UZEM | ONDOKUZ MAYIS ÜNİVERSİTESİ UZAKTAN EĞİTİM MERKEZİ

Ondokuz Mayıs Üniversitesi Fen Edebiyat Fakültesi Matematik Bölümü Dijital Ders Platformu

Temel Kavramlar

Prof. Dr. Şenol EREN

Ders 4

Soru 4: 4 elemanlı bir küme üzerinde kaç farklı işlem tanımlanabilir.

Soru 5: Aynı küme üzerinde değişme özelliğine sahip kaç farklı işlem tanımlanabilir.

Soru 6: $(a,4)=(b,4)=2$ olan $a,b\in\mathbb{Z}$ için $(a+b,4)=4$ olduğunu gösteriniz.

Soru 7: $m,n\in\mathbb{Z}$ için $mx+ny=1$ o.s. $\exists x,y\in\mathbb{Z}$ varsa $(m,n)=1$ dir gösteriniz.

Soru 8: 14732 ve 37149 sayılarının obeb'lerini Öklid Algoritması yoluyla bulunuz. $d = (14732, 37149)$ ise $d = 14732x + 37149y$ yapan $x, y \in \mathbb{Z}$ sayılarını bulunuz

2.2. Modüler Aritmetik

Bu bölümde cebirsel yapıları daha iyi anlayabilmek için tam sayıların bazı aritmetik özellikleri üzerinde durulacaktır.

Tanım 2.2.1 m sıfırdan farklı bir tam sayı olsun. $a, b \in \mathbb{Z}$ için $a \equiv b \pmod{m}$ gerekve yeter şart $m \mid a-b$ ile tanımlanır ve a ile b mod m denktirler denir.

$m \mid a-b \Rightarrow -m \mid a-b$ olduğundan $m > 0$ alınabilir.

Teorem 2.2.2 Yukarıda tanımlanan $\equiv$ bağıntısı $\mathbb{Z}$'de bir denklik bağıntısıdır.

Tanım 2.2.3 $\mathbb{Z}$ deki $\equiv$ denklik bağıntısının belirttiği denklik sınıflarına m modülüne göre (mod m) kalan sınıfları denir ve tüm kalan sınıflarının kümesi $\mathbb{Z}_m$ ile gösterilir. $a \in \mathbb{Z}$ nin denklik sınıfı $\bar{a} = \{x \in \mathbb{Z} \mid m \mid a-x\}$

Teorem 2.2.4 $a \equiv b \pmod m \iff$ a ve b nin m ile bölümünden elde edilen kalanın aynı olmasıdır.

İspat: ($\Rightarrow$) $a \equiv b \pmod m$ olsun $a = qm + r$, $b = q'm + r'$ ve $0 \le r', r < m$ olacak şekilde $\exists\, q, q', r, r' \in \mathbb{Z}$ vardır.

$a \equiv b \pmod m \Rightarrow m \mid a-b \Rightarrow a = b + km = qm + r$, $0 \le r < m$

$b = (q-k)m + r$, $0 \le r < m$ olduğundan, kalanlı bölmenin tekliğinden $q' = q-k$ ve $r = r'$ bulunur.

($\Leftarrow$) $a = qm + r$, $b = q'm + r$ ve $0 \le r, r' < m$ olsun

$a - b = (q-q')m \Rightarrow m \mid a-b \Rightarrow a \equiv b \pmod m$ bulunur.

Not 2.2.5 $a \in \mathbb{Z}$ nin $m>0$ ile bölümünden elde edilen kalanlar $0, 1, \ldots, m-1$ olacağından $\bar{a}$ sınıfı $\bar{0}, \ldots, \overline{m-1}$ sınıflarından biridir. O halde $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$ olup $|\mathbb{Z}_m| = m$ dir.

Örnek 2.2.6 $\mathbb{Z}_8 = \{\bar{0}, \bar{1}, \ldots, \bar{7}\}$ dir. $14 \equiv 6 \pmod 8$ ve $21 \equiv 5 \pmod 8$ olduğundan $14 \in \bar{6}$, $21 \in \bar{5}$ dir.

Teorem 2.2.7 $a \equiv a_1 \pmod m$ ve $b \equiv b_1 \pmod m$ ise $a+b \equiv a_1+b_1 \pmod m$ ve $a \cdot b \equiv a_1 b_1 \pmod m$ dir.

İspat: $a \equiv a_1 \pmod m$, $b \equiv b_1 \pmod m$ ise

$m \mid a-a_1$, $m \mid b-b_1 \Rightarrow m \mid (a+b)-(a_1+b_1)$

$\Rightarrow a+b \equiv a_1+b_1 \pmod m$ bulunur. Diğer yandan

$m \mid a-a_1$, $m \mid b-b_1 \Rightarrow m \mid a_1(b-b_1)+b(a-a_1) = ab-a_1b_1$

$\Rightarrow ab \equiv a_1 b_1 \pmod m$ bulunur.

Tanım: 2.2.8 $\bar{a}, \bar{b} \in \mathbb{Z}_m$ için $\bar{a} \oplus \bar{b} = \overline{a+b}$ ve $\bar{a} \odot \bar{b} = \overline{a.b}$ ile tanımlanır

Örnek 2.2.9 $\mathbb{Z}_9$ da $\bar{3} \oplus \bar{8} = \bar{11} = \bar{2}$, $\bar{3} \odot \bar{8} = \overline{24} = \bar{6}$ dır.

Teorem 2.2.10 $\forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_m$ için

i) $\bar{a} \oplus \bar{b} = \bar{b} \oplus \bar{a}$ dır.

ii) $\bar{a} \oplus (\bar{b} \oplus \bar{c}) = (\bar{a} \oplus \bar{b}) \oplus \bar{c}$

iii) $\bar{a} \oplus \bar{0} = \bar{a}$

iv) $\bar{a} \oplus \bar{x} = \bar{0}$ olacak şekilde $\exists \bar{x} \in \mathbb{Z}_m$ bulunabilir.

Teorem 2.2.11 $\forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_m$ için

i) $\bar{a} \odot \bar{b} = \bar{b} \odot \bar{a}$

ii) $\bar{a} \odot (\bar{b} \odot \bar{c}) = (\bar{a} \odot \bar{b}) \odot \bar{c}$

iii) $\bar{a} \odot \bar{1} = \bar{a}$

iv) $\bar{a} \odot \bar{0} = \bar{0}$ dır.

Teorem 2.2.12 $\forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_m$ için

$\bar{a} \odot (\bar{b} \oplus \bar{c}) = (\bar{a} \odot \bar{b}) \oplus (\bar{a} \odot \bar{c})$ dir.

Örnek 2.2.13 $\mathbb{Z}_9$ da

$\bar{4} \odot (\bar{5} \oplus \bar{7}) = \bar{4} \odot \bar{3} = \bar{12} = \bar{3}$ ve $(\bar{4} \odot \bar{5}) \oplus (\bar{4} \odot \bar{7}) = \bar{2} \oplus \bar{1} = \bar{3}$

Tanım 2.2.14 $\mathbb{Z}_m$ de kendileri $\bar{0}$ den farklı olduğu halde çarpımları $\bar{0}$ olan sınıflara sıfır bölen sınıf denir.

Örnek 2.2.15 $\mathbb{Z}_{12}$ de sıfır bölen sınıflar $\bar{2}, \bar{3}, \bar{4}, \bar{6}, \bar{8}, \bar{9}, \bar{10}$ dir.

Tanım 2.2.16 $\bar{a} \in \mathbb{Z}_m$ sınıfı için $(a, m) = 1$ ise $\bar{a}$ sınıfına asal kalan sınıfı denir. $\mathbb{Z}_m$ nin asal kalan sınıfları $\mathbb{Z}_m^*$ ile gösterilir. $\mathbb{Z}_m^*$ eleman sayısının $\varphi(m)$ Euler fonksiyonu ile verilir $|\mathbb{Z}_m^*| = \varphi(m)$ dir.

Teorem 2.2.17 $a \equiv b \pmod{m}$ ise $(a,m)=(b,m)$ dir.

İspat: $a \equiv b \pmod{m} \Rightarrow m \mid a-b \Rightarrow a = b+mk,\ k \in \mathbb{Z}$

$(a,m)=d$ olsun. $d \mid a \wedge d \mid m$ olduğundan $d \mid b=a-mk$ dir. O halde d b ile m nin bir ortak bölenidir. $t \mid b \wedge t \mid m$ olsun $t \mid a=b+mk$ olduğundan $t \mid d=(a,m)$ bulunur. O zaman $d=(b,m)$ dir.

Teorem 2.2.18 İki asal kalan sınıfının çarpımıda bir asal kalan sınıfıdır.

İspat: $\bar{a}, \bar{b} \in \mathbb{Z}_m^*$ olsun. $(a,m)=(b,m)=1$ dir. $(a,m)=1$ ise $ax+my=1,\ \exists x,y \in \mathbb{Z}$ dir. $abx+bmy=b$

$(ab,m)=t$ olsun. $t \mid ab \wedge t \mid m \Rightarrow t \mid b$ dir.

$t \mid m \wedge t \mid b$ $t \mid (b,m)=1$ olup $(ab,m)=1$ bulunur.

Teorem 2.2.19 $\bar{a} \in \mathbb{Z}_m$, $\bar{a} \neq \bar{0}$ olsun.

$\bar{a}$ sıfır bölen sınıftır $\iff \bar{a} \notin \mathbb{Z}_m^*$.

Ispat: ($\Rightarrow$) $\exists \bar{b} \in \mathbb{Z}_m$, $\bar{b} \neq \bar{0}$ için $\bar{a} \odot \bar{b} = \overline{ab} = \bar{0}$ dir.

$\bar{a} \in \mathbb{Z}_m^*$ kabul edelim. $(a,m) = 1$, $m \mid ab \Rightarrow m \mid b \Rightarrow$

bu bir çelişkidir. $\bar{a} \notin \mathbb{Z}_m^*$ bulunur.

($\Leftarrow$) $\bar{a} \in \mathbb{Z}_m^*$, $\bar{a} \neq \bar{0}$ olsun. $(a,m) = d > 1$ dir. $\bar{a} \neq \bar{0} \Rightarrow m \nmid a$

$\Rightarrow m \nmid d \Rightarrow d \neq m$ dir.

$(a,m) = d \Rightarrow m = dm'$, $a = da'$, $(a',m') = 1$ olacak

şekilde $m', a' \in \mathbb{Z}$ dir. $am' = da'm' = a'm \Rightarrow \overline{a.m'} = \bar{0}$

$\overline{m'} \neq \bar{0}$ olduğundan $\bar{a}$ bir sıfır bölen sınıftır.

Tanım 2.2.20 $\bar{a} \in \mathbb{Z}_m$ olsun. $\bar{a} \odot \bar{c} = \bar{1}$ olacak şekilde

$\exists \bar{c} \in \mathbb{Z}_m$ varsa $\bar{c}$ ye $\bar{a}$ nın tersi denir.

Teorem 2.2.21 Bir $\bar{a} \in \mathbb{Z}_m$, $\bar{a} \neq \bar{0}$ sınıfının tersinin olabilmesi için gerekve yeter şart $\bar{a} \in \mathbb{Z}_m^*$ olmasıdır.

İspat: ($\Rightarrow$) $\bar{a} \odot \bar{c} = \overline{a.c} = \bar{1}$ olsun. $\bar{a}$ nın sıfır bölen olmadığını göstermeliyiz (Teorem 2.2.19). Bir $\bar{0} \neq \bar{b} \in \mathbb{Z}_m$ için $\bar{a} \odot \bar{b} = \overline{a.b} = \bar{0}$ olduğunu kabul edelim.

$\bar{c} \odot (\bar{a} \odot \bar{b}) = (\bar{c} \odot \bar{a}) \odot \bar{b} = \overline{c.a} \odot \bar{b} = \bar{1} \odot \bar{b} = \bar{b} = \bar{0}$ çelişkisi bulunur. O halde $\bar{a}$ sıfır bölen değildir.

$\Leftarrow$ $\bar{a} \in \mathbb{Z}_m^*$ olsun. $(a, m) = 1$ ve $ax + my = 1$, $\exists\, x, y \in \mathbb{Z}$ dir. Buradan $ax \equiv 1 \pmod{m}$ olup $\bar{x} \odot \bar{a} = \bar{1} \Rightarrow \bar{x} = \bar{a}^{-1}$ bulunur.

UZEM | ONDOKUZ MAYIS ÜNİVERSİTESİ UZAKTAN EĞİTİM MERKEZİ

Ondokuz Mayıs Üniversitesi
Fen Edebiyat Fakültesi
Matematik Bölümü
Dijital Ders Platformu

Teşekkürler

Prof. Dr. Şenol EREN

Cebir I

Ders 4