T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

EISENSTEIN-JACOBI TAMSAYILAR KÜMESİ ÜZERİNDE KLASİK VE KUANTUM KODLAR

YÜKSEK LİSANS TEZİ

Ercüment ÇAKIR

Enstitü Anabilim Dalı	**:**	**MATEMATİK**
Enstitü Bilim Dalı	**:**	**CEBİR VE SAYILAR TEORİSİ**
Tez Danışmanı	**:**	**Doç. Dr. Murat GÜZELTEPE**

Haziran 2019

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

EISENSTEIN-JACOBI TAMSAYILAR KÜMESİ ÜZERİNDE KLASİK VE KUANTUM KODLAR

YÜKSEK LİSANS TEZİ

Ercüment ÇAKIR

Enstitü Anabilim Dalı : **MATEMATİK**

Enstitü Bilim Dalı : **CEBİR VE SAYILAR TEORİSİ**

Bu tez 12/06/2019 tarihinde aşağıdaki jüri tarafından oybirliği / ~~oyçokluğu~~ ile kabul edilmiştir.

Doç. Dr. Murat GÜZELTEPE	Doç. Dr. Mustafa ERÖZ	Dr. Öğr. Üyesi Halil ARSLAN
Jüri Başkanı	Üye	Üye

BEYAN

Tez içindeki tüm verilerin akademik kurallar çerçevesinde tarafımdan elde edildiğini, görsel ve yazılı tüm bilgi ve sonuçların akademik ve etik kurallara uygun şekilde sunulduğunu, kullanılan verilerde herhangi bir tahrifat yapılmadığını, başkalarının eserlerinden yararlanılması durumunda bilimsel normlara uygun olarak atıfta bulunulduğunu, tezde yer alan verilerin bu üniversite veya başka bir üniversitede herhangi bir tez çalışmasında kullanılmadığını beyan ederim.

Ercüment ÇAKIR

19.04.2019

TEŞEKKÜR

Yüksek lisans eğitimim boyunca değerli bilgi ve deneyimlerinden yararlandığım, her konuda bilgi ve desteğini almaktan çekinmediğim, araştırmanın planlanmasından yazılmasına kadar tüm aşamalarında yardımlarını esirgemeyen, teşvik eden, aynı titizlikte beni yönlendiren değerli danışman hocam Doç. Dr. Murat GÜZELTEPE'ye teşekkürlerimi sunarım.

Eğitim hayatım boyunca maddi manevi destekleriyle beni hiçbir zaman yalnız bırakmayan sevgili annem ve değerli babama sonsuz teşekkür ederim.

Ayrıca bu çalışma TÜBİTAK tarafından 3001 projesi kapsamında 116F318 proje numarası ile desteklenmiştir. Desteklerinden dolayı TÜBİTAK'a teşekkür ederim.

İÇİNDEKİLER

SİMGELER VE KISALTMALAR LİSTESİ

C	: Kod
$d_H(x,y)$	: x ile y elemanları arası Hamming mesafesi
$d_m(\alpha,\beta)$	: α ile β elemanları arasındaki Mannheim mesafesi
$d_M(\alpha,\beta)$	: α ile β elemanları arasındaki yeni bir Mannheim mesafesi
EB	: Öklid Bölgesi
F_p	: p elemanlı sonlu cisim
G	: Grup
I	: İdeal
$N(\pi)$	: π elemanının normu
R	: Halka
R_π	: $N(\pi)$ elemanlı sonlu halka
$S(r)$	: r vektörünün sendromu
$w_m(\gamma)$	: γ elemanının Mannheim ağırlığı
$w_M(\gamma)$	: γ elemanının yeni bir Mannheim ağırlığı
$\mathbb{Z}$	: Tamsayılar kümesi
$\mathbb{Z}[i]$	: Gauss tamsayılar halkası
$\mathbb{Z}[w]$	: Eisenstein-Jacobi tamsayılar kümesi
$\mathbb{Z}[w]_\pi$	: $\mathbb{Z}[w]$ da π nin kalan sınıflarından oluşan küme
$\bar{a}$	a nın denklik sınıflarının kümesi

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

ÖZET

Anahtar Kelimeler: Lineer kodlar, devirli kodlar, kuantum kodlar, Eisenstein-Jacobi tamsayılar kümesi, Mannheim metrik, Hamming metrik,

Dört bölümden oluşan bu çalışmada, ilk bölümde cebir ve kodlama teorisinden bazı tanım ve teoremler verilmiştir.

İkinci bölümde Eisenstein-Jacobi tamsayılar kümesinin cebirsel özellikleri ve bu küme üzerindeki devirli kodlardan bahsedilmiştir. Ayrıca bu küme üzerinde dekodlama algoritması gösterilerek tek hata ve iki hata düzeltebilen kodlar verilmiştir.

Üçüncü bölümde Eisenstein-Jacobi tamsayılar kümesi üzerinde sonlu bir cisim tanımlanıp, bu cismin cebirsel özellikleri verilmiştir. Daha sonra bu sonlu cisim üzerindeki klasik devirli kodlar yardımıyla kuantum kodlar inşa edilmiştir.

Dördüncü bölümde Eisenstein-Jacobi tamsayılar kümesi üzerinde sonlu bir halka tanımlanıp, bu halkanın cebirsel özellikleri verilmiştir. Daha sonra bu sonlu halkanın küme parçalanışı ve bu küme parçalanışları üzerinde ortalama enerji, *CFM* ve kod kazancı hesaplanmıştır.

CLASSICAL AND QUANTUM CODES OVER EISENSTEIN-JACOBI INTEGERS

SUMMARY

Keywords: Linear codes, cyclic codes, quantum codes, Eisenstein-Jacobi integers, Mannheim metric, Hamming metric,

This study consists of four chapters. First chapter includes definitions and theorems associated with algebra and coding theory.

In the second chapter, algebraic properties of Eisenstein-Jacobi integers set and cyclic codes over this set are given. Also, one-error correcting and double-error correcting codes are given by showing decoding algorithm.

In the third chapter, a finite field is defined over Eisenstein-Jacobi integers set and algebraic properties of this finite field are given. And also quantum codes are studied from classical cyclic codes over this finite field.

In the fourth chapter, a finite ring is defined over Eisenstein-Jacobi integers set and algebraic properties of this finite ring are given. Set partitioning of this finite field are given and also average energy, *CFM* value, and code gain are studied over this set partitioning.

BÖLÜM 1.GİRİŞ

Bu bölümde verilen temel tanım, teorem ve önermeler diğer bölümlerde kullanılacak ön bilgiler niteliğindedir.

1.1.Temel Tanım ve Teoremler

Tanım 1.1.1. $A\times A$ dan A ya bir fonksiyona A da bir ikili işlem denir. "$*$", A da bir ikili işlem ve $a,b\in A$ olsun. (a,b) nin "$*$" işlemi altındaki görüntüsü $a*b$ ile gösterilsin. Fonksiyon olma özelliklerinden $\forall a,b\in A$ için A da bir $a*b$ elemanının var olmasına işlemin kapalılığı denir. Bu $a*b$ elemanının tek türlü belirli olmasına işlemin iyi tanımlığı denir [1].

Tanım 1.1.2. G boş olmayan bir küme ve "$*$", G de bir ikili işlem olsun. $(G,*)$ cebirsel yapısı aşağıdaki aksiyomları sağlıyorsa bu yapıya bir grup denir.

1) "$*$", G de bir ikili işlemdir.
2) "$*$" işleminin G de birleşme özelliği vardır. Yani, $\forall a,b,c\in G$ için $(a*b)*c=a*(b*c)$ dir.
3) "$*$" işleminin, G de birim elemanı vardır. Yani, $\forall a\in G$ için $a*e=e*a=a$ olacak şekilde $e\in G$ vardır.
4) "$*$" işlemine göre, G deki her elemanın tersi vardır. Yani, $\forall a\in G$ için $a*a^{-1}=a^{-1}*a=e$ olacak şekilde $\exists a^{-1}\in G$ bulunabilir [1].

Tanım 1.1.3. G bir grup ve $\forall a,b\in G$ için $a*b=b*a$ oluyor ise G ye bir değişmeli (Abel) grup denir [1].

Tanım 1.1.4. G bir grup ve $\varnothing \neq H \subset G$ olsun. Eğer H, G deki işleme göre kendi başına bir grup ise H alt kümesine G nin bir alt grubu denir ve $H \leq G$ ile gösterilir [1].

Önerme 1.1.1. G bir grup $\varnothing \neq H \subset G$ olsun. H nin G nin alt grubu olması için gerek ve yeter şart aşağıdaki iki şartın sağlanmasıdır.

1) $\forall a,b \in H$ için $ab \in H$ dir,
2) $\forall a \in H$ için $a^{-1} \in H$ dir [1].

Önerme 1.1.2. G bir grup $\varnothing \neq H \subset G$ olsun. H nin G nin alt grubu olması için ve yeter şart $\forall a,b \in H$ için $ab^{-1} \in H$ olmasıdır [1].

Önerme 1.1.3. G bir grup $\varnothing \neq H \subset G$ ve H sonlu elemanlı olsun. Eğer H kümesi G deki işlem göre kapalı ise $H \leq G$ dir [1].

Tanım 1.1.5. M, bir G grubunun alt kümesi olsun. M yi kapsayan, G nin bütün alt gruplarının arakesitine M nin ürettiği alt grup denir ve $\langle M \rangle$ ile gösterilir. M nin elemanlarına da $\langle M \rangle$ grubunun üreteçleri denir.

Eğer bir G grubu için $G = \langle M \rangle$ olacak şekilde bir $M \subset G$ alt kümesi bulunabiliyorsa; G ye M ile üretilmiş grup denir. Eğer M sonlu bir küme ise G ye sonlu üretilmiş grup ve $M = \{a\}$ tek elemanlı bir küme ise G ye a le üretilmiş devirli grup denir ve $G = \langle a \rangle$ yazılır. G çarpımsal olarak alınırsa $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$ dir. G toplamsal olarak alınırsa $\langle a \rangle = \{na : n \in \mathbb{Z}\}$ dir [1].

Önerme 1.1.4. $G = \langle a \rangle$ t. mertebeden bir devirli grup ise G nin her alt grubunun mertebesi t yi böler [1].

Teorem 1.1.1. G bir grup ve $H \leq G$ olsun. G de

$a \equiv b \pmod{H} \Leftrightarrow ab^{-1} \in H$

şeklinde tanımlanan "$\equiv$" bağıntısı denklik bağıntısıdır. Bu denklik bağıntısına göre bir $a \in G$ elemanının sınıfı $\bar{a} = Ha = \{ha : h \in H\}$ alt kümesidir [1].

Tanım 1.1.6. Teorem1.1.1.' de verilen Ha kümesine H alt kümesine göre a nın sağ denklik sınıfı denir [1].

Benzer şekilde sol denklik sınıfları da tanımlanabilir.

Teorem 1.1.1. $N \leq G$ olsun. Aşağıdaki koşullar birbirine denktir.

1) $\forall a \in G$, $\forall x \in N$ için $axa^{-1} \in N$ dir.
2) $\forall a \in G$ için $aNa^{-1} \subset N$ dir.
3) $\forall a \in G$ için $aNa^{-1} = N$ dir.
4) $\forall a \in G$ için $aN = Na$ dır [1].

Tanım 1.1.7. Teorem 1.1.2.'de ki den koşulardan birini sağlayan G nin bir N alt grubuna normal alt grup denir. $N \lhd G$ ile gösterilir. Buna göre $N \lhd G$ ise N ye göre tanımlanan sağ ve sol denklik sınıfları aynıdır $[1]$.

Tanım 1.1.8. $N \lhd G$ olsun. G nin N normal alt grubuna göre sağ(veya sol) denklik sınıfları kümesi G/N ile gösterilir $[1]$.

Teorem 1.1.3. $N \lhd G$ ise G/N gruptur $[1]$.

Tanım 1.1.9. $N \lhd G$ ise G/N grubuna G nin N ye göre bölüm grubu denir $[1]$.

Teorem 1.1.4. G sonlu bir grup ve $N \lhd G$ ise G/N de sonlu bir gruptur ve $\left|G/N\right| = \frac{|G|}{|N|}$ dir $[1]$.

Teorem 1.1.4. (Lagrange Teoremi) G bir grup ve $H \leq G$ ise $|G| = \left|{G}/{N}\right||H|$ dir.

Özel olarak sonlu bir grubun her alt grubunun mertebesi, grubun mertebesini böler [1].

Tanım 1.1.10. $R \neq \varnothing$ kümesi üzerinde "+" ve "•" ikili işlemleri tanımlı olsun. Aşağıdaki aksiyomları sağlayan $(R,+,\bullet)$ cebirsel yapısına bir halka denir.

1) $(R,+)$ bir değişmeli gruptur.
2) "•" işleminin R de birleşme özelliği vardır.
3) "•" işleminin "+" işlemi üzerine sağdan ve soldan dağılma özellikleri vardır. Yani $\forall a,b,c \in R$ için $a\bullet(b+c) = a\bullet b + a\bullet c$ ve $(a+b)\bullet c = a\bullet c + b\bullet c$ dir.

Halkanın "+" işlemine göre etkisiz elemanına halkanın sıfır elemanı denir ve 0_R ile gösterilir. Halkanın "•" işlemine göre etkisiz elemanı varsa buna halkanın birim elemanı denir ve 1_R ile gösterilir. Birim elemanı olan halkaya birimli halka denir. Halka "•" işlemine göre değişme özelliğine sahip ise halkaya değişmeli halka denir [1].

Tanım 1.1.11. R halkasında $0_R \neq a \in R$ elemanı için; $ab = 0_R$ veya $ba = 0_R$ olacak şekilde $\exists 0_R \neq b \in R$ bulunabilirse a ya halkanın bir sıfır böleni denir [1].

Tanım 1.1.12. Sıfır bölensiz bir halkaya tam halka denir. birimli, değişmeli, sıfır bölensiz(tam) halkaya bir tamlık bölgesi denir [1].

Tanım 1.1.13. R birimli ve değişmeli bir halka ve $R - \{0_R\} = R^*$, ikinci işlem olan "•" ya göre bir grup ise R ye bir cisim denir. Yani bir cisimde sıfırdan farklı her elemanın tersi vardır [1].

Önerme 1.1.5. Sonlu elemanlı her tamlık bölgesi bir cisimdir [1].

Tanım 1.1.14. R bir halka ve $\varnothing \neq S \subset R$ olsun. S kümesi R kümesindeki işlemlere göre kendi başına bir halka ise S ye R nin bir alt halkası denir $[1]$.

Önerme 1.1.6. R bir halka ve $\varnothing \neq S \subset R$ olsun. S nin R nin bir alt halkası olması için gerek ve yeter koşul $\forall a,b \in S$ için $a-b \in S$ ve $ab \in S$ olmasıdır $[1]$.

Tanım 1.1.15. R bir halka, $\varnothing \neq I \subset R$ ve $\forall a,b \in I$ için $a-b \in I$ olsun. Eğer $\forall a \in I$ ve $\forall r \in R$ için $ra \in I$ ise I ya R nin bir sol ideali denir. Benzer şekilde $\forall a \in I$ ve $\forall r \in R$ için $ar \in I$ ise I ya R nin bir sağ ideali denir.

Hem sol hem de sağ ideale kısaca ideal denir $[1]$.

Önerme 1.1.7. Bir halkanın bir takım ideallerinin arakesiti de bir idealdir $[1]$.

Tanım 1.1.16. I, R halkasının bir alt kümesi olsun. R nin I yı kapsayan tüm ideallerinin arakesitine I nın ürettiği ideal denir ve $\langle I \rangle$ ile gösterilir. Eğer $I = \{a\}$ tek elemanlı bir küme ise I nın ürettiği ideale temel ideal denir ve $\langle a \rangle$ ile gösterilir. R birimli ve değişmeli bir halka ise $\langle a \rangle = aR = \{ar : r \in R\}$ dir $[1]$.

Tanım 1.1.17. Her ideali temel ideal olan bir tamlık bölgesine temel ideal bölgesi denir ve kısaca TİB ile gösterilir $[1]$.

Tanım 1.1.18. R, S iki halka ve $f : R \to S$ bir fonksiyon olsun. Eğer $\forall a,b \in R$ için

1) $f(a+b) = f(a) + f(b)$
2) $f(ab) = f(a) f(b)$

ise f fonksiyonuna R den S ye bir halka homomorfizması denir [1].

Tanım 1.1.19. $f:R\to S$ homomorfizması bire-bir ve örten ise f ye bir izomorfizma, R ile S ye de izomorf halkalar denir ve $R\cong S$ ile gösterilir [1].

Tanım 1.1.20. R bir halka, x bir bilinmeyen ve $a_0,a_1,\ldots,a_k\in R$ olmak üzere, $a_0+a_1x+\ldots+a_kx^k$ şeklindeki bir ifadeye R den katsayılı bir polinom denir. R den katsayılı tüm polinomlar kümesi $R[x]$ ile gösterilir [1].

Tanım 1.1.21. $f(x)=a_0+a_1x+\ldots+a_nx^n\in R[x]$ ve $a_n\neq 0$ a_n ye polinomun baş katsayısı ve n ye de polinomun derecesi denir. $f(x)$ polinomunun derecesi $der[f(x)]$ ile gösterilir [1].

Önerme 1.1.8. R bir halka ise $R[x]$ de bir halkadır [1].

Tanım 1.1.22. $f(x)=a_0+a_1x+\ldots+a_nx^n\in R[x]$ ve $r\in R$ olsun. $f(r)=a_0+a_1r+\ldots+a_nr^n\in R$ ye f polinomunun r deki değeri denir. Eğer $r\in R$ için, $f(r)=0$ ise r ye f polinomunun bir kökü denir. Eğer $a_n=1$ ise f polinomuna monik polinom denir [1].

Tanım 1.1.23. $f(x)\in R[x]$ olsun. $der[h(x)],der[g(x)]<der[f(x)]$ için $f(x)=g(x)h(x)$ olacak şekilde $g(x),h(x)\in R[x]$ varsa, $f(x)$ polinomuna $R[x]$ üzerinde indirgenemez polinom denir [1].

Tanım 1.1.24. R bir halka ve I, R nin bir ideali olsun. "$\equiv$" bağıntısı, $\forall a,b\in R$ için $a\equiv b\pmod{I}\Leftrightarrow a-b\in I$ olarak tanımlansın [1].

Önerme 1.1.9. Yukarıda tanımlanan "$\equiv$" bağıntısı R de bir denklik bağıntısıdır. Bu bağıntıya göre $r \in R$ nin denklik sınıfı $\bar{r} = r + I = \{r + a : a \in I\}$ dır. Bütün denklik sınıflarının kümesi R/I ile gösterilir [1].

Önerme 1.1.10. R halkasının bir I idealine göre tanımlanan denklik sınıfları arasında $(a+I) \oplus (b+I) = (a+b)+I$ ve $(a+I) \odot (b+I) = (ab)+I$ ile tanımlanan "$\oplus$" ve "$\odot$" işlemlerine göre R/I bir halkadır. Bu halkaya R nin I idealine göre bölüm halkası denir [1].

Tanım 1.1.25. R bir tamlık bölgesi olmak üzere $a, b \in R$ için, $a = bc$ olacak şekilde $\exists c \in R$ var ise b, a yı böler denir ve bu $b \mid a$ ile gösterilir [1].

Tanım 1.1.26. R tamlık bölgesinin tüm elemanlarını bölen R nin bir elemanına birimsel eleman ya da aritmetik birim denir. R nin tüm aritmetik birimlerinin kümesi U_R ile gösterilir [1].

Tanım 1.1.27. $a, b \in R$ için, $b = u_1 a u_2$ olacak şekilde $\exists u_1, u_2 \in U_R$ var ise a ile b ilgilidir denir ve $a \approx b$ ile gösterilir [2].

Önerme 1.1.11. $a, b \in R$ olsun.

1) $a \mid b \Leftrightarrow \langle b \rangle \subset \langle a \rangle$ dır.
2) $b \neq 0$ olmak üzere $a \mid b$ ve $b \mid a \Leftrightarrow a \approx b$ dir [1].

Tanım 1.1.27. R bir tamlık bölgesi ve $a, b \in R$ olsun.

1) $c \in R$ olmak üzere $c \mid a$ ve $a \mid b$ ise c ye a ile b nin ortak böleni denir.
2) c, a ile b nin ortak böleni olmak üzere a ile b nin tüm ortak bölenleri c yi bölüyor ise c ye a ile b nin en büyük ortak böleni denir [1].

Tanım 1.1.28. Ebob leri aritmetik birimler olan elemanlara aralarında asal denir ve a ile b aralarına asal ise $(a,b)=1$ ile gösterilir [1].

Tanım 1.1.29. $x \in R,\ x \in U_R$ ve $x \neq 0_R$ olsun.

1) x in aritmetik birimlerden ve x ile ilgili elemanlardan başka hiçbir böleni yoksa x elemanına, R nin bir indirgenemez elemanı denir.
2) $a,b \in R$ için $x \mid ab \Rightarrow x \mid a$ veya $x \mid b$ oluyorsa $x \in R$ asal eleman denir [1].

Tanım 1.1.30. R bir tamlık bölgesi olsun. Aşağıdaki özellikleri sağlayacak şekilde bir $d : R \to \mathbb{Z}$ fonksiyonu var ise R ye bir Euclid bölgesi denir ve kısaca EB ile gösterilir.

1) $\forall x \in R$ için $d(x) \geq 0$,
2) $d(x)=0 \Leftrightarrow x = 0_R$,
3) $\forall x, y \in R$ için $d(xy) = d(x)d(y)$,
4) $\forall x, y \in R,\ y \neq 0_R$ için $x = qy + r$ ve $0 \leq d(r) < d(y)$ olacak şekilde $\exists q, r \in R$ bulunabilir [1].

Teorem 1.1.6. R bir EB ise TİB dir [1].

Tanım 1.1.31. $\mathbb{Z}[i] = \{a + bi : a,b \in \mathbb{Z}\}$ tamlık bölgesine Gauss tamsayılar bölgesi denir [1].

Önerme 1.1.12. $\mathbb{Z}[i]$ Gauss tamsayılar bölgesi EB dir [1].

Tanım 1.1.32. $(M,+)$ bir değişmeli grup ve R bir değişmeli halka olsun. M deki elemanların, R deki elemanlarla skaler çarpımı, $R \times M \to M$ fonksiyonu aşağıdaki koşulları sağlıyorsa, M ye R üzerinde bir modül veya kısaca $R-$Modül denir.

1) Her $r \in R$, her $m, m' \in M$ için $r(m+m') = rm + rm'$,

2) Her $r, r' \in R,\ m \in M$ için $(r+r')m = rm + r'm$,

3) Her $r, r' \in R,$ her $m \in M$ için $(rr')m = r(r'm)$,

4) Her $m \in M$ için $1_R m = m$ [3].

Eğer R bir değişmeli halka değil ise sağ ve sol $R-$Modül tanımı benzer şekilde yapılabilir.

Tanım 1.1.33. $A = \{a_1, a_2, \ldots, a_q\}$, q elemanlı bir küme olsun. Bu kümeye alfabe kümesi denir [4].

Tanım 1.1.34. Her i için $w_i \in A$ olmak üzere, A^n üzerinde $w = w_1 w_2 \ldots w_n$ şeklinde tanımlanan bir diziye n uzunluklu bir söz denir. n uzunluklu bir söz $w = (w_1, w_2, \ldots w_n)$ şeklinde bir vektör olarak da göz önüne alınabilir. A^n kümesine söz kümesi denir [4].

Tanım 1.1.35. A^n kümesinin boştan farklı bir C alt kümesine $q-$lu blok kod yada kısaca kod denir. C kodunun elemanlarına da kodsöz denir. C nin kodsözlerinin sayısı $|C|$ ile gösterilir ve buna C nin büyüklüğü denir [4].

Tanım 1.1.36. n uzunluklu bir kodsözün hızı $(\log_q |C|)/n$ olarak tanımlanır [4].

Tanım 1.1.37. n uzunluğunda ve M büyüklüğünde bir kod, (n, M) kodu olarak tanımlanır [4].

Tanım 1.1.38. Bir iletişim kanalında kodsözler iletilirken iletişim sırasında bir hata oluştuğunda en çok ihtimalle gönderilmiş kodsözü bulmak için oluşturulan kurala dekodlama kuralı denir [4].

Tanım 1.1.39. x ve y bir A alfabesi üzerinde n uzunluklu iki söz olsun. x ve y arasındaki Hamming uzaklığı $d_H(x,y)$ ile gösterilir ve

$$x = x_1 \ldots x_n, \quad y = y_1 \ldots y_n \text{ ve } d_H(x_i, y_i) = \begin{cases} 1, & x_i \neq y_i \\ 0, & x_i = y_i \end{cases}$$

olmak üzere

$$d_H(x,y) = d_H(x_1, y_1) + \ldots + d_H(x_n, y_n)$$

olarak tanımlanır $[4]$.

Tanım 1.1.40. Bir C kodunun bir kodsözü bir iletişim kanalından geçsin ve bir x sözü olarak alınsın. x in diğer tüm $c \in C$ ler ile arasındaki uzaklık hesaplanarak bu uzaklığın en az olduğu kodsöz c_x olarak bulunur ise x sözü, c_x olarak dekodlanır. Yani $d(x,c_x) = \min_{c \in C} d(x,c)$ ise kananaldan gelen x sözü c_x olarak dekodlanır. Bu dekodlamaya en yakın komşuluk dekodlama kuralı (minimum mesafe dekodlama kuralı) denir $[4]$.

Tanım 1.1.41. En az iki kodsöze sahip bir C kodunun minimum mesafesi $d(C)$ ile gösterilir ve $d(C) = \min\{d(x,y) : x, y \in C, x \neq y\}$ olarak tanımlanır $[4]$.

Tanım 1.1.42. n uzunluklu, M büyüklüğünde ve d minimum mesafesine sahip bir kod (n, M, d) kodu olarak adlandırılır. Burada n, M ve d sayılarına kodun parametreleri denir $[4]$.

Tanım 1.1.43. p bir asal sayı olmak üzere $p^k = q$ ve $\mathbb{F}_q$, karakteristiği p olan sonlu bir cisim olsun. $\mathbb{F}_q^n = \{(v_1, v_2, \ldots, v_n) : v_i \in F_q\}$ ve $V \subset \mathbb{F}_q^n$ boştan farklı bir küme olmak üzere; V vektörel toplama olan "+" işlemi ile $\mathbb{F}_q$ nun elemanları ile skaler çarpım "•" işlemine göre aşağıdaki koşulları sağlıyor ise V ye $\mathbb{F}_q$ üzerinde bir vektör uzayı denir.

Her $u,v \in V$ ve $\lambda,\mu \in \mathbb{F}_q$ için;

1) $(V,+)$ değişmeli grup,
2) $\lambda \bullet v \in V$,
3) $\lambda \bullet (u+v) = \lambda \bullet u + \lambda \bullet v$ ve $(\lambda+\mu)\bullet u = \lambda \bullet u + \mu \bullet u$,
4) $(\lambda\mu)\bullet u = \lambda \bullet (\mu \bullet u)$,
5) Eğer $\mathbb{F}_q$ nun çarpmaya göre etkisiz elemanı 1 ise $1 \bullet u = u$ olur [4].

Tanım 1.1.44. V vektör uzayının boştan farklı bir C alt kümesi, V vektör uzayındaki vektörel toplam ve skalerle çarpma işlemlerine göre kendi başına bir vektör uzayı ise C 'ye V vektör uzayının bir alt vektör uzayı denir [4].

Tanım 1.1.45. $\mathbb{F}_q^n$ vektör uzayının herhangi bir C alt vektör uzayı bir lineer kod olarak tanımlanır [4].

Tanım 1.1.46. C, bir $[n,k]$ lineer kod olsun.

$C^{\perp} = \{x \in \mathbb{F}_q^n : \langle x,c \rangle = 0, \forall c \in C\}$

kümesine C kodunun dual kodu denir [4]

Tanım 1.1.47. C, $\mathbb{F}_q$ üzerinde bir lineer kod olsun. Eğer $\forall c = (c_0, c_1, \ldots c_{n-1}) \in C$ için $(c_{n-1}, c_0, \ldots, c_{n-2}) \in C$ oluyorsa C 'ye $\mathbb{F}_q$ üzerinde devirli kod denir [4].

Teorem 1.1.7. $R_n = \mathbb{F}_q[x] / \langle x^n - 1 \rangle$ olmak üzere $\Phi : \mathbb{F}_q^n \to R_n$, $\Phi((c_0, c_1, \ldots c_{n-1})) = c_0 + c_1 x + \ldots + c_{n-1}x^{n-1}$ şeklinde tanımlanan Φ fonksiyonu bir izomorfizmadır [4].

Teorem 1.1.8. C, $\mathbb{F}_q$ de üzerinde bir lineer kod olsun. Eğer C kodu R_n halkasının bir ideali ise C kodu $\mathbb{F}_q$ üzerinde bir devirli kod olur [4].

Tanım 1.1.48 R_n in sıfırdan farklı bir I idealindeki en düşük dereceli indirgenemez monik polinom $g(x)$ olsun. $g(x)$ polinomuna I idealinin üreteç polinomu denir. Eğer $C=\Phi(I)$ ise I'nın üreteç polinomuna C'nin üreteç polinomu denir. $I=\langle g(x)\rangle$ olduğundan $g(x)\big|(x^n-1)$ dir [4].

Teorem 1.1.9. $g(x)=g_0+g_1x+\ldots+g_{n-k}x^{n-k}$ polinomu, $\mathbb{F}_q^n$ de bir C devirli kodunun üreteç polinomu ve $der[g(x)]=n-k$ olsun. Bu durumda

$$G\begin{pmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{n-k}g(x) \end{pmatrix}=\begin{pmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & 0 & \cdots & g_0 & g_1 & g_2 & \cdots & g_{n-k} \end{pmatrix}$$

matrisi C kodunun üreteç matrisi olur [4].

Tanım 1.1.49. C, kodu $\mathbb{F}_q^n$ de bir devirli kod, $g(x)$ polinomu C kodunun üreteç polinomu olsun ve $h(x)=\dfrac{x^n-1}{g(x)}$ olsun. $h(x)$ polinomuna C kodunun kontol polinomu denir [4].

Teorem 1.1.10. C, $\mathbb{F}_q^n$ de bir devirli kod ve $h(x)$ polinomu C kodunu kontrol polinomu olsun. Eğer $h(x)=h_0+h_1x+\ldots+h_{n-r}x^{n-r}$ ise bu durumda C kodunun kontrol matrisi

$$H=\begin{bmatrix} h_{n-r} & \cdots & h_0 & 0 & 0 & \cdots & 0 \\ 0 & h_{n-r} & \cdots & h_0 & 0 & \cdots & 0 \\ 0 & 0 & h_{n-r} & 0 & h_0 & & \vdots \\ \vdots & \vdots & \ddots & \ddots & \cdots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & h_{n-r} & \cdots & h_0 \end{bmatrix}$$

olur [4].

Tanım 1.1.50. Eğer C $[n,k]$ kodunun üreteç matrisi $k\,x\,n$ boyutlu G matrisisin standart formu $G=(I_k : A)$ ise $C^{\perp}$'in üreteç matrisi $H=(-A^T : I_{n-k})$ olur. H matrisine C kodunun kontrol matrisi de denir [4].

Tanım 1.1.51. C kodu $\mathbb{F}_q$ üzerinde $[n,k,d]$ lineer kod ve H, C kodunun kontrol matrisi olsun. Herhangi bir $u \in \mathbb{F}_q^n$ için u nun sendromu $S(u)=uH^T \in \mathbb{F}_q^{n-k}$ olarak tanımlanır [4].

BÖLÜM 2. $\mathbb{Z}[w]_{\pi}$ ÜZERİNDE DEVİRLİ KODLAR

İlk klasik kodlar $\mathbb{F}_2$ cismi üzerinde tanımlandıktan sonra farklı cisim üzerinde kodlama çalışılmıştır. q bir asalın kuvvet i olmak üzere $\mathbb{F}_q$ üzerinde bugüne kadar birçok makale yazılmıştır. Bu makalelerde genelde Hamming metriği kullanılmıştır. $\mathbb{F}_q$ sonlu cisminden farklı olarak çeşitli yeni metrikler tanımlanarak bu metriklerle uyum içinde çalışan çeşitli sonlu cisimler üzerinde de kodlama yapılmıştır. Örneğin 1994 de Gauss tam sayılarından yararlanılarak oluşturulan $\mathbb{Z}[i]_{\pi}$ sonlu cismi üzerinde Mannheim metriğine göre lineer kodlar inşa edilmiştir [5].

Bu bölümde Eisenstein-Jacobi tamsayılar kümesi ve bu kümenin cebirsel özellikleri verilecektir. Eisenstein-Jacobi tamsayılar kümesinden $\mathbb{Z}^+ \cup \{0\}$ kümesine tanımlı bir norm fonksiyonu verilip, bu norm fonksiyonuna göre normu asal olan bir Eisenstein-Jacobi tamsayısının tam temsilcilerinden oluşan bir küme verilecektir. Daha sonra bu küme üzerinde $w-$devirli kodlar kodlardan bahsedilerek bu küme üzerinde hata düzeltebilen kodlar ve dekodlama algoritmaları verilecektir. Bu konu ile ilgili daha detaylı bilgilere [6] ve [7] den ulaşılabilir.

Eisenstein-Jakobi Tamsayılar Kümesi

Eisenstein-Jacobi tamsayılar kümesi

$$\mathbb{Z}[w]=\left\{a+bw : a,b\in\mathbb{Z}, w=\frac{1}{2}+\frac{i\sqrt{3}}{2}, i^2=-1\right\}$$

şeklinde tanımlanır.

Bu kümede bir $a+bw\in\mathbb{Z}[w]$ elemanının eşleniği $a+bw^*$ ile gösterilir.

$\mathbb{Z}[w]$ üzerinde N norm fonksiyonu

$$N:\mathbb{Z}[w]\to\mathbb{Z}^+\cup\{0\}$$

$$\begin{aligned}N(a+bw)&=(a+bw).(a+bw^*)\\&=(a+bw)(a+bw^*)\\&=a^2+ab+b^2\end{aligned}$$

dir.

Bu norm fonksiyonuna göre bölme algoritması

$\forall x,y\in\mathbb{Z}[w],\ y\neq 0$ için $x=qy+r,\ 0\le N(r)<N(y)$

olarak tanımlanır.

$\pi\in\mathbb{Z}[w]$ ve $N(\pi)=p$ olmak üzere $\mathbb{Z}_p$'nin elemanlarından $\mathbb{Z}[w]_\pi$'nin elemanları aşağıdaki yöntem ile elde edilebilir.

1. p bir tek asal sayı, $\pi=a+bw$ ve $N(\pi)=\pi\pi^*=p$ $N(\pi)=\pi\pi^*=p$ olsun.
2. $a+br\equiv 0\pmod{p}$, denkleminin $0\le r\le p-1$ koşulunu sağlayan tek çözümü s olsun.
3. $l\in\mathbb{Z}_p$ ve $N(\alpha)$ minimum olmak üzere eğer $x+sy\equiv l\pmod{p}$ ise $\alpha=x+yw\in\mathbb{Z}[w]_\pi$ dir.

Örnek : $p=19$ olsun. $19\equiv 1 \pmod 6$ dır.

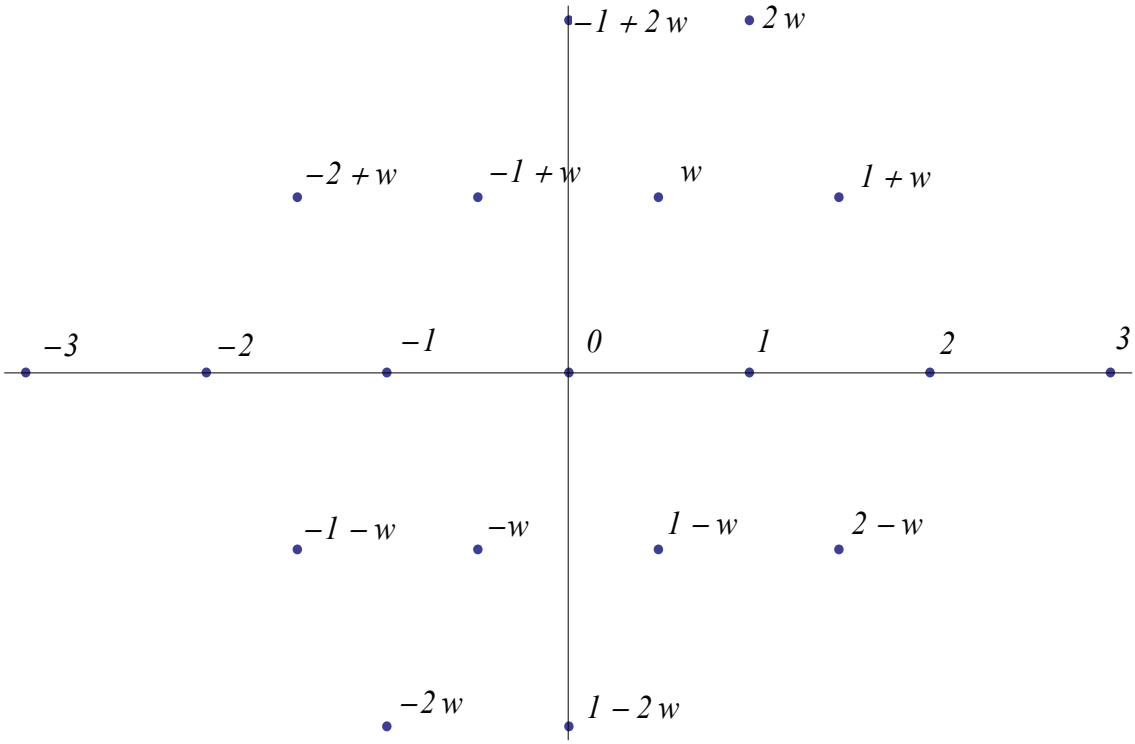
1. $N(a+bw)=a^2+ab+b^2=19$ denkleminin bir çözümü $(a,b)=(2,3)$ dir. O halde $\pi=2+3w$ olur.
2. $2+3r\equiv 0 \pmod{19}$ denkleminin $0\le r\le p-1$ koşulunu sağlayan tek çözüm $r=12$ dir.
3. $l\in\mathbb{Z}_{19}$ ve $N(\alpha)$ minimum olmak üzere $x+12y\equiv l \pmod{19}$ ise $\alpha=x+yw\in\mathbb{Z}[w]_\pi$ olur.

Bu durumda $\mathbb{Z}_{19}$'un elemanlarının $\pi=2+3w\in\mathbb{Z}[w]$ olmak üzere mod π sayısına göre kalan sınıflarından oluşan $\mathbb{Z}[w]_\pi$ kümesinin elemanları Tablo 1.'deki gibidir.

Tablo 1. $\mathbb{Z}_{19}$ un elemanlarının $\mathbb{Z}[w]_\pi$ deki karşılıkları

$0\equiv 0 \pmod{2+3w}$	$7\equiv -w \pmod{2+3w}$	$14\equiv 2w \pmod{2+3w}$
$1\equiv 1 \pmod{2+3w}$	$8\equiv 1-w \pmod{2+3w}$	$15\equiv 1-2w \pmod{2+3w}$
$2\equiv 2 \pmod{2+3w}$	$9\equiv 2-w \pmod{2+3w}$	$16\equiv -3 \pmod{2+3w}$
$3\equiv 3 \pmod{2+3w}$	$10\equiv -2+w \pmod{2+3w}$	$17\equiv -2 \pmod{2+3w}$
$4\equiv -1+2w \pmod{2+3w}$	$11\equiv -1+w \pmod{2+3w}$	$18\equiv -1 \pmod{2+3w}$
$5\equiv 2w \pmod{2+3w}$	$12\equiv w \pmod{2+3w}$	
$6\equiv -1-w \pmod{2+3w}$	$13\equiv 1+w \pmod{2+3w}$	

Bu elemanlar kompleks düzlemde Şekil 1'deki gibidir.



Şekil 1 $\mathbb{Z}[w]_{\pi}$ kümesi

Not: Aksi söylenmedikçe bundan sonra $p \equiv 1 \pmod 6$ bir asal tamsayı ve $n = \frac{p-1}{6}$ alınacaktır.

Tanım: $\alpha, \beta \in \mathbb{Z}[w]_{\pi}$ ve $\alpha - \beta \equiv x + yw \in \mathbb{Z}[w]_{\pi}$ olsun.

Bu durumda α ile β arasındaki Mannheim mesafesi

$d_m(\alpha, \beta) = |x| + |y|$ dir.

$\alpha - \beta \equiv x + yw = \gamma \in \mathbb{Z}[w]_{\pi}$ olmak üzere, γ'nın Mannheim ağırlığı ise

$w_m(\gamma) = d_m(\alpha, \beta)$

olarak tanımlanır.

Teorem 2.1.1. $\pi = a + bw \in \mathbb{Z}_p[w]$ ve $N(\pi) = a^2 + ab + b^2$ olsun. Bu durumda $\mathbb{Z}[w]_{\pi}$ üzerinde herhangi iki elemanın maksimum Mannheim mesafesi

$d_{\max} = \max\{|a|,|b|,|a+b|\} - 1$

dir [7].

$\mathbb{Z}[w]_{\pi}$ Üzerinde Devirli ve w - Devirli Kodlar

Tanım : $\left(\mathbb{Z}[w]_{\pi}\right)^n$ vektör uzayının bir alt vektör uzayı olan C'ye $\mathbb{Z}[w]_{\pi}$ üzerinde bir lineer kod denir.

Tanım : C, $\mathbb{Z}[w]_{\pi}$ üzerinde bir lineer kod olsun. Eğer $\forall\ c = (u_0, u_1, ..., u_{n-1}) \in C$ için $(wu_{n-1}, u_0, ..., u_{n-2}) \in C$ oluyorsa C'ye $\mathbb{Z}[w]_{\pi}$ üzerine bir $w-$devirli kod denir. Burada w, $\mathbb{Z}[w]$'nun bir birimsel elemanıdır.

$p \in \mathbb{Z}$ olmak üzere $p = 6n+1$ şeklinde bir asal sayı, $\pi \in \mathbb{Z}[w]$ olmak üzere $p = \pi\pi^*$ ve

β, $\mathbb{Z}[w]_{\pi}$ da mertebesi $6n$ olan bir eleman olsun. Bu durumda $\beta^{6n} = 1$, yani $\beta^n = \pm w$ olur. β bir ilkel eleman olduğundan

$\mathbb{Z}[w]_{\pi} = \{0, 1, \beta, \beta^2, ..., \beta^{6n-1}\}$

olur.

Örnek : Bir önceki örnekte $\beta = 1+w$ alınırsa $\mathbb{Z}[w]_\pi = \{0, \beta^1, \beta^2, \ldots, \beta^{18}\}$ olarak yazılır ve $\mathbb{Z}[w]_\pi / \{0\}$ kümesinin elemanları β'nın kuvvetleri olarak Tablo 2'deki gibi olur.

Tablo 2 $\mathbb{Z}[w]_\pi / \{0\}$ kümesinin elemanları

$\beta = 1+w$	$\beta^7 = -2+w$	$\beta^{13} = 1-2w$
$\beta^2 = -2$	$\beta^8 = -3$	$\beta^{14} = 2w$
$\beta^3 = w$	$\beta^9 = -1$	$\beta^{15} = 1-w$
$\beta^4 = -1+2w$	$\beta^{10} = -1-w$	$\beta^{16} = 2-w$
$\beta^5 = -2w$	$\beta^{11} = 2$	$\beta^{17} = 3$
$\beta^6 = -1+w$	$\beta^{12} = -w$	$\beta^{18} = 1$

Teorem : $t = 0,1,\ldots,n-1$ ve $\beta^n = w$ olan $\beta \in \mathbb{Z}[w]_\pi$ olmak üzere $g(x) = (x-\beta)(x-\beta^7)\ldots(x-\beta^{6t+1})$ olsun.

O halde $g(x) \mid (x^n - \beta^n)$ ve $g(x)$ polinomu C kodu içi bir üreteç polinomudur.

Burada C kodu, $\mathbb{Z}[w]_\pi[x] / \langle x^n - w \rangle$ halkasının bir esas idealidir.

Bir $c(x)$ kodsözünün $x^n - w$ modülosuna göre x ile çarpımı

$$xc(x) - c_{n-1}(x^n - w) = wc_{n-1} + c_0 x + c_1 x^2 + \cdots + c_{n-2} x^{n-1}$$

dir. C kodu $g(x)$ ile üretilen bir ideal olduğundan $xc(x)$ çarpımı da C'nin bir elemanı olur.

$c(x)$ polinomunun $x^n - w$ modülosuna göre x ile çarpımından aşağıdakiler elde edilir.

1. $c(x)$'in her katsayısı bir konum sağa kaydırılır.

2. c_{n-1} katsayısı kompleks düzlemde $\pi/3$ radyan döndürülerek yeni kodsöz polinomunun ilk katsayısı elde edilir.

Bu durumda elde edilen C kodu $w-$devirli kod olarak tanımlanır. Eğer $\beta^n = -w$ ise C koduna $-w-$devirli kod denir.

Örnek : $p = 19$ olsun. Örnek 1'den $\pi = 2 + 3w$ olur. $\mathbb{Z}[w]_\pi$ de $(1+w)^3 = w$ olduğundan $\beta = 1 + w$ dir. O halde Teorem 1'den

$$x^3 - w = (x-\beta)(x-\beta^7)(x-\beta^{13})$$

olur. $x^3 - w$ nun çarpanlarından $g(x)$ üreteç polinomunu

$$g(x) = (x-\beta)(x-\beta^7)$$

olacak şekilde seçelim. Buradan

$$g(x) = (x-\beta)(x-\beta^7) = x^2 + (-\beta-\beta^7)x + \beta^8 = x^2 + \beta^{13}x + \beta^8$$

olarak hesaplanır. $g(x)$ polinomundan elde edilen üreteç matrisi;

$$G = \begin{bmatrix} \beta^8 & \beta^{13} & 1 \end{bmatrix}_{1x3} = \begin{bmatrix} -3 & 1-2w & 1 \end{bmatrix}_{1x3}$$

şeklinde hesaplanır.

$G=\begin{bmatrix}-3 & 1-2w & 1\end{bmatrix}_{1x3}$ üreteç matrisi ile $19^1=19$ adet kodsöz üretilir. Bu durumda C kodu

$$C=\{(0,0,0),(-3,1-2w,1),(1+w,-1+w,2),(-2+w,-w,3),(-w,3,-1+2w),(-1+2w,-1,2w),$$
$$(1,-2w,-1-w),(-2,-2+w,-w),(-2w,-1-w,1-w),(-1+w,2,2-w),(1-w,-2,-2+w),$$
$$(2w,1+w,-1+w),(2,2-w,w),(-1,2w,1+w),(1-2w,1,-2w),(w,-3,1-2w),(2-w,w,-3),$$
$$(-1-w,1-w,-2),(3,-1+2w,-1)\}$$

olur.

$(0,0,0)$ kodsözü hariç, C kodunun elemanlarının en küçük Mannheim ağırlığı $w_m=5$ olduğundan, minimum mesafe $d_m=5$ dir.

2.3. $\mathbb{Z}[w]_\pi$ Üzerinde Dekodlama

Bu bölümde, $\mathbb{Z}[w]_\pi$ sonlu cismi üzerindeki kodların dekodlama algoritması gösterilecek. $\beta\in\mathbb{Z}[w]_\pi$, mertebesi $6n=p-1$ ve $\beta^n=w$ şeklinde yazılabilen ilkel eleman olsun. Bu durumda $\mathbb{Z}[w]_\pi=\langle\beta\rangle\cup\{0\}$ şeklinde yazılabilir.

Teorem 2.3.1. C kodu $\mathbb{Z}[w]_\pi$ üzerinde

$$H=\begin{bmatrix}1 & \beta & \beta^2 & \cdots & \beta^{n-1}\end{bmatrix}$$

kontrol matrisine sahip bir $w-$devirli kod olsun. $w_M(e_i)=1$ ve $w_M(\pm w^2)=2$ olmak üzere C kodu $0\le i\le n-1$ için her $e(x)=e_ix^i$ şeklindeki hataları düzeltilebilir [7].

Örnek 2.3.1. $p=19$ olsun. Örnek 2.1.1.'den $\pi=2+3w$ olur $n=\dfrac{19-1}{6}=3$ ve Örnek 2.1.2.'den $\beta\in\mathbb{Z}[w]_\pi$ için $\beta^n=\beta^3=w$ olacak şekilde $\beta=1+w$ alalım. Teorem 2.3.1.'den C kodunun kontrol matrisi

$H = \begin{bmatrix} 1 & \beta & \beta^2 \end{bmatrix}$

olur. Bu durumda H kontrol matrisinden C kodunun üreteç matrisi

$$G = \begin{bmatrix} \beta^{10} & \beta^{18} & 0 \\ \beta^{11} & 0 & \beta^{18} \end{bmatrix}$$

şeklinde elde edilir.

$c = (-1-w, 1, 0) = \begin{pmatrix} \beta^{10} & \beta^{18} & 0 \end{pmatrix} \in C$ kodsözü kanala girsin. Kanalda $e = (0, w, 0) = \begin{pmatrix} 0 & \beta^3 & 0 \end{pmatrix}$ hatası oluşursa alınan söz $r = c + e = (-1-w, 1+w, 0) = \begin{pmatrix} \beta^{10} & \beta & 0 \end{pmatrix}$ olur. r 'nin sendromu

$$S(r) = r.H^T = \begin{bmatrix} \beta^{10} & \beta & 0 \end{bmatrix} \begin{bmatrix} 1 \\ \beta \\ \beta^2 \end{bmatrix} = \beta^{10} + \beta^2 = \beta^4 = \beta^L$$

olarak hesaplanır.

Burada $L = 4$ olup, $4 \equiv 1 \pmod 3$ olduğundan hata $1+1=2.$inci bileşende meydana gelmiştir. $\frac{\beta^4}{\beta} = \beta^3$ hatanın ağırlığı olup, kanalda oluşan hatanın $e = (0, \beta^3, 0) = (0, w, 0)$ olduğu tespit edilir.

$c = (2, 0, 1) = \begin{pmatrix} \beta^{11} & 0 & \beta^{18} \end{pmatrix} \in C$ kodsözü kanala girsin. Kanalda $e = (0, w^2, 0) = \begin{pmatrix} 0 & \beta^6 & 0 \end{pmatrix}$ hatası oluşursa alınan söz $r = c + e = (2, -w^2, 1) = \begin{pmatrix} \beta^{11}, \beta^6, \beta^{18} \end{pmatrix}$ olur. r 'nin sendromu

$$S(r) = rH^T = \begin{bmatrix} \beta^{11} & \beta^6 & \beta^{18} \end{bmatrix} \begin{bmatrix} 1 \\ \beta \\ \beta^2 \end{bmatrix} = \beta^{11} + \beta^7 + \beta^{20} = \beta^7 = \beta^L$$

olarak hesaplanır.

Burada $L=7$ olup, $7\equiv 1(\mathrm{mod}\,3)$ olduğundan hata $1+1=2.$inci bileşende meydana gelmiştir. $\frac{\beta^7}{\beta}=\beta^6$ hatanın ağırlığı olup, kanalda oluşan hatanın $e=(0,\beta^6,0)=(0,-w^2,0)$ olduğu tespit edilir.

$c=(1-w,1,1)=(\beta^{15}\quad \beta^{18}\quad \beta^{18})\in C$ kodsözü kanala girsin. Kanalda $e=(0,0,2w)=(0\quad 0\quad \beta^{14})$ hatası oluşursa alınan söz $r=c+e=(1-w,1,1+2w)=(\beta^{15},\beta^{18},\beta^{10})$ olur. r 'nin sendromu

$$S(r)=rH^T=\begin{bmatrix}\beta^{15} & \beta^{18} & \beta^{10}\end{bmatrix}\begin{bmatrix}1\\ \beta\\ \beta^2\end{bmatrix}=\beta^{15}+\beta^{19}+\beta^{12}=\beta^{16}=\beta^L$$

olarak hesaplanır.

Burada $L=16$ olup, $16\equiv 1(\mathrm{mod}\,3)$ olduğundan hata $1+1=2.$inci bileşende meydana gelmiştir. $\frac{\beta^{16}}{\beta}=\beta^{15}$ hatanın ağırlığı olup, kanalda oluşan hatanın $e=(0,\beta^{15},0)=(0,1-w,0)$ olduğu tespit edilir. Halbuki $e=(0,0,2w)$ olmalıydı.

Teorem 2.3.2. C kodu $\mathbb{Z}[w]_\pi$ üzerinde

$$H=\begin{bmatrix}1 & \beta & \beta^2 & \cdots & \beta^{n-1}\\ 1 & \beta^7 & \beta^{14} & \cdots & \beta^{7(n-1)}\end{bmatrix}$$

kontrol matrisine sahip bir $w-$devirli kod olsun. $1\le w_m(e_i)\le d_{\max}$ olmak üzere C kodu $0\le i\le n-1$ için her $e(x)=e_ix^i$ şeklindeki hataları düzeltilebilir [7].

Örnek 2.3.2. $p=19$ olsun. $\beta\in\mathbb{Z}[w]_\pi$ elemanı Örnek 2.3.1.'deki gibi seçilirse, $\beta^3=w$ olur. O halde Teorem 2.3.2.'den C kodunun kontrol matrisi

$$H=\begin{bmatrix}1 & \beta & \beta^2\\ 1 & \beta^7 & \beta^{14}\end{bmatrix}$$

olur. Bu durumda C kodunun üreteç matrisi

$G = \begin{bmatrix} \beta^8 & \beta^{13} & 1 \end{bmatrix}$

şeklinde elde edilir.. $c = (-3, 1-2w, 1) = \begin{pmatrix} \beta^8 & \beta^{13} & \beta^{18} \end{pmatrix} \in C$ kodsözü kanala girsin. Kanalda $e = (0, 0, 2w) = \begin{pmatrix} 0 & 0 & \beta^{14} \end{pmatrix}$ hatası oluşursa alınan söz $r = c + e = (-3, 1-2w, 1+2w) = \left(\beta^8, \beta^{13}, \beta^{10}\right)$ olur. r 'nin sendromu

$$S(r) = rH^T = \begin{bmatrix} \beta^8 & \beta^{13} & \beta^{10} \end{bmatrix} \begin{bmatrix} 1 & 1 \\ \beta & \beta^7 \\ \beta^2 & \beta^{14} \end{bmatrix} = \begin{bmatrix} \beta^{16} & \beta^{10} \end{bmatrix} = \begin{bmatrix} \beta^{L_1} & \beta^{L_2} \end{bmatrix}$$

olarak hesaplanır.

Burada $L_1 = 16$ ve $L_2 = 10$ olup, $\frac{10-16}{6} \equiv 2 \pmod 3$ olduğundan hata $2+1=3.$ bileşende meydana gelmiştir. $16-2 \equiv 14 \pmod{18}$ olup, hatanın ağırlığı β^{14} olur. Kanalda oluşan hatanın $e = \left(0, 0, \beta^{14}\right) = (0, 0, 2w)$ olduğu tespit edilir.

Teorem 2.3.3. C kodu $\mathbb{Z}[w]_\pi$ üzerinde

$$H = \begin{bmatrix} 1 & \beta & \cdots & \beta^j & \cdots & \beta^k & \cdots & \beta^{n-1} \\ 1 & \beta^7 & \cdots & \beta^{7j} & \cdots & \beta^{7k} & \cdots & \beta^{7(n-1)} \\ 1 & \beta^{13} & \cdots & \beta^{13j} & \cdots & \beta^{13k} & \cdots & \beta^{13(n-1)} \end{bmatrix}$$

kontrol matrisine sahip bir $w-$devirli kod olsun. $0 \le w_m(e_j), w_m(e_k) \le 1$ olmak üzere C kodu $0 \le j, k \le n-1$ için her $e(x) = e_j x^j + e_k x^k$ şeklindeki hataları düzeltilebilir [7].

İki hatalı kodlar aşağıdaki yöntem ile dekodlanır [7].

1. $j = 1, 7, 13$ için $S_j = r\left(\beta^j\right)$ sendromları hesaplanır.
2. Eğer $S_1 = 0$ ise hata yoktur ve işlem biter.
3. Eğer $S_7 = S_1^7$ ve $S_{13} = S_1^{13}$ ise bir hata oluşmuştur. $S_1 = \beta^{L_1}$ olup, $j \equiv L_1 \pmod n$ dir. Burada j hatanın konumunu $\beta^{L_1 - j}$ ise hatanın değerini gösterir.

4. $S_7 \neq S_1^{\,7}$ veya $S_{13} \neq S_1^{\,13}$ ise iki bileşende 1 ağırlığında hata oluşmuştur. $x^2 - (S_1)x - \dfrac{t_0}{t_1}$ denkleminin kökleri $x_1 = \beta^{L_1}$ ve $x_2 = \beta^{L_2}$ olmak üzere $j \equiv L_1 \pmod n$ ve $k \equiv L_2 \pmod n$ hataların konumlarını, $\beta^{L_1 - j}$ ve $\beta^{L_2 - k}$ ise hataların ağırlıklarını gösterir. $\begin{pmatrix} t_0 = S_1^{\,2}\left(S_1^{\,14} + 26S_1^{\,14}S_7 + 169S_7^{\,2} - 196S_1S_{13}\right) \\ t_1 = -\left(4S_1^{\,14} + 104S_1^{\,14}S_7 + 39S_7^{\,2} - 147S_1S_{13}\right) \end{pmatrix}$

Örnek 2.3.3. $p = 31$ olsun. $N(a + bw) = a^2 + ab + b^2 = 31$ denkleminin bir çözümü $(a,b) = (5,1)$ olduğundan $\pi = 5 + w$ olur. $n = \dfrac{31-1}{6} = 5$ ve $\beta \in \mathbb{Z}[w]_\pi$ için $\beta^5 = w$ olacak şekilde $\beta = 3$ alalım. Teorem 2.3.3.'ten C kodunun kontrol matrisi

$$H = \begin{bmatrix} 1 & \beta & \beta^2 & \beta^3 & \beta^4 \\ 1 & \beta^7 & \beta^{14} & \beta^{21} & \beta^{28} \\ 1 & \beta^{13} & \beta^{26} & \beta^9 & \beta^{22} \end{bmatrix}$$

olur. Bu durumda H kontrol matrisinden C kodunun üreteç matrisi

$$G = \begin{bmatrix} 1 & 0 & \beta & \beta^{13} & \beta^{21} \\ 0 & 1 & \beta^{12} & \beta^{20} & \beta^{24} \end{bmatrix}$$

şeklinde elde edilir. $c = (1 \quad 0 \quad \beta \quad \beta^{13} \quad \beta^{21}) = (1 \quad 0 \quad 3 \quad -2 + w \quad -3w) \in C$ kodsözü kanala girsin. Kanalda $e = (\beta^{15} \quad 0 \quad 0 \quad \beta^{20} \quad 0) = (-1 \quad 0 \quad 0 \quad -w \quad 0)$ hatası oluşursa alınan söz $r = c + e = (0 \quad 0 \quad 3 \quad -2 \quad -3w)(0 \quad 0 \quad \beta \quad \beta^9 \quad \beta^{21})$ olur. r 'nin sendromu

$$S(r) = Hr^T = \begin{bmatrix} 1 & \beta & \beta^2 & \beta^3 & \beta^4 \\ 1 & \beta^7 & \beta^{14} & \beta^{21} & \beta^{28} \\ 1 & \beta^{13} & \beta^{26} & \beta^9 & \beta^{22} \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ \beta \\ \beta^9 \\ \beta^{21} \end{bmatrix} = \begin{bmatrix} \beta^{14} \\ \beta^{19} \\ \beta^8 \end{bmatrix} = \begin{bmatrix} S_1 \\ S_7 \\ S_{13} \end{bmatrix}$$

olarak hesaplanır.

$S_7 \neq S_1^{\,7}$ olduğundan iki bileşende 1 ağırlığında hata oluşmuştur. Burada $t_0 = \beta^{22}$ ve $t_1 = \beta^{15}$ olup, $x^2 - \beta^{14}x + \beta^8 = 0$ denkleminin kökleri $x_1 = \beta^{L_1} = \beta^{15}$ ve $x_2 = \beta^{L_2} = \beta^{23}$ olur.

$$\begin{cases} j = 0 \equiv 15 \pmod 5 \\ k = 3 \equiv 23 \pmod 5 \end{cases}$$

$j = 0$ ve $k = 3$ hataların konumlarını gösterip, $\beta^{15-0} = \beta^{15}$ ve $\beta^{23-3} = \beta^{20}$ hataların ağırlığını gösterir. O halde $e = \begin{pmatrix} \beta^{15} & 0 & 0 & \beta^{20} & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 & 0 & -w & 0 \end{pmatrix}$ olarak tespit edilir.

Teorem 2.3.4. C kodu $A_p[w]$ üzerinde

$$H = \begin{bmatrix} 1 & \beta & \beta^7 & \cdots & \beta^{(n-1)} \\ 1 & \beta^7 & \beta^{14} & \cdots & \beta^{7(n-1)} \\ 1 & \beta^{13} & \beta^{21} & \cdots & \beta^{13(n-1)} \\ 1 & \beta^{19} & \beta^{38} & \cdots & \beta^{19(n-1)} \end{bmatrix}$$

kontrol matrisine sahip bir $w-$devirli kod olsun. $1 \le w_m(e_i), w_m(e_j) \le d_{\max}$ olmak üzere C kodu $0 \le i, j \le n-1$ için her $e(x) = e_i x^i + e_j x^j$ şeklindeki hataları düzeltilebilir [7].

İki hatalı kodlar aşağıdaki yöntem ile dekodlanır.

1. $j = 1,7,13,19$ için $S_j = r(\beta^j)$ sendromları hesaplanır.
2. Eğer $S_1 = 0$ ise hata yoktur ve işlem biter.
3. Eğer $S_1 S_{13} - S_7^{\,2} = 0$ ise bir hata gerçekleşmiştir. $S_1 = \beta^{L_1}$ ve $S_7 = \beta^{L_2}$ olup, $i \equiv \dfrac{L_2 - L_1}{6} \pmod n$ hatanın konumunu, $k \equiv L_1 - i \pmod{p-1}$ ise hatanın değerini gösterir.
4. Eğer $S_1 S_{13} - S_7^{\,2} \neq 0$ ise iki bileşende hata gerçekleşmiştir.

$x^2 - Sx + P = 0$ denkleminin kökleri $x_1 = \beta^{6i}$ ve $x_2 = \beta^{6j}$ olup, hata $i.$ inci ve $j.$ inci bileşende gerçekleşmiştir. Burada $S = \dfrac{\left(S_1 S_{19} - S_7 S_{13}\right)}{\left(S_1 S_{13} - {S_7}^2\right)}$ ve $P = \dfrac{\left(S_7 S_{19} - {S_{13}}^2\right)}{\left(S_1 S_{13} - {S_7}^2\right)}$ dir.

Hataların ağırlıkları $e_i = \dfrac{S_7 - \beta^{6j} S_1}{\beta^i \left(\beta^{6i} - \beta^{6j}\right)}$ ve $e_j = \dfrac{S_7 - \beta^{6i} S_1}{\beta^j \left(\beta^{6j} - \beta^{6i}\right)}$ dir [7].

Örnek 2.3.4. $p = 31$ olsun. $\beta \in \mathbb{Z}[w]_\pi$ Örnek 2.3.3.'teki gibi $\beta = 3$ olarak seçilirse, $\beta^5 = w$ olur. Teorem 2.3.4.'ten C kodunun kontrol matrisi

$$H = \begin{bmatrix} 1 & \beta & \beta^2 & \beta^3 & \beta^4 \\ 1 & \beta^7 & \beta^{14} & \beta^{21} & \beta^{28} \\ 1 & \beta^{13} & \beta^{26} & \beta^9 & \beta^{22} \\ 1 & \beta^{19} & \beta^8 & \beta^{27} & \beta^{16} \end{bmatrix}$$

olur. Bu durumda H kontrol matrisinden C kodunun üreteç matrisi

$$G = \begin{bmatrix} \beta^{10} & \beta^{15} & \beta^{20} & \beta^{25} & 1 \end{bmatrix}$$

şeklinde hesaplanır.

$c = \left(\beta^{10} \quad \beta^{15} \quad \beta^{20} \quad \beta^{25} \quad 1\right) \in C$ kodsözü kanala girsin. Kanalda $e = \left(0 \quad 0 \quad \beta^5 \quad \beta^{10} \quad 0\right) = \left(0 \quad 0 \quad w \quad -1+w \quad 0\right)$ hatası oluşursa alınan söz $r = c + e = \left(\beta^{10} \quad \beta^{15} \quad 0 \quad 0 \quad 1\right)$ olur.

r'nin sendromu

$$S(r) = Hr^T = \begin{bmatrix} 1 & \beta & \beta^2 & \beta^3 & \beta^4 \\ 1 & \beta^7 & \beta^{14} & \beta^{21} & \beta^{28} \\ 1 & \beta^{13} & \beta^{26} & \beta^9 & \beta^{22} \\ 1 & \beta^{19} & \beta^8 & \beta^{27} & \beta^{16} \end{bmatrix} \begin{bmatrix} \beta^{10} \\ \beta^{15} \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \beta^{24} \\ \beta^{11} \\ \beta^{11} \\ \beta^{24} \end{bmatrix} = \begin{bmatrix} S_1 \\ S_7 \\ S_{13} \\ S_{19} \end{bmatrix}$$

olarak hesaplanır.

$S_1 S_{13} - S_7{}^2 \neq 0$ olduğundan iki bileşende hata meydana gelmiştir. Burada $S = \beta^{29}$ ve $P = \beta^0 = 1$ olup, $x^2 - \beta^{29} x + 1 = 0$ denkleminin kökleri $x_1 = \beta^{6i} = \beta^{12}$ ve $x_2 = \beta^{6j} = \beta^{18}$ olur. $i = 2$ ve $j = 3$ olup, 3. ve 4. bileşenlerde hata gerçekleşmiştir. $e_2 = \dfrac{\beta^{11} - \beta^{18}\beta^{24}}{\beta^2\left(\beta^{12} - \beta^{18}\right)} = \dfrac{\beta^{25}}{\beta^{20}} = \beta^5$ ve $e_3 = \dfrac{\beta^{11} - \beta^{12}\beta^{24}}{\beta^3\left(\beta^{18} - \beta^{12}\right)} = \dfrac{\beta^{16}}{\beta^6} = \beta^{10}$ hata ağırlıklarıdır. O halde $e = \left(0 \quad 0 \quad \beta^5 \quad \beta^{10} \quad 0\right)$ olarak tespit edilir.

BÖLÜM 3. F_p ÜZERİNDE KUANTUM KODLAR

Bugüne kadar birçok yazar farklı halkalar veya farklı cisimler üzerinde hata düzeltebilen klasik kodlar ve kuantum kodlar üzerine çalışmıştır. Aşağıda yapılmış çalışmalar bunlara birer örnektir. 1950 de Hamming hata tespit edebilen ve hata düzeltilebilen kodları Hamming metriğine göre $\mathbb{Z}_2$ sonlu cismi üzerinde elde etmiştir [9]. 1958 de Lee $\mathbb{Z}_m$ sonlu halkası üzerinde Lee metriğine göre hata düzeltebilen kodlar elde etmiştir [10]. 1994 te Huber Gauss tamsayıları üzerinde Mannheim metriğine göre hata düzeltebilen kodlar tanımlamıştır [5]. Ayrıca Huber bu çalışmasında bu kodların iki boyutlu uzayda Mannheim metriğinin QAM (Quadrature Amplitude Modulation) için Lee ve Hamming metrikten daha uygun olduğunu göstermiştir. 2001 de Neto ve diğerleri kuadratik cisimler üzerinde yeni bir Mannheim metriğine göre lineer kodlar inşa etmiştir [7]. 2009 da Martinez ve diğerleri ve bundan bağımsız olarak Özen ve Güzeltepe Lipschitz sayıları üzerinde Lipschitz metriğini tanımlayarak yeni lineer kodlar oluşturmuşlardır. 2013 te Güzeltepe Hurwitz sayıları üzerinde Hurwitz metriğini tanımlayarak kod hızı, minimum enerji ve bant genişliği açısından o güne kadar elde edilmiş kodlardan daha iyi kodlar oluşturmuştur [11].

Ayrıca günümüze kadar $\mathbb{F}_2+u\mathbb{F}_2$, $\mathbb{F}_2+v\mathbb{F}_2$, $\mathbb{F}_q+v\mathbb{F}_q$, $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$ gibi birçok halka üzerinde hem klasik hem de kuantum kod çalışması yapılmıştır.

Bu bölümde F_p sonlu cismi tanımlanıp, bu cismin cebirsel özelikleri incelenecektir. Daha sonra bu cisim üzerindeki klasik devirli kodlar yardımıyla kuantum kodlar inşa edilecektir. Bu klasik kodların minimum mesafeleri Mathematica programı ile hesaplanacaktır. Hazırlanan bu program kuantum kodlar için bir veri tabanı formundadır.

3.1. F_p Kümesi ve Cebirsel Özellikleri

F_p kümesini tanımlamak için $N(\pi_1)=N(\pi_2)=p$ olan $\pi_1=a+bw$, $\pi_2=b+aw$ olmak üzere $\pi_1,\pi_2\in\mathbb{Z}[w]$ asal elemanları alınıp, $\mathbb{Z}[w]_{\pi_1}$ ve $\mathbb{Z}[w]_{\pi_2}$ kümeleri oluşturulacaktır. Bu kümeler sırası ile $\mathbb{Z}[w]/\langle\pi_1\rangle$ ve $\mathbb{Z}[w]/\langle\pi_2\rangle$ kümeleridir. Yani $\mathbb{Z}[w]_{\pi_1}$ kümesi $\langle\pi_1\rangle$ normal alt grubuna göre elde edilen gruptur. Ayrıca $\langle\pi_1\rangle$ idealine göre $\mathbb{Z}[w]_{\pi_1}$ ve benzer şekilde $\mathbb{Z}[w]_{\pi_2}$ kümeleri birer halkadır. Bu kümelerde kalan sınıflar vardır. Bu kalan sınıflar tam temsilciler kullanılarak yazılmaktadır. Yani $\pi_1=a+bw$ ve $u=x+yw\in\mathbb{Z}[w]_{\pi_1}$ ise $|x|+|y|\le|a|+|b|$ ve $v=x'+y'w\in\overline{x+yw}$ için $|x'|+|y'|\le|x|+|y|$ dir. Bu kümeler oluşturulduktan sonra $\mathbb{Z}[w]_{\pi_1}$ ile $\mathbb{Z}[w]_{\pi_2}$ kümelerinin izomorf olduğu gösterilerek, bu kümelerin elemanları ile F_p kümesi inşa edilecektir.

Teorem 3.1.1. $\pi_1=a+bw$, $\pi_2=b+aw$ sayıları $\mathbb{Z}[w]$ kümesinde ilgili olmayan iki asal ve $\mathbb{Z}[w]_{\pi_1}$ ile $\mathbb{Z}[w]_{\pi_2}$ sırasıyla mod π_1 ve mod π_2 kalan sınıflar olsun. Bu durumda $\mathbb{Z}[w]_{\pi_1}$ ile $\mathbb{Z}[w]_{\pi_2}$ birbirine izomorftur.

İspat:

$f:\mathbb{Z}[w]_{\pi_1}\to\mathbb{Z}[w]_{\pi_2}$,

$f(x+yw)=x+yw^*$ fonksiyonunu göz önüne alalım. Bu fonksiyon iyi tanımlıdır. Çünkü $x_1+y_1w=x_2+y_2w\pmod{\pi_1}$ iken $f(x_1+y_1w)=f(x_2+y_2w)$

olur. Gerçekte $x_1+y_1w=x_2+y_2w\Rightarrow x_1=x_2, y_1=y_2$ olduğunda

$f(x_1+y_1w)=x_1+y_1w^*=x_2+y_2w^*=f(x_2+y_2w)$

olur. f birebirdir. Çünkü

$f(x_1+y_1w)=f(x_2+y_2w)$ $\left(0\le N(x_1+y_1w),N(x_1+y_1w)\le N(\pi_1)\right)$

$$\Rightarrow x_1 + y_1 w^* = x_2 + y_2 w \text{ , } \left(0 \le N\left(x_1 + y_1 w^*\right), N\left(x_1 + y_1 w^*\right) \le N\left(\pi_2\right) = N\left(\pi_1\right)\right)$$
$$\Rightarrow x_1 = x_2,\ y_1 = y_2$$
$$\Rightarrow x_1 + y_1 w = x_2 + y_2 w$$

olur. f fonksiyonunun birebir oluşu ve $\mathbb{Z}[w]_{\pi_1}$ ile $\mathbb{Z}[w]_{\pi_2}$ kümelerinin eleman sayıları eşit ve sonlu oluşu f fonksiyonunun örtenliğini gerektirir.

Ayrıca $\forall a = a_1 + a_2 w,\ b = b_1 + b_2 w \in \mathbb{Z}[w]_{\pi_1}$ için

$$\begin{aligned} f(a+b) &= f\left(\left(a_1 + a_2 w\right) + \left(b_1 + b_2 w\right)\right) \\ &= f\left(\left(a_1 + b_1\right) + \left(a_2 + b_2\right) w\right) \\ &= \left(a_1 + b_1\right) + \left(a_2 + b_2\right) w^* \\ &= \left(a_1 + a_2 w^*\right) + \left(b_1 + b_2 w^*\right) \\ &= f\left(a_1 + a_2 w\right) + f\left(b_1 + b_2 w\right) \\ &= f(a) + f(b) \end{aligned}$$

ve

$$\begin{aligned} f(ab) &= f\left(\left(a_1 + a_2 w\right)\left(b_1 + b_2 w\right)\right) \\ &= f\left(a_1 b_1 - a_2 b_2 + \left(a_1 b_2 + a_2 b_1 + a_2 b_2\right) w\right) \\ &= a_1 b_1 - a_2 b_2 + \left(a_1 b_2 + a_2 b_1 + a_2 b_2\right) w^* \\ &= \left(a_1 + a_2 w^*\right)\left(b_1 + b_2 w^*\right) \\ &= f\left(a_1 + a_2 w\right) f\left(\left(b_1 + b_2 w\right)\right) \\ &= f(a) f(b) \end{aligned}$$

olduğundan f fonksiyonu homomorfizmadır. f fonksiyonu, birebir, örten ve homomorfizma olduğundan bir izomorfizmadır. Dolayısıyla $\mathbb{Z}[w]_{\pi_1}$ ile $\mathbb{Z}[w]_{\pi_2}$ izomorf olur.

Tanım 3.1.1. $\mathbb{Z}[w]_{\pi_1}$ ve $\mathbb{Z}[w]_{\pi_2}$ yukarıdaki gibi tanımlansın. $a + bw \in \mathbb{Z}[w]_{\pi_1}$ ve $f(a+bw) = a' + b'w \in \mathbb{Z}[w]_{\pi_2}$ olmak üzere

$$F_p = \left\{a + bw : |a| + |b| \le |a'| + |b'|\right\} \cup \left\{a' + b' w^* : |a'| + |b'| < |a| + |b|\right\}$$

olarak tanımlanır.

Teorem 3.1.2. Yukarıda tanımlanan F_p kümesi eleman sayısı $N(\pi)=p$ olan sonlu bir cisimdir.

İspat: F_p kümesinin adi toplama işlemine göre bir değişmeli grup, ayrıca çarpma işlemine göre kapalı olduğu kolayca görülebilir. Yani F_p bir tamlık bölgesidir. Diğer yandan her $0 \neq a \in F_p$ elemanı bir asal kalan sınıf olduğundan tersi vardır. Dolayısıyla F_p bir sonlu cisimdir.

Örnek 3.1.1. $p=7,\ \pi_1 = 2+w$ ve $\pi_2 = 1+2w$ olsun. Bu durumda

$\mathbb{Z}[w]_{\pi_1} = \{0,1,-w,1-w,-1+w,w,-1\}$ ve

$\mathbb{Z}[w]_{\pi_2} = \{0,1,-1+w,w,-w,1-w,-1\}$

olur. $\mathbb{Z}[w]_{\pi_1}$ ve $\mathbb{Z}[w]_{\pi_2}$ kümelerinin elemanlarının kompleks düzlemde gösterimi sırasıyla Şekil 3.1. ve Şekil 3.2.'deki gibidir. Yukarıda tanımlanan

$f : \mathbb{Z}[w]_{\pi_1} \to \mathbb{Z}[w]_{\pi_2}$

$f(x+yw) = x+yw^*$ fonksiyonuna göre

$f(0)=0$

$f(1)=1$

$f(-w) = -w^* = -1+w$

$f(1-w) = 1-w^* = w$

$f(-1+w) = -1+w^* = -w$

$f(w) = w^* = 1-w$

$f(-1) = -1$

olur.

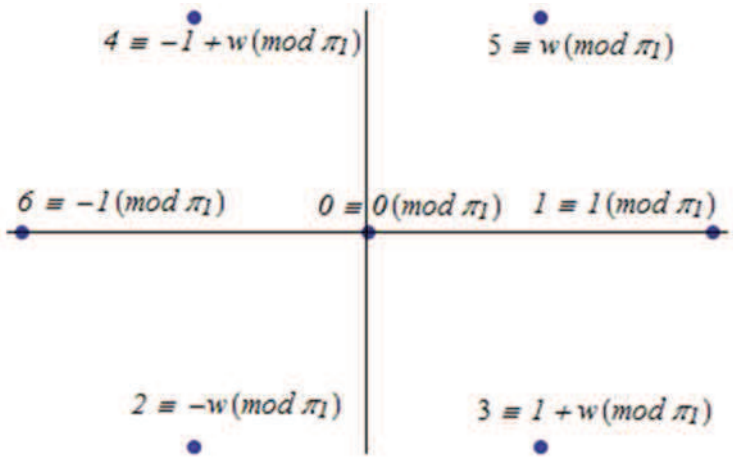
Tanım3.1.1.'den F_7 kümesi

$F_7 = \left\{\bar{0},\bar{1},\overline{-w},\overline{w^*},\overline{-w^*},\overline{w},\overline{-1}\right\}$

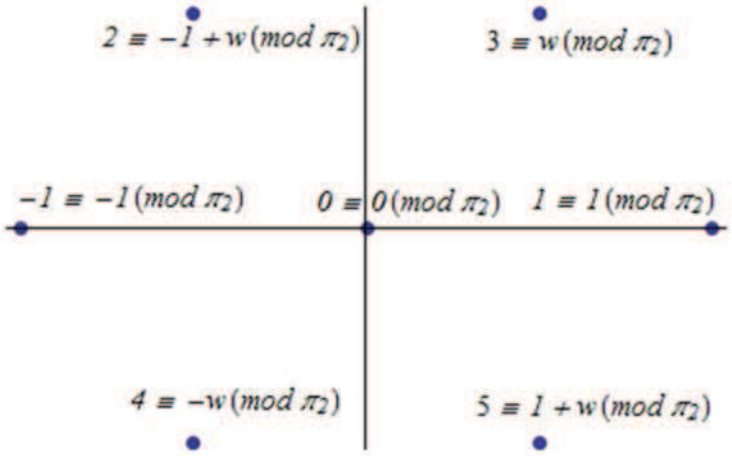
şeklinde elde edilir. $\mathbb{Z}[w]_{\pi_1}$ ile $\mathbb{Z}[w]_{\pi_2}$ kümelerinin yardımıyla $\mathbb{Z}_7$ kümesinin elemanları ile F_{2+w} kümesinin elemanlarının eşleştirilmesi Tablo 3.1.'deki gibidir. Şekil 3.3.'te ise F_7 kümesinin elemanlarının kompleks düzlemdeki konumları gösterilmiştir.

Tablo 3.1. $\mathbb{Z}_7$ kümesinin elemanları ile F_7 kümesinin elemanlarının eşleştirilmesi

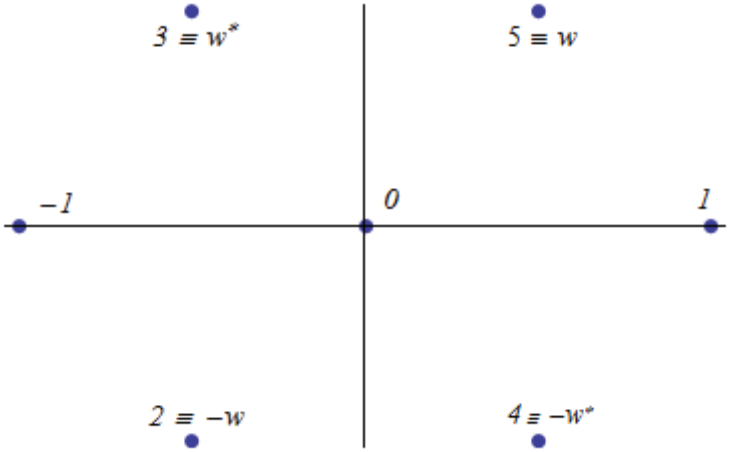
$\mathbb{Z}_7$	$\mathbb{Z}[w]_{\pi_1}$	$\mathbb{Z}[w]_{\pi_2}$	F_7
0	0	0	0
1	1	1	1
2	$-w$	$-1+w$	$-w$
3	$1-w$	w	w^*
4	$-1+w$	$-w$	$-w^*$
5	w	$1-w$	w
6	-1	-1	-1



Şekil 3.1. $\mathbb{Z}[w]_{\pi_1}$ kümesinin elemanlarının kompleks düzlemdeki yerleri



Şekil 3.2. $\mathbb{Z}[w]_{\pi_2}$ kümesinin elemanlarının kompleks düzlemdeki yerleri



Şekil 3.3. F_7 kümesi elemanlarının kompleks düzlemde yeri

3.2. F_p Üzerinde Kuantum Kodlar

$w = \frac{1}{2} + \frac{i\sqrt{3}}{2} = \cos\frac{\pi}{3} + i\sin\frac{\pi}{3}$ elemanı birimin 6. mertebeden köküdür. $w \in F_p$ olduğundan, F_7 de mertebesi $6n$ olan bir eleman her zaman vardır. Bu eleman β olsun. Yani $\beta^{6n} = 1$ dir. $\beta^{6n} = 1$ ise $\beta^n = \pm w$ olur. Bu durumda $x^n - w$ ve $x^n + w$ polinomları $t = 0,1,\ldots n-1$ olmak üzere β elemanının yardımı ile

$$x^n - w = (x-\beta)(x-\beta^7)\ldots(x-\beta^{6t+1})$$

$$x^n + w = (x+\beta)(x+\beta^7)\ldots(x+\beta^{6t+1})$$

şeklinde çarpanlarına ayrılır. $x^n - w$ polinomu ile $x^n + w$ polinomlarının çarpımı ise aşağıdaki gibi çarpanlarına ayrılır.

$$x^{2n} + w^* = (x-\beta)(x-\beta^7)\ldots(x-\beta^{6t+1})(x+\beta)(x+\beta^7)\ldots(x+\beta^{6t+1}) \qquad (*)$$

Not: $p = 13$ için $\beta = 2$ seçilirse $\beta^2 = w$ olur ve F_{13}'te $x^2 + w$ polinomu

$$x^2 + w = (x-\beta^4)(x+\beta^4)$$

olarak çarpanlarına ayrılır.

Tanım 3.2.1. $\theta \in \{w, w^*\}$ olmak üzere $z = a + b\theta \in F_p$ elemanının ağırlığı

$$w_M(z) = |a| + |b|$$

ve

$z_1 = a_1 + b_1\theta$, $z_2 = a_2 + b_2\theta \in F_p$ için z_1 ile z_2 arasındaki mesafe $z_1 - z_2 \equiv z = a + b\theta \in F_p$ olmak üzere

$$d_M(z_1, z_2) = w_M(z) = |a| + |b|$$

olarak tanımlanır.

Teorem 3.2.1. $\theta \in \{w, w^*\}$ olsun. Eğer $x + y\theta \in F_p$ ise $\forall m + n\theta \in \overline{x + y\theta}$ için $|x| + |y| \le |m| + |n|$ dir.

İspat: $\theta = w$ olsun. Bu durumda $m + nw \in \mathbb{Z}[w]_{\pi_1}$ olur. $\mathbb{Z}[w]_{\pi_1}$ in tanımından $|x| + |y| \le |m| + |n|$ olur. $\theta = w^*$ olsun. Bu durumda $f(m + nw^*) = m + nw \in \mathbb{Z}[w]_{\pi_2}$ olur. $\mathbb{Z}[w]_{\pi_2}$ nin tanımından $|x| + |y| \le |m| + |n|$ olur.

Teorem 3.2.2. Yukarıda tanımlanan d_M mesafesi F_p üzerinde bir metriktir.

İspat: *i*. $\forall z = a + b\theta \in F_p$ için $d_M(z, z) = w_M(a + b\theta - (a + b\theta)) = w(0) = 0$ dır.

$d_M(z_1,z_2)=0 \Rightarrow \ w(z_1-z_2)=0 \Rightarrow \ z_1 \equiv z_2 \pmod{\pi_1} \Rightarrow z_1 \in \mathbb{Z}[w]_{\pi_1}$ ve $z_2 \in \mathbb{Z}[w]_{\pi_1}$ olduğundan $\overline{z_1}=\overline{z_2}$ dir.

ii. $z_1,z_2 \in F_p$ olmak üzere $d(z_1,z_2)=d(z_2,z_1)$ dir. Gerçekten de

$$\begin{aligned} d_M(z_1,z_2) &= w_M(z_1-z_2) \\ &= |a_1-a_2|+|b_1-b_2| \\ &= |a_2-a_1|+|b_2-b_1| \\ &= w(z_2-z_1)=d(z_2,z_1) \end{aligned}$$

olur.

iii. $d_M(z_1,z_2)=w_M(z_1-z_2)=w_M(\delta_1)=|a_1|+|b_1|$ burada $\delta_1 \equiv \overline{z_1-z_2}=a_1+b_1\theta \in F_p$ ve $|a_1|+|b_1|$ minimumdur.

$d_M(z_1,z_3)=w_M(z_1-z_3)=w_M(\delta_2)=|a_2|+|b_2|$ ve $\delta_2 \equiv \overline{z_1-z_3}=a_2+b_2\theta \in F_p$ dir.

$d_M(z_3,z_2)=w_M(z_3-z_2)=w_M(\delta_3)=|a_3|+|b_3|$ ve $\delta_3 \equiv \overline{z_3-z_2}=a_3+b_3\theta \in F_p$ dir.

Ancak $w_M(\delta_2+\delta_3) \geq w_M(\delta_1)$

dir. Çünkü $\delta_2+\delta_3 \in \overline{z_1-z_2}$ ve biliyoruz ki $\forall x+y\theta \in \overline{z_1-z_2}$ için $|a_1|+|b_1| \leq |x|+|y|$ dir.

Teorem 3.2.3. $\mathbb{F}_p$ de $[n,k_1,d_1]$ parametrelerine sahip C_1 kodunun üreteç polinomu $g_1(x)$ ve $[n,k_2,d_2]$ parametrelerine sahip C_2 kodunun üreteç polinomu $g_2(x)$ olsun. Eğer $g_1(x)|g_2(x)$ ise $C_2 \subseteq C_1$ dir.[12]

Teorem 3.2.4. C_1 ve C_2 yukarıdaki şartları sağlayan devirli kodlar olsun. Bu durumda $\mathbb{F}_p$ üzerinde $\left[\left[n,k_1-k_2,\min\left\{d_1,d_2^{\perp}\right\}\right]\right]_p$ parametreli bir kuantum kod vardır [12].

Teorem 3.2.5. β, F_p de mertebesi $6n$ olan bir eleman olsun. Bu durumda (*) eşitliği kullanılarak F_p üzerinde kuantum kodlar elde edilir.

(*) eşitliği ve Teorem 3.2.4. göz önüne alındığında $g_1(x)|g_2(x)$ olacak şekilde $g_1(x)$ ve $g_2(x)$ üreteç polinomları, $f_1, f_2, \ldots f_n, f_{n+1}, \ldots, f_{2n}$ polinomları kullanılarak faklı ihtimaller dahilinde seçilebilir.

Örnek 3.2.1. $p=7$ olsun. Örnek 3.1.1.'den $F_7=\{0,1,-w,w^*,-w^*,w,-1\}$ olur. $\beta=w^*\in F_7$ alınırsa, F_7 üzerinde x^2+w^* polinomu $\beta=w\in F_7$ olmak üzere

$$x^2+w^*=(x-\beta)(x+\beta)=(x-w)(x+w)$$

olarak çarpanlarına ayrılır.

Burada $g_1(x)|g_2(x)$ olacak şekilde, $g_1(x)=g_2(x)=(x-\beta)=(x+\beta^4)$ alalım. Tablo 3.2. de β nın kuvvetleri verilmektedir.

Tablo 3.2. β nın kuvvetleri

$\beta=w$	$\beta^3=-1$	$\beta^5=w^*$
$\beta^2=-w^*$	$\beta^4=-w$	$\beta^6=1$

Teorem 1.1. 9.'dan $g_1(x)$ üreteç polinomuna karşılık gelen üreteç matrisi

$$G_1=(-w \quad 1)_{1x2}=(\beta^4 \quad 1)_{1x2}$$

olur. G_1 üreteç polinomu $|C_1|=7^1=7$ olacak şekilde C_1 lineer kodunu üretir. Buradan

$$C_1=\{(0,0),(-w,1),(1,-w^*),(w^*,w),(-w^*,w),(-1,w^*),(w,-1)\}$$
$$=\{(0,0),(\beta^4,1),(1,\beta^2),(\beta^5,\beta),(\beta^2,\beta^4),(\beta^3,\beta^5),(\beta,\beta^3)\}$$

olarak hesaplanır. C_1 kodunda $(0,0)\in C_1$ kodsözü hariç minimum Mannheim ağırlığı $w_M=2$ olduğundan, minumum mesafe $d_M(C_1)=2$ olur. O halde C_1 kodu $[2,1,2]_7$ parametreli lineer bir kod olur. $g_1(x)=g_2(x)$ olarak seçildiğinden, $C_1=C_2$ olur. Tanım 1.1.46.'dan C_2 kodunun duali

$$C_2^{\perp}=\{(0,0),(w,1),(-1,-w^*),(-w^*,w),(w^*,-w),(1,w^*),(-w,-1)\}$$

olarak hesaplanır. $C_2^{\perp}$ kodunun minumum mesafesi $d_M\left(C_2^{\perp}\right)=2$ olur.Teorem 3.2.5.'ten F_7 üzerinde $\left[\left[2,0,2\right]\right]_7$ kuantun kodu elde edilir.

Örnek 3.2.2. $p=13$ olsun. Bu durumda F_{13} kümesi Tanım 3.1.1.'den

$$F_{13}=\left\{0,1,2,-w^*,w,-2w,-2w^*,2w^*,2w,-w,w^*,-2,-1\right\}$$

olarak hesaplanır. $\beta=2\in F_{13}$ alınırsa, F_{13} üzerinde x^2-w ile x^2+w

$$x^2-w=\left(x-\beta\right)\left(x-\beta^7\right),$$

$$x^2+w=\left(x-\beta^4\right)\left(x+\beta^4\right)$$

olarak çarpanlarına ayrılır. Buradan da

$$x^4+w^*=\left(x-\beta\right)\left(x-\beta^7\right)\left(x-\beta^4\right)\left(x+\beta^4\right)=f_1f_2f_3f_4$$

elde edilir.

Burada $g_1\left(x\right)=g_2\left(x\right)=f_1f_4=\left(x-\beta\right)\left(x+\beta^4\right)=x^2+x+\beta^{11}$ alalım. Teorem 1.1.9.'dan $g_1\left(x\right)$ üreteç polinomuna karşılık gelen üreteç matrisi

$$G_1=\begin{pmatrix}1 & 1 & \beta^{11} & 0\\ 0 & 1 & 1 & \beta^{11}\end{pmatrix}$$

olur. G_1 üreteç matrisi ile elde edilen C_1 lineer kodunun eleman sayısı $\left|C_1\right|=13^2$ olur. C_1 lineer kodunun parametreleri $\left[4,2,4\right]_{13}$ tür. $g_1\left(x\right)=g_2\left(x\right)$ olduğundan $C_1=C_2$ olur. Yani $C_2\subset C_1$ şartı sağlanır. C_2 lineer kodunun üreteç polinomu $g_2\left(x\right)=\left(x-\beta\right)\left(x+\beta^4\right)$ olduğundan $C_2^{\perp}$ kodunun üreteç polinomu $g_2^{\perp}\left(x\right)=f_2f_3=\left(x-\beta^7\right)\left(x-\beta^4\right)=x^2+\beta^6x+\beta^{11}$ olur. Teorem 1.1.9.'dan $g_2^{\perp}\left(x\right)$ üreteç polinomuna karşılık gelen üreteç matrisi

$$G_2^{\perp}=\begin{pmatrix}1 & \beta^6 & \beta^{11} & 0\\ 0 & 1 & \beta^6 & \beta^{11}\end{pmatrix}$$

olur. $G_2^{\perp}$ üreteç matrisi ile elde edilen C_2 kodunun diki olan $C_2^{\perp}$ lineer kodunun eleman sayısı $\left|C_2^{\perp}\right|=13^2$ olur. $C_2^{\perp}$ lineer kodunun parametreleri $\left[4,2,4\right]_{13}$ tür.

Teorem 3.2.5.'ten C_1 ve C_2 kodlarının parametreleri kullanılarak $\left[\left[4,0,4\right]\right]_{13}$ kuantum kodu elde edilir.

Teorem 3.2.5'ten $g_1(x)$ ile $g_2(x)$ üreteç polinomları $g_1(x)\big|g_2(x)$ olacak şekilde seçilirse, oluşabilecek kuantum kod parametreleri Tablo 3.3.'de verilmiştir. Tablo 3.4.'te $p=19$ alındığında elde edilebilecek kuantum kod parametreleri verilmiştir.

Yukarıdakiler dikkate alınarak elde edilebilecek mümkün tüm kuantum kodlar aşağıdaki Mathematica programı kullanılarak hesaplanabilir. Bu programın InPutları ve OutPutları sırasıyla Şekil 3.4. ve Şekil 3.5.'te verilmiştir.

```
Do[
 If[Element[p = 6*n + 1, Primes],
  {nn = (p - 1) / 6;
   Do[
     Do[
      If[t^2 + t*k + k^2 == p, {a = t, b = k}]
      , {t, 1, p}]
     , {k, 1, p}]
    tt = a + b - 1;
   AR = Table[1, {p}, {2}];
   Do[If[Mod[a + b*s, p] == 0, r = s], {s, 0, p - 1}]
    f[g_] := (Reap[Do[Do[If[Mod[x + y*r, p] == g && Abs[x] + Abs[y] < Abs[tt] + Abs[tt], Sow[x]],
          {x, -tt, tt}], {y, -tt, tt}]][[2, 1]]);
   h[u_] := Reap[Do[Do[If[Mod[x + y*r, p] == u && Abs[x] + Abs[y] < Abs[tt] + Abs[tt], Sow[y]],
        {x, -tt, tt}], {y, -tt, tt}]][[2, 1]];
   Do[While[f[kk] && h[kk], {x, y}]; ttt = Ordering[Abs[f[kk]] + Abs[h[kk]], 1][[1]];
    AR[[kk + 1, 1]] = f[kk][[ttt]]; AR[[kk + 1, 2]] = h[kk][[ttt]], {kk, 0, p - 1}];

   Do[
     Do[
      If[t^2 + t*k + k^2 == p, {a = t, b = k}]
      , {t, 1, p}]
     , {k, 1, p}]
    tt = a + b - 1;
   BR = Table[1, {p}, {2}];
   Do[If[Mod[b + a*s, p] == 0, r = s], {s, 0, p - 1}]
    f[n_] := (Reap[Do[Do[If[Mod[x + y*r, p] == n && Abs[x] + Abs[y] < Abs[tt] + Abs[tt], Sow[x]],
          {x, -tt, tt}], {y, -tt, tt}]][[2, 1]]);
   h[m_] := Reap[Do[Do[If[Mod[x + y*r, p] == m && Abs[x] + Abs[y] < Abs[tt] + Abs[tt], Sow[y]],
        {x, -tt, tt}], {y, -tt, tt}]][[2, 1]];
   Do[While[f[kk] && h[kk], {x, y}]; ttt = Ordering[Abs[f[kk]] + Abs[h[kk]], 1][[1]];
    BR[[kk + 1, 1]] = f[kk][[ttt]]; BR[[kk + 1, 2]] = h[kk][[ttt]], {kk, 0, p - 1}];
```

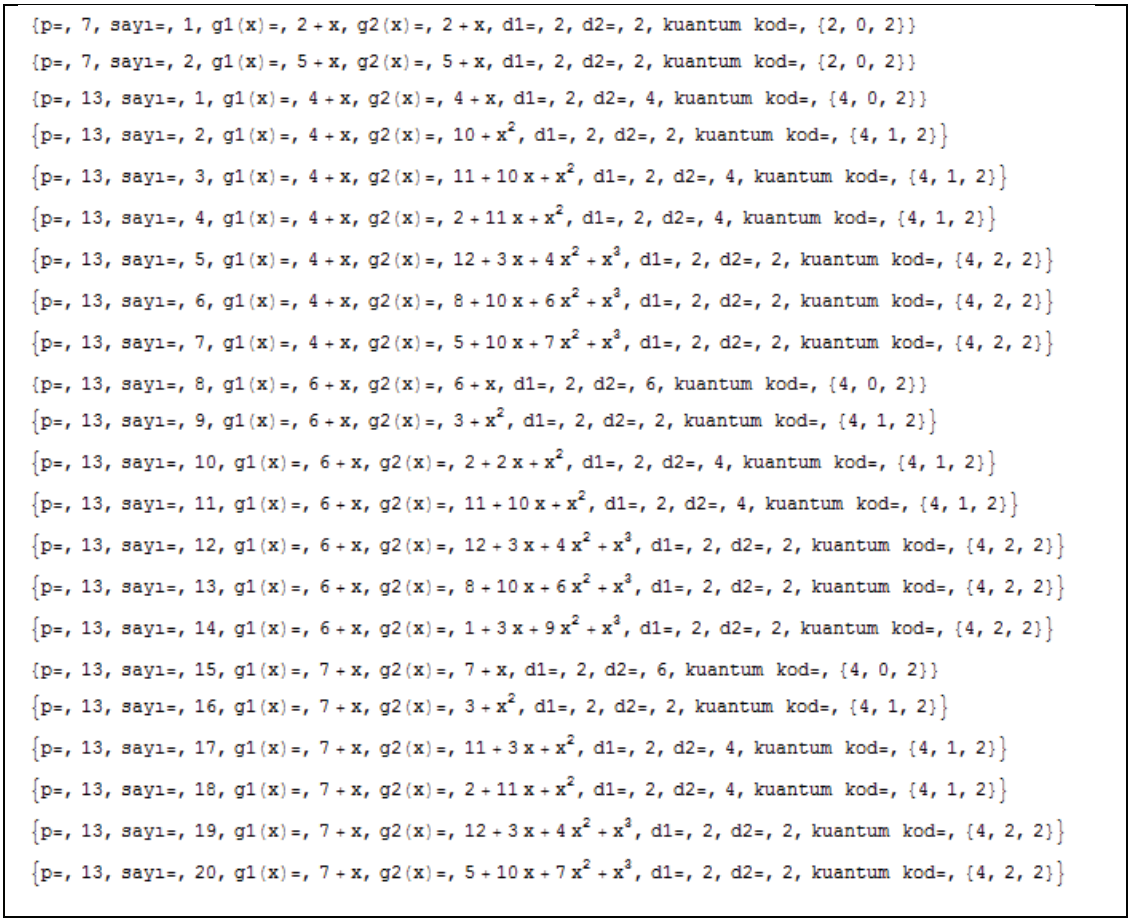
Şekil 3.4. Mathematica programın kuantum kodların hesaplanmasında kullanılışı

```
A = Table[1, {p}, {2}];
Do[If[Abs[AR[[i + 1, 1]]] + Abs[AR[[i + 1, 2]]] < Abs[BR[[i + 1, 1]]] + Abs[BR[[i + 1, 2]]],
    {A[[i + 1, 1]] = AR[[i + 1, 1]], A[[i + 1, 2]] = AR[[i + 1, 2]]} ,  {A[[i + 1, 1]] = BR[[i + 1, 1]] ,
     A[[i + 1, 2]] = BR[[i + 1, 2]]}], {i, 0, p - 1}]

 Do[aa = Mod[tt^nn, p]; If[aa == r || aa == p - r, A[[tt + 1]]], {tt, 1, p - 1}];
B = Table[1, {nn}];
Do[B[[gg]] = FactorList[x^nn + r, Modulus → p][[gg + 1, 1]], {gg, 1, nn}];
BB = Table[1, {nn}];
Do[BB[[gg]] = FactorList[x^nn - r, Modulus → p][[gg + 1, 1]], {gg, 1, nn}];
CC = Subsets[B];
CCC = Table[1, {2^nn - 1}];
Do[CCC[[kk - 1]] = Expand[ ∏_{j=1}^{Dimensions[CC[[kk]]][[1]]} CC[[kk]][[j]], Modulus → p], {kk, 2, 2^nn}];

DD = Subsets[BB];
DDD = Table[1, {2^nn - 1}];
Do[DDD[[kk - 1]] = Expand[ ∏_{j=1}^{Dimensions[DD[[kk]]][[1]]} DD[[kk]][[j]], Modulus → p], {kk, 2, 2^nn}];|

v = ∑_{i=1}^{nn} Binomial[nn, i];
KK = Table[1, {v^2}];
t = 0;
Do[
 Do[t = t + 1;
  KK[[t]] = Expand[CCC[[k]] * DDD[[kk]], Modulus → p]
  , {k, 1, v}]
 , {kk, 1, v}];
fs = Union[KK, CCC, DDD];
zzmaks = ( ∑_{i=1}^{2*nn} (2 * nn) ! / (i ! * (2 * nn - i) !) );
GD1 = Table[1, {2 * nn}];
sayı = 0;
Do[
 Do[
  If[PolynomialRemainder[fs[[zz2]], fs[[zz1]], x, Modulus → p] == 0,
   {sayı = sayı + 1, G1 = Table[1, {2 * nn}];
    Do[G1[[i + 1]] = Coefficient[fs[[zz1]], x, i], {i, 0, 2 * nn - 1}]
     G = Table[1, {2 * nn - Exponent[fs[[zz1]], x]}];
    Do[G[[j + 1]] = RotateRight[G1, j], {j, 0, 2 * nn - 1 - Exponent[fs[[zz1]], x]}];
    G // MatrixForm
      PP = Tuples[Range[0, p - 1], 2 * nn - Exponent[fs[[zz1]], x]];
    LK = Table[1, {p^(2 * nn - Exponent[fs[[zz1]], x])}];
    Do[
     LK[[i]] = Mod[ ∑_{j=1}^{2*nn-Exponent[fs[[zz1]],x]} PP[[i, j]] * G[[j]], p]
     , {i, 1, p^(2 * nn - Exponent[fs[[zz1]], x])}];
    d = nn * tt;
    Do[If[ ∑_{i=1}^{2*nn} (Abs[A[[LK[[k, i]] + 1]][[1]]] + Abs[A[[LK[[k, i]] + 1]][[2]]]) < d,
      d = ∑_{i=1}^{2*nn} (Abs[A[[LK[[k, i]] + 1]][[1]]] + Abs[A[[LK[[k, i]] + 1]][[2]]])], {k, 2, Dimensions[LK][[1]]}];
```

Şekil 3.4. (Devamı)

```
G2 = Table[1, {2 * nn}];
Do[G2[[i + 1]] = Coefficient[fs[[zz2]], x, i], {i, 0, 2 * nn - 1}]
 GG = Table[1, {2 * nn - Exponent[fs[[zz2]], x]}];
Do[GG[[j + 1]] = RotateRight[G2, j], {j, 0, 2 * nn - 1 - Exponent[fs[[zz2]], x]}];
GG // MatrixForm
  PP2 = Tuples[Range[0, p - 1], 2 * nn - Exponent[fs[[zz2]], x]];
LK2 = Table[1, {p^(2 * nn - Exponent[fs[[zz2]], x])}];
Do[
 LK2[[i]] = Mod[ Sum_{j=1}^{2*nn-Exponent[fs[[zz2]],x]} PP2[[i, j]] * GG[[j]], p]
 , {i, 1, p^(2 * nn - Exponent[fs[[zz2]], x])}];

fs2 = PolynomialQuotient[fs[[Dimensions[fs]]][[1]], fs[[zz2]], x, Modulus → p];
Do[GD1[[i + 1]] = Coefficient[fs2, x, i]
 , {i, 0, 2 * nn - 1}];
GD = Table[1, {2 * nn - Exponent[fs2, x]}];
Do[
 GD[[j + 1]] = RotateRight[GD1, j]
 , {j, 0, 2 * nn - 1 - Exponent[fs2, x]}];
PPD = Tuples[Range[0, p - 1], 2 * nn - Exponent[fs2, x]];
LKD = Table[1, {p^(2 * nn - Exponent[fs2, x])}];
Do[
 LKD[[rr]] = Mod[ Sum_{j=1}^{2*nn-Exponent[fs2,x]} PPD[[rr, j]] * GD[[j]], p]
 , {rr, 1, p^(2 * nn - Exponent[fs2, x])}];
dd = nn * tt;
Do[If[ Sum_{i=1}^{2*nn} (Abs[A[[LKD[[k, i]] + 1]][[1]]] + Abs[A[[LKD[[k, i]] + 1]][[2]]]) < dd,
  dd = Sum_{i=1}^{2*nn} (Abs[A[[LKD[[k, i]] + 1]][[1]]] + Abs[A[[LKD[[k, i]] + 1]][[2]]])], {k, 2, Dimensions[LKD][[1]]}]
      minmsf = Min[d, dd];
      Print[{"p=", p, "sayı=", sayı, "g1(x)=", fs[[zz1]],   "g2(x)=", fs[[zz2]], "d1=", d, "d2=", dd,
        "kuantum kod=", {2 * nn, Exponent[fs[[zz2]], x] - Exponent[fs[[zz1]], x], minmsf}}]}]
    , {zz2, 1, zzmaks - 1}]
   , {zz1, 1, zzmaks - 1}]}]
, {n, 1, 2}]
```

Şekil 3.4. (Devamı)



Şekil 3.5. Mathematica Programının Çıktıları

Tablo 3.3. Mannheim ve Hamming mesafesine göre F_{13} üzerinde kuantum kod parametreleri

$g_1(x)$	$g_2(x)$	Mannheim metriğine göre QEEC	Hamming metriğine göre QEEC
f_1	f_1	$[[4,0,2]]_{13}$	$[[4,0,2]]_{13}$
f_1	$f_1 f_2$	$[[4,1,2]]_{13}$	$[[4,1,2]]_{13}$
f_1	$f_1 f_2 f_3$	$[[4,2,2]]_{13}$	$[[4,2,2]]_{13}$
$f_1 f_2$	$f_1 f_2$	$[[4,0,2]]_{13}$	$[[4,0,2]]_{13}$
$f_1 f_2$	$f_1 f_2 f_3$	$[[4,1,2]]_{13}$	$[[4,1,2]]_{13}$
$f_1 f_4$	$f_1 f_4$	$[[4,0,4]]_{13}$	$[[4,0,3]]_{13}$
$f_1 f_2 f_3$	$f_1 f_2 f_3$	$[[4,0,2]]_{13}$	$[[4,0,2]]_{13}$

Tablo 3.4. Mannheim ve Hamming mesafesine göre F_{19} üzerinde kuantum kod parametreleri

$g_1(x)$	$g_2(x)$	Mannheim metriğine göre QEEC	Hamming metriğine göre QEEC
f_1	f_1	$[[6,0,2]]_{19}$	$[[6,0,2]]_{19}$
f_1	f_1f_2	$[[6,1,2]]_{19}$	$[[6,1,2]]_{19}$
f_1	$f_1f_2f_3$	$[[6,2,2]]_{19}$	$[[6,2,2]]_{19}$
f_1	$f_1f_2f_3f_4$	$[[6,3,2]]_{19}$	$[[6,3,2]]_{19}$
f_1	$f_1f_2f_3f_4f_5$	$[[6,4,2]]_{19}$	$[[6,4,2]]_{19}$
f_1f_2	$f_1f_2f_3$	$[[6,1,2]]_{19}$	$[[6,1,2]]_{19}$
f_1f_2	$f_1f_2f_3f_4$	$[[6,2,2]]_{19}$	$[[6,2,2]]_{19}$
f_1f_2	$f_1f_2f_3f_4f_5$	$[[6,3,2]]_{19}$	$[[6,3,2]]_{19}$
f_1f_4	f_1f_4	$[[6,0,3]]_{19}$	$[[6,0,2]]_{19}$
f_1f_4	$f_1f_4f_5$	$[[6,1,3]]_{19}$	$[[6,1,2]]_{19}$
f_1f_4	$f_1f_3f_4f_5$	$[[6,2,3]]_{19}$	$[[6,2,2]]_{19}$
f_1f_6	f_1f_6	$[[6,0,4]]_{19}$	$[[6,0,3]]_{19}$
f_1f_6	$f_1f_3f_6$	$[[6,1,4]]_{19}$	$[[6,1,3]]_{19}$
f_1f_6	$f_1f_2f_5f_6$	$[[6,2,4]]_{19}$	$[[6,2,3]]_{19}$
$f_1f_2f_6$	$f_1f_2f_6$	$[[6,0,5]]_{19}$	$[[6,0,4]]_{19}$
$f_1f_2f_6$	$f_1f_2f_5f_6$	$[[6,1,4]]_{19}$	$[[6,1,3]]_{19}$
$f_1f_2f_6$	$f_1f_2f_3f_5f_6$	$[[6,2,2]]_{19}$	$[[6,2,2]]_{19}$
$f_1f_2f_4$	$f_1f_2f_4$	$[[6,0,5]]_{19}$	$[[6,0,3]]_{19}$
$f_1f_2f_4$	$f_1f_2f_4f_6$	$[[6,1,4]]_{19}$	$[[6,1,3]]_{19}$
$f_1f_2f_4$	$f_1f_2f_4f_5$	$[[6,1,3]]_{19}$	$[[6,1,3]]_{19}$
$f_1f_2f_4f_5$	$f_1f_2f_4f_5$	$[[6,0,3]]_{19}$	$[[6,0,2]]_{19}$
$f_1f_2f_4f_5$	$f_1f_2f_4f_5f_6$	$[[6,1,2]]_{19}$	$[[6,1,2]]_{19}$
$f_1f_3f_5f_6$	$f_1f_3f_5f_6$	$[[6,0,4]]_{19}$	$[[6,0,3]]_{19}$
$f_1f_2f_3f_4f_5$	$f_1f_2f_3f_4f_5$	$[[6,0,2]]_{19}$	$[[6,0,2]]_{19}$

Örnek 3.2.4. Yukarıda verilen Mathematica programı kullanılarak elde edilen ve Tablo 3.4.'te verilen $[[6,0,5]]_{19}$ parametrelerine sahip kuantum kodu, aşağıdaki $[6,3,5]_{19}$ kendine-dik klasik kod yardımı ile hesaplanır. Bu kodu için üreteç polinomu

$$g_1(x) = f_1 f_2 f_4 = -1 + (-1+2w)x + 2w^* x^2 + x^3$$

olup, bu üreteç polinomu yardımı ile kodun üreteç matrisi

$$G = \begin{pmatrix} 18 & 15 & 5 & 1 & 0 & 0 \\ 0 & 18 & 15 & 5 & 1 & 0 \\ 0 & 0 & 18 & 15 & 5 & 1 \end{pmatrix}$$

olarak bulunur. Bu kod kendine-dik olduğundan kodun kontrol matrisi üreteç matrisine eşittir. Bu kod 2 Hurwitz ağırlığına sahip tüm hataları düzeltebilir. Örneğin

$$c = (18 \quad 14 \quad 1 \quad 6 \quad 1 \quad 0)$$

kodsözü kanaldan

$$e = (15 \quad 2 \quad 0 \quad 0 \quad 0 \quad 0)$$

hatası ile

$$r = c + e = (14 \quad 16 \quad 1 \quad 6 \quad 1 \quad 0)$$

olarak alınsın. Bu durumda r nin sendromu

$$S(r) = (7 \quad 11 \quad 18)$$

olur.

BÖLÜM 4. EISENSTAIN-JACOBI TAMSAYILARI ÜZERİNDE YENİ SİNYAL YILDIZ KÜMELERİ

Bu bölümde R_π sonlu halkası tanımlanıp, bu halkanın cebirsel özelikleri incelenecektir. $N(\pi)=m$ elemanlı bir takım yıldızının (Constellation) kod kazancı için önce bu takım yıldızının ortalama enerji hesabı olan E_π hesaplanacaktır. M takım yıldızı boyutu ve d_M de bu takım yıldızında kullanılan metriğe göre minimum mesafe olsun. Bu durumda m elemanlı bir takım yıldızı üzerinde inşa edilen kodun takım yıldızının değer katsayısı olan CFM (Constellation Figure of Merit) değeri

$$CFM = \frac{Md_M^2}{2E_\pi}$$

ile hesaplanır. CFM arttıkça kod kazancının arttığı bilinmektedir. Dolayısıyla daha iyi bir kodlama elde edilir. CFM değeri hesaplarken M ve 2 sabit olduğundan amaç ortalama enerjiyi küçültürken minimum mesafeyi büyültmektir. Bu çalışmada p elemanlı bir takım yıldızı $p|m$ olmak üzere m elemanlı bir takım yıldızına gömülecektir ve CFM değerleri karşılaştırılacaktır. Bu takım yıldızı Eisenstein-Jacobi tamsayıları kullanılarak oluşturulacaktır.

4.1. R_π Kümesi ve Cebirsel Özellikleri

p_1 ve p_2, $p_1 \equiv p_2 \equiv 1 \pmod 6$ şartını sağlayan farklı iki tek asal tamsayı, $N(\pi)=N(\pi')=p_1p_2=m$ olmak üzere $\mathbb{Z}[w]_\pi$ ve $\mathbb{Z}[w]_{\pi'}$ sırasıyla mod π ve mod π' de kalan sınıflar olsun. Bu durumda $\mathbb{Z}[w]_\pi$ ve $\mathbb{Z}[w]_{\pi'}$ kümeleri halkadır ve Teorem 3.1.1.'den bu halkalar birbirine izomorftur.

Tanım 4.1.1. $\mathbb{Z}[w]_\pi$ ve $\mathbb{Z}[w]_{\pi'}$ yukarıdaki gibi tanımlansın. $x+yw \in \mathbb{Z}[w]_\pi$ ve $f(x+yw) = x'+y'w \in \mathbb{Z}[w]_{\pi'}$ olmak üzere

$$R_\pi = \{x+yw : |x|+|y| \le |x'|+|y'|\} \cup \{x'+y'w^* : |x'|+|y'| < |x|+|y|\}$$

olarak tanımlanır. R_π nin $N(\pi) = N(\pi') = p_1.p_2 = m$ elemanlı bir halka olduğu Tanım 3.1.1. ve Teorem 3.1.2.'den açıktır.

Örnek 4.1.1. $p_1 = 7$ ve $p_2 = 13$ olsun. Bu durumda $\pi_1 = 1+2w$, $\pi_2 = 3+w$ olmak üzere $\pi = (1+2w)(3+w) = 1+9w$ ve $\pi' = 9+w$ olur. Buradan $m = 7.13 = 91$ olup R_π halkasının elemanları Tablo 4.1.'deki gibi olur.

Tablo 4.1. $\mathbb{Z}_{91}$ kümesi ile R_π kümesinin elemanlarının eşleştirilmesi

$\mathbb{Z}_{91}$	$\mathbb{Z}[w]_\pi$	$\mathbb{Z}[w]_{\pi'}$	R_π	$\mathbb{Z}_{91}$	$\mathbb{Z}[w]_\pi$	$\mathbb{Z}[w]_{\pi'}$	R_π
0	0	0	0	46	$-5-4w$	$5w$	$5w^*$
1	1	1	1	47	$-4-4w$	$1+5w$	$1+5w^*$
2	2	2	2	48	$-3-4w$	$2+5w$	$-3-4w$
3	3	3	3	49	$-2-4w$	$3+5w$	$-2-4w$
4	4	4	4	50	$-1-4w$	$-5+4w$	$-1-4w$
5	5	$-4-w$	5	51	$-4w$	$-4+4w$	$-4w$
6	$-4+w$	$-3-w$	$-3-w^*$	52	$1-4w$	$-3+4w$	$1-4w$
7	$-3+w$	$-2-w$	$-2-w^*$	53	$2-4w$	$-2+4w$	$2-4w$
8	$-2+w$	$-1-w$	$-1-w^*$	54	$3-4w$	$-1+4w$	$-1+4w^*$
9	$-1+w$	$-w$	$-w^*$	55	$4-4w$	$+4w$	$+4w^*$
10	$+w$	$1-w$	$+w$	56	$-5-3w$	$1+4w$	$1+4w^*$
11	$1+w$	$2-w$	$1+w$	57	$-4-3w$	$2+4w$	$2+4w^*$
12	$2+w$	$3-w$	$2+w$	58	$-3-3w$	$3+4w$	$-3-3w$
13	$3+w$	$4-w$	$3+w$	59	$-2-3w$	$-5+3w$	$-2-3w$
14	$4+w$	$-4-2w$	$4+w$	60	$-1-3w$	$-4+3w$	$-1-3w$
15	$5+w$	$-3-2w$	$-3-2w^*$	61	$-3w$	$-3+3w$	$-3w$
16	$-4+2w$	$-2-2w$	$-2-2w^*$	62	$1-3w$	$-2+3w$	$1-3w$
17	$-3+2w$	$-1-2w$	$-1-2w^*$	63	$2-3w$	$-1+3w$	$-1+3w^*$
18	$-2+2w$	$-2w$	$-2w^*$	64	$3-3w$	$+3w$	$+3w^*$
19	$-1+2w$	$1-2w$	$-1+2w$	65	$4-3w$	$1+3w$	$1+3w^*$

Tablo 4.1. (Devamı)

$\mathbb{Z}_{91}$	$\mathbb{Z}[w]_{\pi}$	$\mathbb{Z}[w]_{\pi'}$	R_{π}	$\mathbb{Z}_{91}$	$\mathbb{Z}[w]_{\pi}$	$\mathbb{Z}[w]_{\pi'}$	R_{π}
20	$+2w$	$2-2w$	$+2w$	66	$-5-2w$	$2+3w$	$2+3w^*$
21	$1+2w$	$3-2w$	$1+2w$	67	$-4-2w$	$3+3w$	$-4-2w$
22	$2+2w$	$4-2w$	$2+2w$	68	$-3-2w$	$-5+2w$	$-3-2w$
23	$3+2w$	$-4-3w$	$3+2w$	69	$-2-2w$	$-4+2w$	$-2-2w$
24	$4+2w$	$-3-3w$	$4+2w$	70	$-1-2w$	$-3+2w$	$-1-2w$
25	$5+2w$	$-2-3w$	$-2-3w^*$	71	$-2w$	$-2+2w$	$-2w$
26	$-4+3w$	$-1-3w$	$-1-3w^*$	72	$1-2w$	$-1+2w$	$1-2w$
27	$-3+3w$	$-3w$	$-3w^*$	73	$2-2w$	$+2w$	$+2w^*$
28	$-2+3w$	$1-3w$	$1-3w^*$	74	$3-2w$	$1+2w$	$1+2w^*$
29	$-1+3w$	$2-3w$	$-1+3w$	75	$4-2w$	$2+2w$	$2+2w^*$
30	$+3w$	$3-3w$	$+3w$	76	$-5-w$	$3+2w$	$3+2w^*$
31	$1+3w$	$4-3w$	$1+3w$	77	$-4-w$	$-5+w$	$-4-w$
32	$2+3w$	$-4-4w$	$2+3w$	78	$-3-w$	$-4+w$	$-3-w$
33	$3+3w$	$-3-4w$	$3+3w$	79	$-2-w$	$-3+w$	$-2-w$
34	$4+3w$	$-2-4w$	$-2-4w^*$	80	$-1-w$	$-2+w$	$-1-w$
35	$5+3w$	$-1-4w$	$-1-4w^*$	81	$-w$	$-1+w$	$-w$
36	$-4+4w$	$-4w$	$-4w^*$	82	$1-w$	$+w$	$+w^*$
37	$-3+4w$	$1-4w$	$1-4w^*$	83	$2-w$	$1+w$	$1+w^*$
38	$-2+4w$	$2-4w$	$-2+4w$	84	$3-w$	$2+w$	$2+w^*$
39	$-1+4w$	$3-4w$	$-1+4w$	85	$4-w$	$3+w$	$3+w^*$
40	$+4w$	$4-4w$	$+4w$	86	-5	-5	-5
41	$1+4w$	$-4-5w$	$-5w$	87	-4	-4	-4
42	$1-5w$	$-3-5w$	$1-5w$	88	-3	-3	-3
43	$2-5w$	$-2-5w$	$2-5w$	89	-2	-2	-2
44	$3-5w$	$-1-5w$	$-1-5w^*$	90	-1	-1	-1
45	$4-5w$	$-5w$	$-5w^*$	91	0	0	0

Tanım 4.1.2. $\pi \in \mathbb{Z}[w]$ ve $N(\pi) = m$ olmak üzere R_{π} kümesinin ortalama enerjisi, tüm elemanları eşit olasılıkla kullanıldığındaki umulan enerjidir. Bu enerji E_{π} ile gösterilir ve

$$E_{\pi} = \frac{1}{N(\pi)} \sum_{z \in R_{\pi}} w_M(z)$$

ile hesaplanır.

Tanım 4.1.3. *CFM* (Constellation Figure of Merit), ortalama enerji ve minimum mesafesi d_M olan iki boyutlu sinyal enerjisinin normalize edilmiş halidir. M – boyutlu yıldız kümesi için *CFM* değeri aşağıdaki eşitlik yardımı ile hesaplanmaktadır.

$$CFM\left(R_\pi\right)=\frac{M.d_M}{2.E_\pi}$$

R_π kümesinin boyutu $M=2$ olduğundan, R_π kümesi için

$$CFM\left(R_\pi\right)=\frac{d_M}{E_\pi}=\frac{N(\pi).d_M}{\sum_{z\in R_\pi} w_M(z)}$$

olarak hesaplanır.

Bir kodun *CFM* değeri artarsa, *AWGN* performansı da artar.

Tanım 4.1.4. Bit başına enerji $\left(E_b\right)$ ile ortalama enerji $\left(E_\pi\right)$

$$E_b=\frac{E_\pi}{Log_2^p}$$

ilişkisi vardır.

4.2. R_π Kümesinin Bölüntüsü

Bu bölümde R_π halkasının küme parçalanışından ve bu küme parçalanışlarının *CFM* değerleri hesaplamalarından bahsedeceğiz.

Teorem 4.2.1. $\mathbb{Z}_m$ ile R_π izomorftur.

İspat: $0\le r\le m-1$, $a+br\equiv 0\left(\text{mod } m\right)$, $x+yr\equiv l\left(\text{mod } m\right)$ ve $x+yw=x'+y'w^*$ olsun.

$g:\mathbb{Z}_m\to R_\pi$

$$g=(l)=\begin{cases} x+yw, |x|+|y|\le|x'|+|y'| \\ x'+y'w^*, |x'|+|y'|<|x|+|y| \end{cases}$$

fonksiyonunu göz önüne alalım [6]. Tanım 3.1.1. ve Teorem 3.1.2. göz önüne alınırsa g'nin birebir ve örten bir halka homomorfizması olduğu görülür. Dolayısıyla $\mathbb{Z}_m$ ile R_π izomorftur.

Bu fonksiyon yardımı ile R_π'nin bölüntüsü $\mathbb{Z}_m$'nin bölüntüsü kullanılarak şu şekilde elde edilebilir;

$\pi_1, \pi_2 \in \mathbb{Z}[w]$ iki asal, $\pi=\pi_1\pi_2=a+bw$, $\pi'=b+aw$ ve $N(\pi)=m$ ise $R_\pi \cong \mathbb{Z}_m$ dir. N çarpımsal norm olduğundan $N(\pi_1)=p_1$ ve $N(\pi_2)=p_2$ alınırsa $m=p_1p_2$ olur. Bu durumda R_π kümesi, $R_\pi^{(0)}=\{g(0), g(p_1), g(2p_1),\ldots,g((p_2-1)p_1)\}$ ve $R_\pi^{(i)}=\{g(i+0), g(i+p_1), g(i+2p_1),\ldots,g(i+(p_2-1)p_1)\}$ $(1\le i\le p_1)$ olmak üzere $R_\pi=R_\pi^{(1)}\cup R_\pi^{(2)}\cup\cdots\cup R_\pi^{(p_1)}$ olacak şekilde $R_\pi^{(1)}, R_\pi^{(2)},\ldots,R_\pi^{(p_1)}\subset R_\pi$ alt kümelerine bölünür. $\mathbb{Z}_m^{(p_1)}=\{0, p_1, 2p_1,\ldots,(p_2-1)p_1\}$ ve $1\le i\le p_1$ için $\mathbb{Z}_m^{(i)}=\{z: z-i\in\mathbb{Z}_m^{(p_1)}\}$ olmak üzere $R_\pi^{(1)}, R_\pi^{(2)},\ldots,R_\pi^{(p_1)}\subset R_\pi$ kümeleri sırasıyla $\mathbb{Z}_m^{(1)}, \mathbb{Z}_m^{(2)},\ldots,\mathbb{Z}_m^{(p_1)}$ kümelerine izomorf olur.

Teorem 4.2.2. R_π'nin p_1 tane alt kümeye bölüntüsü $R_\pi^{(1)}, R_\pi^{(2)},\ldots,R_\pi^{(p_1)}\subset R_\pi$ olsun. Bu durumda $\forall 0\ne z\in R_\pi^{(p_1)}$ için

$w_M(z)\ge w_M(\pi_1)$

dir.

İspat: $z\in R_\pi^{(p_1)}$ ise $\mathbb{Z}_m^{(p_1)}$ de z ile eşleşen eleman z' olsun. Bu durumda $z'=p_1t$ olacak şekilde $\exists t\in\mathbb{Z}$ vardır. Dolayısıyla

$z=\pi_1(u+vw)$

olur. O halde $z\in\overline{\pi_1}$ dir. Teorem 3.2.1'den

$w_M(z) \geq w_M(\pi_1)$

olur.

Örnek 4.2.1. $\pi_1 = 1+2w,\ \pi_2 = 3+w \in \mathbb{Z}[w]$ olsun. Bu durumda $\pi = \pi_1\pi_2 = (1+2w)(3+w) = 1+9w$ ve $\pi' = 9+w$ olur. $\mathbb{Z}[w]_\pi$ ve $\mathbb{Z}[w]_{\pi'}$ den R_π halkası Örnek 4.1.1.'deki gibi elde edilir.

$$R_\pi^{(13)} = \left\{ \begin{matrix} 0, -2-w^*, 4+w, 1+2w, 1-3w^*, -1-4w^*, 1-5w, -2-4w, 1+4w^*, -1+3w^*, \\ -1-2w, -4-w, 2+w^* \end{matrix} \right\}$$

kümesi R_π kümesinin 13 elemanlı bir alt kümesi olur ve $R_\pi^{(13)} \cong \mathbb{Z}_{13}$ olduğundan $R_\pi^{(13)}$ sonlu bir cisimdir. $R_\pi^{(13)}$ için ortalama enerji

$$E_{R_\pi^{(13)}} = \frac{1}{13}\sum_{z \in R_\pi^{(13)}} w_M(z) = \frac{52}{13} = 4 \text{ ve}$$

$R_\pi^{(13)}$ için CFM değeri ise

$$CFM\left(R_\pi^{(13)}\right) = \frac{d_M}{E_{R_\pi^{(13)}}} = \frac{3.13}{52} = 0,75$$

olarak hesaplanır.

Örnek 3.2.1.'deki $F_{13} = \{0,1,2,-w^*,w,-2w,-2w^*,2w^*,2w,-w,w^*,-2,-1\}$ cismi için ortalama enerji ve CFM değeri hesapları aşağıdaki gibidir.

$$E_{F_{13}} = \frac{1}{13}\sum_{z \in F_{13}} w_M(z) = \frac{18}{13} = 1,3846,$$

$$CFM(F_{13}) = \frac{d_M}{E_{F_{13}}} = \frac{1.13}{18} = 0,7\overline{2}$$

olarak hesaplanır.

F_{13} ile $R_\pi^{(13)}$ için CFM değerleri karşılaştırıldığında R_π halkasına gömülü 13 elemanlı $R_\pi^{(13)}$ cismi için daha yüksek CFM değeri elde edilmiştir.

Aşağıdaki tabloda aynı eleman sayısına sahip takım yıldızlarının CFM değerleri verilmiştir.

Tablo 4.2. F_p ile $R_\pi^{(p)}$ takım yıldızlarının CFM değerlerinin karşılaştırılması

Takım Yıldızı Eleman Sayısı (p)	π_1	π_2	$\pi=\pi_1\pi_2$	$CFM\left(F_p\right)$	$CFM\left(R_\pi^{(p)}\right)$
13	$3+w$	$1+2w$	$1+9w$	0,72222	0,75
13	$3+w$	$2+w$	$5+6w$		0,8125
13	$3+w$	$3+4w$	$5+19w$		0,784483
19	$3+2w$	$2+w$	$4+9w$	0,59375	0,662791
19	$3+2w$	$4+3w$	$6+23w$		0,671717
31	$5+w$	$1+3w$	$2+19w$	0,442857	0,48062
31	$5+w$	$2+w$	$9+8w$		0,553571
37	$3+4w$	$2+w$	$2+15w$	0,4111	0,454918
37	$4+3w$	$3+2w$	$6+23w$		0,484293
43	$6+w$	$2+w$	$11+9w$	0,377193	0,444828
43	$6+w$	$3+2w$	$16+17w$		0,473568

4.3. R_π Üzerinde Kod Kazancı

Bu kısımda, R_π kümesinin küme parçalanışları üzerinde tanımlı kodlar ile 3. bölümde verilen F_p kümesi üzerinde tanımlı kodların eleman sayıları eşit olması durumundaki kod kazancı (KK) hesaplanacaktır. Kod kazancı, bir kodun performansı için bir ölçüdür. Kod kazancı genellikle desibel (dB) cinsinden verilir ve minimum mesafe ve kod hızının bir fonksiyonudur.

$\pi\in\mathbb{Z}[w]$ bir asal sayı, $N(\pi)=p$ ve C_1 kodu $\mathbb{F}_p$ üzerinde tanımlı $[n_1,k_1,d_H]_p$ parametreli bir lineer kod olmak üzere eleman sayısı p ve bit başına enerjisi E_b olan bir küme üzerindeki $[n_2,k_2,d_2]_p$ parametreli bir C_2 lineer kodu için kod kazancı

$$KK=10\log\left(\frac{k_1}{n_1}\frac{k_2}{n_2}d_Hd_2\right)-10\log 4E_b$$

olarak hesaplanır.

Örnek 4.3.1. $p=13$ olsun, F_{13} ile $R_{\pi}^{(13)}$ kümeleri sırasıyla Örnek 3.2.1. ve Örnek 4.2.1.'deki gibi olmak üzere $\mathbb{F}_{13}$ üzerinde $[170,5,150]_{13}$ lineer kodunu göz önüne alalım. Bu durumda $F_{13}=\{0,1,2,-w^*,w,-2w,-2w^*,2w^*,2w,-w,w^*,-2,-1\}$ olur ve F_{13} üzerinde $[1,1,1]_{13}$ lineer kodu vardır. Benzer şekilde

$$R_{\pi}^{(13)}=\begin{Bmatrix}0,-2-w^*,4+w,1+2w,1-3w^*,-1-4w^*,1-5w,-2-4w,1+4w^*,-1+3w^*,\\-1-2w,-4-w,2+w^*\end{Bmatrix}$$

olur ve $R_{\pi}^{(13)}$ üzerinde $[1,1,3]_{13}$ lineer kodu vardır.

F_{13} üzerinde kod kazancı

$$KK\left(F_{13}\right)=10\log\left(\frac{5}{170}.\frac{1}{1}.150.1\right)-10\log 4E_b=6.45-1.75=4.7\ dB$$

olarak hesaplanır.

$R_{\pi}^{(13)}$ üzerinde kod kazancı ise

$$KK\left(R_{\pi}^{13}\right)=10\log\left(\frac{5}{170}.\frac{1}{1}.150.3\right)-10\log 4E_b=11.22-6.36=4.86\ dB$$

olarak hesaplanır.

Sonuç olarak $R_{\pi}^{(13)}$ üzerindeki kod kazancının F_{13} üzerindeki kod kazancından daha yüksek olduğu gözlemlenmiştir.

$\pi\in\mathbb{Z}[w]$'nun seçimine göre $R_{\pi}^{(13)}$ ile F_{13} arasındaki kod kazancı farkları Tablo 4.3.'teki gibi hesaplanmıştır.

Tablo 4.3. $R_{\pi}^{(13)}$ ile F_{13} arasında kod kazançlarının karşılaştırılması

Takım Yıldızı	Kod Parametresi	Ortalama Enerji (E_{π})	Bit Başına Enerji (E_b)	$10\log(4E_b)$	Kod Kazancı (KK)	Yeni Kod Kazancı
F_{13}	$[1,1,1]_{13}$	1.38462	0.37418	1.75136	4.69487	0
$R_{1+9w}^{(13)}$	$[1,1,3]_{13}$	4	1.08095	6.35866	4.85868	0.16381
$R_{5+6w}^{(13)}$	$[1,1,3]_{13}$	3.69231	0.9978	6.01103	5.20631	0.51144

Tablo 4.3. (Devamı)

Takım Yıldızı	Kod Parametresi	Ortalama Enerji (E_π)	Bit Başına Enerji (E_b)	$10\log(4E_b)$	Kod Kazancı (KK)	Yeni Kod Kazancı
$R^{(13)}_{3+14w}$	$[1,1,5]_{13}$	6.46154	1.74615	8.44144	5.04438	0.34951
$R^{(13)}_{7+11w}$	$[1,1,5]_{13}$	6.15385	1.663	8.22952	5.2563	0.56143
$R^{(13)}_{2+19w}$	$[1,1,6]_{13}$	8.15385	2.20348	9.45169	4.77595	0.08108
$R^{(13)}_{14+9w}$	$[1,1,6]_{13}$	7.38462	1.9956	9.02133	5.20631	0.51144
$R^{(13)}_{5+19w}$	$[1,1,7]_{13}$	8.92308	2.41136	9.84322	5.05388	0.35901
$R^{(13)}_{9+16w}$	$[1,1,7]_{13}$	8.61538	2.32821	9.68522	5.21188	0.51701
$R^{(13)}_{3+22w}$	$[1,1,7]_{13}$	9.53846	2.57766	10.13286	4.76424	0.06937
$R^{(13)}_{17+10w}$	$[1,1,7]_{13}$	11.0769	2.99341	10.78226	4.11484	-0.58003
$R^{(13)}_{7+24w}$	$[1,1,9]_{13}$	11.3846	3.07656	10.90125	5.0873	0.39243

KAYNAKLAR

[1] Çallıalp, F., Örneklerle Soyut Cebir, Birsen Yayınevi, 2011.

[2] Davidoff, G., Sarnak, P., Valette, A., Elementery Number Theory, Group Theory, and Ramanujan Graphs, Cambridge, 2003.

[3] Çallıalp, F., Tekir, Ü., Değişmeli halkalar ve Modüller, Birsen Yayınevi, 2009.

[4] Ling, S., Xing, C., Coding Theory, Cambridge, 2004.

[5] Huber, K., Codes over Gaussian integers, IEEE Trans. Inform. Theory 40, 1994.

[6] Güzeltepe, M., On Perfect Codes Over $A_p[w]$, Journal of Applied Mathematics and Computation, 2017.

[7] Neto, T.P.de N., Interlando, J.C., Favareto, O.M., Elia, M., Palazzo, R., Lattice Constallations and Codes From Quadratic Number Fields, Transactions on Information Theory, 2001.

[8] Hardy, G.H., Wright, E.M. An Introduction to The Theory of Numbers, Oxford, 1979.

[9] Hamming, R.W., Error Detecting and Error Correcting Codes, Bell System Technical Journal 29, 1950.

[10] Lee, C.Y., Some properties of non-binary error correcting codes, IEEE Trans. Inform. Theory 4, 1958.

[11] Güzeltepe, M., Codes over Hurwitz integers, Discrete Mathematics, 2013.

[12] Ketkar, A., Klappenecker A., Nonbinary Stabilizer Codes Over Finite Fields. IEEE Transactions Information Theory, 2006.

ÖZGEÇMİŞ

Ercüment Çakır, 15.07.1989'da Sakarya'da doğdu. İlk, orta ve lise eğitimini Sakarya'da tamamladı. 2012 yılında başladığı Sakarya Üniversitesi Matematik Bölümü'nü 2015 yılında bitirdi. 2016 yılında Sakarya Üniversitesi Matematik Bölümü'nde yüksek lisans eğitimine başladı. Halen Sakarya Üniversitesi Matematik Bölümü'nde yüksek lisans eğitimine devam etmektedir. Ercüment Çakır'ın yabancı dili İngilizcedir.