 1)$ parametrelili bir fark kümesidir.

Teorem 1.6.5. (*İkiz Asal Fark Kümeleri*) $p, (p + 2) \in \mathbb{P}$ olmak üzere $G = \mathbb{Z}_p \oplus \mathbb{Z}_{p+2}$ olsun. D kümesi G 'nin bir alt kümesi olmak üzere;

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

bu koşulları sağlayan $D_1, D_2, D_3 \subseteq G$ alt kümeleri ayık olup birleşimlerinden oluşan $D = D_1 \cup D_2 \cup D_3$ bir fark kümesi teşkil eder (Cunsheng Ding, 2014).

Örnek 1.6.8. 5 ile 7 ikiz asal olmak üzere Teorem 1.6.5'ya göre $G = \mathbb{Z}_5 \cup \mathbb{Z}_7$ üzerinde fark kümesi tanımlanabilir. Teoremin uygulanabilmesi için 5 ile 7 asal sayılarının kuadratik rezidülerin ve kuadratik non-rezidülerin kümeleri bulunması gerekmektedir. $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ kümesinde kuadratik rezidüler $\{1, 4\}$ kuadratik non-rezidüler $\{2, 3\}$. $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ kümesinde kuadratik rezidüler $\{1, 2, 4\}$ kuadratik non-rezidüler $\{3, 5, 6\}$ Teorem 1.6.5'den,

- i) $D_1 = \{(0,0), (1,0), (2,0), (3,0), (4,0)\}$
- ii) $D_2 = \{(1,1), (1,2), (1,4), (4,1), (4,2), (4,4)\}$
- iii) $D_3 = \{(2,3), (2,5), (2,6), (3,3), (3,5), (3,6)\}$

kümeleri elde edilir. O halde burada oluşan fark kümesi;

$$\begin{aligned} D &= D_1 \cup D_2 \cup D_3 \\ &= \{(0,0), (1,0), (2,0), (3,0), (4,0), (1,1), (1,2), (1,4), (4,1), (4,2), (4,4), (2,3), \\ &\quad (2,5), (2,6), (3,3), (3,5), (3,6)\}. \end{aligned}$$

Teorem 1.6.6. (*Hadamard Fark Kümeleri*) $t \in \mathbb{Z}^+$ olmak üzere mertebesi $v = 4t - 1$ olan devirli değişmeli gruplar üzerinde tanımlanmıştır. $t \in \{0, 1, \dots, v - 1\}$ olmak üzere $(v, k, \lambda) = (4t - 1, 2t - 1, t - 1)$ parametrelerine sahip fark kümesidir.

Teorem 1.6.7. (*McFarland Kümeleri*) $q \in \mathbb{P}$ olmak üzere $\mathbb{F} = GF(q)$ cismi üzerinde $s + 1$ boyutlu V vektör uzayı ile devirli ve değişmeli olmayan gruplar üzerinde fark kümesi oluşturmuştur. Parametreleri ise;

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

şekilindedir (Cunsheng Ding, 2014).

Tanım 1.6.6. (*Hemen Hemen Fark Kümesi*) $(G, +)$ mertebesi v olan toplamsal bir grup ve D, G 'nin k elemanlı bir alt kümesi olsun. G birim elemanı hariç t elemanı D kümesinin elemanlarının farkları tarafından λ kez temsil edilirken benzer şekilde birim ve t eleman haricinde $v - t - 1$ eleman $\lambda + 1$ kez temsil edilir. Buna göre D alt kümesi G grubu içerisinde (v, k, λ, t) parametrelili bir hemen hemen fark kümesidir (Moore ve Pollatsek, 2013).

Teorem 1.6.8. $(G, *)$ mertebesi v olan bir değişmeli grup ve D ise k elemanlı (v, k, λ, t) – hemen hemen fark kümesi olsun. Bu durumda;

$$k.(k - 1) = \lambda(v - 1) + t = (\lambda + 1)(v - 1) - t$$

eşitliği her zaman sağlanır (Moore ve Pollatsek, 2013).

İspat. $D, (v, k, \lambda, t)$ parametrelili bir hemen hemen fark kümesi olsun. Bu takdirde Δ çoklu kümesinde D 'nin k tane elemanı mevcut olduğundan $d_i, d_j \in D$ ve $d_i \neq d_j$ olmak üzere $d_i * d_j^{-1}$ şeklinde $k(k - 1)$ tane eleman bulunabileceğinden Δ çoklu kümesinin eleman sayısı $k(k - 1)$ olarak bulunur. Diğer taraftan D hemen hemen fark kümesi olduğundan G grubunun birim elemanı hariç $(v - 1 - t)$ elemanı λ kez diğer t elemanı ise $\lambda + 1$ kez görüneceğinden Δ kümesinin eleman sayısı $\lambda(v - 1 - t) + (\lambda + 1)t = \lambda(v - 1) + t = (\lambda + 1)(v - 1) - t$ olarak bulunur.

Örnek 1.6.9. $(\mathbb{Z}_{17}, \oplus)$ grubunda $D = \{1, 2, 4, 8, 9, 13, 15, 16\}$ alt kümesinin bir tablo yardımı ile hemen hemen fark kümesi olduğunu gösterelim.

Tablo 3. $(\mathbb{Z}_{17}, \oplus)$ grubunda $D = \{1, 2, 4, 8, 9, 13, 15, 16\}$ fark kümesi için çoklu küme tablosu.

$\mathbb{Z}_{17}/\{0\}$		$\lambda = 3$		$\lambda = 4$
1	2 – 1	9 – 8	16 – 15	-
2	4 – 2	15 – 13	1 – 16	-
3	4 – 1	16 – 13	1 – 15	2 – 16
4	8 – 4	13 – 3	2 – 15	-
5	9 – 4	1 – 13	4 – 16	13 – 8
6	8 – 2	2 – 13	4 – 15	15 – 9
7	9 – 2	8 – 1	15 – 8	16 – 9
8	9 – 1	8 – 16	16 – 8	-
9	13 – 4	1 – 9	4 – 13	-
10	1 – 8	2 – 9	8 – 15	9 – 16
11	2 – 8	9 – 15	13 – 2	15 – 4
12	4 – 9	8 – 13	13 – 1	16 – 8
13	4 – 8	9 – 13	15 – 2	-
14	1 – 4	13 – 16	15 – 1	16 – 2
15	16 – 1	2 – 4	13 – 15	-
16	1 – 2	8 – 9	15 – 16	-

Tabloda görüldüğü üzere Δ kümesi $(\mathbb{Z}_{17}, \oplus)$ grubundaki birim eleman haricinde 8 elemanını $\lambda = 3$ kez içerirken diğer 8 elemanı $\lambda + 1 = 4$ içerdiğinden D alt kümesi $(17, 8, 3, 8) -$ hemen hemen fark kümesi olur.

Tanım 1.6.7. (Hemen Hemen Fark Fonksiyonu) $(G, +)$ mertebesi v olan bir değişmeli grup ve D, G 'nin $(v, k, \lambda, t) -$ hemen hemen fark kümesi olsun. Bu takdirde hemen hemen fark fonksiyonu şu şekilde tanımlanır:

$$d_D(x) = |(D + x) \cap D| = \lambda \text{ veya } \lambda + 1$$

burada $x \in G / 0_G$ ve G 'nin birimden farklı t elemanı için λ değeri alırken $v - 1 - t$ elemanı içinse $\lambda + 1$ değerini alır (Cunsheng Ding, 2014).

Tanım 1.6.8. (Tümleyen) D_1 ve D_2 ayrık alt kümeleri mertebesi v olan G grubunda sırasıyla (v, k_1, λ_1, t) ve (v, k_2, λ_2, t) parametrelili iki hemen hemen fark kümeleri olsun. Eğer $D_1 \cup D_2 = G$ oluyorsa D_1 ve D_2 birinin tümleyenidir denir.

Fark kümelerinde de olduğu gibi birbirinin tümleyenini olan D_1 ve D_2 hemen hemen fark kümelerinin parametreleri birbirleri ile ilişkilidir. Yani $k_1 + k_2 = v$ olup $k_2 = v - k_1$ ve Teorem 1.6.1'e göre $\lambda_2 = v - 2k_1 + \lambda_1$ olarak bulunur (Lander, 1953).

Teorem 1.6.9. $(G, +)$ mertebesi v olan bir değişmeli grup ve $D, \left(v, \frac{v-1}{4}, \frac{v-5}{16}\right)$ parametrelili bir fark kümesi ve $d \in G/D$ olsun. Eğer $2d, D$ kümesinin iki farklı elemanın toplamı şeklinde yazılamıyorsa $D \cup \{d\}$ kümesi G 'de bir $\left(v, \frac{v+3}{4}, \frac{v-5}{16}, \frac{v-1}{2}\right)$ parametrelili bir hemen hemen fark kümesidir (Thomas R. Morrice, 2015).

Örnek 1.6.10. $(\mathbb{Z}_{21}, \oplus)$ grubunda $D = \{0, 1, 4, 14, 16\}$ alt kümesi $(21, 5, 1) -$ fark kümesidir. Burada $d = 3 \in G/D$ için $2d = 2.3 = 6$ sayısı D kümesinin keyfi iki elemanın toplamı olarak yazılmaz. Bu nedenle Teorem 1.6.9 gereği $D \cup \{3\} = \{0, 1, 3, 4, 14, 16\}$ kümesi bir $(21, 6, 1, 10) -$ hemen hemen fark kümesi olur.

Teorem 1.6.10. $(G, +)$ mertebesi v olan bir değişmeli grup ve $D, \left(v, \frac{v+3}{4}, \frac{v+3}{16}\right)$ parametrelili bir fark kümesi ve $d \in D$ olsun. Eğer $2d, D$ kümesinin iki farklı elemanın toplamı şeklinde yazılamıyorsa $D / \{d\}$ kümesi G 'de bir $\left(v, \frac{v-1}{4}, \frac{v-13}{16}, \frac{v-1}{2}\right)$ parametrelili bir hemen hemen fark kümesidir (Thomas R. Morrice, 2015).

Örnek 1.6.11. $(\mathbb{Z}_{13}, \oplus)$ grubunda $D = \{0, 1, 4, 9\}$ alt kümesi $(13, 4, 1) -$ fark kümesidir. Burada $d = 0 \in D$ için $2d = 2.0 = 0$ sayısı D kümesinin keyfi iki elemanın toplamı olarak yazılamaz. Bu nedenle Teorem 1.6.10'den dolayı $D / \{0\} = \{1, 4, 9\}$ alt kümesi G 'de bir $(13, 3, 0, 6) -$ hemen hemen fark kümesidir.

Tanım 1.6.9. (*Kısmi Fark Kümesi*) G mertebesi v olan bir grup, bu grubun k elemanlı bir D alt kümesi olsun. D kümesinin elemanlarını Δ çoklu kümesi λ kez içeriyorken G / D kümesinin elemanları μ kez içeriyorsa bu yapıya $(v, k, \lambda, \mu) -$ kısmi fark kümesi denir.

Özel olarak $\mu = \lambda$ ise D bir fark kümesi, $\mu = \lambda + 1$ olursa D bir hemen hemen fark kümesi olur (Cunsheng Ding, 2014).

Örnek 1.6.12. $(\mathbb{Z}_{13}, \oplus)$ grubunda $D = \{1, 3, 4, 9, 10, 12\}$ alt kümesinin $(13, 6, 2, 3) -$ parametrelili kısmi fark kümesi olduğunu gösterelim.

Tablo 4. $(\mathbb{Z}_{13}, \oplus)$ grubunda $D = \{1, 3, 4, 9, 10, 12\}$ fark kümesi için çoklu küme tablosu.

$\mathbb{Z}_{13}/\{0\}$	$\lambda = 2$	$\mu = 3$
1	4 – 3	10 – 9
2	3 – 1	12 – 10
3	4 – 1	12 – 9
4	1 – 10	3 – 12
5	1 – 9	4 – 12
6	9 – 3	3 – 10
7	3 – 9	4 – 10
8	9 – 1	4 – 9
9	10 – 1	12 – 3
10	1 – 4	9 – 12
11	1 – 3	10 – 12
12	3 – 4	9 – 10

Tabloda görüldüğü üzere $(\mathbb{Z}_{13}, \oplus)$ grubunda $D = \{1, 3, 4, 9, 10, 12\}$ alt kümesi $(13, 6, 2, 3) -$ kısmi fark kümesidir. Ayrıca bu yapı $\mu = \lambda + 1$ olup tabloda da görüldüğü üzere $(13, 9, 2, 6) -$ hemen hemen fark kümesidir.

1.7 Döngüsel Sınıflar İle Elde Edilen Fark Kümeleri ve Hemen Hemen Fark Kümeleri

Teorem 1.7.1. (*Lehmer Teoremi*) $q \in \mathbb{P}$ olmak üzere $q = ef + 1$ formunda bir asal sayı ve g ise $GF(q)$ cisminin bir ilkel kök olsun. Bu takdirde C_0 döngüsel sınıfı, $(q, (f-1), (f-1)/e)$ parametrelerine sahip $GF(q)$ 'da bir fark kümesidir ancak ve ancak

$$\lambda = (i, 0) = (f-1)/e$$

burada $i = 0, \dots, e-1$ şeklindedir (Lehmer, 1965).

İspat. $D = C_0$ bir fark kümesi ise Teorem 1.4.1'de $v-1 = q-1 = ef$ ve $k = f$ $f(f-1) = (q-1)\lambda = (f-1)/e = \lambda$ olarak bulunur. $a \in C_i$ olsun. Bu durumda $a^{-1} \in C_{e-i}$ olduğu açıktır. Fark fonksiyonunu tanımlayalım;

$$\begin{aligned} d_D(a) &= |(C_0 + a) \cap C_0| = \lambda \\ &= |(a^{-1}C_0 + a.a^{-1}) \cap a^{-1}C_0| = \lambda \\ &= |(a^{-1}C_0 + 1) \cap a^{-1}C_0| = \lambda \\ &= |(C_{e-i} + 1) \cap C_{e-i}| = \lambda. \end{aligned}$$

Tanım 1.4.1. gereği aşağıdaki ifade elde edilir

$$= (e-i, e-i) = \lambda$$

Teorem 1.4.1'den ise,

$$= (i, 0) = \lambda$$

elde edilir. Son olarak $\lambda = (i, 0) : i = 0, \dots, e-1$ ise Teorem 1.4.3'e göre,

$$e\lambda = \sum_{i=0}^{e-1} (i, 0) = f-1$$

olup $(f-1)/e = (i, 0) = \lambda$ istenen elde edilir.

Teorem 1.7.2. $q \in \mathbb{P}$ olmak üzere $q = ef + 1$ formunda bir asal sayı ve g ise $GF(q)$ cisminin bir ilkel kök olsun. Bu takdirde;

$C_0^2 \cup \{0\}$ döngüsel sınıfı, $GF(p)$ 'da $(q, (f+1), (f+1)/e)$ parametrelili bir fark kümesidir ancak ve ancak

$$1 + (0, 0) = (i, 0) = (f+1)/e,$$

burada $i = 0, \dots, e-1$.

İspat: Teorem 1.7.1 ispatı ile benzer şekilde yapılır (Lehmer, 1965).

Teorem 1.7.3. Aşağıdakiler $(GF(r), +)$ cismi üzerinde döngüsel fark kümesi listesidir.

i. C_0^2 döngüsel sınıfı, $\left(r, \frac{r-1}{2}, \frac{r-3}{4}\right)$ parametreleri ile bir fark kümesidir.

Burada $r \equiv 3 \pmod{4}$ formundadır (Cunsheng Ding, 2014).

ii. C_4^2 döngüsel sınıfı, $\left(r, \frac{r-1}{4}, \frac{r-5}{16}\right)$ parametreleri ile bir fark kümesidir.

Burada $r = 4t^2 + 1$ ve t tek sayı formundadır (Cunsheng Ding, 2014).

iii. $C_4^2 \cup \{0\}$ döngüsel sınıfı, $\left(r, \frac{r+3}{4}, \frac{r+3}{16}\right)$ parametreleri ile bir fark kümesidir.

Burada $r = 4t^2 + 9$ ve t tek sayı formundadır (Cunsheng Ding, 2014).

iv. C_8^2 döngüsel sınıfı, $\left(r, \frac{r-1}{8}, \frac{r-9}{64}\right)$ parametreleri ile bir fark kümesidir.

Burada $r = 8t^2 + 1 = 64u^2 + 9$, u ve t tek sayı formundadır (Cunsheng Ding, 2014).

v. $C_8^2 \cup \{0\}$ döngüsel sınıfı, $\left(r, \frac{r+7}{8}, \frac{r+7}{64}\right)$ parametreleri ile bir fark kümesidir.

Burada $r = 9t^2 + 49 = 64u^2 + 441$, u ve t tek sayı formundadır (C. Ding, 2014).

Örnek 1.7.1. $r = 7$ olsun. Bu durumda,

$C_0^2 = \{1, 2, 4\}$ sınıfı $(\mathbb{Z}_7, \oplus)$ 'de $(7, 3, 1)$ – fark kümesidir.

Örnek 1.7.2. $r = 37$ olsun. Bu durumda,

$C_0^4 = \{1, 7, 9, 10, 12, 16, 26, 33, 34\}$ sınıfı $(\mathbb{Z}_{37}, \oplus)$ 'de $(37, 9, 2)$ – fark kümesidir.

Örnek 1.7.3. $r = 13$ olsun. Bu durumda,

$C_0^8 \cup \{0\} = \{0, 1, 3, 9\}$ sınıfı $(\mathbb{Z}_{13}, \oplus)$ 'de $(13, 4, 1)$ – fark kümesidir.

Örnek 1.7.4. $r = 73$ olsun. Bu durumda,

$C_0^8 = \{1, 2, 4, 8, 16, 32, 37, 55, 64\}$ sınıfı $(\mathbb{Z}_{73}, \oplus)$ 'de $(73, 9, 1)$ – fark kümesidir.

Teorem 1.7.4. $C_0^6 \cup C_1^6 \cup C_3^6$ döngüsel sınıfı, $(GF(r), +)$ cismi üzerinde $\left(r, \frac{r-1}{2}, \frac{r-3}{4}\right)$ parametreleriyle bir fark kümesidir. Burada $r = 4t^2 + 27$ ve $(3, t)_{ebob} = 1$ formundadır (Cunsheng Ding, 2014).

Örnek 1.7.5. $r = 31 = 4 \cdot 1^2 + 27$ ve ilkel kökü $g = 3$ olsun. Bu durumda;

$$D = C_0^6 \cup C_1^6 \cup C_3^6 = \{1, 2, 3, 4, 5, 6, 8, 12, 15, 16, 17, 23, 24, 27, 29, 30\}$$

$(\mathbb{Z}_{31}, \oplus)$ 'de $(31, 15, 7)$ – fark kümesidir.

Teorem 1.4.5. Varsayalım $l = t^2 + 2 \equiv 3 \pmod{8}$ bir asal sayının kuvveti ve $q = l^2$ olsun. Burada $t \in \mathbb{Z}$ olmak üzere,

$$D = C_0^8 \cup C_1^8 \cup C_2^8 \cup C_5^8$$

kümesi $(GF(r), +)$ cismi üzerinde $\left(r, \frac{r-1}{2}, \frac{r-5}{4}, \frac{r-1}{2}\right)$ parametreleriyle bir hemen hemen fark kümesidir (Cunsheng Ding, 2012).

Bu yapının, bu parametrelerle sonsuz sayıda hemen hemen fark kümesi oluşturabildiğini açıkça görülür. Örneğin $q = 3^2, 11^2, 3^6, 83^2, 227^2, \dots$ bu teoremi ispat etmek için 8.mertebeden döngüsel sayıları kullanacağız. 64 döngüsel sayı (j, k) , belirli bir $q = 8f + 1$ için en fazla 15 değere sahiptir. Bu değerler q, x, y, a ve b cinsinden ifade edilebilir

$$q = x^2 + 4y^2 = a^2 + b^2, x \equiv a \equiv 1 \pmod{4}.$$

Burada $q \equiv 1 \pmod{16}$ ve $q \equiv 9 \pmod{16}$ olmak üzere iki durum mevcuttur. Bu iki durum için de döngüsel sayılar ve 15 temel sabit arasındaki ilişkiler hesaplanır. Teorem için biz sadece ikinci durumu yani $q \equiv 9 \pmod{16}$ denkleğini ele alacağız ve döngüsel sayılar ve 15 temel sabitler arasında olan ilişki için ise aşağıda vereceğimiz Tablo 1.5 ve Tablo 1.6 kullanılmıştır.

Tablo 5. $q \equiv 9 \pmod{16}$ olduğunda 8.mertebedeki döngüsel sayıların ilişkileri

(j, k)	0	1	2	3	4	5	6	7
0	(0, 0)	(0, 1)	(0, 2)	(0, 3)	(0, 4)	(0, 5)	(0, 6)	(0, 7)
1	(1, 0)	(1, 1)	(1, 2)	(1, 3)	(0, 5)	(1, 3)	(1, 3)	(1, 7)
2	(2, 0)	(2, 1)	(2, 0)	(1, 7)	(0, 6)	(1, 3)	(0, 2)	(1, 2)
3	(1, 1)	(2, 1)	(2, 1)	(1, 0)	(0, 7)	(1, 7)	(1, 2)	(0, 1)
4	(0, 0)	(1, 0)	(2, 0)	(1, 1)	(0, 0)	(1, 0)	(2, 0)	(1, 1)
5	(1, 0)	(0, 7)	(1, 7)	(1, 2)	(0, 1)	(1, 1)	(2, 1)	(2, 1)
6	(2, 0)	(1, 7)	(0, 6)	(1, 3)	(0, 2)	(1, 2)	(2, 0)	(2, 1)
7	(1, 1)	(1, 2)	(1, 3)	(0, 5)	(0, 3)	(1, 3)	(1, 7)	(1, 0)

Teoremi ispatlamak için aşağıdaki lemmalardan faydalanılmıştır.

Lemma 1.4.1. $e = 8$ olduğunda, $64(j, k)$ döngüsel sayısının $q = p^m = x^2 + 4y^2 = a^2 + b^2$ fonksiyonun tek gösterimi aşağıda belirtilmiştir.

(i) Eğer $p \equiv 1 \pmod{4}$ ise $q = x^2 + 4y^2$, $x \equiv 1 \pmod{4}$ p^m nin tek gösterimidir.

Aksi halde,

$q = (\pm p^{m/2})^2 + 4 \cdot 0^2$, başka bir deyişle $x = \pm p^{m/2}$, $y = 0$.

Tablo 6. $q \equiv 9 \pmod{16}$ iken 8. mertebeden döngüsel sayılar

	2 kuadratik rezidü ise	2 non-kuadratik rezidü ise
64(0, 0)	$q - 15 - 2x$	$q - 15 - 10x - 8a$
64(0, 1)	$q + 1 + 2x - 4a - 16y$	$q + 1 + 2x - 4a - 16b$
64(0, 2)	$q + 1 + 6x + 8a - 16y$	$q + 1 - 2x + 16y$
64(0, 3)	$q + 1 + 2x - 4a - 16y$	$q + 1 + 2x - 4a - 16b$
64(0, 4)	$q + 1 - 18x$	$q + 1 + 6x + 24a$
64(0, 5)	$q + 1 + 2x - 4a + 16y$	$q + 1 + 2x - 4a + 16b$
64(0, 6)	$q + 1 + 6x + 8a + 16y$	$q + 1 - 2x - 16y$
64(0, 7)	$q + 1 + 2x - 4a - 16y$	$q + 1 + 2x - 4a + 16b$
64(1, 0)	$q - 7 + 2x + 4a$	$q - 7 + 2x + 4a + 16y$
64(1, 1)	$q - 7 + 2x + 4a$	$q - 7 + 2x + 4a - 16y$
64(1, 2)	$q + 1 - 6x + 4a + 16b$	$q + 1 + 2x - 4a$
64(1, 3)	$q + 1 + 2x - 4a$	$q + 1 - 6x + 4a$
64(1, 7)	$q + 1 - 6x + 4a - 16b$	$q + 1 + 2x - 4a$
64(2, 0)	$q - 7 - 2x - 8a$	$q - 7 + 6x$
64(2, 1)	$q + 1 + 2x - 4a$	$q + 1 - 6x + 4a$

(ii) Eğer $p \equiv 1 \pmod{8}$ veya $p \equiv 3 \pmod{8}$ ise $q = a + 4b^2$, $a \equiv 1 \pmod{4}$ p^m 'nin tek gösterimidir. Aksi halde,

$q = (\pm p^{m/2})^2 + 2 \cdot 0^2$, başka bir deyişle $a = \pm p^{m/2}$, $b = 0$. Burada y ve b 'de işaret belirsizliği mevcuttur.

Lemma 1.4.2. $p \equiv 3 \pmod{8}$ ve m çift olsun. Burada $q = p^m$ olmak üzere $GF(q)$ da 2 kuadratik rezidüdür.

İspat. Genelliği bozmadan θ , $GF(q)^*$ cisminin primitif kökü kabul edelim. Bu takdirde $\alpha = \frac{p^{m-1}}{\theta^{p-1}}$, $GF(q)^*$ da bir primitif köktür. $p \equiv 3 \pmod{8}$ olduğundan, $GF(p)$ 'de 2 bir kuadratik rezidü olmayıp 2'nin logaritmasını $GF(p)$ 'de r ile ifade ettiğimiz bir tek sayıdır. O halde $GF(q)$ 'da 2'nin logaritması $\frac{p^{m-1}}{p-1}r$ formunda olup burada $\frac{p^{m-1}}{p-1} \equiv 0 \pmod{4}$ olduğunu göstermek yeterlidir. $\frac{p^{m-1}}{p-1} \equiv 0 \pmod{4}$ olduğu ise tanım gereği açıktır.

Şimdi teoremi ispatlayalım.

$j = 0, 1, \dots, 7$ için;

$$\begin{aligned}
\Delta_j &= |(D + \theta^j) \cap D| \\
&= ((C_0 \cap C_1 \cap C_2 \cap C_5) + \theta^j) \cap (C_0 \cap C_1 \cap C_2 \cap C_5) \\
&= |((C_0 \cap C_1 \cap C_2 \cap C_5) + \theta^j) \cap (C_0 \cap C_1 \cap C_2 \cap C_5)| \\
&= |(C_0 + \theta^j) \cap C_0| + |(C_0 + \theta^j) \cap C_1| + |(C_0 + \theta^j) \cap C_2| \\
&\quad + |(C_0 + \theta^j) \cap C_5| \\
&\quad + |(C_1 + \theta^j) \cap C_0| + |(C_1 + \theta^j) \cap C_1| + |(C_1 + \theta^j) \cap C_2| + |(C_1 + \theta^j) \cap C_5| \\
&\quad + |(C_2 + \theta^j) \cap C_0| + |(C_2 + \theta^j) \cap C_1| + |(C_2 + \theta^j) \cap C_2| + |(C_2 + \theta^j) \cap C_5| \\
&\quad + |(C_5 + \theta^j) \cap C_0| + |(C_5 + \theta^j) \cap C_1| + |(C_5 + \theta^j) \cap C_2| + |(C_5 + \theta^j) \cap C_5| \\
&= (-j, -j) + (-j, 1-j) + (-j, 2-j) + (-j, 5-j) + (1-j, -j) + (1-j, 1-j) \\
&\quad + (1-j, 2-j) + (1-j, 5-j) + (2-j, -j) + (2-j, 1-j) + (2-j, 2-j) \\
&\quad + (2-j, 5-j) + (5-j, -j) + (5-j, 1-j) + (5-j, 2-j) + (5-j, 5-j) \\
l &\equiv 3 \pmod{8} \text{ olduğundan dolayı ikinci duruma yani } q \equiv 9 \pmod{16} \text{ denklemi elde} \\
&\text{edilir. O halde Tablo 1.6'da bulunan döngüsel sayılar ve Tablo 1.5'deki 8. mertebedeki} \\
&\text{döngüsel sayılar arasındaki ilişki kurulabilir. Buradan } p, \text{ bazı } t \text{ tam sayıları için} \\
&t^2 + 2 \text{ formunda bir asalın kuvveti ve bununla birlikte } p \equiv 3 \pmod{8} \text{ ve } r \text{ tek olmak} \\
&\text{üzere } l = p^m \text{ formundadır. Böylece aşağıdaki denklemlere ulaşılır.}
\end{aligned}$$

$$\Delta_0 = \Delta_4 = \frac{16q - 48 + 8x - 8a - 48y}{64}$$

$$\Delta_1 = \Delta_5 = \frac{16q - 80 - 16x + 16a - 32y}{64}$$

$$\Delta_2 = \Delta_6 = \frac{16q - 48 + 8x - 8a - 16y}{64}$$

$$\Delta_3 = \Delta_7 = \frac{16q - 16}{64}.$$

Lemma 1.4.1'e göre $x = -l, y = 0, a = -l + 4$ ve $b = \pm 2t$ olduğu görülür.

Yukarıda yer alan $\Delta_0, \Delta_1, \Delta_2, \Delta_3, \Delta_4, \Delta_5, \Delta_6, \Delta_7$ ifadelerinde yerine yazılırsa;

$$\Delta_0 = \Delta_2 = \Delta_4 = \Delta_6 = \frac{q - 5}{4}$$

$$\Delta_1 = \Delta_3 = \Delta_5 = \Delta_7 = \frac{q - 1}{4}$$

olur. Böylece D kümesi $(GF(q), +)$ cismi üzerinde $(q, \frac{(q-1)}{2}, \frac{(q-5)}{4}, \frac{(q-1)}{2})$

parametrelili bir hemen hemen fark kümesidir.

Örnek 1.7.6. $(\mathbb{Z}_9, \oplus)$ grubunda $D = \{1, 2, 4, 5\}$ alt kümesinin hemen hemen fark kümesi olduğunu gösterelim.

Tablo 7. $(\mathbb{Z}_9, \oplus)$ grubunda $D = \{1, 2, 4, 5\}$ fark kümesi için çoklu küme tablosu.

$\mathbb{Z}_9/\{0\}$	$\lambda = 1$	$\lambda + 1 = 2$
1	5 - 4	2 - 1
2	4 - 2	—
3	5 - 2	4 - 1
4	5 - 1	—
5	1 - 5	—
6	2 - 5	1 - 4
7	2 - 4	—
8	4 - 5	1 - 2

Tabloda görüldüğü üzere $(\mathbb{Z}_9, \oplus)$ grubunda $D = \{1, 2, 4, 5\}$ alt kümesi $(9, 4, 1, 4) -$ hemen hemen fark kümesidir.

2.YAPILAN ÇALIŞMALAR

Bu çalışma da döngüsel sayılar, döngüsel sınıflar ve fark kümelerinin tanımları ve teoremleri verilmiş ve döngüsel sınıflar ile fark kümelerinin arasındaki bağlantı ele alınmıştır. Ayrıca bazı döngüsel sayılardan elde edilen sınıflar verilmiş olup MATLAB programlama dilinde döngüsel sınıfın elemanlarından oluşan kümelerin tekrarlama matrisi oluşturularak uygun koşullar altında uygun parametrelili fark kümesi olduğunu gösteren bir kod çalışması yapılmıştır.

Döngüsel sınıfları elde etmek için üzerinde çalışılan sınıfın ilkel köküne ihtiyaç duyulduğundan ilk olarak ilkel kökün elde edilmesine yönelik kod yazılmıştır. Sonrasında ise MATLAB uygulaması üzerinden özel olarak ele almış olduğumuz uygun koşulları sağlayan kuadratik rezidülerden elde edilen sınıfı, C_0^2 döngüsel sınıfı, C_4^2 döngüsel sınıfı, $C_4^2 \cup \{0\}$ döngüsel sınıfı, C_8^2 döngüsel sınıfı ve $C_0^6 \cup C_1^6 \cup C_3^6$ sınıfları elde edilmiştir. Fark kümesi olabilmesi için bu sınıflarda yer alan elemanların birbirlerinin farklarına bakılarak matris oluşturulmuş ve bu farklarının kaç defa tekrarlandığı ele alınmıştır. Bu farklardan oluşan elemanların tekrarlanma sayısına göre ise fark kümesi olup olmadığı incelenmiştir.

2.1. Kuadratik Rezidülerden Elde Edilen Fark Kümeleri için MATLAB Uygulaması

Burada MATLAB programlama dili üzerinde $GF(q)$ cismi üzerinde kuadratik rezidülerinden elde edilen sınıfın $(r, \frac{r-1}{2}, \frac{r-3}{4})$ parametrelili fark kümesi teşkil edip etmediği kontrol edilmiştir.

```
% Fark Kümeleri
%Burada ele alacağımız kalan sınıflarının kümesi içinde kuadratik
rezidü sınıflarının fark kümesi olup olmadığını göstereceğiz.
%Yasin YILMAZ...

x =59 ; %G grubunu mertebesi
list = []; %Kuadratik rezidü için oluşturduğumuz Sınıf...

% Fark kümesi için bir D sınıfı oluşturuyoruz.

for i=1:((x-1)/2)
    list(i) = mod(i^2,x);%Kuadratik rezidü sınıfını oluşturuyoruz.
end

% Fark Kümesi olması durumunda D sınıfında elde edilen fark kümesi
için Lamda elde ediyoruz.

k = length(list); %Elde etmiş olduğumuz rezidüler sınıfı ile
Lamda = (k*(k-1))/(x-1); %Parametreleri oluşturuyoruz.
Lamda

%D sınıfının elemanların birbirlerinden farkını alarak matris elde
%ediyoruz.

for i=1:k
    for j=1:k
        matris(i,j) = mod(list(i)-list(j),x);
    end
end

matris

% D sınıfında kalan sınıfını hangi elemanı tekrar ettiğini daha
rahat görebilmek adına matrisi vektör haline getiriyoruz.

sayac=0;
```

Şekil 3. Kuadratik Rezidülerden Elde Edilen Fark Kümeleri için MATLAB Uygulaması

```

for i=1:k
    for j=1:k
        sayac=sayac+1;
        vektor(sayac)=matris(i,j);
    end
end

as_vektor=sort(vektor);

matris;

%Vektörde birim elemanı hariç diğer tüm kalan sınıfının diğer
elemanların kaç defa tekrarlandığını sayıyoruz. Başka bir deyişle
çoklu kümeyi oluşturuyoruz.

for i=1:x-1
    saycheck=0;
    for j=1:sayac
        if i==as_vektor(j)
            saycheck=saycheck+1;
        end
    end

    diffcheck(i)=saycheck;

end

%Tekrarlanan elemanların sayısı aynı olup olmaması durumuna göre
fark kümesi teşkil edip etmediğini kontrol ediyoruz.

u = sort(diffcheck)

farkcheck=0;

for i=2:x-1
    if diffcheck(i)~=diffcheck(i-1)
        fprintf('fark kümesi değildir')
        farkcheck=1;
        break
    end
end

if farkcheck==0
    fprintf('(%d , %d , %d) parametrelili fark kümesidir',x,Lamda,k)
end

```

Şekil 3 (Devam). Kuadratik Rezidülerden Elde Edilen Fark Kümeleri için MATLAB Uygulaması

Tablo 8. Kuadratik Rezidü Programın Çalışma Süreleri

Kuadratik Rezidülerden Elde Edilen Fark Kümeleri İçin Programın Çalışma Süreleri	
(v, k, l)	Programın Çalışma Süresi
(11,2,5)	0.001086
(19,4,9)	0.007533
(23,5,11)	0.007545
(31,7,11)	0.026996
(43,10,21)	0.012141
(47,11,23)	0.016246
(59,14,29)	0.0146884

2.2. İlkel Kök Elde Eden MATLAB Uygulaması

Döngüsel sınıfları elde etmek için ilkel köke ihtiyaç duyuyoruz. Burada mertebesi asal veya asalın bir kuvveti olan sayılar için ilkel kök hesaplıyoruz.

```
% GF(q) cismi için ilkel kök
% Burada herhangi bir cisim için ilkel kök elde edeceğiz.
% Yasin YILMAZ...

G = 61; % G burada ilkel kökünü bulacağımız cismin mertebesi...
say=0;

for k = 1:(G-1)
    for i = 1:(G-1)
        s=sym(k); % Matlab büyük sayıları double cinsine çeviriyor.
        yani yaklaşık olarak 16 digit.16 digitten büyük çıkan sayıları
        Matlab yorumlamakta yetersiz kalıyor.
        list(i) = mod(s^i,G);
    end

    kok=sort(list);
    if kok == (1:(G-1))
        fprintf('%d ilkel köktür\n ',k)
        say=say+1;
    end
end
```

Şekil 4. İlkel Kök Elde Eden MATLAB Uygulaması

Tablo 9. Bazı Sonlu Cisimlerin Üreteçleri Bulduran Programın Çalışma Süreleri

Cismin Mertebesi	Bazı Üreteçleri	Çalışma Süreleri
$GF = 7$	$g = 3, 5$	2.286035
$GF = 11$	$g = 2, 6, 7, 8$	2.641429
$GF = 13$	$g = 2, 6, 7, 11$	2.671315
$GF = 17$	$g = 3, 5, 6, 7, 10, 11, 12, 14$	2.944777
$GF = 19$	$g = 2, 3, 10, 13, 14, 15$	3.411356
$GF = 23$	$g = 5, 7, 10, 11, 14, 15, 17, 19, 20, 21$	4.166111
$GF = 29$	$g = 2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26$	5.781075
$GF = 31$	$g = 3, 11, 12, 13, 17, 21, 22, 24$	6.212491
$GF = 41$	$g = 6, 7, 11, 12, 13, 15, 17, 19, 22, 24$	9.468939
$GF = 43$	$g = 3, 5, 12, 18, 19, 20, 26, 28, 30, 33$	10.288304
$GF = 47$	$g = 5, 10, 11, 13, 15, 19, 20, 22, 23, 26$	11.843020
$GF = 53$	$g = 2, 3, 5, 8, 12, 14, 18, 19, 20, 21, 22$	14.059225
$GF = 59$	$g = 2, 6, 8, 10, 11, 13, 14, 18, 23, 24, 30$	17.466538
$GF = 61$	$g = 2, 6, 7, 10, 17, 18, 26, 30, 31, 35, 43$	17.632158
$GF = 67$	$g = 2, 7, 11, 13, 18, 20, 28, 31, 32, 34,$	20.986326
$GF = 71$	$g = 7, 11, 13, 21, 22, 28, 31, 33, 35, 42$	23.315177
$GF = 73$	$g = 5, 11, 13, 14, 15, 20, 26, 28, 29, 31$	24.783640
$GF = 79$	$g = 3, 6, 7, 28, 29, 30, 34, 35, 37, 39$	28.457946
$GF = 83$	$g = 2, 5, 6, 8, 13, 14, 15, 18, 19, 20, 22$	32.704982
$GF = 89$	$g = 3, 6, 7, 13, 14, 15, 19, 23, 24, 26$	37.505741
$GF = 97$	$g = 5, 7, 10, 13, 14, 15, 17, 21, 23, 26$	42.518980
$GF = 101$	$g = 2, 3, 7, 8, 11, 12, 15, 18, 26, 27, 28$	46.424824
$GF = 103$	$g = 5, 6, 11, 12, 20, 21, 35, 40, 43, 44$	46.525955

Yukarıda verilen cisimlerin bazı üreteçleri ve çalışma süreleri saniye olarak ele alınmıştır. Cismin mertebesi arttıkça istisnai durumlar hariç genel olarak üreteç sayıları artmaktadır. Bu nedenle programdan elde edilen bazı üreteçlere tabloda yer verilmiştir. Bu üreteçler yukarıda yer alan kod çalışmasından elde edilmiştir.

2.3. C_0^2 Döngüsel Sınıf ile Elde Edilen Fark Kümesinin MATLAB Uygulaması

C_0^2 döngüsel sınıfı, $\left(r, \frac{r-1}{2}, \frac{r-3}{4}\right)$ parametreleri ile bir fark kümesidir.

Burada $r \equiv 3 \pmod{4}$ formundadır. İlk olarak $p \equiv 3 \pmod{4}$ formunda olan asal sayıları bulalım.

```
% Asal Sayılar
%3 = mod4 formunda olan asal sayıları elde ediyoruz.
%Yasin YILMAZ

a = primes(100);
b = length(a);

for i=1:b
    if mod(a(i),4)==3
        fprintf('%d ',a(i))
    end
end
```

Şekil 5. C_0^2 Döngüsel Sınıf ile Elde Edilen Fark Kümesi İçin Uygun Parametrelerin MATLAB Uygulaması

Şimdi elde etmiş olduğumuz p asal sayıları için $GF(p)$ cismi üzerinde C_0^2 döngüsel sınıfının fark kümesi olduğunu gösterelim.

```
% Fark Kümeleri
%Burada C0 döngüsel sınıfı ile elde edilen sınıftan (r, (r-1)/2,
(r-3)/4) parametrelili fark kümesi olduğunu gösteriyoruz.
%Yasin YILMAZ...

g = 2; %Grubun ilkel kökünü giriyoruz.
r = 59; %Grubun mertebesini giriyoruz.
% r = e.f+1 formundaki asal sayısı için e = 2 döngüsel sınıfını elde
edeceğiz.

e = 2; %Döngüsel sınıfın mertebesi
f = (r-1)/2;
for i=1:f
    s = sym(g);
    C0(i) = mod(s^((e*(i-1))+0),r);
end
```

Şekil 6. C_0^2 Döngüsel Sınıf ile Elde Edilen Fark Kümesinin MATLAB Uygulaması

```

% Fark Kümesi olması durumunda C0 döngüsel sınıfından elde edilen
fark kümesi için Lamda elde ediyoruz.

k = length(C0);
Lamda = (k*(k-1))/(r-1);
Lamda
k

%C0 sınıfının elemanların birbirlerinden farkını alarak matris elde
%ediyoruz.

for i=1:k
    for j=1:k
        matris(i,j) = mod(C0(i)-C0(j),r);
    end
end

% C0 sınıfında kalan sınıfını hangi elemanı tekrar ettiğini daha
rahat
% görebilmek adına matrisi vektör haline getiriyoruz.

sayac=0;

for i=1:k
    for j=1:k
        sayac=sayac+1;
        vektor(sayac)=matris(i,j);
    end
end

as_vektor=sort(vektor);

%Vektörde birim elemanı hariç kalan sınıfındaki diğer elemanların
kaç defa tekrarlandığını sayıyoruz.

for i=1:r-1
    saycheck=0;

    for j=1:sayac
        if i==as_vektor(j)
            saycheck=saycheck+1;
        end
    end

    diffcheck(i)=saycheck;
end

```

Şekil 6(Devam). C_0^2 Döngüsel Sınıf ile Elde Edilen Fark Kümesinin MATLAB Uygulaması

```

%Tekrarlanan elemanların sayısı aynı olup olmaması durumuna göre
fark
%kümesi teşkil edip etmediğini kontrol ediyoruz.

for i=2:r-1

farkcheck=0;

if diffcheck(i)~=diffcheck(i-1)
    fprintf('fark kümesi değildir')
    farkcheck=1;
    break
end

end

if farkcheck==0
    fprintf('C0 döngüsel sınıfı (%d , %d , %d) parametrelili fark
    kümesidir',r,k,Lamda)
end

```

Şekil 6(Devam). C_0^2 Döngüsel Sınıf ile Elde Edilen Fark Kümesinin MATLAB Uygulaması

Tablo 10. C_0^2 Sınıfından Elde Edilen Fark Kümesi Programının Çalışma Süreleri

C_0^2 Sınıfından Elde Edilen Fark Kümesi Programının Çalışma Süreleri		
(v, k, l)	Üreteç	Programın Çalışma Süresi
(11,5,2)	$g = 2$	1.243149
(19,9,4)	$g = 2$	5.108764
(23,11,5)	$g = 5$	9.331579
(31,15,7)	$g = 3$	21.994241
(43,15,7)	$g = 3$	60.475515
(59,29,14)	$g = 2$	164.789183
(67,33,16)	$g = 2$	249.156928
(83,41,20)	$g = 2$	492.955801
(107,53,26)	$g = 2$	1089.295520

2.4. C_4^2 Döngüsel Sınıf ile Elde Edilen Fark Kümesinin MATLAB Uygulaması

C_4^2 döngüsel sınıfı, $\left(r, \frac{r-1}{4}, \frac{r-5}{16}\right)$ parametreleri ile bir fark kümesidir.

Burada $r = 4t^2 + 1$ ve t tek sayı formundadır. İlk olarak $r = 4t^2 + 1$ ve t tek sayı formunda olan sayıları bulalım.

```
% Asal Sayılar
%r = 4.t^2 +1 ve t = 2k+1 formunda olan asal sayıları elde
ediyoruz.
%Yasin YILMAZ

for t=1:2:19
    r = 4*(t^2)+1;
    if primes(r)
        a(t)= r;
    end
end

b = sort(a);

for i=1:length(b)
    if b(i) ~=0
        k = b(i:length(b))
        break
    end
end
```

Şekil 7. C_4^2 Döngüsel Sınıf İçin Uygun Parametreleri Bulduran MATLAB Uygulaması

Şimdi elde etmiş olduğumuz r asal sayıları için $GF(r)$ cismi üzerinde C_4^2 döngüsel sınıfının fark kümesi olduğunu gösterelim.

```
% Fark Kümeleri
%Burada C4 döngüsel sınıfı ile elde edilen sınıftan(r, (r-1)/4, (r-5)/16) parametrelili fark kümesi olduğunu gösteriyoruz.
%Yasin YILMAZ...
r = 101; %Grubun mertebesini girelim.
g = 2; %Grubun ilkel kökünü girelim.
e = 4; %Döngüsel sınıfın mertebesi...
f = (r-1)/4;
```

Şekil 8. C_4^2 Döngüsel Sınıf ile Elde Edilen Fark Kümesinin MATLAB Uygulaması

```

for i=1:f
    s = sym(g)
    C4(i) = mod(s^((e*(i-1))+2),r); %C4 Döngüsel sınıf oluşturulur.
end

% Fark kümesi olması durumunda C0 döngüsel sınıfından elde edilen
fark kümesi için Lamda elde ediyoruz.

k = length(C4);
Lamda = (k*(k-1))/(r-1);
Lamda
k

%C4 sınıfının elemanların birbirlerinden farkını alarak matris
elde
%ediyoruz.
for i=1:k
    for j=1:k
        matris(i,j) = mod(C4(i)-C4(j),r);
    end
end

% C4 sınıfında kalan sınıfını hangi elemanı tekrar ettiğini daha
rahat görebilmek adına matrisi vektör haline getiriyoruz.

sayac=0;

for i=1:k
    for j=1:k
        sayac=sayac+1;
        vektor(sayac)=matris(i,j);
    end
end

as_vektor=sort(vektor);

%Vektörde birim elemanı hariç kalan sınıfının diğer elemanların kaç
defa tekrarlandığını sayıyoruz.

for i=1:r-1
    saycheck=0;
    for j=1:sayac
        if i==as_vektor(j)
            saycheck=saycheck+1;
        end
    end
    diffcheck(i)=saycheck;
end

%Tekrarlanan elemanların sayısının aynı olup olmaması durumuna göre
fark kümesi teşkil edip etmediğini kontrol ediyoruz.

```

Şekil 8(Devam). C_4^2 Döngüsel Sınıf ile Elde Edilen Fark Kümesi İçin Uygun Parametrelerin MATLAB Uygulaması

```

farkcheck=0;

for i=2:r-1
    if diffcheck(i)~=diffcheck(i-1)
        fprintf('fark kümesi değildir')
        farkcheck=1;
        break
    end
end

if farkcheck==0
    fprintf('C4 döngüsel sınıfı (%d , %d , %d) parametrelili fark kümesidir',r,k,Lamda)
end

```

Şekil 8(Devam). C_4^2 Döngüsel Sınıf ile Elde Edilen Fark Kümesi İçin Uygun Parametrelerin MATLAB Uygulaması

Tablo 11. C_4^2 Sınıfından Elde Edilen Fark Kümesi Programının Çalışma Süreleri

C_4^2 Sınıfından Elde Edilen Fark Kümesi Programının Çalışma Süreleri		
(v, k, l)	Üreteç	Programın Çalışma Süresi
(5,1,0)	$g = 2$	0.129343
(37,9,2)	$g = 2$	9.879958
(101,25,6)	$g = 2$	198.434371

2.5. $C_4^2 \cup \{0\}$ Döngüsel Sınıf ile Elde Edilen Fark Kümesinin MATLAB Uygulaması

$C_4^2 \cup \{0\}$ döngüsel sınıfı, $\left(r, \frac{r+3}{4}, \frac{r+3}{16}\right)$ parametreleri ile bir fark kümesidir.

Burada $r = 4t^2 + 9$ ve t tek sayı formundadır. İlk olarak $r = 4t^2 + 9$ ve t tek sayı formunda olan sayıları bulalım.

```

% Asal Sayılar
%r = 4.t^2 +1 ve t = 2k+1 formunda olan asal sayıları elde ediyoruz.
%Yasin YILMAZ

for i=1:2:40
    r(i) = 4*(i^2)+9;
end

b = sort(r);

for i=1:length(b)
    if b(i) ~=0
        k = b(i:length(b));
        break
    end
end
k

```

Şekil 9. $C_4^2 \cup \{0\}$ Döngüsel Sınıf ile Elde Edilen Fark Kümesi İçin Uygun Parametrelerin MATLAB Uygulaması

Şimdi elde etmiş olduğumuz r asal sayıları için $GF(r)$ cismi üzerinde $C_4^2 \cup \{0\}$ döngüsel sınıfının fark kümesi olduğunu gösterelim.

```

%Burada C4 U {0} döngüsel sınıfı ile elde edilen sınıftan(r,
(r+3)/4, (r+3)/16) parametrelili fark kümesi olduğunu gösteriyoruz.
%Yasin YILMAZ...
r = 109; %Grubun mertebesi girelim.
g = 41; %Grubun ilkel kökünü girelim.

e = 4; %Döngüsel sınıfın mertebesi...
f = (r-1)/4;

for i=1:f
    s = sym(g);
    C4(i) = mod(s^((e*(i-1))+2),r);
    if i == f
        C4(i+1) = 0
    end
end

% Fark Kümesi olması durumunda C4 döngüsel sınıfından elde edilen
fark kümesi için Lamda elde ediyoruz.
k = length(C4);
Lamda = (k*(k-1))/(r-1);
Lamda

```

Şekil 10. $C_4^2 \cup \{0\}$ Döngüsel Sınıf ile Elde Edilen Fark Kümesinin MATLAB Uygulaması

```

%C4 sınıfının elemanların birbirlerinden farkını alarak matris
elde ediyoruz.

for i=1:k
    for j=1:k
        matris(i,j) = mod(C4(i)-C4(j),r);
    end
end
matris

% C4 sınıfında kalan sınıfını hangi elemanı tekrar ettiğini daha
rahat görebilmek adına matrisi vektör haline getiriyoruz.

sayac=0;
for i=1:k
    for j=1:k
        sayac=sayac+1;
        vektor(sayac)=matris(i,j);
    end
end
as_vektor=sort(vektor)

%Vektörde birim elemanı hariç kalan sınıfının diğer elemanların kaç
defa tekrarlandığını sayıyoruz.

for i=1:r-1
    saycheck=0;
    for j=1:sayac
        if i==as_vektor(j)
            saycheck=saycheck+1;
        end
    end
    diffcheck(i)=saycheck;

end

%Tekrarlanan elemanların sayısı aynı olup olmaması durumuna göre
fark kümesi teşkil edip etmediğini kontrol ediyoruz.

farkcheck=0;
for i=2:r-1
    if diffcheck(i)~=diffcheck(i-1)
        fprintf('fark kümesi değildir')
        farkcheck=1;
        break
    end
end
if farkcheck==0
    fprintf('C4 U {0} döngüsel sınıfı (%d , %d , %d) parametreli
fark kümesidir',r,k,Lamda)
end

```

Şekil 10(Devam). $C_4^2 \cup \{0\}$ Döngüsel Sınıf ile Elde Edilen Fark Kümesinin
MATLAB Uygulaması

Tablo 12. $C_4^2 \cup \{0\}$ Sınıfından Elde Edilen Fark Kümesi Programının Çalışma Süreleri

$C_4^2 \cup \{0\}$ Sınıfından Elde Edilen Fark Kümesi Programının Çalışma Süreleri		
(v, k, l)	Üreteç	Programın Çalışma Süresi
(13,4,1)	$g = 2$	6.485963
(109,38,7)	$g = 6$	109.855609

2.6. C_8^2 Döngüsel Sınıf ile Elde Edilen Fark Kümesinin MATLAB Uygulaması

C_8^2 döngüsel sınıfı, $\left(r, \frac{r-1}{8}, \frac{r-9}{64}\right)$ parametreleri ile bir fark kümesidir.

Burada $r = 8t^2 + 1 = 64u^2 + 9$, u ve t tek sayı formundadır. İlk olarak $r = 8t^2 + 1 = 64u^2 + 9$, u ve t tek sayı formunda olan sayıları bulalım.

```
% Asal Sayılar
%r = 4.t^2 +1 ve t = 2k+1 formunda asal sayıları elde ediyoruz.
%Yasin YILMAZ

for t=1:2:100
    a(t) = 8*(t^2)+1;
end

b = sort(a);
for i=1:length(b)
    if b(i) ~=0
        k = b(i:length(b));
        break
    end
end

for u=1:2:300
    m(u) = 64*(u^2)+9;
end

p = sort(m);
for i=1:length(p)
    if p(i) ~=0
        l = p(i:length(p));
        break
    end
end
```

Şekil 11. C_8^2 Döngüsel Sınıf İçin Uygun Parametreleri Bulduran MATLAB Uygulaması

```

for j=1:length(l)
    if k(i) == l(j)
        v(i) = k(i);
    end
end
end

f = sort(v);

for i=1:length(f)

    if f(i) ~=0
        s = f(i:length(f));
        break
    end
end
end

```

Şekil 11 (Devam). C_8^2 Döngüsel Sınıf İçin Uygun Parametreleri Bulduran MATLAB Uygulaması

Şimdi elde etmiş olduğumuz r asal sayıları için $GF(r)$ cismi üzerinde C_8^2 döngüsel sınıfının fark kümesi olduğunu gösterelim.

```

% Fark Kümeleri
%Burada C8 döngüsel sınıfı ile elde edilen sınıftan
%(r, (r-1)/8, (r-9)/64) parametrelili fark kümesi olduğunu
gösteriyoruz.
%Yasin YILMAZ...

r = 78409; %Grubun mertebesi girelim.
g = 2; %Grubun ilkel kökünü girelim.

e = 8; %Döngüsel sınıfın mertebesi..
f = (r-1)/8;

for i=1:f
    s = sym(g)
    C8(i) = mod(s^((e*(i-1))+4), r);
end

% Fark kümesi olması durumunda C8 döngüsel sınıfından elde edilen
fark kümesi için Lamda elde ediyoruz.

k = length(C8);
Lamda = (k*(k-1))/(r-1);

```

Şekil 12. C_8^2 Döngüsel Sınıf ile Elde Edilen Fark Kümesinin MATLAB Uygulaması

```

%C8 sınıfının elemanların birbirlerinden farkını alarak matris elde ediyoruz.

for i=1:k
    for j=1:k
        matris(i,j) = mod(C8(i)-C8(j),r);
    end
end

% C8 sınıfında kalan sınıfını hangi elemanı tekrar ettiğini daha rahat görebilmek adına matrisi vektör haline getiriyoruz.
sayac=0;
for i=1:k
    for j=1:k
        sayac=sayac+1;
        vektor(sayac)=matris(i,j);
    end
end
as_vektor=sort(vektor);

%Vektörde birim elemanı hariç kalan sınıfının diğer elemanların kaç defa tekrarlandığını sayıyoruz.

for i=1:r-1
    saycheck=0;
    for j=1:sayac
        if i==as_vektor(j)
            saycheck=saycheck+1;
        end
    end

    diffcheck(i)=saycheck;

end

%Tekrarlanan elemanların sayısı aynı olup olmaması durumuna göre fark kümesi teşkil edip etmediğini kontrol ediyoruz.

farkcheck=0;
for i=2:r-1
    if diffcheck(i)~=diffcheck(i-1)
        fprintf('fark kümesi değildir')
        farkcheck=1;
        break
    end
end
if farkcheck==0
    fprintf('C8 döngüsel sınıfı (%d , %d , %d) parametrelili fark kümesidir',r,k,Lamda)
end

```

Şekil 12 (Devam). C_8^2 Döngüsel Sınıf ile Elde Edilen Fark Kümesinin MATLAB Uygulaması

2.7. $C_0^6 \cup C_1^6 \cup C_3^6$ Döngüsel Sınıf ile Elde Edilen Fark Kümesinin MATLAB Uygulaması

$C_0^6 \cup C_1^6 \cup C_3^6$ döngüsel sınıfı, $(GF(r), +)$ cismi üzerinde $\left(r, \frac{r-1}{2}, \frac{r-3}{4}\right)$ parametreleriyle bir fark kümesidir.

```
% Fark Kümeleri
%Burada C6-0 U C6-1 U C6-3 döngüsel sınıfı ile elde edilen
sınıftan
%(r, (r-1)/2, (r-3)/4) parametrelili fark kümesi olduğunu
gösteriyoruz.
%Yasin YILMAZ...

r = 31; % Grubun mertebesini
g = 3; %İlkel kökü giriniz

e = 6; %Döngüsel sınıfın mertebesi
f = (r-1)/6;

for i=1:f
    s = sym(g)
    C6(i) = mod(s^((e*(i-1))+0),r); %C6-0 Döngüsel sınıfı
end

for i=1:f
    s = sym(g)
    C6(i+f) = mod(s^((e*(i-1))+1),r); % C6-1 Döngüsel sınıfı
end

for i=1:f
    s = sym(g)
    C6(i+2*f) = mod(s^((e*(i-1))+3),r); % C6-3 Döngüsel sınıfı
end
% Fark kümesi olması durumunda C6-0 U C6-1 U C6-3 döngüsel sınıfından
elde edilen fark kümesi için Lamda elde ediyoruz.

k = length(C6);
Lamda = (k*(k-1))/(r-1);

%C6-0 U C6-1 U C6-3 sınıfının elemanların birbirlerinden farkını
olarak matris elde ediyoruz.

for i=1:k
    for j=1:k
        matris(i,j) = mod(C6(i)-C6(j),r);
    end
end
```

Şekil 13. $C_0^6 \cup C_1^6 \cup C_3^6$ Döngüsel Sınıf ile Elde Edilen Fark Kümesinin MATLAB Uygulaması

```

% C6-0 U C6-1 U C6-3 sınıfında kalan sınıfını hangi elemanı tekrar
ettiğini daha rahat görebilmek adına matrisi vektör haline
getiriyoruz.

sayac=0;

for i=1:k
    for j=1:k
        sayac=sayac+1;
        vektor(sayac)=matris(i,j);
    end
end

as_vektor=sort(vektor);
matris

%Vektörde birim elemanı hariç kalan sınıfının diğer elemanların
kaç defa tekrarlandığını sayıyoruz.

for i=1:r-1
    saycheck=0;
    for j=1:sayac
        if i==as_vektor(j)
            saycheck=saycheck+1;
        end
    end
    diffcheck(i)=saycheck;

end

%Tekrarlanan elemanların sayısı aynı olup olmaması durumuna göre
fark kümesi teşkil edip etmediğini kontrol ediyoruz.

farkcheck=0;

for i=2:r-1
    if diffcheck(i)~=diffcheck(i-1)
        fprintf('fark kümesi değildir')
        farkcheck=1;
        break
    end
end

if farkcheck==0
    fprintf('C0 döngüsel sınıfı (%d , %d , %d) parametreli fark
kümesidir',r,k,Lamda)
end

```

Şekil 13 (Devam). $C_0^6 \cup C_1^6 \cup C_3^6$ Döngüsel Sınıf ile Elde Edilen Fark Kümesinin
MATLAB Uygulaması

Tablo 13. C_8^2 Sınıfından ve $C_0^6 \cup C_1^6 \cup C_3^6$ Sınıfından Elde Edilen Fark Kümesi Programının Çalışma Süreleri

C_8^2 Sınıfından Elde Edilen Fark Kümesi Programının Çalışma Süreleri		
(v, k, l)	Üreteç	Programın Çalışma Süresi
(13,1,0)	$g = 2$	0.105881
(73,9,1)	$g = 5$	47.122384
$C_0^6 \cup C_1^6 \cup C_3^6$ Sınıfından Elde Edilen Fark Kümesi Programının Çalışma Süreleri		
(v, k, l)	Üreteç	Programın Çalışma Süresi
(31,15,7)	$g = 3$	7.549850

2.8. Bulgular

Bu tez çalışmasında döngüsel sayılar, döngüsel sınıflar ve fark kümeleri ve özellikleri ile ilgili bir literatür özeti verilmiş olup özellikleri incelenmiş ve ihtiyacımız olan tanım, teorem verilerek, fark kümesi ile döngüsel sınıflar arasındaki ilişki verilmiştir.

Üzerinde çokça çalışmalar yapılan fark kümeleri için birçok yöntem geliştirilmiştir. Döngüsel sınıflarda bu metotlardan birisidir. Bu çalışmada fark kümelerini elde etmek için döngüsel sınıflardan elde edilen sınıfların fark kümesi olduğunu göstermeye yönelik MATLAB programlama diliyle fark kümeleri elde edilmiştir. Özel olarak kuadratik rezidüler, C_0^2 döngüsel sınıfları, C_4^2 döngüsel sınıfları, $C_4^2 \cup \{0\}$ döngüsel sınıfları, C_8^2 döngüsel sınıfları ve $C_0^6 \cup C_1^6 \cup C_3^6$ döngüsel sınıflarından elde edilen sınıfların yönelik fark kümesi olduğuna yönelik kod çalışmaları yapılmıştır. Aynı zamanda bu kod çalışması Intel(R) Core(TM) i5 – 5200U, 2.20Hz işlemci ve 4 GB yüklü belleğe sahip bir bilgisayarda yürütülmüş olup ayrıyeten çalışma süreleri verilmiştir. Yapılan çalışmalar doğrultusunda daha yüksek işlemci ve yüklü belleğe sahip farklı bir bilgisayarlarda yürütüldüğünde bu sürenin azaldığı gözlemlenmiştir.

3. TARTIŞMA ve SONUÇ

Bu çalışmada döngüsel sayıların tanımı, 1. mertebeden, 2. mertebeden, 3. mertebeden ve 4. mertebeden döngüsel sayılar, döngüsel sınıflar ve fark kümeleri ile ilgili bazı teoremler ve ispatları verilmiştir. Ayrıca döngüsel sınıflardan özel olarak elde edilmiş olan sınıfların fark kümesi teşkil ettiği teoremler ile ifade edilmiş ve bu sınıfların fark kümesi olduğuna yönelik örnekler verilmiştir.

Yapılan çalışmalar kısmında ise ilk olarak bir cisim için kuadratik rezidü sınıfının fark kümesi olduğunu ve bu özel olarak ele almış olduğumuz döngüsel sınıfların fark kümeleri olduğunu gösteren MATLAB programlama diliyle yazılmış kod çalışmaları sunulmuştur ve çıkan sonuçların çalışma süreleri verilmiştir.

MATLAB programlama dilinde mertebesini ve ilkel kökünü girdiğimiz cisim için C_0^2 döngüsel sınıflarının, C_4^2 döngüsel sınıflarının, $C_4^2 \cup \{0\}$ döngüsel sınıflarının, C_8^2 döngüsel sınıflarının ve $C_0^6 \cup C_1^6 \cup C_3^6$ döngüsel sınıflarının fark kümesi olduğuna yönelik örnekler sunulmuştur.

3.1. Öneriler

Döngüsel sayılardan oluşturulan döngüsel sınıflardan fark kümesi, hemen hemen fark kümesi vb. fark kümeleri elde etmek mümkündür. Fakat döngüsel sayılarının mertebesi arttıkça cismin mertebesi de arttığından, döngüsel sınıflarda elde edilecek olan fark kümesini veya hemen hemen fark kümesini olduğunu göstermek daha zor olacaktır. Bunun için bu yapıları ele alabilmek için bilgisayar yardımına matematiksel programlara, farklı program dillerine ihtiyaç duyulabilir. Programlama dilinde yazılmış bu kodlar vasıtası ile şimdiye kadar elde edilmemiş farklı parametrelere sahip fark kümeleri, hemen hemen fark kümeleri veya kısmi fark kümeleri elde edilip teoremler oluşturulabilir.

KAYNAKÇA

- Arasu, K. T, Ding C., Hellesteth T., Kumar P. ve Matinsen H. (2001) *Almost difference sets and their sequence with optimal autocorrelation*. IEEE Trans. Inform. Teory 47, no.7, 2934 – 2943.
- Baumert L. D. ve Fredricksen H. 1967. *The cyclotomic numbers of order eighteen with applications to difference sets*. Math Comp. 21, 204 – 219.
- Berndt B. C., Williams K. S., & Evans R. J. (1998). *Gauss and Jacobi sums*. Wiley.
- Beth, Thomas, Dieter Jungnickel, ve Hanfried Lenz.1999. *Design Theory*. Vol. 1. Cambridge: Cambridge University Press.
- Buck N., Smith L and Spearman B K., et al. 1987. *The cyclotomic numbers of order fifteen*. Math Comp. 48, 67 – 83.
- Çallıalp F., 2013. *Örneklerle Soyut Cebir*. İstanbul: Birsen Yayınevi.
- Dembowski P. (1997). Finite geometries. Mathematics Subject Classification (1991): 51E, Volume 44, ISBN-13: 978-3-540-61786-0.
- Dickson L. E. 1935 *Cyclotomy, higher congruences and Waring's problem*. Amer J. Math. 57, 391 – 424.
- Ding C. 2014. *Codes From Difference Sets*. Singapore:World Scientific.
- Evans R. J. 1980. *Table of cyclotomic numbers of order twenty four*. Math. Comp. Review 12, 1036 – 1038.
- Gauss C. F. 1966. *Disquisitiones Arithmeticae* (Translated by Clarke A A). New Haven, Yale University press
- Hall M. Jr. 1965. *Characters and cyclotomy*, Amer. Math. Soc. Proc. Symp. Pure Math. 8,31 – 43.
- Kathleen Nowak. 2014. A Survey on Almost Difference Sets. arXiv:1409.0114.
- Katre S. A. ve Rajwade A. R., 1985. *On the unique determination of cyclotomic numbers of order five*. Manuscr. Math. 53, 65 – 75.
- Lehmer E. 1955. *On the number of solutions of $u^k + D \equiv w^2 \pmod{p}$* . Pasific J. Math. 5, 103 – 118.
- Lehmer E. 1953. "On Residue Difference Sets", Canad. J. Math 5, 425-432.

- Leonard P. A. ve Williams K. S. 1974. *Diophantine system of Dickson*. Rend. Accad. Naz. Lincei 56, 145 – 150.
- Leonard P. A. ve Williams K. S. 1975. *The cyclotomic number of order eleven*. Acta Arith. 26, 367 – 383.
- Leonard P. A. ve Williams K. S. 1975. *The cyclotomic number of order seven*. Proc. Amer. Math. Soc. 51 295 – 300.
- MATLAB and Statistics Toolbox Release Trailer Version, The MathWorks, Inc., Natick, Massachusetts, United States.
- Mehmet Erdoğan ve Gülşen Yılmaz. 2008, *Çözümlü Problemlerle Soyut Cebir ve Sayılar Teorisi*. İstanbul: Beykent Üniversitesi Yayınevi.
- Moore, E.H. ve Pollatsek. H.S. (2013). Difference sets. American Mathematical Society, 298 s, 253-266.
- Moore, Emily H. ve Harriet S. Pollatsek. 2013. *Difference Sets: Connecting Algebra, Combinatorics, and Geometry*. Providence, RI:American Mathematical Society.
- Morrice, R.T. (2015). Difference Sets- An investigation into the properties and criteria for existence.
- Muskat J.B. 1966. *The cyclotomic numbers of order twelve*. Acta Arith. 11, 263 – 279.
- Muskat J.B. ve Whiteman A L. 1970. *The cyclotomic numbers of order twenty*. Acta Arith. 17, 185 – 216.
- Parnami J.C., Atgawal M K ve Rajwade A R. 1982. *Jacobi sums and cyclotmic numbers for a finite field*. Acta Arith. 41. 1 – 13.
- Ryser, H.J. (1982). The existence of symmetric block designs. *Journal of Combinatorial Theory A*, 32(1), 103-105.
- Halberstam, H., ve R. R. Laxton 1964 "Perfect Difference Sets", Proc. Glasgow Math. Assoc. 6, 177-184.
- Storer T., 1967. *On the unique determination of cyclotomic numbers for Galois fields and Galois domain*. J. Combinatorial Theory. 2, 296 – 300.
- Whiteman A. L. 1952. *Cyclotomy and Jacobsthal sums*. Amer. J. Math 74, 89 – 99.
- Whiteman A. L. 1957. *The cyclotomic numbers of order sixteen*. Trans. Amer. Math. Soc. 86, 401 – 413.

Whiteman A. L. 1960. *The cyclotomic numbers of order ten*. Proc. Sympos. Appl. Math. 10, Amer. Math. Soc. Providence, R. I., 95 – 111.

Whiteman A. L. 1960. *The cyclotomic numbers of order twelve*. Acta Arith. 6, 53 – 76.

Zee Y. C. 1971. *Jacobi sums of order 22*. Proc Amer. Math. Soc. 28, 25 – 31.