BLM 323
BİLGİ GÜVENLİĞİ VE KRİPTOGRAFİ

Dr. Öğr. Üyesi Meltem KURT PEHLİVANOĞLU

W2

BİLGİSAYAR BİLİMLERİ İÇİN SONLU CİSİMLER TEORİSİ

Bu teori:

- Hata düzeltme Kodları,
- Kriptografi,
- Sayısal Sinyal İşleme gibi önemli alanlarda kullanılmaktadır. Bu teori ders açısından kriptografi tabanlı değerlendirileceğinden kriptografi konusu ile ilgili olarak örnekler verilip incelenecektir.

Cisim: Toplama, çıkarma, çarpma ve bölme işlemlerini yapabileceğimiz bir yerdir.

BİLGİSAYAR BİLİMLERİ İÇİN SONLU CİSİMLER TEORİSİ

Tanım 1:

a, b tamsayı ve m pozitif tamsayı olsun. Eğer m, b-a'yı bölüyorsa $a \equiv b \pmod m$ şeklinde yazabiliriz. $a \equiv b \pmod m$ ifadesine denklik denir ve a, b'ye mod m'e göre denktir denir. Tamsayı m'ye de modulo denir.

Biz aritmetik modulo m: $Z_m \{0,1,...,m-1\}$ seti ile iki işlem toplama ve çarpma tabanlı tanımlayabiliriz. Z_m'de toplama ve çarpma işlemleri gerçek toplama ve çarpma işlemleri olacak sadece sonuçlar modulo m'ye göre indirgenecektir.

Z_m'de toplama ve çarpmanın tanımları bilinen bir çok aritmetik kuralı sağlar. Bu aksiyomlar aşağıdaki gibi listelenebilir.

1- Toplamada kapalılık: $a,b \in Z_m$ için $a+b \in Z_m$
2- Toplamada değişme: $a,b \in Z_m$ için $a+b=b+a$
3- Toplamada geçişme: $a,b \in Z_m$ için $(a+b)+c=a+(b+c)$
4- Toplama etkisiz eleman 0: $a,b \in Z_m$ için $a+0=0+a=a$
5- $a \in Z_m$ için a'nin toplamaya göre tersi $m-a$ 'dır.
6- Çarpmada kapalılık: $a,b \in Z_m$ için $a.b \in Z_m$
7- Çarpmada değişme: $a,b \in Z_m$ için $a.b=b.a$
8- Çarpmada geçişme $a,b \in Z_m$ için $(a.b).c=a.(b.c)$
9- Çarpma işleminde etkisiz eleman 1'dir. $a \in Z_m$ için $a.1=1.a=a$
10- Dağılma özelliği sağlanır. $a,b,c \in Z_m$ olmak üzere $(a+b).c=ac+bc$ ve $a.(b+c)=ab+ac$

Yanda verilen aksiyomlardan;

- 1, 3, 4, 5 aksiyomlarını sağlayan cebirsel yapısına **grup** denir.
- Eğer bahsedilen özelliklerle beraber 2'yide sağlıyorsa **abelian grup** adını alır.
- Yine verilen aksiyomlardan 1, 2,.., 10 aksiyomlarını sağlayan cebirsel yapısına **halka** denir.
- Örnek olarak tamsayılar, reel sayılar ve kompleks sayılar halka örneklerindendir.

Bu aksiyomlara ek olarak toplama ve çarpmaya göre ters alma işlemini sağlayan cebirsel yapıya cisim adı verilir.

BİLGİSAYAR BİLİMLERİ İÇİN SONLU CİSİMLER TEORİSİ

Çarpmaya göre ters: a'nın tersi demek a^{-1}

$a.a^{-1} = 1 \bmod m$

Toplamaya göre ters: a'nın tersi demek –a

$-a = (m-a)$

BİLGİSAYAR BİLİMLERİ İÇİN SONLU CİSİMLER TEORİSİ

İpucu:
Toplama ve çarpmaya göre ters alma işlemini sağlayan cebirsel yapıya cisim adı verilir.

Örnek 1. Z_4'ü düşünelim.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

x	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Z_4 cisim oluşturur mu?

BİLGİSAYAR BİLİMLERİ İÇİN SONLU CİSİMLER TEORİSİ

İpucu:
Toplama ve çarpmaya göre ters alma işlemini sağlayan cebirsel yapıya cisim adı verilir.

Örnek 1. Z_4'ü düşünelim.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

X	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Görüldüğü gibi Z_4 bir cisim oluşturmaz. Çünkü çarpma işlemine göre 2'nin tersi yoktur.

BİLGİSAYAR BİLİMLERİ İÇİN SONLU CİSİMLER TEORİSİ

$\{0,1,2,3\}$ elemanları ile tanımlı aşağıda tabloda verilen ve farklı toplama ve çarpma işlemleri ile tanımlı yapı cisim oluşturur mu?

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

X	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

BİLGİSAYAR BİLİMLERİ İÇİN SONLU CİSİMLER TEORİSİ

Grup derecesi: Bir grubun derecesi $|G|$, gruptaki eleman sayısıdır. Eğer grup sonlu değilse derecesi de sonsuzdur. Eğer grup sonlu ise derecesi de sonlu olur.

Alt gruplar: H bir G grubun alt seti olmak üzere H, G üzerinde tanımlı işleme dayalı olarak bir grup oluşturuyorsa G'nin alt grubu olarak adlandırılır. Tanıma göre

1- a ve b her iki grubun elemanı ise $c = a \bullet b$ her iki grubun elemanıdır.
2- Aynı etkisiz ya da birim elemanına sahiptirler.
3- a her iki grubun elemanı ise a'nın tersi de her iki grubun elemanıdır.
4- G'nin etkisiz elemanından elde edilen grup G grubunun bir alt grubudur.
5- Her grup kendisinin alt grubudur.

BİLGİSAYAR BİLİMLERİ İÇİN SONLU CİSİMLER TEORİSİ

Devirsel Alt gruplar (Cyclic Alt Gruplar): Bir grubun alt grubu bir elemanın üsleri kullanılarak elde edilebiliyorsa bu gruba devirsel alt grup adı verilir. Üs terimi burada grup işlemini elemana devamlı uygulama anlamına gelmektedir.

$$a^n = a \bullet a \bullet ... \bullet a \text{ (n kere)}$$

Bu prosesle elde edilen set $\langle a \rangle$ ile tanımlanır. Bu işlem sonucu elde edilen birden fazla aynı eleman ayıklanır ve $a^0 = e$ (e etkisiz eleman) olarak ifade edilir.

Devirsel gruplar: Devirsel bir grup kendi devirsel alt grubudur. Diğer bir deyişle bu grup bir üreteç elemanına sahiptir. Eğer g bir üreteç elemanına sahipse

$$\left\{e, g, g^2, ..., g^{n-1}\right\}, \mathrm{g}^{\mathrm{n}} = e$$

olacak şekilde yazılabilir.

BİLGİSAYAR BİLİMLERİ İÇİN SONLU CİSİMLER TEORİSİ

İpucu:
Grubun derecesi I*G*I gruptaki eleman sayısıdır!

ÖRNEK:

Grup $G = \{1,2,3,4,5,6\}$ yi çarpmaya göre mod 7 altında düşünelim.

a-) G'nin çarpma tablosunu bulunuz.

b-) $2^{-1}, 3^{-1}, 6^{-1}$'i bulunuz.

c-) 2 ve 3 tarafından üretilen dereceleri (orders) ve alt grupları (subgroups) bulunuz.

d-) G devirsel (cyclic) midir?

BİLGİSAYAR BİLİMLERİ İÇİN SONLU CİSİMLER TEORİSİ

X	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

$2^{-1} = 4$

b-) $3^{-1} = 5 \Rightarrow 2.4 = 1 \pmod 7$

$6^{-1} = 6$

$2^1 = 2$

c-) $2^2 = 4$ $|2| = 3$ ve $gp(2) = \{1, 2, 4\}.$

$2^3 = 1$

$3^1 = 3$

$3^2 = 2$

$3^3 = 6$

d-) $|3| = 6$ ve $gp(3) = G.$

$3^4 = 4$

$3^5 = 5$

$3^6 = 1$

e-) G grubu devirseldir (cyclic). Çünkü en azından bir elemanı grup elemanlarını üretmektedir.

$G = gp(3)$

BİLGİSAYAR BİLİMLERİ İÇİN SONLU CİSİMLER TEORİSİ

Lagrange Teoremi: Lagrange teoremi bir grubun derecesi ve onun alt grubunun derecesi ile ilgilidir. G bir grup ve H de onun bir alt grubu olsun. Eğer G ve H gruplarının dereceleri $|G|$ ve $|H|$ ise bu teoreme göre $|G|$, $|H|$ 'yi böler.

Örneğin $|G| = 6$ ise bu teoreme göre alt grupların dereceleri sırasıyla $|H_1| = 1, |H_2| = 3, |H_3| = 2$ ve $|H_4| = 6$ olacaktır.

BİLGİSAYAR BİLİMLERİ İÇİN SONLU CİSİMLER TEORİSİ-Temel Matematik Altyapı

OBEB ve Euclidean Algoritması

a ve b her ikisi de 0 olmayan tamsayılar olsun. Tamsayı d, her iki tamsayıyı da bölüyorsa tamsayı d'ye a ve b'nin ortak böleni denir. Eğer d, hem a'yı hem de b'yi bölüyorsa $d \setminus a$ ve $d \setminus b$ şeklinde gösterilir. $\gcd(a,b)$ ya da $OBEB(a,b)$ a ve b'nin en büyük ortak böleni olarak isimlendirilir.

Teorem 2. $ax+by$ formunun en küçük tamsayısı d olsun. O zaman $d = \gcd(a,b)$ şeklinde ifade edilebilir.

Önerme 2. $d = \gcd(a,b)$ olsun. O zaman herhangi $d = ax+by$ şeklinde x ve y tamsayıları mevcuttur.

Teorem 3. $d = \gcd(a,b)$ ise d aşağıdaki iki özelliğe sahiptir.

1- d, hem a'yı hem de b'yi böler.
2- c, hem a'yı hem de b'yi bölerse o zaman $c \setminus d$ şeklinde ifade edilebilir.

BİLGİSAYAR BİLİMLERİ İÇİN SONLU CİSİMLER TEORİSİ-Temel Matematik Altyapı

Euclidean Algoritması

a ve b tamsayılar ve $d = \gcd(a,b)$ olsun. $d = ax + by$ ifadesinde x ve y'yi bulmak için euclidean algoritması kullanılabilir. Bu algoritma ile bölme algoritmasının tekrar tekrar uygularız.

Birbirine Göre Asal Sayılar (Relatively Prime Integers)

İki tamsayı a ve b, $\gcd(a,b) = 1$ şeklinde ise o zaman bu iki tamsayı aralarında asaldır ve x ve y gibi iki tamsayı $ax + by = 1$ olacak şekilde vardır.

BİLGİSAYAR BİLİMLERİ İÇİN SONLU CİSİMLER TEORİSİ-Temel Matematik Altyapı

Örnek 7. 60 sayısını asal sayılar cinsinden yazalım.

$$60 = 2^2.3^1.5^1$$

Örnek 8. a-) $\gcd(12,18) = 6$

b-) $\gcd(12,16) = 4$

c-) $\gcd(29,15) = 1$

BİLGİSAYAR BİLİMLERİ İÇİN SONLU CİSİMLER TEORİSİ-Temel Matematik Altyapı

$a = 540, \mathrm{b} = 168$ olsun. $d = \gcd(a,b)$ değerini a'ya b'yi bölerek ve tekrar tekrar her kalanı 0 kalanı elde edene kadar bölünene böleriz

$$\gcd(540,168) = \gcd(168,36) = \gcd(36,24) = \gcd(24,12) = 12$$

$$\frac{540}{168} = 168.3 + 36,\ \frac{168}{36} = 36.4 + 24,\ \frac{36}{24} = 24.1 + 12,\ \frac{24}{12} = 12.2 + 0$$

$12 = 540\mathrm{x} + 168\mathrm{y}$ denklemindeki x ve y değerlerini elde edelim.

$$\begin{aligned} 540 &= 3.168 + 36 \\ 168 &= 4.36 + 24 \\ 36 &= 1.24 + 12 \end{aligned} \quad \Rightarrow \quad \begin{aligned} 12 &= 36 - 1.24 \\ 12 &= 36 - 1.(168 - 4.36) \\ 12 &= 5.36 - 1.168 \\ 12 &= 5(540 - 3.168) - 1.168 \\ 12 &= 5.540 - 16.168 \end{aligned}$$

Yukarıdaki gösterimden de anlaşılacağı gibi $x = 5$ ve $y = -16$ bulunur.

BİLGİSAYAR BİLİMLERİ İÇİN SONLU CİSİMLER TEORİSİ-Temel Matematik Altyapı

$\gcd(12,35)=1$ olduğunu gösterelim.

$$35 = 2.12 + 11$$
$$12 = 11.1 + 1$$

$$\Rightarrow$$

$$1 = 12 - 11.1$$
$$1 = 12 - 1.(35 - 2.12)$$
$$1 = 3.12 - 35$$

Yukarıdaki gösterimden de anlaşılacağı gibi $x = 3$ ve $y = -1$ bulunur.

Kaynaklar

- https://ocw.mit.edu/courses/mathematics/18-310-principles-of-discrete-applied-mathematics-fall-2013/lecture-notes/MIT18_310F13_Ch14.pdf
- https://ocw.mit.edu/courses/mathematics/18-310-principles-of-discrete-applied-mathematics-fall-2013/lecture-notes/
- M. Tolga SAKALLI, Bilgisayar Bilimi için Sonlu Cisimler Teorisi Ders Notları, Trakya Üniversitesi.
- Meltem KURT PEHLİVANOĞLU, Maksimum uzaklıkta ayrılabilen matrislerin elde edilebilmesi için yeni bir matris formu ve bir hafif sıklet blok şifreye uygulaması, Doktora Tezi, Kocaeli Üniversitesi, Fen Bilimleri Enstitüsü, Kocaeli, 2018, 519410.