CYCLOTOMY VE ŞİFRELEMEDEKİ BAZI UYGULAMALARI

KAMİL OTAL

YÜKSEK LİSANS TEZİ

MATEMATİK BÖLÜMÜ

TOBB EKONOMİ VE TEKNOLOJİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

EYLÜL 2012

ANKARA

Fen Bilimleri Enstitü onayı

_____

Prof. Dr. Ünver KAYNAK
Müdür

Bu tezin Yüksek Lisans derecesinin tüm gereksinimlerini sağladığını onaylarım.

_____

Prof. Dr. Mustafa BAYRAKTAR
Anabilim Dalı Başkanı

KAMİL OTAL tarafından hazırlanan CYCLOTOMY VE ŞİFRELEMEDEKİ BAZI UYGULAMALARI adlı bu tezin Yüksek Lisans tezi olarak uygun olduğunu onaylarım.

Yrd. Doç. Dr. Zülfükar SAYGI	Yrd. Doç. Dr. Çetin ÜRTİŞ
1. Tez Danışmanı	2. Tez Danışmanı

Tez Jüri Üyeleri

Başkan : Doç. Dr. Emrah KILIÇ _____

Üye : Yrd. Doç. Dr. Zülfükar SAYGI _____

Üye : Dr. Muhiddin UĞUZ _____

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada orijinal olmayan her türlü kaynağa eksiksiz atıf yapıldığını bildiririm.

Kamil OTAL

Üniversitesi : **TOBB Ekonomi ve Teknoloji Üniversitesi**
Enstitüsü : **Fen Bilimleri**
Anabilim Dalı : **Matematik Bölümü**
1. Tez Danışmanı : **Yrd. Doç. Dr. Zülfükar SAYGI**
2. Tez Danışmanı : **Yrd. Doç. Dr. Çetin ÜRTİŞ**
Tez Türü ve Tarihi : **Yüksek Lisans – Eylül 2012**

Kamil OTAL

CYCLOTOMY VE ŞİFRELEMEDEKİ BAZI UYGULAMALARI

ÖZET

Cyclotomic sayılar, şifreleme alanında kullanılan önemli cebirsel argümanlardandır. Yalnız bu sayıları tanım üzerinden hesaplama işi, parametreler büyüdükçe çeşitli zorlukları da beraberinde getirmektedir. Cyclotomic sayıların bazı temel özellikleri, bu sayıları Diyofant denklemler yoluyla ifade etmeye imkan tanır. Böylelikle problem sayılar teorisiyle ilişkilendirilir ve bazı durumlarda cyclotomic sayıları hesaplamak kolaylaşır. Bu konudaki ilk hesaplamalar genelde $\mathbb{Z}_p$ üzerinden yapılmış, daha sonra çalışmalar $\mathbb{F}_{p^n}$ ye genelleştirilmeye çalışılmıştır. $\mathbb{Z}_p$ üzerinden bakıldığında mertebe 24'e kadar çalışmaların olduğu görülür [12–16]. $\mathbb{F}_{p^n}$ üzerinde incelendiğinde ise yedinci mertebeye kadar çalışmaların tamamlandığı [4, 5, 20] görülmüştür. Bu tez çalışmasında öncelikle cyclotomy tanıtılmış, sonra $\mathbb{F}_{p^n}$ üzerinde mertebe yedi incelenmiş ve konuyla ilgili sonuçlar derlenmiştir. Ayrıca cyclotomy probleminin şifrelemedeki uygulamalarından bahsedilmiş, güncel ve önemli bir uygulaması olan Sidel'nikov dizileri de örneklerle anlatılmaya çalışılmıştır.

Anahtar Kelimeler: Cyclotomy, cyclotomic sayılar, uniform cyclotomy, Sidel'nikov dizileri, otokorelasyon, otokorelasyon dağılımı.

University	:	**TOBB University of Economics and Technology**
Institute	:	**Institute of Natural and Applied Sciences**
Science Programme	:	**Mathematics**
Supervisor 1	:	**Asst. Prof. Zülfükar SAYGI**
Supervisor 2	:	**Asst. Prof. Çetin ÜRTİŞ**
Degree Awarded and Date	:	**M.Sc. – September 2012**

Kamil OTAL

CYCLOTOMY AND SOME APPLICATIONS IN CRYPTOLOGY

ABSTRACT

Cyclotomic numbers are quite useful algebraic arguments in cryptology. However calculation of these numbers in terms of the definition is getting harder while parameters are getting larger. Some of the properties of cyclotomic numbers provide to express them in terms of Diophant equations. In this way the problem is linked to number theory and in some cases the calculations become easier. Primary works on the problem are usually on $\mathbb{Z}_p$ and later generalizations to $\mathbb{F}_{p^n}$ are sought. On $\mathbb{Z}_p$ there are several works on order 2-24 [12–16], on $\mathbb{F}_{p^n}$ there are works on order 2-6 and 8 [4, 5, 20]. In this work, order 7 cyclotomic numbers on $\mathbb{F}_{p^n}$ are examined and the results are compiled. Additionally some applications of cyclotomy on cryptology are mentioned and Sidel'nikov sequences which are the current and important applications are explained by examples.

Keywords: Cyclotomy, cyclotomic numbers, uniform cyclotomy, Sidel'nikov sequences, autocorrelation, autocorrelation distribution.

TEŞEKKÜR

Bu çalışmayı tamamlamamda ve hayatımın diğer birçok aşamasında emeği geçen başta tez danışmanlarım Zülfükar SAYGI ve Çetin ÜRTİŞ olmak üzere tüm TOBB ETÜ Matematik Bölümü hocalarıma, birçok konuda yardımlarını esirgemeyen asistan arkadaşlarıma, maddi ve manevi manada en büyük destekçim olan aileme teşekkür ederim. Ayrıca çalışmalarımı 109T344 Cebirsel Eğriler ve Üssel Toplamlar Kullanarak Bazı Kriptografik Uygulamalar isimli proje kapsamında destekleyen TÜBİTAK'a teşekkür ederim.

İçindekiler

1. ÖN BİLGİLER

Bu bölümde, sonraki bölümlerde kullanılacak bazı temel matematiksel ifadeler tanıtılmaktadır. Burada verilen tüm tanımlar, teoremler ve kullanılan notasyonlar için [1] den faydalanılmıştır. Bu bölümden itibaren

- p ile bir asal sayı,
- q ile p asalının bir kuvveti,
- $\mathbb{F}_q$ ile q elemanlı sonlu cisim,
- $\mathbb{F}_{q^m}$ ile de $\mathbb{F}_q$ cisminin m. mertebeden bir sonlu genişlemesi ($m \in \mathbb{Z}^+$)

belirtilecektir.

1.1 İz ve Norm Fonksiyonları

$F = \mathbb{F}_{q^m}$ ve $K = \mathbb{F}_q$ olmak üzere F den K ya

$$Tr_{F/K}(x) = x + x^q + x^{q^2} + ... + x^{q^{m-1}}$$

şeklinde tanımlanan $Tr_{F/K}$ fonksiyonuna **iz fonksiyonu** denir.

Örnek 1 *$K = \mathbb{F}_2$ ve $F = \mathbb{F}_8 = \mathbb{F}_2(\alpha)$, $\alpha^3 + \alpha + 1 = 0$ olmak üzere $Tr_{F/K}(x) = x + x^2 + x^4$ olup*

F		K
0	$\longmapsto$	0
1	$\longmapsto$	1
α	$\longmapsto$	0
α^2	$\longmapsto$	0
$\alpha + 1$	$\longmapsto$	1
$\alpha^2 + 1$	$\longmapsto$	1
$\alpha^2 + \alpha$	$\longmapsto$	0
$\alpha^2 + \alpha + 1$	$\longmapsto$	1

Örnek 2 *$K = \mathbb{F}_4 = \mathbb{F}_2(u)$, $u^2 + u + 1 = 0$ ve $F = \mathbb{F}_{16} = \mathbb{F}_4(\beta)$, $\beta^2 + \beta + u = 0$ olmak üzere $Tr_{F/K}(x) = x + x^4$ olup*

F		K
0	$\longmapsto$	0
1	$\longmapsto$	0
u	$\longmapsto$	0
$u + 1$	$\longmapsto$	0
β	$\longmapsto$	1
$\beta + 1$	$\longmapsto$	1
$\beta + u$	$\longmapsto$	1
$\beta + u + 1$	$\longmapsto$	1
$u\beta$	$\longmapsto$	u
$u\beta + 1$	$\longmapsto$	u
$u\beta + u$	$\longmapsto$	u
$u\beta + u + 1$	$\longmapsto$	u
$u\beta + \beta$	$\longmapsto$	$u + 1$
$u\beta + \beta + 1$	$\longmapsto$	$u + 1$
$u\beta + \beta + u$	$\longmapsto$	$u + 1$
$u\beta + \beta + u + 1$	$\longmapsto$	$u + 1$

İz fonksiyonunda değer kümesi asal cisim olursa, yani $K = F_p$ olursa, iz fonksiyonuna **mutlak iz fonksiyonu** denir.

Teorem 3 (İz Fonksiyonunun Temel Özellikleri) *$F = \mathbb{F}_{q^m}$ ve $K = \mathbb{F}_q$ olsun. Buna göre*

1. *Her $\alpha, \beta \in F$ için $Tr_{F/K}(\alpha + \beta) = Tr_{F/K}(\alpha) + Tr_{F/K}(\beta)$ dir.*
2. *Her $\alpha \in F$ ve $c \in K$ için $Tr_{F/K}(c\alpha) = cTr_{F/K}(\alpha)$ dir.*
3. *İz dönüşümü örten bir dönüşümdür.*
4. *Her $a \in K$ için $Tr_{F/K}(a) = ma$ dir.*
5. *Her $\alpha \in F$ için $Tr_{F/K}(\alpha^{q^k}) = Tr_{F/K}(\alpha)$ dir ($k \in \mathbb{N}$).*

K bir sonlu cisim ve F onun bir sonlu genişlemesi olsun, ikisi de K üzerinde vektör uzaylarıdır. Bu teoremde verilen ilk iki özellik de $Tr_{F/K}$ nın F den K ya bir lineer dönüşüm olduğunu söyler. Hatta F den K ya tüm lineer dönüşümler iz fonksiyonu kullanılarak inşa edilebilir. Bu sayede, ileride toplamsal karakterler olarak isimlendirilecek yapılar incelenirken belirli bir karakterizasyon elde edilebilecektir.

Teorem 4 *K bir sonlu cisim ve F onun sonlu bir genişlemesi olsun. Her $\alpha \in F$ için $L_\beta(\alpha) = Tr_{F/K}(\beta\alpha)$, $\beta \in F$ şeklinde tanımlanan fonksiyonlar lineer dönüşümlerdir ve F den K ya tüm lineer dönüşümler bu şekilde elde edilir. Ayrıca $\alpha \neq \beta$ iken $L_\alpha \neq L_\beta$ olur.*

Görüldüğü üzere iz fonksiyonu sonlu cisim elemanını eşleniklerinin toplamına götürüyor. Eşleniklerinin çarpımına götüren fonksiyona ise norm fonksiyonu denir. Yani,

$F = \mathbb{F}_{q^m}$ ve $K = \mathbb{F}_q$ olmak üzere F den K ya

$$N_{F/K}(\alpha) = x \cdot x^q \cdot x^{q^2} \cdots x^{q^{m-1}} = x^{(q^m-1)/(q-1)}$$

şeklinde tanımlanan $N_{F/K}$ fonksiyonuna **norm fonksiyonu** denir.

Örnek 5 *$K = \mathbb{F}_2$ ve $F = \mathbb{F}_8 = \mathbb{F}_2(\alpha)$, $\alpha^3+\alpha+1 = 0$ olsun. $N_{F/K}(x) = x \cdot x^2 \cdot x^4 = x^7$ olmak üzere*

$$\begin{array}{ccc} F & & K \\ 0 & \longmapsto & 0 \\ 1 & \longmapsto & 1 \\ \alpha & \longmapsto & 1 \\ \alpha^2 & \longmapsto & 1 \\ \alpha+1 & \longmapsto & 1 \\ \alpha^2+1 & \longmapsto & 1 \\ \alpha^2+\alpha & \longmapsto & 1 \\ \alpha^2+\alpha+1 & \longmapsto & 1 \end{array}$$

Örnek 6 *$K = \mathbb{F}_3$ ve $F = \mathbb{F}_9 = \mathbb{F}_3(\alpha)$, $\alpha^2+1 = 0$ olmak üzere $N_{F/K}(x) = x \cdot x^3 = x^4$ olup*

$$\begin{array}{ccc} F & & K \\ 0 & \longmapsto & 0 \\ 1 & \longmapsto & 1 \\ 2 & \longmapsto & 1 \\ \alpha & \longmapsto & 1 \\ 2\alpha & \longmapsto & 1 \\ \alpha+1 & \longmapsto & 2 \\ \alpha+2 & \longmapsto & 2 \\ 2\alpha+1 & \longmapsto & 2 \\ 2\alpha+2 & \longmapsto & 2 \end{array}$$

Teorem 7 (Norm Fonksiyonunun Temel Özellikleri) *$F = \mathbb{F}_{q^m}$ ve $K = \mathbb{F}_q$ olsun. Buna göre*

1. *Her $\alpha, \beta \in F$ için $N_{F/K}(\alpha\beta) = N_{F/K}(\alpha)N_{F/K}(\beta)$ dir.*
2. *Norm fonksiyonu örtendir, ayrıca $N_{F/K}(F^*) = K^*$ dir.*
3. *Her $a \in K$ için $N_{F/K}(a) = a^m$ dir.*
4. *Her $\alpha \in F$ için $N_{F/K}(\alpha^{q^k}) = N_{F/K}(\alpha)$ dir ($k \in \mathbb{N}$).*

1.2 Karakterler

G değişmeli bir grup ve $U = \{z \in \mathbb{C} : |z| = 1\}$ olsun. U çarpma işlemine göre bir gruptur. χ, G den U ya tanımlanan bir grup homomorfizması (yani her $g, h \in G$ için $\chi(gh) = \chi(g)\chi(h)$) ise χ fonksiyonuna G **nin karakteri** denir.

Örnek 8 *$G = \mathbb{Z}_2 \times \mathbb{Z}_2$ olmak üzere*

$$\begin{array}{ccc} G & \xrightarrow{\chi} & U \\ (0,0) & \longmapsto & 1 \\ (0,1) & \longmapsto & -1 \\ (1,0) & \longmapsto & -1 \\ (1,1) & \longmapsto & 1 \end{array}$$

şeklinde tanımlanan χ dönüşümü bir karakterdir.

Örnek 9 *$G = \mathbb{Z}_6$ olmak üzere $\chi(k) = e^{2\pi ik/3}$ dönüşümü bir karakterdir.*

Örnek 10 *Bir önceki örnek genelleştirilebilir. G bir sonlu devirli grup, yani $G = \mathbb{Z}_n$, $n \in \mathbb{Z}^+$ olsun. G üzerinde $\chi_j(k) = e^{2\pi ijk/n}$ şeklinde tanımlanan χ_j dönüşümleri birer karakterdir ve $\mathbb{Z}_n$ üzerinde tanımlanan tüm karakterler bu şekildedir.*

Her $g \in G$ için $\chi(g) = 1$ olan karaktere **aşikar karakter** denir ve özel olarak χ_0 ile gösterilir. χ, G nin bir karakteri olmak üzere $\overline{\chi}$ karakteri $\overline{\chi}(g) = \overline{\chi(g)}$ şeklinde tanımlanırsa, bu $\overline{\chi}$ karakterine de χ karakterinin **eşlenik karakteri** denir. G üzerinde tanımlanan tüm karakterlerin kümesi $G\hat{}$ ile gösterilip $G\hat{}$ üzerinde $\chi_1\chi_2(g) = \chi_1(g)\chi_2(g)$ olacak şekilde bir çarpma işlemi tanımlanır ise $G\hat{}$ bu işleme göre bir grup oluşturur, bu grubun birim elemanı aşikar karakter ve χ karakterinin tersi de χ in eşlenik karakteridir. Ayrıca $|G\hat{}| = |G|$ dir.

Teorem 11 *G bir sonlu değişmeli grup olsun. χ onun üzerinde aşikar olmayan bir karakter ise*

$$\sum_{g \in G} \chi(g) = 0$$

olur. $g \in G$ *birim elemandan farklı bir eleman ise*

$$\sum_{\chi \in \hat{G}} \chi(g) = 0$$

olur.

Teorem 12 (Karakterlerde Ortogonallik Bağıntıları) $\chi, \psi \in \hat{G}$ *olmak üzere*

$$\frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\psi(g)} = \begin{cases} 0, & \chi \neq \psi \\ 1, & \chi = \psi \end{cases}$$

$g, h \in G$ *olmak üzere*

$$\frac{1}{|G|} \sum_{\chi \in \hat{G}} \chi(g)\overline{\chi(h)} = \begin{cases} 0, & g \neq h \\ 1, & g = h \end{cases}$$

Sonlu cisimlerde iki tane grup vardır, biri toplama işlemine göre grup diğeri ise çarpımsal grup. Dolayısıyla bir sonlu cisimden iki tür karakter tanımlanabilir. Bu karakterler de üzerinde tanımlandıkları gruba göre **toplamsal karakter** ve **çarpımsal karakter** diye adlandırılır.

Tr ile $\mathbb{F}_q$ sonlu cisminden tanımlanan mutlak iz fonksiyonu belirtilirse, $\mathbb{F}_q$ üzerinde tanımlanan $\chi_1(x) = e^{2\pi i Tr(x)/p}$ fonksiyonu bir toplamsal karakter olur ve **kanonik toplamsal karakter** ismini alır. Bu karakter yardımıyla tüm toplamsal karakterler inşa edilebilir, şöyle ki:

Teorem 13 $b \in \mathbb{F}_q$ *olmak üzere* χ_b *fonksiyonu* $\chi_b(x) = \chi_1(bx)$ *şeklinde tanımlansın.* χ_b *de bir toplamsal karakter olur ve* $\mathbb{F}_q$ *üzerindeki tüm toplamsal karakterler bu yolla elde edilir.*

Örnek 14 $\mathbb{F}_4 = \{0, 1, \alpha, \alpha + 1\}$; $\alpha^2 + \alpha + 1 = 0$ *olmak üzere* $\mathbb{F}_4$ *üzerinde tanımlanan tüm toplamsal karakterleri inceleyelim. Bunun için öncelikle* $\mathbb{F}_4$

üzerindeki mutlak iz fonksiyonu

$$\begin{array}{ccc} \mathbb{F}_4 & \overset{Tr(x)=x+x^2}{\longrightarrow} & \mathbb{F}_2 \\ 0 & \longmapsto & 0 \\ 1 & \longmapsto & 0 \\ \alpha & \longmapsto & 1 \\ \alpha+1 & \longmapsto & 1 \end{array}$$

şeklinde bulunur. $\chi_1(x) = e^{2\pi i Tr(x)/2}$ *olduğundan*

$$\begin{array}{ccc} (\mathbb{F}_4,+) & \overset{\chi_1}{\longrightarrow} & \mathbb{U} \\ 0 & \longmapsto & 1 \\ 1 & \longmapsto & 1 \\ \alpha & \longmapsto & -1 \\ \alpha+1 & \longmapsto & -1 \end{array}$$

elde edilir, diğer karakterler Teorem 13 kullanılarak hesaplanırsa

$$\begin{array}{ccc|ccc|ccc} (\mathbb{F}_4,+) & \overset{\chi_0}{\longrightarrow} & \mathbb{U} & (\mathbb{F}_4,+) & \overset{\chi_\alpha}{\longrightarrow} & \mathbb{U} & (\mathbb{F}_4,+) & \overset{\chi_{\alpha+1}}{\longrightarrow} & \mathbb{U} \\ 0 & \longmapsto & 1 & 0 & \longmapsto & 1 & 0 & \longmapsto & 1 \\ 1 & \longmapsto & 1 & 1 & \longmapsto & -1 & 1 & \longmapsto & -1 \\ \alpha & \longmapsto & 1 & \alpha & \longmapsto & -1 & \alpha & \longmapsto & 1 \\ \alpha+1 & \longmapsto & 1 & \alpha+1 & \longmapsto & 1 & \alpha+1 & \longmapsto & -1 \end{array}$$

olacak şekilde elde edilir. Bu dört karakter dışında toplamsal karakter yoktur.

Çarpımsal karakterler ise haliyle $\mathbb{F}_q^*$ üzerinden tanımlanacaktır, $\mathbb{F}_q^*$ devirli olduğu için

Teorem 15 *g, $\mathbb{F}_q$ nun sabit bir ilkel elemanı olsun. Her bir $j = 0, 1, 2, ..., q-2$ için $\psi_j(g^k) = e^{2\pi ijk/(q-1)}$ şeklinde tanımlanan ψ_j fonksiyonları birer çarpımsal karakterdir ve $\mathbb{F}_q^*$ üzerinde tanımlanan tüm karakterler bu şekilde elde edilir.*

Örnek 16 *$\mathbb{F}_7^*$ üzerinde $g = 3$ üreteci dikkate alınırsa, $\psi_j(3^k) = e^{2\pi ijk/6}$; $j = 0, 1, ..., 6$ şeklinde inşa edilir çarpımsal karakterler. Buna göre $6 = 3^3$ olmak üzere $\psi_4(6) = e^{12\pi i/3} = 1$ olur.*

Örnek 17 *q tek olmak üzere $\mathbb{F}_q$ nun $\psi_{(q-1)/2}$ çarpımsal karakterine ikinci dereceden (quadratic) karakter denir. Bu karakter $q = p$ için sayılar teorisindeki Legendre sembolüne denk olur.*

1.3 Gauss Toplamları

$\mathbb{F}_q$ üzerinde χ toplamsal karakter ve ψ çarpımsal karakter olmak üzere

$$G(\psi, \chi) = \sum_{c \in \mathbb{F}_q^*} \psi(c)\chi(c)$$

ifadesi **Gauss toplamı**nı verir.

Bu tanımdan görüldüğü üzere Gauss toplamı karakterlere ve karakterlerin üzerinde tanımlandığı sonlu cisme bağlıdır. Yalnız bazen Gauss toplamı (denk şekilde) bir çarpımsal karakter ve bir cisim elemanına bağlı olarak da verilebilir, örneğin yukardaki ifade, $u \in \mathbb{F}_q$ olmak üzere

$$G(\psi, u) = \sum_{c \in \mathbb{F}_q^*} \psi(c) e^{2\pi i Tr(uc)/p}$$

şeklinde yazılabilir (ikinci ifadedeki üssel gösterim ilk ifade için Teorem 13 te belirtilen χ_u ya denktir, dolayısıyla toplamda karakter gezdirmek yerine ona denk olarak eleman gezdirmiş olunur).

Örnek 18 *$\mathbb{F}_8^* = \{1, \alpha, \alpha^2, ...\alpha^6\}$; $\alpha^3 + \alpha + 1 = 0$ olmak üzere $\chi(\alpha^k) = e^{2\pi i Tr(\alpha^{k+2})}$ ve $\psi(\alpha^k) = e^{6\pi i k/7}$ olsun (yani $\chi = \chi_{\alpha^2}$ ve $\psi = \psi_3$). Buna göre*

$$\begin{aligned} G(\psi, \chi) &= \sum_{c \in \mathbb{F}_q^*} \psi(c)\chi(c) \\ &= \sum_{k=0}^{6} \psi(\alpha^k)\chi(\alpha^k) \\ &= e^{6\pi i/7} + e^{12\pi i/7} + e^{18\pi i/7} + e^{24\pi i/7} \end{aligned}$$

olur.

Teorem 19 *χ toplamsal karakter ve ψ çarpımsal karakter olmak üzere*

$$G(\psi,\chi) = \begin{cases} q-1, & \chi=\chi_0 \text{ ve } \psi=\psi_0 \\ -1, & \chi\neq\chi_0 \text{ ve } \psi=\psi_0 \\ 0, & \chi=\chi_0 \text{ ve } \psi\neq\psi_0 \end{cases} \tag{1.3.1}$$

dir. Ayrıca $\chi \neq \chi_0$ ve $\psi \neq \psi_0$ için

$$|G(\psi,\chi)| = q^{1/2}$$

olur.

Bazen de sıfırın çarpımsal karakterdeki değeri uygun bir şekilde belirlenip Gauss toplamı $\mathbb{F}_q^*$ yerine $\mathbb{F}_q$ üzerinden alınır. Bunun için, ψ bir çarpımsal karakter olmak üzere

$$\psi(0) = \begin{cases} 1, & \psi=\psi_0 \text{ için} \\ 0, & \psi\neq\psi_0 \text{ için} \end{cases} \tag{1.3.2}$$

şeklinde sıfırın karakterdeki değeri belirlenir. Burada karakterin işlem koruma (her $a,b \in \mathbb{F}_q$ için $\psi(ab)=\psi(a)\psi(b)$) özelliği korunmuş olur, ayrıca toplamlar üzerinde çalışıldığında farklılık yaşanmaz. Yalnız böyle bir tanım kümesi genişletmesi bazı özellikleri de etkileyebilir. Örneğin (1.3.1) ifadesi

$$G(\psi,\chi) = \begin{cases} q, & \chi=\chi_0 \text{ ve } \psi=\psi_0 \text{ için} \\ 0, & \chi\neq\chi_0,\ \psi=\psi_0 \text{ veya } \chi=\chi_0,\ \psi\neq\psi_0 \text{ için} \end{cases}$$

haline dönüşür.

Teorem 20 *$\mathbb{F}_q$ üzerinde alınan bir Gauss toplamı için*

1. $a \in \mathbb{F}_q^*, b \in \mathbb{F}_q$ için $G(\psi,\chi_{ab}) = \overline{\psi(a)}G(\psi,\chi_b)$
2. $G(\overline{\psi},\chi) = \psi(-1)\overline{G(\psi,\chi)}$
3. $\chi \neq \chi_0$ *ve* $\psi \neq \psi_0$ için $G(\psi,\chi)G(\overline{\psi},\chi) = \psi(-1)q$

4. $b \in \mathbb{F}_q$ için $G(\psi^p, \chi_b) = G(\psi, \chi_{b^p})$

Bu özellikler kullanılarak karakterler Gauss toplamları cinsinden ifade edilebilir.

$$\psi(c) = \frac{1}{q} \sum_{\chi \in (\mathbb{F}_q, +)\hat{}} G(\psi, \overline{\chi})\chi(c);\ c \in \mathbb{F}_q^*$$
$$\chi(c) = \frac{1}{q-1} \sum_{\psi \in (\mathbb{F}_q^*)\hat{}} G(\overline{\psi}, \chi)\psi(c);\ c \in \mathbb{F}_q^*$$

Yani Gauss toplamları sanki Fourier katsayılarıymış gibi bir rol oynar.

1.4 Jacobi Toplamları

Çarpımsal karakterler cismin sıfır harici elemanlarının üzerinden tanımlanır ama bazen tanım kümesi uygun bir şekilde genişletilebilir, bunun için sıfırın değeri (1.3.2) deki gibi belirlenir, bu tanım kümesi genişletmesi ile $\mathbb{F}_q$ üzerinde

$$J_a(\lambda_1, ..., \lambda_k) = \sum_{c_1 + ... + c_k = a} \lambda_1(c_1) \cdots \lambda_k(c_k)$$

toplamı verilsin ($\lambda_1, ..., \lambda_k$ lar çarpımsal karakterler ve $a \in \mathbb{F}_q$). Burada $a \neq 0$ iken $c_1 = ab_1, ..., c_k = ab_k$ dönüşümü ile

$$J_a(\lambda_1, ..., \lambda_k) = (\lambda_1 \cdots \lambda_k)(a) J_1(\lambda_1, ..., \lambda_k)$$

eşitliği elde edilir. Yani J_1 toplamı J_a lar için karakteristik bir rol oynar. O yüzden bu toplam indissiz olarak, yani J şeklinde gösterilecek ve bundan sonraki çalışmalar bu toplam üzerinden yapılacaktır. İşte bu şekilde belirtilen toplama Jacobi toplamı denir.

Yani, $\lambda_1, ..., \lambda_k$ lar çarpımsal karakterler olmak üzere $\mathbb{F}_q$ üzerinde

$$J(\lambda_1, ..., \lambda_k) = \sum_{c_1 + ... + c_k = 1} \lambda_1(c_1) \cdots \lambda_k(c_k)$$

şeklinde verilen toplama **Jacobi toplamı** denir.

$k = 1$ durumunda Jacobi toplamının (her karakter için) 1 e eşit olduğu aşikar, ayrıca toplamda çarpımsal karakterlerin sırasının önemsiz olduğu da görülebilir. Bu durum J_0 için de geçerlidir. Jacobi toplamları için için diğer bazı temel özellikler:

Teorem 21 *$\mathbb{F}_q$ üzerinde $\lambda_1, ..., \lambda_k$ ler çarpımsal karakterler ve χ aşikar olmayan toplamsal karakter olsun. Buna göre*

1. *Eğer $\lambda_1, ..., \lambda_k$ lerin hepsi aşikar karakterler ise*

$$J_0(\lambda_1, ..., \lambda_k) = J(\lambda_1, ..., \lambda_k) = q^{k-1}$$

2. *Eğer $\lambda_1, ..., \lambda_k$ lerin içinde aşikar olmayan karakter de aşikar olan karakter de mevcut ise*

$$J_0(\lambda_1, ..., \lambda_k) = J(\lambda_1, ..., \lambda_k) = 0$$

3. *Eğer λ_k aşikar değil ise*

$$J_0(\lambda_1, ..., \lambda_k) = \begin{cases} 0, & \lambda_1 \cdots \lambda_k \neq \lambda_0 \text{ için} \\ \lambda_k(-1)(q-1)J(\lambda_1, ..., \lambda_{k-1}), & \lambda_1 \cdots \lambda_k = \lambda_0 \text{ için} \end{cases}$$

4. *Eğer $\lambda_1, ..., \lambda_k$ lerin hepsi aşikar olmayan karakterler ise*

   (a) $\lambda_1 \cdots \lambda_k \neq \lambda_0$ *ise*

$$J(\lambda_1, ..., \lambda_k) = \frac{G(\lambda_1, \chi) \cdots G(\lambda_k, \chi)}{G(\lambda_1 \cdots \lambda_k, \chi)}$$

   (b) $\lambda_1 \cdots \lambda_k = \lambda_0$ *ise*

$$J(\lambda_1, ..., \lambda_k) = -\lambda_k(-1)J(\lambda_1, ..., \lambda_{k-1}) = -\frac{1}{q}G(\lambda_1, \chi) \cdots G(\lambda_k, \chi)$$

5. *Eğer $\lambda_1, ..., \lambda_k$ lerin hepsi aşikar olmayan karakterler ise*

$$|J(\lambda_1, ..., \lambda_k)| = \begin{cases} q^{(k-1)/2}, & \lambda_1 \cdots \lambda_k \neq \lambda_0 \text{ için} \\ q^{(k-2)/2}, & \lambda_1 \cdots \lambda_k = \lambda_0 \text{ için} \end{cases}$$

2. CYCLOTOMY

2.1 Giriş

Cyclotomy, veya çembereşbölüm, (klasik manada) bir çemberi n eşit parçaya ayırma işlemidir. Binlerce yıl önce Yunanlı geometricilerin bir çemberi bir cetvel ve bir pergel yardımıyla eşit parçalara ayırmaya çalışmasıyla başlamıştır (yalnız burada cetvel uzunluk ölçmek için değil sadece iki noktayı birleştirmek için kullanılmaktadır). Bu problem n nin

$$2^s, 3 \cdot 2^s, 5 \cdot 2^s, 15 \cdot 2^s;\ s = 0, 1, 2, ...$$

değerleri için çözülebilmekteydi lakin genel bir çözüm bulunamamıştı. Özellikle 5 ten büyük asal sayılar için çözüm bulma önemli araştırma konularından biriydi. Neden sonra Gauss $n = 17$ için çözüm buldu. Burada 17 nin özelliği, 1 eksiğinin 2^{2^k} formatında olmasıdır (yani Fermat asalı olmasıdır). Zaten problem, problemin çözülebilmesi için gerek ve yeter şart

$$n = 2^s \cdot (2^{2^k} + 1);\ s, t = 0, 1, 2, ... \text{ ve } (2^{2^k} + 1) \text{ asal}$$

olmasıdır, şeklinde tamamlandı.

Modern cebir ve uygulamaları açısından bakıldığında ise cyclotomy bazı matematiksel argümanlar şeklinde karşımıza çıkar, bu bölümde de bu matematiksel argümanlar kısaca tanıtılacaktır.

2.2 Cyclotomic Sınıflar ve Sayılar

g ile $\mathbb{F}_q$ sonlu cisminin bir ilkel elemanı gösterilsin. Ayrıca $q-1 = ef$ olsun ($e, f \in \mathbb{Z}$ ve $e, f \geq 2$).

$$C_j = \{g^{es+j} : s = 0, 1, ..., f-1\}$$

kümelerine **cyclotomic sınıflar** denir.

Cyclotomic sınıflar $\mathbb{F}_q^*$ üzerinde bir parçalanış verir, yani

$$\text{Her } i \neq j \text{ için } C_i \cap C_j = \varnothing \quad \text{ve} \quad \bigcup_{i=0}^{e-1} C_i = \mathbb{F}_q^* \tag{2.2.1}$$

dir. Çünkü C_0 kümesi $\mathbb{F}_q^*$ (çarpımsal) grubunun bir alt grubudur ve $j \neq 0$ için $C_j = g_j C_0$ olacak şekilde $g_1, g_2, ..., g_{f-1} \in \mathbb{F}_q^*$ mevcuttur. Yani parçalanıştaki kümeler, $\mathbb{F}_q^*$ grubunun C_0 altgrubuna bölümüyle üretilmiş yan kümeleridir.

Örnek 22 *Cyclotomic sınıf örnekleri:*

1. $\mathbb{F}_7^*$ *için* $g = 3$ *ve* $e = 2$, $f = 3$ *olsun. Böylelikle* $C_0 = \{3^0, 3^2, 3^4\} = \{1, 2, 4\}$ *ve* $C_1 = \{3^1, 3^3, 3^5\} = \{3, 6, 5\}$ *şeklinde cyclotomic sınıflar belirlenir. Burada* C_0 *ile* C_1 *kümeleri* $\mathbb{F}_7^*$ *nin bir parçalanışını oluştururlar ve* C_0 *kümesi* $\mathbb{F}_7^*$ *nin bir alt grubu olup* $C_1 = 3C_0$ *olur.*

2. *Yine* $\mathbb{F}_7$ *de, g=5 için üçüncü mertebe (e=3) cyclotomic sınıflar* $C_0 = \{1, 6\}, C_1 = \{5, 2\}$ ve $C_1 = \{4, 3\}$ *olur.*

3. *Farklı bir asal için de, örneğin* $\mathbb{F}_{13}$ *de,* $C_0 = \{1, 4, 3, 12, 9, 10\}, C_1 = \{2, 8, 6, 11, 5, 7\}$ *sınıfları örnek olarak verilebilir (*$e = 2$, $f = 6$ *ve* $g = 2$*).*

4. *Asal olmayan bir cisim üzerinden örnek olarak,* $\mathbb{F}_9 = \{a + b\beta : a, b \in \mathbb{F}_3$ *ve* $\beta^2 + 1 = 0\}$ *üzerinde* $e = 2$, $f = 4$ *ve* $g = \beta + 1$ *olmak üzere* $C_0 = \{2\beta, 2, \beta, 1\}$ *ve* $C_1 = \{1 + \beta, 1 + 2\beta, 2 + \beta, 2 + 2\beta\}$ *verilebilir.*

5. *Yine* $\mathbb{F}_9$ *üzerinde,* $\beta^2+1=0$ için $e=4$, $f=2$ *ve* $g=\beta+1$ *olmak üzere* $C_0=\{1,2\}, C_1=\{1+\beta, 2+2\beta\}, C_2=\{2\beta,\beta\}, C_3=\{1+2\beta, 2+\beta\}$ *olur.*

Cyclotomic sayılar, cyclotomic sınıflar kullanılarak şu şekilde tanımlanır:

$$(i,j)_e = |(C_i+1 \cap C_j)|; \quad i,j \in 0,1,2,...,e-1$$

ifadesine e. **mertebeden cyclotomic sayı** denir. e değeri belli olduğunda (i,j) ile de gösterilir, bazen de (i,j) yerine A_{ij} ifadesi kullanılır.

Örnek 23 *Örnek 22 de verilen cyclotomic sınıflar için cyclotomic sayılar hesaplanırsa,*

1. $\mathbb{F}_7$ *de göre belirlenen* $C_0=\{1,2,4\}$, $C_1=\{3,5,6\}$ *sınıfları için* $C_0+1=\{2,3,5\}$ *ve* $C_1+1=\{4,6,0\}$ *olmak üzere ikinci mertebe cyclotomic sayılar*

$$\begin{aligned}
(0,0)_2 &= |C_0+1 \cap C_0| = |\{2,3,5\} \cap \{1,2,4\}| = |\{2\}| &&= 1\\
(0,1)_2 &= |C_0+1 \cap C_1| = |\{2,3,5\} \cap \{3,5,6\}| = |\{3,5\}| &&= 2\\
(1,0)_2 &= |C_1+1 \cap C_0| = |\{4,6,0\} \cap \{1,2,4\}| = |\{4\}| &&= 1\\
(1,1)_2 &= |C_1+1 \cap C_1| = |\{4,6,0\} \cap \{3,5,6\}| = |\{6\}| &&= 1
\end{aligned}$$

olarak belirlenir.

2. *Yine* $\mathbb{F}_7$ *de,* $C_0=\{1,6\}, C_1=\{2,5\}, C_2=\{3,4\}$ *için* $C_0+1=\{2,0\}, C_1+1=\{3,6\}, C_2+1=\{4,5\}$ *olur. Böylelikle*

$$\begin{aligned}
(0,0)_3 &= |C_0+1 \cap C_0| = |\{2,0\} \cap \{1,6\}| = |\varnothing| &&= 0\\
(0,1)_3 &= |C_0+1 \cap C_1| = |\{2,0\} \cap \{2,5\}| = |\{2\}| &&= 1\\
(0,2)_3 &= |C_0+1 \cap C_2| = |\{2,0\} \cap \{3,4\}| = |\varnothing| &&= 0\\
(1,0)_3 &= |C_1+1 \cap C_0| = |\{3,6\} \cap \{1,6\}| = |\{6\}| &&= 1\\
(1,1)_3 &= |C_1+1 \cap C_1| = |\{3,6\} \cap \{2,5\}| = |\varnothing| &&= 0\\
(1,2)_3 &= |C_1+1 \cap C_2| = |\{3,6\} \cap \{3,4\}| = |\{3\}| &&= 1\\
(2,0)_3 &= |C_2+1 \cap C_0| = |\{4,5\} \cap \{1,6\}| = |\varnothing| &&= 0\\
(2,1)_3 &= |C_2+1 \cap C_1| = |\{4,5\} \cap \{2,5\}| = |\{5\}| &&= 1\\
(2,2)_3 &= |C_2+1 \cap C_2| = |\{4,5\} \cap \{3,4\}| = |\{4\}| &&= 1
\end{aligned}$$

olur.

3. $\mathbb{F}_{13}$ için $C_0 = \{1,4,3,12,9,10\}, C_1 = \{2,8,6,11,5,7\}$ *sınıfları verilmişti, bunlar için* $C_0 + 1 = \{2,5,4,0,10,11\}$ *ve* $C_1 + 1 = \{3,9,7,12,6,8\}$ *olup*

$$\begin{aligned}(0,0)_2 &= |C_0 + 1 \cap C_0| = |\{4,10\}| &= 2\\ (0,1)_2 &= |C_0 + 1 \cap C_1| = |\{2,5,11\}| &= 3\\ (1,0)_2 &= |C_1 + 1 \cap C_0| = |\{3,9,12\}| &= 3\\ (1,1)_2 &= |C_1 + 1 \cap C_1| = |\{6,7,8\}| &= 3\end{aligned}$$

olur.

4. $\mathbb{F}_9$ *üzerinde* $(\beta^2 + 1 = 0$ *olmak üzere*$\}$ *verilen* $C_0 = \{2\beta, 2, \beta, 1\}$ *ve* $C_1 = \{1+\beta, 1+2\beta, 2+\beta, 2+2\beta\}$ *için* $C_0 + 1 = \{1+2\beta, 0, 1+\beta, 2\}$ *ve* $C_1 + 1 = \{2+\beta, 2+2\beta, \beta, 2\beta\}$ *olup*

$$\begin{aligned}(0,0)_2 &= |C_0 + 1 \cap C_0| = |\{2\}| &= 1\\ (0,1)_2 &= |C_0 + 1 \cap C_1| = |\{1+\beta, 1+2\beta\}| &= 2\\ (1,0)_2 &= |C_1 + 1 \cap C_0| = |\{\beta, 2\beta\}| &= 2\\ (1,1)_2 &= |C_1 + 1 \cap C_1| = |\{2+\beta, 2+2\beta\}| &= 2\end{aligned}$$

5. $\mathbb{F}_9$ *üzerinde,* $C_0 = \{1,2\}, C_1 = \{1+\beta, 2+2\beta\}, C_2 = \{2\beta, \beta\}, C_3 = \{1+2\beta, 2+\beta\}$ *için* $C_0 + 1 = \{0,2\}, C_1 + 1 = \{2+\beta, 2\beta\}, C_2 + 1 = \{1+2\beta, 1+\beta\}, C_3 + 1 = \{2+2\beta, \beta\}$ *olur ve*

$$\begin{pmatrix} (0,0)_4 & (0,1)_4 & (0,2)_4 & (0,3)_4 \\ (1,0)_4 & (1,1)_4 & (1,2)_4 & (1,3)_4 \\ (2,0)_4 & (2,1)_4 & (2,2)_4 & (2,3)_4 \\ (3,0)_4 & (3,1)_4 & (3,2)_4 & (3,3)_4 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

Bu son örnekte de görüldüğü üzere, ikililerin değerleri bazen (gösterim açısından daha sade olması amacıyla) matris şeklinde gösterilir. Bunun için $(i,j)_e$ sayısı matrisin $i+1$. satır ve $j+1$. sütun elemanı olarak belirtilir ve böylelikle $e \times e$ boyutlu bir matris elde edilir. Bu matrise e**. mertebeden cyclotomic matris** denir. Yukarda belirttilen örneklerin ilk dördü için matris gösterimleri sırasıyla yazılırsa

$$\begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 3 \\ 3 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}$$

matrisleri elde edilir.

Sabit bir q için e. mertebe cyclotomic sınıflar (varsa, yani $e|(q-1)$ ise) tek türlü olarak mevcuttur. Çünkü $\mathbb{F}_q^*$ devirli grup olduğundan, f elemanlı alt grupları (varsa, yani $f|(q-1)$ ise) sadece bir tanedir, yani C_0 tektir. Yalnız ilkel elemanın seçimine bağlı olarak indisler farklılaşabilir (g ilkeli için C_i ile g' ilkeli için C_i farklı kümeler olabilir, $i \neq 0$ ve $g \neq g'$). Aynı şekilde cyclotomic sayılar da tek türlüdür, lakin ilkel elemanın seçimine bağlı olarak cyclotomic matris üzerinde pozisyon değiştirirler.

Örnek 24 $\mathbb{F}_7$ *de,* $g = 5$ *için* $C_0 = \{1, 6\}, C_1 = \{2, 5\}, C_2 = \{3, 4\}$ *ve* $g = 3$ *alındığında* $C_0 = \{1, 6\}, C_1 = \{3, 4\}, C_2 = \{2, 5\}$ *olacaktır, yani* C_1 *ile* C_2 *yer değiştirir. Buna paralel olarak da üçüncü mertebe cyclotomic matiris*

$$\underset{g=5 \text{ için}}{\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}} \quad \underset{g=3 \text{ için}}{\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}}$$

olur. Yani $\mathbb{F}_7$ *de üçüncü mertebeden cyclotomic sınıflar ve sayılar tek türlüdür, yalnız ilkel elemanın seçimine göre indis değiştirirler.*

2.3 Cyclotomic Polinomlar ve Cisimler

Cyclotomy klasik manada bir çemberi n eşit parçaya ayırma işlemidir diye belirtilmişti. Kompleks düzlemde çember birim çember ($z(\theta) = e^{i\theta}; 0 \leq \theta < 2\pi$) olarak düşünülürse problem cebirsel olarak $z^n = 1$ in köklerini ($e^{\frac{2\pi ik}{n}}; k = 0, 1, 2, ..., n-1$), bir başka deyişle birimin köklerini (roots of unity) bulmaya tekabül eder. Dolayısıyla $x^n - 1$ formatındaki polinomların kökleri ve çarpanları cyclotomy nin ilgi alanına girer.

$x^n - 1$ polinomunun kökleri çarpmaya göre bir devirli grup oluşturur. ζ_n ile bu devirli grubun bir üreteci gösterilirse, $\gcd(n,k) = 1$ şartını sağlayan k değerleri için ζ_n^k ler de üreteç olacaktır. Kökleri bu üreteçler olan polinoma da cyclotomic polinom denir. Yani

$$\Phi_n(x) = \prod_{\substack{k=1 \\ \gcd(n,k)=1}}^{n} x - \zeta_n^k$$

ifadesine n. **mertebeden cyclotomic polinom** denir.

Böylelikle

$$\begin{aligned}
\Phi_1(x) &= x - 1 \\
\Phi_2(x) &= x + 1 \\
\Phi_3(x) &= x^2 + x + 1 \\
\Phi_4(x) &= x^2 + 1 \\
\Phi_5(x) &= x^4 + x^3 + x^2 + x + 1 \\
\Phi_6(x) &= x^2 - x + 1 \\
\Phi_7(x) &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\
\Phi_8(x) &= x^4 + 1 \\
\Phi_9(x) &= x^6 + x^3 + 1 \\
&\vdots
\end{aligned}$$

şeklinde cyclotomic polinomlar elde edilir. Bu polinomlar için derece$(\Phi_n(x)) = \phi(n)$ dir. (ϕ burada Euler-totient fonksiyonunu gösteriyor, yani $\phi(n) = |\{k \in \mathbb{N} : 1 \leq k \leq n \text{ ve ebob}(n,k) = 1\}|$)

Dikkat edilirse $\Phi_1(x) = x - 1$ olmak üzere

$$\prod_{\substack{k|n \\ 1 \leq k \leq n}} \Phi_k(x) = x^n - 1$$

olduğu görülür.

Cyclotomic polinomlar (her mertebeden) tek türlü olarak mevcuttur ve rasyonel sayılar cismi üzerinde indirgenemezdirler.

n. dereceden birimin köklerinin bir üreteci bir cisme eklendiğinde oluşan cisim genişlemesine cyclotomic cisim denir. Yani, F bir cisim ve $\zeta_n = e^{2\pi i/n}$ olmak üzere

$$F(\zeta_n) = \{\sum_{i=0}^{n-1} a_i(\zeta_n)^i : a_0, a_1..., a_{n-1} \in F\}$$

şeklinde inşa edilen cisme **cyclotomic cisim** denir. Özetle, bir cismin $x^n - 1$ polinomuna göre parçalanış cismine (splitting field'ına) cyclotomic cisim denir.

Cyclotomic cisimler, üzerinde tanımlandıkları cisim üzerinde bir vektör uzayı oluştururlar. Bu vektör uzayının boyutuna genişleme derecesi denir ve $[F(\zeta_n) : F]$ ile gösterilir.

Bir cismin $x^n - 1$ ile oluşturulan parçalanış cismi ile $\Phi_n(x)$ ile oluşturulan parçalanış cismi aynıdır, dolayısıyla cyclotomic cisim tanımı cyclotomic polinomlar üzerinden de verilebilir. Çünkü, $\Phi_n(x)$ in kökleri $x^n - 1$ in kökleriyle oluşturulan (çarpımsal) grubun üreteçleridir, dolayısıyla $x^n - 1$ in her kökü $\Phi_n(x)$ nin kökleriyle üretilebilir. Böylelikle, rasyonel sayılar üzerinde cyclotomic polinomlar indirgenemez olduğundan, rasyonel sayılardaki cyclotomic cisimler için $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$ olduğu görülür.

Örnek 25 *Rasyonel sayılar cismi üzerinden cyclotomic cisimler:*

1. $\mathbb{Q}$ *üzerinde* $x^2 - 1$ *in parçalanış cismi yine* $\mathbb{Q}$ olur *(*$x^2 - 1$ *in kökleri yine rasyonel sayılar). Yani* $[\mathbb{Q}(\zeta_2) : \mathbb{Q}] = 1$ *ve* $\mathbb{Q}(\zeta_2) = \mathbb{Q}$ *dir.*

2. $\mathbb{Q}$ *üzerinde* $x^3 - 1$ *in parçalanış cismi (*$\zeta_3 = (-1 + i\sqrt{3})/2$ *olmak üzere)* $\mathbb{Q}(\zeta_3) = \{a + b\zeta_3 : a, b \in \mathbb{Q}\}$ *cismidir,* $x^4 - 1$ *in parçalanış cismi ise (*$\zeta_4 = i$ *olduğu için)* $\mathbb{Q}(\zeta_4) = \{a + bi : a, b \in \mathbb{Q}\}$ *cismidir, yalnız burada* $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = [\mathbb{Q}(\zeta_4) : \mathbb{Q}] = 2$ *olmasına rağmen* $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] \neq [\mathbb{Q}(\zeta_4) : \mathbb{Q}]$ *olduğuna dikkat etmek gerekiyor.*

3. $\mathbb{Q}$ *üzerinde* $x^5 - 1$ *in parçalanış cismi* $\mathbb{Q}(\zeta_5) = \{a + b\zeta_5 + c\zeta_5^2 + d\zeta_5^3 + e\zeta_5^4 : a, b, c, d, e \in \mathbb{Q}\}$ dir ve $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 4$ tür.

4. $\mathbb{Q}$ *üzerinde* x^6-1 *in parçalanış cismi (*$\zeta_6 = (1+i\sqrt{3})/2$ *olmak üzere)* $\mathbb{Q}(\zeta_6) = \{a + b\zeta_6 : a, b \in \mathbb{Q}\}$ *cismidir, ayrıca* $\mathbb{Q}(\zeta_3)$ *cismi bu cismin altcismidir. Burada da yine* $[\mathbb{Q}(\zeta_6) : \mathbb{Q}] = 2$ *olduğu görülür.*

Örnek 26 *Sonlu bir cisim üzerinden örnek:* $F = \mathbb{F}_2$ *cisminin* $x^3 - 1$ *ile oluşturulan parçalanış cismi* $\mathbb{F}_4$ *olurken* $x^4 - 1$ *ile oluşturulan parçalanış cismi kendisi olur. Yani* $[\mathbb{F}_2(\zeta_4) : \mathbb{F}_2] = 1$ *olup* $\phi(4)$ *ten farklıdır. Dolayısıyla cyclotomic cisimlerin* $F = \mathbb{Q}$ *durumundan farklı olduğu görülür. Bunun sebebi cyclotomic polinomların sonlu cisimlerde her zaman indirgenemez olmak zorunda olmamasıdır. Mesela bu örnekte* $\Phi_4(x) = (x - 1)^4$ *dir.*

3. CYCLOTOMIC SAYILAR

Bölüm 2.2 de verilen cyclotomic sayı tanımına denk olarak şöyle bir tanım da verilebilir: $q = ef + 1$ için e. **mertebeden cyclotomic sayı** $(i, j)_e$

$$z_i + 1 = z_j,\ z_i \in C_i \text{ ve } z_j \in C_j \tag{3.0.1}$$

denkleminin köklerinin sayısıdır, yani

$$g^{es+i} + 1 = g^{et+j};\ 0 \leq s, t \leq f - 1 \tag{3.0.2}$$

denklemini sağlayan (s, t) ikililerinin sayısıdır. Bu bölümde bu tanım kullanılarak cyclotomic sayıların özellikleri incelenecek ve hesaplamada kullanılan yöntemlerden bahsedilecektir.

3.1 Temel Özellikler

Örnek 23 deki cyclotomic matrisler

$$\begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix},\ \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix},\ \begin{pmatrix} 2 & 3 \\ 3 & 3 \end{pmatrix},\ \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix},\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

idi. Bu matrislerin satır elemanlarının toplamına, sütun elemanlarının toplamına, elemanların hanelerdeki dağılımına vs. dikkat edilirse belirli bir düzen olduğu

düşünülebilir, bunun matematiksel boyutu araştırıldığında karşımıza şu önemli teorem çıkar.

Teorem 27 [2, 4]

1. *Her* K, L *tamsayıları için* $(i + Ke, j + Le)_e = (i, j)_e$
2. $(i, j)_e = (e - i, j - i)_e$
3. $(i, j)_e = \begin{cases} (j, i)_e, & f \text{ çift için} \\ (j + \frac{e}{2}, i + \frac{e}{2})_e, & f \text{ tek için} \end{cases}$
4. $\sum_{j=0}^{e-1} (i, j)_e = f - \theta_i;\ \theta_i = \begin{cases} 1, & f \text{ çift ve } i = 0, \text{ veya } f \text{ tek ve } i = \frac{e}{2} \text{ için} \\ 0, & \text{diğer durumlar için} \end{cases}$
5. $\sum_{i=0}^{e-1} (i, j)_e = \begin{cases} f - 1, & j = 0 \text{ için} \\ f, & \text{diğer durumlar için} \end{cases}$
6. $(i, j)'_e = (Ni, Nj)_e$, *Üs işareti ilkel eleman olarak* g^N *alındığını belirtiyor*

İspat: (3.0.2) eşitliği göz önüne alındığında

1. Tanımdan aşikar olarak çıkar.
2. Eşitliğin iki tarafı da ilk terimin tersiyle, yani $g^{e(f-s-1)+e-i}$ ile çarpılırsa eşitlik
$$1 + g^{e(f-s-1)+(e-i)} = g^{e(t-s)+(j-i)}$$
halini alır.
3. $\mathbb{F}_q$ cisminde $-1 = g^{(q-1)/2}$ dir. Burada da (f çiftse $k = 0$, f tekse $k = e/2$ olmak üzere) $-1 = g^{ev+k}$ olacak şekilde bir v tamsayısının mevcut olduğu görülebilir. Şimdi g^{ev+k} ile (3.0.2) eşitliğin iki tarafı da çarpılırsa,
$$g^{e(t+v)+(j+k)} + 1 = g^{e(s+v)+(i+k)}$$
olur. Bu da (f nin teklik - çiftlik durumuna göre) k nın alacağı değerlerle bize istediğimiz sonucu verir.

4. Cyclotomic sınıfların $\mathbb{F}_q^*$ üzerinde bir parçalanış verdiği (2.2.1) den biliniyor, dolayısıyla C_j ler ikili olarak ayrık olur, o zaman C_j lerin sabit bir kümeyle kesişimi de ayrık olur, ayrıca ayrık kümelerin eleman sayıları toplamı da bileşimlerinin eleman sayısıdır. $|C_i| = f$ olduğu da dikkate alınarak

$$\begin{aligned}
\sum_{j=0}^{e-1}(i,j)_e &= |(C_i+1)\cap C_0| + |(C_i+1)\cap C_1| \cap ... |(C_i+1)\cap C_{f-1}| \\
&= \left|\bigcup_{j=0}^{f-1}((C_i+1)\cap C_j)\right| \\
&= |(C_i+1)\cap \bigcup_{j=0}^{f-1} C_j| \\
&= \left|(C_i+1)\cap \mathbb{F}_q^*\right| \\
&= \begin{cases} f-1, & -1 \in C_i \\ f, & -1 \notin C_i \end{cases} \\
&= \begin{cases} f-1, & f \text{ çift ve } i=0, \text{ veya } f \text{ tek ve } i=\frac{e}{2} \text{ için} \\ f, & \text{diğer durumlar için} \end{cases}
\end{aligned}$$

olur.

5. Bir önceki adımdakine benzer mantıkla

$$\begin{aligned}
\sum_{i=0}^{e-1}(i,j)_e = ... &= \begin{cases} f-1, & 1 \in C_j \\ f, & 1 \notin C_j \end{cases} \\
&= \begin{cases} f-1, & j \neq 0 \text{ için} \\ f, & \text{diğer durumlar için} \end{cases}
\end{aligned}$$

6. (3.0.2) denkleminde g yerine g^N yazıldığında görülür.

■

Teorem 27 deki özellikler kullanılarak ikinci mertebe cyclotomic sayılar şu şekilde inşa edilebilir: İkinci özellik $(1,0)_2 = (1,1)_2$ olduğunu söyler, üçüncü özellik sayesinde f tek için $(1,0)_2 = (0,1)_2$ ve f çift için $(0,0)_2 = (1,1)_2$ olur, böylelikle ikinci mertebeden cyclotomic matris

$$f \text{ çift ise } \begin{pmatrix} A & B \\ B & B \end{pmatrix}, \; f \text{ tek ise } \begin{pmatrix} B & A \\ B & B \end{pmatrix}$$

halini alır. Dördüncü özellikle beraber

$$f \text{ çift ise } \begin{cases} A+B & = f-1 & = \frac{q-3}{2} \\ 2B & = f & = \frac{q-1}{2} \end{cases}$$
$$f \text{ tek ise } \begin{cases} A+B & = f & = \frac{q-1}{2} \\ 2B & = f-1 & = \frac{q-3}{2} \end{cases}$$

olur. Bu sonuçlar birleştirilip sade bir halde yazılırsa:

Teorem 28 *İkinci mertebeden cyclotomic sayılar, $q = 2f+1$ olmak üzere*

$$\begin{aligned} (0,0)_2 &= \tfrac{q-4-(-1)^f}{4} \\ (0,1)_2 &= \tfrac{q-(-1)^f}{4} \\ (1,0)_2 = (1,1)_2 &= \tfrac{q-2+(-1)^f}{4} \end{aligned} \tag{3.1.1}$$

şeklinde belirlenir.

3.2 Gauss Periyotları ve Cyclotomic Sayılar

χ kanonik toplamsal karakteri göstermek üzere, **Gauss periyotları**

$$\eta_i = \sum_{x \in C_i} \chi(x), \quad i = 0, 1, 2, ..., f-1$$

şeklinde tanımlanan toplamlardır.

Lemma 29 [4] *Gauss periyotları ile cyclotomic sayılar arasındaki ilişki:*

$$\eta_m \eta_{m+k} = \sum_{h=0}^{e-1} (k,h)\eta_{m+h} + f\theta_k; \ \theta_k = \begin{cases} 1, & f \text{ çift ve } k=0, \text{ veya } f \text{ tek ve } k = \frac{e}{2} \\ 0, & \text{diğer durumlarda} \end{cases}$$

3.2.1 Bir Uygulama: Üçüncü Mertebeden Cyclotomic Sayıların Hesaplanması

$q = 3f + 1$ durumunda f mecburen çift olacağından Teorem 27 deki ikinci ve üçüncü özelliklerle üçüncü mertebe cyclotomic matrisin

$$\begin{pmatrix} A & B & C \\ B & C & D \\ C & D & B \end{pmatrix} \tag{3.2.1}$$

formatında olacağı görülür. Dördüncü özellikle

$$\begin{aligned} A + B + C &= f - 1 \\ B + C + D &= f \end{aligned} \tag{3.2.2}$$

denklemleri elde edilir. A,B,C,D yi tek türlü olarak belirlemek için bu iki denklem yeterli olmayacaktır. Bu yüzden, örneğin

$$1 + z_0 + z_1 + z_2 = 0 \ (z_i \in C_i, \ i = 0, 1, 2) \tag{3.2.3}$$

denkleminin çözüm sayısından yararlanılabilir [4].

(3.2.3) denkleminin çözüm sayısı N olsun. Burada z_0, f tane C_0 elemanı üzerinde gezerken $1 + z_0$ değeri de A kez C_0 ın içinde, B kez C_1 in içinde ve C kez C_2 nin içinde bulunacaktır. Her bir sabit $z_i' \in C_i$, $z_i' = z_0 + 1$ için (3.2.3) nın çözümünü sağlayan (z_1, z_2) lerin sayısı ise sırasıyla D, B, C olacaktır; örneğin, sabit bir $z_1' \in C_1$ için $z_1' + z_1 + z_2 = 0$ eşitliğini sağlayan B tane (z_1, z_2) ikilisi vardır, çünkü $z_1' + z_1 + z_2 = 0$ nın çözüm sayısı ile $z_1(z_1')^{-1} + 1 = z_2(z_1')^{-1}$ denkleminin çözüm sayısı aynıdır ($e = 3$ için $-1 \in C_0$ olduğundan $-z_2 \in C_2$ ve $z_i(z_1')^{-1} \in C_{i-1}$). Sonuç olarak $N = AD + B^2 + C^2$ elde edilir.

Şimdi de z_1, C_1 üzerinde gezsin, aynı zamanda $1+z_0$ değeri de B kez C_0 ın içinde, C kez C_1 in içinde ve D kez C_2 nin içinde bulunacaktır. Yine her bir sabit $z_i' \in C_i$, $z_i = z_0+1$ için (3.2.3) nın çözümünü sağlayan (z_0, z_2) lerin sayısı sırasıyla C, D, B olacaktır, sonuçta $N = BC + CD + BD$ olduğu görülür.

Bu iki sonuç birleştirilirse

$$AD + B^2 + C^2 = BC + CD + BD \tag{3.2.4}$$

olur. (3.2.2) denklemleri kullanılarak

$$D = A + 1$$
$$C = f - 1 - A - B$$

elde edilir ve bunlar (3.2.4) de yerine konulursa

$$3A^2 + 3AB + 3B^2 - (3f - 5)A - (3f - 3)B = -f^2 + 3f - 2$$

sonucuna ulaşılır. Bu eşitliğin iki tarafı da 36 ile çarpılıp gerekli sadeleştirmeler yapılırsa

$$(9A - 3f + 7)^2 + 27(f - 1 - A - 2B)^2 = 12f + 4 = 4q$$

veya daha sade şekilde $4q = c^2 + 27d^2$, c$\equiv 1 (\mathrm{mod}\, 3)$ elde edilir (burada d nin işareti ilkel elemana bağlıdır). Dolayısıyla (3.2.2) denklemlerine ek olarak ($4q = c^2 + 27d^2$ ve $c \equiv 1 (\mathrm{mod}\, 3)$ olmak üzere)

$$\begin{aligned} 9A &= 3f - 7 + c \\ A + 2B &= f - 1 - d \end{aligned} \tag{3.2.5}$$

denklemleri elde edilir. Hesaplanırsa

Teorem 30 [4] *Üçüncü mertebeden cyclotomic sayılar için cyclotomic matris*

$$\begin{pmatrix} A & B & C \\ B & C & D \\ C & D & B \end{pmatrix}$$

formatındadır ve buradaki A, B, C, D *sayıları* $4q = c^2 + 27d^2, c \equiv 1 (\mathrm{mod}\, 3)$ *özelliklerini sağlayan bir* (c, d) *ikilisiyle*

$$\begin{aligned} 9A &= q - 8 + c \\ 18B &= 2q - 4 - c - 9d \\ 18C &= 2q - 4 - c + 9d \\ 9D &= q + 1 + c \end{aligned} \tag{3.2.6}$$

şeklinde elde edilir (d nin işareti ilkel elemanın seçimine bağlıdır).

Örnek 31 $\mathbb{F}_7$ *için hesaplayınca* $(c,d) = (1,\pm 1)$ *bulunur. Örnek 24 de ilkel elemanın seçimine göre iki farklı üçüncü mertebe cyclotomic matris verilmişti. İlkel eleman* 5 *alınırsa üçüncü mertebeden cyclotomic matris*

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

olur, yani $d = -1$ *dir. Ama ilkel elemanı* 3 *aldığımızda*

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

olur ($d = 1$ *dir). Yani* B *ile* C *yer değiştirir (birinde* d *yi eklerken diğerinde çıkarılıyor (3.2.6) denklemlerinde).*

Yalnız acaba her q değeri için $4q = c^2 + 27d^2, c \equiv 1 (\mathrm{mod}\, 3)$ olacak şekilde (c,d) ikilileri mevcut mudur, mevcutsa kaç tanedir? Bu problem için, yani $q = p^m \equiv 1 (\mathrm{mod}\, 3)$ durumunda, en az bir $(c,d) \in \mathbb{Z}^2$ ikilisi vardır, hatta $m = 1$ ise bu ikililerin sayısı (d yi işaretinden bağımsız düşünüldüğünde) tam olarak bir tanedir [4]. Dolayısıyla $m = 1$ için üçüncü mertebeden cyclotomic sayılar, cyclotomic sınıfları inşa etmeye veya (3.0.2) denklemlerini çözmeye gerek kalmadan $4q = c^2 + 27d^2, c \equiv 1 (\mathrm{mod}\, 3)$ sisteminin mevcut olan tek çözümüyle oluşturulabilir (ilkel elemanın seçiminden bağımsız olarak). Peki $m > 1$ iken $4q = c^2 + 27d^2, c \equiv 1 (\mathrm{mod}\, 3)$ sisteminin birden fazla (c,d) tamsayı çözümü olması durumunda hangi çözüm tercih edilmelidir? Bunun cevabına $p \equiv 1 (\mathrm{mod}\, 3)$ ve $p \equiv 2 (\mathrm{mod}\, 3)$ durumu için ayrı ayrı bakmak gerekmektedir.

$p \equiv 1 (\mathrm{mod}\, 3)$ **için:** Bu durumda (c,d) ikililerinden **has** (proper) çözüm (yani obeb$(q, |c|) = 1$ şartını sağlayacak (c,d) çözümleri) tercih edilmelidir [4]. p$\equiv 1 (\mathrm{mod}\, 3)$ durumunda has çözüm bir tane olacağından [4] üçüncü mertebeden cyclotomic sayılar tam olarak belirlenebilir.

Örnek 32 $\mathbb{F}_{343} = \mathbb{F}_7(\theta)$, $\theta^3 + 3\theta + 2 = 0$ *cismi üzerinde üçüncü mertebe cyclotomic sayılar incelendiğinde,* $1372 = c^2 + 27d^2$ *denklemi için* $(c,d) =$

$(\pm 7, \pm 7)$ *ve* $(c,d) = (\pm 20, \pm 6)$ *ikilileri birer çözümdür,* $c \equiv 1 (\mathrm{mod}\, 3)$ *şartıyla bu çözümler* $(c,d) = (7, \pm 7)$ *ve* $(c,d) = (-20, \pm 6)$ *haline gelir. Bu cismin üçüncü mertebe cyclotomic matrisi ise, ilkel elemanın tercihine göre*

$$\begin{pmatrix} 35 & 36 & 42 \\ 36 & 42 & 36 \\ 42 & 36 & 36 \end{pmatrix} \quad veya \quad \begin{pmatrix} 35 & 42 & 36 \\ 42 & 36 & 36 \\ 36 & 36 & 42 \end{pmatrix}$$

olacaktır. Bu matrisleri oluşturabilmek için, (3.2.6) denklemlerinde kullanılabilecek (c,d) *ikilisi* $(-20, \pm 6)$ *dir. Yani* $(c,d) = (7, \pm 7)$ *çözümü kullanışsız olacaktır. Burada dikkat edilirse* $(-20, \pm 6)$ *çözümü* $obeb(q, |c|) = obeb(343, 20) = 1$ *olduğundan has bir çözümdür, ama* $(c,d) = (7, \pm 7)$ *çözümü has çözüm değildir.*

$p \equiv 2 (\mathrm{mod}\, 3)$ **için:** Bu durum için (c,d) ikilisini tespit ederken Gauss periyotları ile cyclotomic sayılar arasındaki ilişkidenfaydalanılacaktır. Ayrıca belirtilmelidir ki $q = p^m \equiv 1 (\mathrm{mod}\, 3)$ olması gerektiğinden m çifttir.

Lemma 33 [5] $p \equiv 2 (\mathrm{mod}\, 3)$ *ve* m *çift sayı olsun.* $q = p^m$ *olmak üzere,* $\mathbb{F}_q$ *üzerinde üçüncü mertebe Gauss periyotları*

$$\eta_0 = \frac{-1+2(-1)^{(m-2)/2}\sqrt{q}}{3}$$
$$\eta_1 = \eta_2 = \frac{-1-(-1)^{(m-2)/2}\sqrt{q}}{3}$$

şeklindedir.

Şimdi bu Lemmalar ile, cyclotomic sayılar yerine (3.2.1) te verilen harfler kullanıldığında

$$\begin{aligned} \eta_0\eta_1 &= B\eta_0 + C\eta_1 + D\eta_2 \\ \eta_0\eta_2 &= C\eta_0 + D\eta_1 + B\eta_2 \end{aligned}$$

elde edilir, bu da $\eta_0 \neq \eta_1 = \eta_2$ olduğundan

$$\begin{aligned} \eta_0\eta_1 &= B\eta_0 + C\eta_1 + D\eta_1 \\ &= C\eta_0 + D\eta_1 + B\eta_1 \end{aligned}$$

haline gelir, düzenleme yapılınca

$$(\eta_0 - \eta_1)(B - C) = 0$$

olacaktır, yani $B = C$ dir. O zaman 3.2.6 denklemleri dikkate alındığında $d = 0$ olduğu görülür. Dolayısıyla $c = 2\sqrt{q}$ olur.

Örnek 34 $\mathbb{F}_{25} = \mathbb{F}_5(\theta)$, $\theta^2 + \theta + 2 = 0$ *üzerinde* $g = \theta$ *yı kullanılarak üçüncü mertebe cyclotomic sayılar hesaplandığında matrisin*

$$\begin{pmatrix} 3 & 2 & 2 \\ 2 & 2 & 4 \\ 2 & 4 & 2 \end{pmatrix}$$

olduğu görülür. Burada $A = 2$, $B = C = 2$, $D = 4$ *olup* $c = 2\sqrt{25} = 10$ *ve* $d = 0$ *dır.*

3.3 Jacobi Toplamları ve Cyclotomic Sayılar

g ile $\mathbb{F}_q$ nun bir ilkel elemanı, ζ ile $e.$ birim kök ve ψ ile $\mathbb{F}_q$ üzerinde tanımlı $e.$ mertebeden bir çarpımsal karakter gösterilsin ($\psi(g) = \zeta = \exp(2\pi i/e)$).

$$J(\psi^i, \psi^j) = \sum_{\alpha \in \mathbb{F}_q} \psi^i(\alpha)\psi^j(1-\alpha); \quad 0 \le i, j \le e-1$$

şeklinde verilen ikili Jacobi toplamı için,

Teorem 35 [6]*Jacobi toplamı ile e. mertebeden cyclotomic sayılar arasında*

$$e^2(s,t)_e = \sum_{i=0}^{e-1}\sum_{j=0}^{e-1}(-1)^{if}\zeta^{-(si+tj)}J(\psi^i, \psi^j)$$
$$J(\psi^u, \psi^v) = \sum_{i=0}^{e-1}\sum_{j=0}^{e-1}\zeta^{ui+vj}(i,j)$$

bağıntısı vardır.

İspat: C_i ile $\mathbb{F}_q^*$ nun g ile üretilmiş e. mertebe cyclotomic sınıfını göstermek üzere, üstteki ifade

$$\begin{aligned}
\sum_{i=0}^{e-1}\sum_{j=0}^{e-1}(-1)^{if}\zeta^{-(si+tj)}J(\psi^i,\psi^j) &= \sum_{i=0}^{e-1}\sum_{j=0}^{e-1}\psi^i(-1)\zeta^{-(si+tj)}\sum_{\alpha\in\mathbb{F}_q}\psi^i(\alpha)\psi^j(1-\alpha)\\
&= \sum_{i=0}^{e-1}\sum_{j=0}^{e-1}\sum_{\alpha\in\mathbb{F}_q}\psi^i(g^{-s}(-\alpha))\psi^j(g^{-t}(1-\alpha))\\
&= \sum_{i=0}^{e-1}\sum_{j=0}^{e-1}\sum_{\alpha\in\mathbb{F}_q}\psi^i(g^{-s}\alpha)\psi^j(g^{-t}(1+\alpha))\\
&= \sum_{\alpha\in\mathbb{F}_q}\left(\sum_{i=0}^{e-1}\psi^i(g^{-s}\alpha)\sum_{j=0}^{e-1}\psi^j(g^{-t}(\alpha+1))\right)\\
&= \sum_{\alpha\in\mathbb{F}_q}\left\{\begin{array}{ll} 0, & \alpha=0 \text{ veya } \alpha\notin C_s\\ e, & \alpha\in C_s\end{array}\right\}\\
&\qquad\times\left\{\begin{array}{ll} 0, & \alpha+1=0 \text{ veya } \alpha+1\notin C_t\\ e, & \alpha+1\in C_t\end{array}\right\}\\
&= \sum_{\alpha\in\mathbb{F}_q}\left\{\begin{array}{ll} e^2, & \alpha\in C_s \text{ ve } \alpha+1\in C_t\\ 0, & \text{diğer}\end{array}\right\}\\
&= e^2(s,t)_e
\end{aligned}$$

şeklinde ispatlanır. Alttaki ifade ise Sonlu Fourier Dönüşümü ile gösterilir. ■

3.3.1 Bir Uygulama: Dördüncü Mertebeden Cyclotomic Sayıların Hesaplanması

Öncelikle Teorem 27 den dördüncü mertebe cyclotomic matrisin

$$\overset{f \text{ tek ise}}{\begin{pmatrix} A & B & C & D\\ E & E & D & B\\ A & E & A & E\\ E & D & B & E\end{pmatrix}},\quad \overset{f \text{ çift ise}}{\begin{pmatrix} A & B & C & D\\ B & D & E & E\\ C & E & C & E\\ D & E & E & B\end{pmatrix}}$$

olduğu görülür. Ayrıca, g ifadesi $\mathbb{F}_q$ nun bir ilkel kökü ve $q=4f+1$ olmak üzere,

$$q = a + 4b^2,\ a \equiv 1 (\mathrm{mod}\, 4),\ 2b = ag^{(q-1)/4}$$

şartını sağlayan a ve b tamsayıları için $J(\psi^u, \psi^v)$ Jacobi toplamları,

u\v	**0**	**1**	**2**	**3**
0	q	0	0	0
1	0	$(-1)^f(a+2bi)$	$a+2bi$	$-(-1)^f$
2	0	$a+2bi$	-1	$a-2bi$
3	0	$-(-1)^f$	$a-2bi$	$(-1)^f(a-2bi)$

şeklinde belirlenir [2, 4]. $\psi(g) = \zeta = \exp(2\pi i/4) = i$ olduğunu dikkate alarak hesaplandığında,

f tek ise			f çift ise		
A	$=$	$q-7+2a$	A	$=$	$q-11+6a$
B	$=$	$q+1+2a-8b$	B	$=$	$q-3+2a+8b$
C	$=$	$q+1-6a$	C	$=$	$q-3+2a$
D	$=$	$q+1+2a+8b$	D	$=$	$q-1+2a-8b$
E	$=$	$q-3-2a$	E	$=$	$q+1-2a$

çıkar.

3.4 Mertebesi Tek Asal Olan Cyclotomic Sayılar ($q = p^n,\ p \equiv 1 (\mathrm{mod}\, e)$ İçin)

Teorem 36 [7]*e bir tek asal, ω_e ifadesi e. dereceden birim kök, $p \equiv 1 (\mathrm{mod}\, e)$ olsun. $(k, e) = 1$ için σ_k, $\mathbb{Q}(\omega_e)$ nin $\omega_e \longmapsto \omega_e^k$ olacak şekildeki otomorfizması olsun. $\lambda(r)$, $r (\mathrm{mod}\, e)$ nin en küçük negatif olmayan tamsayı değerini göstersin. $1 \le m \le e-2$ sabit bir tamsayı olsun. α, bir ilkel eleman olmak üzere $b = \alpha^f$ olsun. $H = \sum_{i=0}^{e-1} a_i \omega_e^i \in \mathbb{Z}[\omega_e]$ olsun.*

1. $p^n = \sum_{i=0}^{e-1} a_i^2 - \sum_{i=0}^{e-1} a_i a_{i+1}$,

2. $\sum_{i=0}^{e-1} a_i a_{i+1} = \sum_{i=0}^{e-1} a_i a_{i+2} = \sum_{i=0}^{e-1} a_i a_{i+(e-1)/2}$

3. $1 + a_0 + a_1 + ... + a_{e-1} = 0 (\mathrm{mod}\, e)$

4. $a_1 + 2a_2 + ... + (e-1)a_{e-1} = 0 (\mathrm{mod}\, e)$

5. $p \nmid \prod_{\lambda((m+1)k)>k} H^{\sigma_k}$

6. $p \mid \bar{H} \prod_{\lambda((m+1)k)>k} (b - \omega_e^{\sigma_{k^{-1}}})$

şartları sağlansın (Burada $\bar{H}$ ile H nin kompleks eşleniği belirtilmektedir, k^{-1} değeri de $(\mathrm{mod}\, e)$ *de hesaplanmıştır). O zaman bu α ilkeli için $H = J(1, m)$ olur. Bu önermenin diğer yönü de doğrudur.*

Bu teoremle elde edilen $J(1, m)$ ile, Jacobi toplamının özellikleri kullanılarak $J(m, n)$ değerleri bulunur ve Jacobi toplamları ile cyclotomic sayılar arasındaki ilişki kullanılarak cyclotomic sayılar hesaplanır. Yalnız bu teoremde sadece q değerinin değil aynı zamanda p değerinin de $\equiv 1 (\mathrm{mod}\, e)$ olması gerektiğine dikkat edilmelidir. Örneğin $e = 5$ için $\mathbb{F}_{11^2}$ üzerinde bu teorem kullanılabilir ama $\mathbb{F}_{7^4}$ üzerinde kullanılamaz, çünkü $11 \equiv 1 (\mathrm{mod}\, 5)$ iken $7 \not\equiv 1 (\mathrm{mod}\, 5)$ dir.

Bu teoreme benzer şekilde, (e tek asal olmak üzere) mertebesi $2e$ için olan cyclotomic sayılar için ilgili teoremler [8] de verilmiştir.

3.4.1 Bir Uygulama: Beşinci Mertebeden Cyclotomic Sayılarda $p \equiv 1 (\mathrm{mod}\, 5)$ Durumu

Beşinci mertebeden cyclotomic matris, Teorem 27 kullanılarak şu şekilde oluşturulur:

$$\begin{pmatrix} A & E & D & C & B \\ E & B & F & G & F \\ D & F & C & G & G \\ C & G & G & D & F \\ B & F & G & F & E \end{pmatrix}$$

Burada belirtilen A, B, C, D, E, F, G sayıları için $p \equiv 1 (\mathrm{mod}\, 5)$ durumunda Teorem 36 kullanılabilir. Hesaplandığında,

$$\begin{aligned} 25A &= p^n + 3a - 14 \\ 100B &= 4p^n - 3a + 25d + 50c - 16 \\ 100C &= 4p^n - 3a - 25d + 50b - 16 \\ 100D &= 4p^n - 3a - 25d - 50b - 16 \\ 100E &= 4p^n - 3a + 25d - 50c - 16 \\ 50F &= 2p^n + a - 25d + 2 \\ 50G &= 2p^n + a + 25d + 2 \end{aligned}$$

çıkar. Buradaki a, b, c, d sayıları $a^2 + 125d^2 + 50b^2 + 50c^2 = 16q$, $c^2 - 4bc - b^2 = ad$, $a \equiv 1 (\mathrm{mod}\, 5)$ sisteminin çözümüdür.

3.5 Kullanışlı bir Durum: Uniform Cyclotomy

Baumert ve Mills [9] $p \not\equiv 1 (\mathrm{mod}\, e)$ durumunda bazı özel şartlar altında kullanışlı bir teorem vermişlerdir.

Eğer $p^t \equiv -1 (\mathrm{mod}\, e)$ olacak şekilde bir t tamsayısı mevcut ise $\mathbb{F}_{p^n}$ üzerinde e. mertebeden cyclotomic sayılar **uniform**dur.

Teorem 37 [9] $\mathbb{F}_{p^n}$ *üzerinde* e. *mertebe cyclotomic sayılar uniform olsun. Bu durumda ya* p *ya da* f *çifttir, ayrıca* n *değeri de çifttir. Üstelik* $\eta = \frac{p^{n/2}-1}{e}$, $p^{n/2} \equiv 1 (\mathrm{mod}\, e)$ *olmak üzere*

$$\begin{aligned}
(0,0) &= \eta^2 - (e-3)\eta - 1 \\
(0,i) = (i,0) = (i,i) &= \eta^2 + \eta, \quad i \neq 0 \text{ için} \\
(i,j) &= \eta^2, \quad 0 \neq i \neq j \neq 0 \text{ için}
\end{aligned}$$

şeklindedir.

Bu teorem cyclotomic sayıları 3 şekilde belirlediği için hesaplamada büyük kolaylık sağlar.

3.5.1 Bir Uygulama: Beşinci Mertebeden Cyclotomic Sayılarda $p \not\equiv 1 (\mathrm{mod}\, 5)$ Durumu

$p \not\equiv 1 (\mathrm{mod}\, 5)$ iken baktığımızda,

$$\begin{aligned}
p \equiv 2 (\mathrm{mod}\, 5) \text{ ise} \quad & 2^t \equiv -1 (\mathrm{mod}\, 5) \text{ olacak şekilde } t = 2 \\
p \equiv 3 (\mathrm{mod}\, 5) \text{ ise} \quad & 3^t \equiv -1 (\mathrm{mod}\, 5) \text{ olacak şekilde } t = 2 \\
p \equiv 4 (\mathrm{mod}\, 5) \text{ ise} \quad & 4^t \equiv -1 (\mathrm{mod}\, 5) \text{ olacak şekilde } t = 1
\end{aligned}$$

olduğundan hepsinin uniform cyclotomic olduğu görülür ve Teorem 37 in hipotezlerinin sağlandığı durumlar için belirtilen şekilde hesaplama yapılabilir. Uniformluk durumunda $B = C = D = E$ ve $F = G$ dir ve $\sqrt{q} \equiv 1 (\mathrm{mod}\, 5)$ için

$$\begin{aligned}
25A = &\quad q - 12\sqrt{q} - 14 \\
25B = &\quad q + 3\sqrt{q} - 4 \\
25F = &\quad q - 2\sqrt{q} + 1
\end{aligned}$$

çıkar.

Örnek 38 $p = 19$ *ve* $q = 19^4$ *olsun.* $\sqrt{q} = 341 \equiv 1 (\mathrm{mod}\, 5)$ *olduğu için Teorem[baumert]'in hipotezleri sağlanır ve* $\mathbb{F}_q$ *üzerinde beşinci mertebeden*

cyclotomic sayılar $B = C = D = E$ *ve* $F = G$ *olmak üzere*

$$\begin{aligned} A = &\quad (19^4 - 12 \cdot 19^2 - 14)/25 &= 5039 \\ B = &\quad (19^4 + 3 \cdot 19^2 - 4)/25 &= 5256 \\ F = &\quad (19^4 - 2 \cdot 19^2 + 1)/25 &= 5184 \end{aligned}$$

şeklinde belirlenir. Yani cyclotomic matris

$$\begin{pmatrix} 5039 & 5256 & 5256 & 5256 & 5256 \\ 5256 & 5256 & 5184 & 5184 & 5184 \\ 5256 & 5184 & 5256 & 5184 & 5184 \\ 5256 & 5184 & 5184 & 5256 & 5184 \\ 5256 & 5184 & 5184 & 5184 & 5256 \end{pmatrix}$$

şeklindedir.

Not 39 *Mertebe* 5*"tekine benzer bir durum mertebe* 17 *için de vardır. Çünkü* $p^n \equiv 1 (\mathrm{mod}\, 17)$, $p \not\equiv 1 (\mathrm{mod}\, 17)$ *şartını sağlayan her* p *asal için* p *nin* $\mathrm{mod}\, 17$ *deki çarpımsal mertebesi çifttir, çünkü Lagrange Teoremine göre* $17 - 1 = 16$ *değerini bölmelidir. Böylelikle* $e = 17$ *için* $p \not\equiv 1 (\mathrm{mod}\, 17)$ *şartını sağlayan tüm* p *lerde cyclotomic sayıların uniform olduğu görülür. Burada* 5 *ve* 17 *nin ortak özelliği Fermat asalı olmalarıdır.*

3.5.2 Bir İnceleme: Yedinci Mertebe Cyclotomic Sayıların Uniformluğu

Uniform cyclotomy'nin Fermat asalı olmayan asal mertebelerde işe yaramadığı söylenebilir. Buna dair örnek olarak mertebe 7 verilebilir. Mertebe 7'de $p \equiv 3, 5, 6 (\mathrm{mod}\, 7)$ iken cyclotomic sayılar uniformdur ama $p \equiv 2, 4 \pmod 7$ iken uniform değildirler.

Mertebe 7 cyclotomic sayılar incelendiğinde Teorem 27 den cyclotomic matrisin

$$\begin{pmatrix} A & B & C & D & E & F & G \\ B & G & H & I & J & K & H \\ C & H & F & K & L & L & I \\ D & I & K & E & J & L & J \\ E & J & L & J & D & I & K \\ F & K & L & L & I & C & H \\ G & H & I & J & K & H & B \end{pmatrix}$$

şeklinde olduğu görülür. Bunlar uniformluk durumunda

$$\begin{aligned} &A, \\ &B = C = D = E = F = G, \\ &H = I = J = K = L \end{aligned}$$

şeklinde 3 farklı durumdadır. Ancak uniform olmama durumunda böyle bir zorunluluk yoktur.

Örnek 40 *$p = 13$, $q = 13^4$ olsun. Bu durumda mertebe 7 cyclotomic sayılar uniform olur ve $\sqrt{q} \equiv 1 (\mathrm{mod}\, 7)$ olup*

$$\begin{aligned} 479 &= A, \\ 600 &= B = C = D = E = F = G, \\ 576 &= H = I = J = K = L \end{aligned}$$

çıkar.

Örnek 41 *$p = 2$, $q = 2^{12}$ olsun. Bu durumda mertebe 7 cyclotomic sayılar uniform olmaz ve $\sqrt{q} \equiv 1 (\mathrm{mod}\, 7)$ olmasına rağmen*

$$\begin{aligned} 86 &= A = B = C = E, \\ 80 &= D = F = G, \\ 82 &= H = J = L \\ 73 &= I \\ 100 &= K \end{aligned}$$

olduğundan üçten fazla sayıda farklı değer elde edilir ve $B \neq D$, $K \neq H$ *vb. olduğu görülür.*

4. UYGULAMALAR

4.1 Şifrelemedeki Uygulamalar Hakkında

Cyclotomy'nin kodlama teorisi ve şifreleme teorisi alanlarında birçok uygulaması mevcuttur, bu alanlardaki başlıca uygulamalarına bakılırsa,

- Kriptografik fonksiyonların doğrusal fonksiyonlardan uzaklığını belirlemede (nonlinearity analysis) [3],
- Akan şifrelerin (stream ciphers) bazılarının dizayn ve analizinde [3],
- Fark kümelerini (difference sets) inşa etmede ve parametrelerini belirlemede [4, 17],
- Kodlama teorisinde ağırlık numaralandırma ve dağılımını (weight enumerator, weight distribution) belirlemede ve bazı kodların inşasında [5],
- Frekans atlaması dizilerin (frequency hopping sequences, FHS) parametre hesabını belirlemede [10],
- Sidel'nikov dizilerinin otokorelasyon dağılımlarını belirlemede [19–21]

kullanıldığı görülür. Bu bölümde cyclotomic sayıların Sidel'nikov dizilerinin otokorelasyon dağılımlarını belirlemede nasıl bir rol oynadığı anlatılmaya çalışılacaktır.

4.2 Sidel'nikov Dizileri ve Cyclotomic Sayılar

Yüksek hızlı veri transferinde, genelde M-li modülasyon sistemleri iletim standardı olarak kabul görmektedir. Yüksek hızlı veri transferine olan ihtiyacın artmasıyla birlikte, iyi hata düzeltme değerlerine sahip M-li kodlara ve iyi korelasyon özelliklerine sahip M-li dizilere olan ihtiyaç da artmıştır. M-li Sidel'nikov dizileri [21] de bu konuda oldukça kullanışlı dizilerdendir.

Kim, Chung, No ve Chung [19] $M|(p^n-1)$ olmak üzere periyodu p^n-1 olan M-li Sidel'nikov dizilerinin otokorelasyon dağılımı değerleri ile cyclotomic sayılar arasındaki birebir ilişkiyi göstermişlerdir. Böylelikle cyclotomic sayıları hesaplama problemi konunun ilgi alanına girmiştir.

Bu alt bölümde, öncelikle Sidel'nikov dizileri ve otokorelasyon fonksiyonları hakkında kısa bir ön bilgi verilmiş, sonrasında cyclotomic sayıların konuyla ilgili rolünden bahsedilip örnekler verilmiştir.

4.2.1 Sidel'nikov Dizileri ve Otokorelasyon Fonksiyonu

p bir asal sayı, M ile n pozitif tamsayı, $M|(p^n-1)$ ve $f=\frac{p^n-1}{M}$ olsun. α, $\mathbb{F}_{p^n}$ nin bir ilkel elemanı olmak üzere sıfırdan farklı bir $b\in\mathbb{F}_{p^n}$ elemanının **indeksi** $\mathrm{ind}(b)=t,\ b=\alpha^t$ şartını sağlayan $t\in\{0,1,...,p^n-1\}$ olarak tanımlanır. ω_M ile $M.$ dereceden birim kök, yani $\mathrm{e}^{2\pi\sqrt{-1}/M}$ değeri belirtilsin. $\mathbb{F}_{p^n}$ nin

$$S_k=\left\{\alpha^{Ms+k}-1 : s=0,1,...,f-1\right\}$$

alt kümeleri verilsin $(k=0,1,...,M-1)$. **M-li Sidel'nikov dizisi** $s(t)$, herhangi bir sabit $k_0\in\{0,1,...,M-1\}$ için

$$s(t)=\begin{cases} k, & \alpha^t\in S_k,\ k=0,1,...,M-1 \\ k_0, & t=\mathrm{ind}(-1) \end{cases} \tag{4.2.1}$$

şeklinde tanımlanır [21]. Bu dizinin periyodu p^n-1 dir.

$$N_k=|\{t : s(t)=k,\ 0\le t\le p^n-2\}|$$

ifadesi dikkate alınırsa, $k_0 = 0$ durumunda her $k = 0, 1, ..., M-1$ için $N_k = f$ olduğu görülür. Yani M-li Sidel'nikov dizisi dengelidir.

$u(t)$, periyodu N olan M-li bir dizi olsun. $u(t)$ nin **otokorelasyon fonksiyonu**

$$R(\tau) = \sum_{t=0}^{N-1} \omega_M^{u(t)-u(t+\tau)}, \ \tau = 0, 1, ..., N-1$$

şeklinde tanımlanır.

4.2.2 Sidel'nikov Dizilerinin Otokorelasyon Dağılımlarını Hesaplamada Cyclotomic Sayıların Rolü

Teorem 42 [19] *$y = \alpha^\tau \in \mathbb{F}_{p^n} - \{0, 1\}$ olmak üzere $\psi(\frac{1}{1-y}) = \omega_M^u$ ve $\psi(\frac{y-1}{y}) = \omega_M^v$ olsun. $p^n - 1$ periyotlu M-li Sidel'nikov dizisi $s(t)$ nin aşikar olmayan ($\tau \not\equiv 0 (\mathrm{mod}\, p^n - 1)$) otokorelasyon fonksiyonu $R(\tau) = R_{u,v}$,*

$$R_{u,v} = \begin{cases} -(\omega_M^{u+k_0} - 1)(\omega_M^{v-k_0} - 1), & \psi(-1) = 1 \\ (\omega_M^{u+k_0} + 1)(\omega_M^{v-k_0} + 1), & \psi(-1) = -1 \end{cases}$$

şeklindedir.

Teorem 43 [19] *$N(R_{u,v})$ ile $R(\tau) = R_{u,v}$ şartını sağlayan $y = \alpha^\tau \in \mathbb{F}_{p^n} - \{0, 1\}$ lerin sayısı belirtilsin. $p^n - 1$ periyotlu M-li Sidel'nikov dizisinin faz dışı otokorelasyon dağılımı aşağıdaki gibidir.*

$\psi(-1) = 1$ ise

1. $N(0) = \sum_{i=1}^{M-1} ((i, i+k_0)_M + (i, k_0)_M) + (0, k_0)_M$
2. $N(R_{k,k}) = (2k, k+k_0)_M$, $1 \le k \le M-1$
3. $N(R_{u,v}) = (u+v, v+k_0)_M + (u+v, u+k_0)_M$, $1 \le u < v \le M-1$

$\psi(-1) = -1$ ise

1. $N(-2) = \sum_{\substack{i=0 \\ i \neq M/2}}^{M-1} \left((\frac{M}{2}+i, i+k_0)_M + (\frac{M}{2}+i, \frac{M}{2}+k_0)_M \right) + (0, \frac{M}{2}+k_0)_M$

2. $N(R_{k,k}) = (2k, k+k_0)_M$, $0 \leq k \leq M-1$ *ve* $k \neq M/2$

3. $N(R_{u,v}) = (u+v, v+k_0)_M + (u+v, u+k_0)_M$, $1 \leq u < v \leq M-1$ *ve* $u \neq \frac{M}{2}, v \neq \frac{M}{2}$

Örnek 44 $p \equiv 1 (\mathrm{mod}\, 7)$ *şartını sağlayacak şekilde,* $\mathbb{F}_{29}$ *üzerinde* $\alpha = 2$ *ilkeliyle oluşturulan mertebe 7 cyclotomic sayılar*

$$\begin{aligned} 0 &= T_0 = T_2 = T_3 = T_5 = T_6 = T_8 = T_9 \\ 1 &= T_1 = T_7 = T_{10} = T_{11} \\ 2 &= T_4 \end{aligned}$$

şeklinde belirlenir. Yine bu ilkel eleman ile (4.2.1) kullanılarak üretilen 7-li Sidel'nikov dizisi

$$\begin{aligned} s = \; & (1,5,1,3,0,2,5,4,2,3,2,2,3,6,k_0,0,5,5,6,1,1, \\ & 4,6,4,3,0,6,4) \end{aligned}$$

olur. Ayrıca mertebe 7 çarpımsal karakter $\psi(2^t) = \omega_7^t$, $\psi(0) = 0$ *şeklinde olup* $\psi(-1) = \psi(2^{14}) = 1$ *çıkar ve böylelikle* $k_0 = 0$ *için Teorem 43 kullanılarak bu dizinin otokorelasyon dağılımları* $R(\tau)$

0, *6 kez*	$\omega_7 + \omega_7^2 - \omega_7^3 - 1$, *1 kez*
$-(\omega_7 - 1)^2$, *1 kez*	$\omega_7^2 + \omega_7^3 - \omega_7^5 - 1$, *2 kez*
$-(\omega_7^2 - 1)^2$, *1 kez*	$\omega_7^2 + \omega_7^4 - \omega_7^6 - 1$, *1 kez*
$-(\omega_7^3 - 1)^2$, *0 kez*	$\omega_7^2 + \omega_7^5 - 2$, *0 kez*
$-(\omega_7^4 - 1)^2$, *0 kez*	$\omega_7^2 + \omega_7^6 - \omega_7 - 1$, *2 kez*
$-(\omega_7^5 - 1)^2$, *1 kez*	$\omega_7^3 + \omega_7^4 - 2$, *2 kez*
$-(\omega_7^6 - 1)^2$, *1 kez*	$\omega_7^3 + \omega_7^5 - \omega_7 - 1$, *1 kez*
$\omega_7 + \omega_7^2 - \omega_7^3 - 1$, *1 kez*	$\omega_7^3 + \omega_7^6 - \omega_7^2 - 1$, *1 kez*
$\omega_7 + \omega_7^3 - \omega_7^4 - 1$, *0 kez*	$\omega_7^4 + \omega_7^5 - \omega_7^2 - 1$, *2 kez*
$\omega_7 + \omega_7^4 - \omega_7^5 - 1$, *1 kez*	$\omega_7^4 + \omega_7^6 - \omega_7^3 - 1$, *0 kez*
$\omega_7 + \omega_7^5 - \omega_7^6 - 1$, *2 kez*	$\omega_7^5 + \omega_7^6 - \omega_7^4 - 1$, *1 kez*

şeklinde hesaplanır. Dikkat edilirse 3 farklı karakterde sayı bulunmasına rağmen cyclotomic sayılar uniform değildir.

Örnek 45 *$p \not\equiv 1 (\mathrm{mod}\, 7)$ durumuna örnek olarak, $\mathbb{F}_{64} = \mathbb{F}_2(\theta)$ cismi üzerinde (θ, $x^6 + x^5 + 1$ polinomunun bir kökü) θ ilkel elemanı kullanılarak oluşturulan mertebe 7 cyclotomic sayılar*

$$\begin{aligned} 0 &= T_3 = T_5 = T_6 = T_{10} \\ 1 &= T_8 \\ 2 &= T_0 = T_1 = T_2 = T_4 = T_7 = T_9 = T_{11} \end{aligned}$$

şeklinde belirlenir. Yine bu ilkel eleman kullanılarak üretilen 7-li Sidel'nikov dizisi

$$\begin{aligned} s = \; & (k_0, 2, 4, 6, 1, 6, 5, 2, 2, 6, 5, 0, 3, 6, 4, 5, 4, 5, 5, 5, 3, \\ & 0, 0, 1, 6, 0, 5, 2, 1, 4, 5, 4, 1, 3, 3, 1, 3, 0, 3, 3, 6, 6, \\ & 0, 4, 0, 1, 2, 2, 5, 4, 0, 5, 3, 2, 4, 1, 2, 5, 1, 4, 3, 2, 1) \end{aligned}$$

olur. Burada karakteristik 2 olduğundan $-1 = 1$ dir. Dolayısıyla k_0 değeri 1 in indeksi olan sıfır hanesine konmuştur. Ayrıca mertebe 7 çarpımsal karakter ψ için $\psi(-1) = \psi(1) = 1 = -1$ çıkar. Yani $k_0 = 0$ için Teorem 43 deki formüllerden ikisi de kullanılabilir. Hesaplandığında periyodu 63 olan bu 7-li dizinin otokorelasyon dağılımları $R(\tau)$

0,	*14 kez*	$\omega_7 + \omega_7^2 - \omega_7^3 - 1$,	*2 kez*
$-(\omega_7 - 1)^2$,	*2 kez*	$\omega_7^2 + \omega_7^3 - \omega_7^5 - 1$,	*4 kez*
$-(\omega_7^2 - 1)^2$,	*2 kez*	$\omega_7^2 + \omega_7^4 - \omega_7^6 - 1$,	*1 kez*
$-(\omega_7^3 - 1)^2$,	*2 kez*	$\omega_7^2 + \omega_7^5 - 2$,	*2 kez*
$-(\omega_7^4 - 1)^2$,	*2 kez*	$\omega_7^2 + \omega_7^6 - \omega_7 - 1$,	*4 kez*
$-(\omega_7^5 - 1)^2$,	*2 kez*	$\omega_7^3 + \omega_7^4 - 2$,	*2 kez*
$-(\omega_7^6 - 1)^2$,	*2 kez*	$\omega_7^3 + \omega_7^5 - \omega_7 - 1$,	*1 kez*
$\omega_7 + \omega_7^2 - \omega_7^3 - 1$,	*1 kez*	$\omega_7^3 + \omega_7^6 - \omega_7^2 - 1$,	*1 kez*
$\omega_7 + \omega_7^3 - \omega_7^4 - 1$,	*4 kez*	$\omega_7^4 + \omega_7^5 - \omega_7^2 - 1$,	*4 kez*
$\omega_7 + \omega_7^4 - \omega_7^5 - 1$,	*1 kez*	$\omega_7^4 + \omega_7^6 - \omega_7^3 - 1$,	*4 kez*
$\omega_7 + \omega_7^5 - \omega_7^6 - 1$,	*4 kez*	$\omega_7^5 + \omega_7^6 - \omega_7^4 - 1$,	*1 kez*

şeklinde çıkar.

Not 46 *Son örnekte $x^6+x^4+x^3+x+1$ veya x^6+x+1 polinomlarının kökleri olan ilkel elemanlar kullanıldığında da aynı otokorelasyon dağılımlarının elde edildiği görülür.*

5. SONUÇ

Cyclotomic sayıları, tanım üzerinden değil de cyclotomic sayıların ortak özellikleri ve bazı cebirsel argümanlar kullanarak hesaplama işi ilk olarak [12] de görülmektedir, hatta cyclotomic sayı tabiri de ilk olarak bu çalışmada geçmektedir [18]. Burada amaç, bazı temel özellikler vasıtasıyla farklı ve kullanışlı hesaplama yöntemleri ve formüller elde edebilmektir. İlk hesaplamalar genelde $\mathbb{Z}_p$ üzerinden yapılmış, sonraları çalışma $\mathbb{F}_{p^n}$ ye genelleştirilmeye çalışılmıştır.

$\mathbb{Z}_p$ üzerinden bakıldığında mertebe 24'e kadar çalışmaların olduğu görülür [12–16]. $\mathbb{F}_{p^n}$ üzerinde incelendiğinde ise yedinci mertebeye kadar çalışmaların tamamlandığı [4, 5, 20] görülmüştür. Bu tez çalışmasında $\mathbb{F}_{p^n}$ üzerinde mertebe yedi incelenmiş ve konuyla ilgili sonuçlar derlenmiştir. Ayrıca cyclotomy probleminin şifrelemedeki güncel ve önemli bir uygulamasından da bahsedilmiştir.

$\mathbb{Z}_p$ üzerinden $\mathbb{F}_{p^n}$ ye genelleştirilmeler olduğu gibi $\mathbb{Z}_n$ ye genelleştirilmeler de mevcuttur (n kompozit bir sayı) [18]. Bu tarz genelleştirmelerin de şifreleme vb. alanlarda uygulamaları çalışılmaktadır.

Kaynakça

[1] Lidl, R., Niederrreiter, H., *Finite Fields,* Cambridge Univ. Press, 1997.

[2] Berndt, B. C., Evans, R. J., Williams, K. S., *Gauss and Jacobi Sums,* Canadian Mathematical Society Series of Monographs and Advanced Texts, John Wiley & Sons Inc., New York, 1998.

[3] Cusick, T. W., Ding, C., Renvall, A., *Stream Ciphers and Number Theory,* North-Holland Mathematical Library, 2004.

[4] Storer, T., *Cyclotomy and Difference Sets,* Markham Publishing Company, 1967.

[5] Ding, C., Niederreiter, H., Cyclotomic linear codes of order 3, *IEEE Transactions on Information Theory,* **53** (6): 2274-2277, 2007.

[6] Parnami, J. C., Agrawal, M. K., Rajwade, A. R., Jacobi sums and cyclotomic numbers, *Acta Arithmetica,* **41**: 1-13, 1982.

[7] Katre, S. A., Rajwade, A. R., Complete solution of the cyclotomic problem in $\mathbb{F}_q$ for any prime modulus l, $q = p^\alpha$, $p \equiv 1 (\mathrm{mod}\, l)$, *Acta Arithmetica,* **45**: 183-199, 1985.

[8] Vinaykumar, V. A., Katre (Pune), S. A., Cyclotomic numbers of order $2l$, l an odd prime, *Acta Arithmetica,* **69** (1): 51-74, 1995.

[9] Baumert, L. D., Williams, W. H., Ward, R. L., Uniform cyclotomy, *Journal of Number Theory*, **14**: 67-81, 1982.

[10] Ding, C., Fuji-Hara, R., Fujiwara, Y., Jimbo, M., Mishima, M., Sets of frequency hopping sequences: Bounds and optimal constructions, *IEEE Transactions on Information Theory,* **55** (7): 3297-3304, 2009.

[11] Sury, B., Cyclotomy and cyclotomic polynomials (The story of how Gauss narrowly missed becoming a philologist), *Resonance,* **4**: 41-53, 1999.

[12] Gauss, C. F., *Disquisitiones Arithmeticae*, 1801, English translation, Yale, New Haven, 1966.

[13] Dickson, L. E., Cyclotomy, higher congruences and Waring's problem I, *American J. of Math.,* **57** (2): 391-424, 1935.

[14] Dickson, L. E., Cyclotomy, higher congruences and Waring's problem II, *American J. of Math.,* **57** (3): 463-474, 1935.

[15] Whiteman, A. L., The cyclotomic numbers of order twelve, *Acta Arith.* **6**: 53-76, 1960.

[16] Whiteman, A. L., The cyclotomic numbers of order sixteen, *Trans. Amer. Math. Soc.* **86**: 401-413, 1957.

[17] Baumert, L. D., Fredricksen, H., The cyclotomic numbers of order eighteen with applications to difference sets, *Math. Comp.* **21**: 204-219, 1967.

[18] Ding, C., Helleseth, T., New generalized cyclotomy and its applications, *Finite Fieldsand Their Applications* **4**: 140-166, 1998.

[19] Kim, Y. S., Chung, Y. S., No, J.-S., Chung, H., On the autocorrelation distribution of Sidel'nikov sequences, *IEEE Trans. Inf. Theory,* **51** 9: 3303-3307, 2005.

[20] Chung, Y. S., Kim, Y. S., Lim, T. H., No, J. S., Chung, H., Cyclotomic numbers of order 5 over F_{p^n}," *in Proceedings of International Symposium on Information Theory (ISIT)*, 1962-1966, 2005.

[21] Sidel'nikov, V. M., Some k-valued pseudo-random sequences and nearly equidistant codes, *Probl. Inf. Transm.,* **5** 1: 12-16, 1969.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, Adı	: OTAL, Kamil
Uyruğu	: T.C.
Doğum tarihi ve yeri	: 1987, Konya
Medeni hali	: Bekar
Telefon	: +90 312 2924328
e-mail	: kotal@.etu.edu.tr

Eğitim

Derece	**Eğitim Birimi**	**Mezuniyet Tarihi**
Y. Lisans	TOBB Ekonomi ve Teknoloji Üniversitesi	
Lisans	TOBB Ekonomi ve Teknoloji Üniversitesi	2010

Yabancı Dil

İngilizce (Çok iyi)

Yayınlar

K. Otal, Z. Saygı, Ç. Ürtiş, Cyclotomic Sayılar ve Sidel'nikov Dizileri, ISC-TURKEY 2012, Proceedings of 5th International Conference on Information Security and Cryptology, pp. 175-178, May 17-18, 2012, Ankara, Turkey.