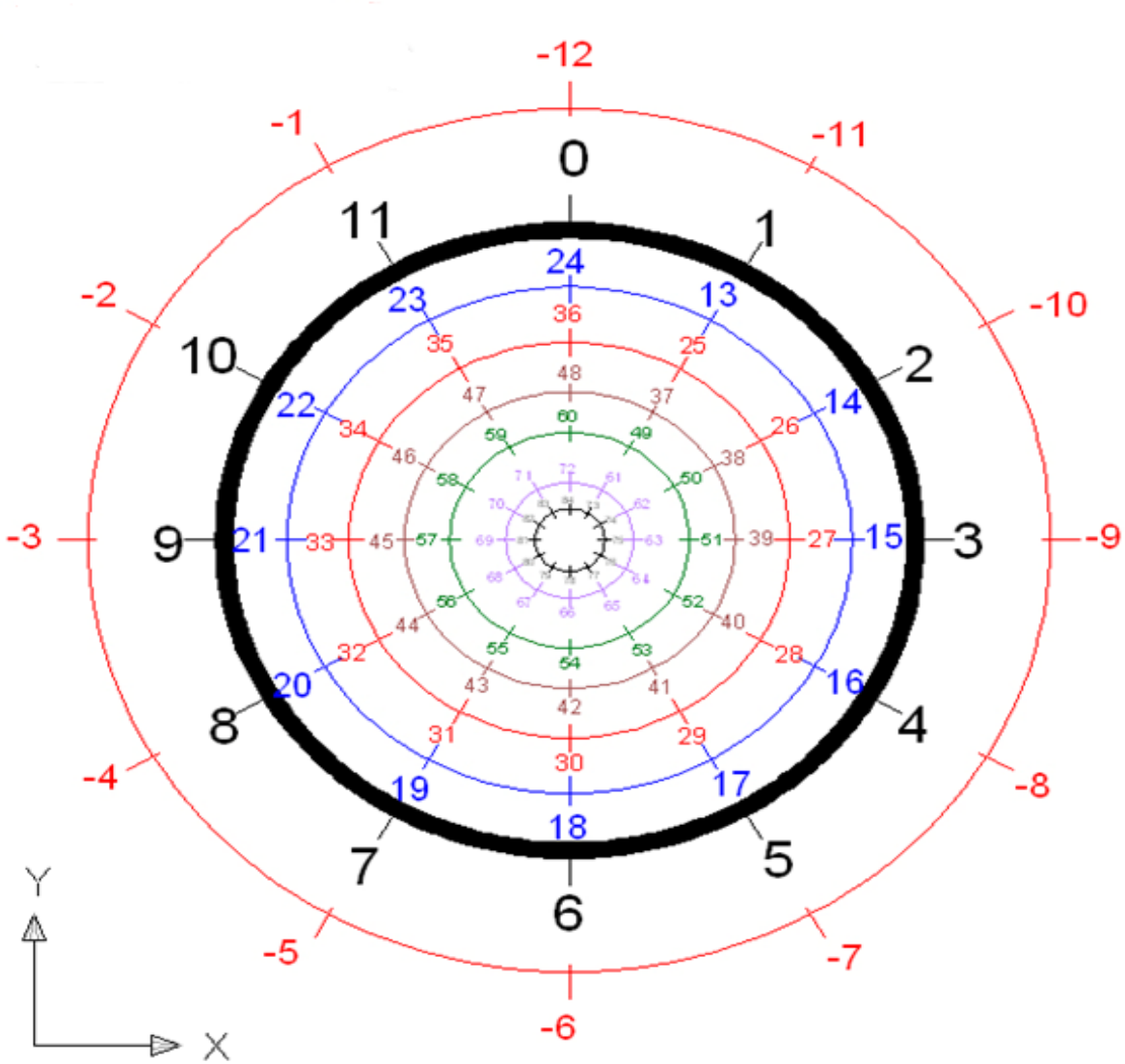
ÇANAKKALE ONSEKİZ MART ÜNİVERSİTESİ

FEN EDEBİYAT FAKÜLTESİ MATEMATİK BÖLÜMÜ

MODÜLER ARİTMETİK



ÇANAKKALE 2012

ÖNSÖZ

Bu kitap Çanakkale Onsekiz Mart Üniversitesi Matematik Bölümünde lisans dersi olarak Cebirden Seçmeli Konular dersinde işlenen Modüler Aritmetik konusunu öğrencilere anlatabilmek amacıyla dördüncü sınıf öğrencileri tarafından hazırlanmıştır.

Modüler Aritmetikle ilgilenen herkes ek kaynak olarak bu kitaptan yararlanabilirler. Kitabı benzerlerinden ayrı kılan ve öne çıkaran daha yalın bir dille verilmesidir.

Kitabımız uzun bir çalışmadan sonra titizlikle hazırlanmıştır. Kitabı hazırlarken gösterdiğimiz özveriye rağmen, yanlışlar ve unutulmuş noktalar bulunabilir. Okurlarımızın yapacağı her türlü eleştiri ve önerileri memnuniyetle karşılayacağımızı bildirir, saygı ve sevgilerimizi sunarız.

Öğr. Ebru AYDINDAĞ

Öğr. Gülden DİKMEN

İçindekiler

MODÜLER ARİTMETİK

TANIM: $m \neq 0$ bir tamsayı olsun. $a, b \in \mathbb{Z}$ için $a \equiv b(mod\ m) \Rightarrow m|a-b$ ile tanımlanır ve **"a ile b mod m ye göre denktirler"** denir.

ÖNERME: Yukarıda tanımlanan "≡" bağıntısı $\mathbb{Z}$'de bir denklik bağıntısıdır.

İSPAT: "≡" bağıntısının denklik bağıntısının koşullarını sağladığını gösterelim:

i. Yansıma: $\forall\ a\ \in \mathbb{Z}$ için $m|0 = a - a$ olduğundan $a \equiv a(mod\ m)$'dir.

ii. Simetri: $a, b\ \in\ \mathbb{Z}$ için $a \equiv b(mod\ m)$ olsun.
O halde $m|a-b$'dir.$\Rightarrow a - b = mk\ , k \in \mathbb{Z}$

$$\Rightarrow \underbrace{b-a} = -(a-b) = -(mk) = \underbrace{m(-k)}\ , -k \in \mathbb{Z}$$

$$\Rightarrow m|b-a$$

$$\Rightarrow b \equiv a\ (mod\ m)$$

iii. Geçişme: $a, b, c \in \mathbb{Z}$ için $a \equiv b\ (mod\ m)$ ve $b \equiv c\ (mod\ m)$ olsun.

$\Rightarrow a - b = mk$ ve $\ b - c = mt\ ,\ k, t \in \mathbb{Z}$

$\Rightarrow (a-c) + (b-c) = mk + mt\ ,\ k, t \in \mathbb{Z}$

$\Rightarrow \quad a - c = m(k+t)\ , k + t \in \mathbb{Z}$

$\Rightarrow m|a - c\ dir.$ Dolayısıyla $\ a \equiv c\ (mod\ m)$ olur.

O halde tanımlanan "≡" bağıntısı bir denklik bağıntısıdır.

ÖNERME: Eğer $\ a \equiv b\ (mod\ m)$ ve $c \equiv d\ (mod\ m)$ ise;

(i) $a + c \equiv b + d\ (mod\ m)$

(ii) $ac = bd\ (mod\ m)$ dir.

İSPAT: (i) $a \equiv b\ (mod\ m)\ , c \equiv d\ (mod\ m) \Rightarrow m|a-b\ ,\ m|c-d$

$$\Rightarrow a - b = mk\ , c - d = mt\ \ , k, t \in \mathbb{Z}$$

$$\Rightarrow a - b + c - d = mk + mt$$

$$\Rightarrow (a+c) - (b+d) = m(k+t), \quad k + t \in \mathbb{Z}$$

$$\Rightarrow m|(a+c) - (b+d) \quad (mod\ m)$$

$$\Rightarrow a + c \equiv b + d \quad (mod\ m)$$

(ii) $a \equiv b\ (mod\ m)\ ,\ c \equiv d\ (mod\ m)\ \Rightarrow m|a-b\ ,\ m|c-d$

$$\Rightarrow a-b=mk\ , c-d=mt \qquad k,t \in \mathbb{Z}$$

$0 = bc - bc$ olarak alalım: $ac-bd = ac+0-bd = ac+bc-bc-bd$

$$= (a-b)c+(c-d)b$$

$$= (mk)c+(mt)b \qquad k,t \in \mathbb{Z}$$

$$= m(kc+tb)$$

$$\Rightarrow ac-bd = m(kc+tb)$$

$$\Rightarrow m|ac-bd$$

$$\Rightarrow ac \equiv bd\ \ (mod\ m)$$

NOT: "≡" bağıntısı denklik bağıntısının koşullarına ek olarak;

$a \equiv b\ (mod\ m)\ , c \equiv d\ (mod\ m)$ olduğunda $ac \equiv bd\ \ (mod\ m)$ koşulunu da sağladığından aynı zamanda bir kongruens bağıntısıdır.

TANIM: $\mathbb{Z}$ deki "≡" denklik bağıntısının belirttiği denklik sınıflarına **m modülüne göre (mod m) kalan sınıfları** denir. Ve tüm kalan sınıfları kümesi $\mathbb{Z}_m$ ile gösterilir.

$a \in \mathbb{Z}$ olmak üzere a'nın denklik sınıfı $\bar{a} = \{x \in \mathbb{Z} : m|a-x\}$ şeklinde gösterilir.

TEOREM: $a \equiv c\ (mod\ m) \Leftrightarrow \bar{a} = \bar{c}$

İSPAT: ($\Rightarrow$) $a \equiv c\ (mod\ m)$ olsun. $b \in \bar{a}$ alalım.

$$\Rightarrow m|a-b$$

$$\Rightarrow b \equiv a\ (mod\ m)$$

$\Rightarrow \left.\begin{matrix} a \equiv c\ (mod\ m) \\ b \equiv a\ (mod\ m) \end{matrix}\right\}\ b \equiv c\ (mod\ m) \Rightarrow b \in \bar{c}$ olur. Dolayısıyla $\bar{a} \subseteq \bar{c}$ 'dir.

Benzer şekilde $\bar{c} \subseteq \bar{a}$ olduğu gösterilir. O halde $\bar{a} = \bar{c}$ 'dir.

($\Leftarrow$) $\bar{a} = \bar{c}$ olsun. Yansıma özelliğinden $a \equiv a\ (mod\ m)$ olduğundan $a \in \bar{a}$ 'dir. Buradan $a \in \bar{c}$ olur. O halde $m|c-\ a \Rightarrow a \equiv c\ (mod\ m)$ 'dir.

SONUÇ: Her $\bar{a}, \bar{b} \in \mathbb{Z}_m$ için ya $\bar{a} \cap \bar{b} = \emptyset$ ya da $\bar{a} = \bar{b}$ 'dir.

İSPAT: Kabul edelim ki $\bar{a} \cap \bar{b} \neq \emptyset$ olsun. $c \in \mathbb{Z}$ olmak üzere $c \in \bar{a}$ ve $c \in \bar{b}$ 'dir.

$\Rightarrow c \equiv a \ (mod\ m)$ ve $c \equiv b \ (mod\ m)$

$\Rightarrow a \equiv b \ (mod\ m)$ (simetri ve geçişme özelliğinden)

$\Rightarrow \bar{a} = \bar{b}$ dir.

SONUÇ: m>1 bir tamsayı ve modülo m kongruenslerini ele alalım.

(i) a herhangi bir tamsayı ve r de a nın m ye bölümünden kalan ise $\bar{a} = \bar{r}$ dır.

(ii) Kesinlikle n tane farklı kongruens sınıfları vardır. Bunlar $\bar{0}, \bar{1}, \bar{2}, \ \dots\ , \overline{m-1}$ dir.

İSPAT:

(i) $a \in \mathbb{Z}$ alalım. Bölme algoritmasından $a = mq + r\ , 0 \leq r < m$ yazabiliriz. Buradan $a - r = mq$ olup $a \equiv r \ (mod\ m)$ olduğu görülür. Bir önceki teoremden de $\bar{a} = \bar{r}$ ' dır.

(ii) $\bar{a}$ herhangi bir kongruens sınıfı olsun. (i) den $\bar{a} = \bar{r}\ , 0 \leq r < m$ yazabiliriz. O halde

$\bar{a}\ ;\ \bar{0}, \bar{1}, \bar{2}, \dots, \overline{m-1}$ lerden en az birine eşit olmalıdır.

İspatı tamamlamak için $\bar{0}, \bar{1}, \bar{2}, \dots, \overline{m-1}$ sınıflarının hepsinin birbirlerinden farklı olduğunu göstermeliyiz. Kabul edelim ki; $t, s \in \mathbb{Z}$ için $0 \leq s < t < m$ olsun.

$\Rightarrow t - s \ \in \mathbb{Z}^+$ve $t - s < m$' dir.

$\Rightarrow m \nmid t - s \ \Rightarrow t \not\equiv s \ (mod\ m)$ olur.

$0,1,2, \dots, m-1$'lerden herhangi iki tanesi birbirine eşit olamaz. O zaman $\bar{0}, \bar{1}, \bar{2}, \dots, \overline{m-1}$ denklik sınıfları birbirinden farklıdır. O halde $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{m-1}\}$ şeklinde yazılır.

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

İSPAT: $\forall\ \bar{a}, \bar{b}, \bar{c}\ , \bar{d} \ \in \mathbb{Z}_m$ için; $(\bar{a},\bar{b}) = (\bar{c},\bar{d})$ olsun.

$\Rightarrow \ \bar{a} = \bar{c} \Rightarrow a \equiv c \ (mod\ m) \Leftrightarrow m|a - c \Leftrightarrow a - c = mx\ , x \ \in \mathbb{Z} \ \Leftrightarrow a = mx + c$

$\bar{b} = \bar{d} \Rightarrow \ b \equiv d \ (mod\ m) \Leftrightarrow m|b - d \Leftrightarrow b - d = my\ , y \in \mathbb{Z} \Leftrightarrow b = my + d$

$\Rightarrow \ a + b = mx + c + my + d = m(x + y) + c + d \Rightarrow a + b \equiv c + d \ (mod\ m)$

$\Rightarrow \overline{a+b} = \overline{c+d}$

$\Rightarrow \bar{a} \oplus \bar{b} = \bar{c} \oplus \bar{d}$ olduğundan $\mathbb{Z}_m$ üzerinde tanımladığımız $\oplus$ işlemi iyi tanımlıdır.

TANIM: $\bar{a}, \bar{b} \in \mathbb{Z}_m$ için; $\bar{a} \odot \bar{b} = \overline{ab}$ ile tanımlanır.

İSPAT: $\forall\, \bar{a}, \bar{b}, \bar{c}, \bar{d} \in \mathbb{Z}_m$ için; $(\bar{a},\bar{b}) = (\bar{c},\bar{d})$ olsun.

$\Rightarrow \bar{a} = \bar{c} \Leftrightarrow a \equiv c\ (mod\ m) \Leftrightarrow m|a-c \Leftrightarrow a - c = mx\,, x \in \mathbb{Z} \Leftrightarrow a = mx + c$

$\bar{b} = \bar{d} \Rightarrow\ b \equiv d\ (mod\ m) \Leftrightarrow m|b-d \Leftrightarrow b - d = my\,, y \in \mathbb{Z} \Leftrightarrow b = my + d$

$\Rightarrow ab = (mx + c)(my + d)$

$\Rightarrow ab = mxmy + mxd + cmy + cd$

$\Rightarrow ab = m(mxy + xd + cy) + cd$

$\Rightarrow ab \equiv cd\ (mod\ m)$

$\Rightarrow \overline{ab} = \overline{cd}$

$\Rightarrow \bar{a} \odot \bar{b} = \bar{c} \odot \bar{d}$ olduğundan $\mathbb{Z}_m$ üzerinde tanımlanan $\odot$ işlemine göre iyi tanımlıdır.

ÖNERME: $\mathbb{Z}_m$**'** de $\oplus$ işleminin şu özellikleri vardır. $\forall\, \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_m$ için;

i) $\bar{a} \oplus \bar{b} = \bar{b} \oplus \bar{a}$ (değişme özelliği)

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

iii) $\bar{a} \oplus \bar{0} = \bar{0} \oplus \bar{a} = \bar{a}$ ($\bar{0}$ etkisiz eleman)

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

İSPAT:

(i) $\forall\, a, b \in \mathbb{Z}$ için, $a + b = b + a$ olduğundan;

$\bar{a} \oplus \bar{b} = \overline{a + b} = \overline{b + a} = \bar{b} \oplus \bar{a}$ elde edilir.

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

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

$\mathbb{Z}\ de\ +$ nın birleşme özelliğinden dolayı istenen eşitlik elde edilir.

(iii) $\bar{a} \oplus \bar{0} = \overline{a + 0} = \bar{a}$ olduğu açıktır.

iv) $\forall\, a \in \mathbb{Z}$ için, a nın ters işaretlisi $-a$ ile gösterilirse $a + (-a) = 0$ dır.

Buradan $\bar{a} \oplus \overline{(-a)} = \overline{a + (-a)} = \bar{0}$ bulunur. O halde $\bar{a}$ nın tersi $\overline{-a}$ sınıfıdır.

NOT: $\mathbb{Z}_m$ de tanımlanan $\oplus$ işlemine göre yukarıdaki özellikler sağlandığından ($\mathbb{Z}_m$,$\oplus$) bir değişmeli gruptur.

ÖNERME: $\mathbb{Z}_m$ de $\odot$ işleminin şu özellikleri vardır. $\forall\ \bar{a}, \bar{b}, \bar{c}\ \in \mathbb{Z}_m$ için;

i) $\bar{a}\ \odot\ \bar{b} = \bar{b} \odot \bar{a}$ (değişme özelliği)

ii) $\bar{a} \odot \left(\bar{b} \odot \bar{c}\right) = \left(\bar{a} \odot \bar{b}\right) \odot \bar{c}$ dir. (birleşme özelliği)

iii) $\bar{a}\ \odot \bar{1} = \bar{1}\ \odot \bar{a} = \bar{a}$ ($\bar{1}$ birim eleman)

iv) $\bar{a}\ \odot \bar{0} = \bar{0} \odot \bar{a}\ = \bar{0}$ ($\bar{0}$ yutan eleman)

İSPAT:

i) $\forall\ a, b\ \in \mathbb{Z}$ için, $ab = ba$ olduğundan;

$\bar{a}\ \odot \bar{b} = \overline{ab} = \overline{ba} = \ \bar{b} \odot \bar{a}$ elde edilir.

ii) $\bar{a} \odot \left(\bar{b} \odot \bar{c}\right) = \bar{a} \odot (\overline{bc}) = \overline{a(bc)} = \overline{(ab)c} = \overline{(ab)} \odot \bar{c}\ = \left(\bar{a} \odot \bar{b}\right) \odot \bar{c}$

iii) $\bar{a}\ \odot \bar{1} = \overline{a1} = \bar{a}$

iv) $\bar{a}\ \odot \bar{0} = \overline{a0} = \bar{0}$

NOT: $\mathbb{Z}_m$ de tanımlanan $\odot$ işlemine göre yukarıdaki özellikler sağlandığından ($\mathbb{Z}_m$, $\odot$) bir değişmeli monoiddir.

ÖNERME: . $\forall\ \bar{a}, \bar{b}, \bar{c}\ \in \mathbb{Z}_m$ için;

$\bar{a} \odot \left(\bar{b} \oplus \bar{c}\right) = \left(\bar{a}\ \odot\ \bar{b}\right) \oplus (\bar{a} \odot \bar{c})$ dir. ($\odot$ işleminin $\oplus$ işlemi üzerine dağılma özelliği)

İSPAT: $\bar{a} \odot \left(\bar{b} \oplus \bar{c}\right) = \bar{a} \odot \overline{(b + c)} = \overline{a(b + c)}$ ve

$\left(\bar{a}\ \odot\ \bar{b}\right) \oplus (\bar{a} \odot \bar{c}) = \overline{ab} \oplus \overline{ac} = \overline{ab + ac}$ dir.

$\mathbb{Z}\ de$, çarpmanın toplama üzerine dağılma özelliğinden istenen eşitlik elde edilir.

NOT: Yukarıdaki önermeler göz önüne alındığında ($\mathbb{Z}_m$,$\oplus$,$\odot$) nın bir halka olduğu anlaşılır.

ÖRNEK: $\mathbb{Z}_7 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{6}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$

$\odot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{1}$	$\bar{3}$	$\bar{5}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{2}$	$\bar{5}$	$\bar{1}$	$\bar{4}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{1}$	$\bar{5}$	$\bar{2}$	$\bar{6}$	$\bar{3}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{3}$	$\bar{1}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{6}$	$\bar{0}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

■$\bar{5} \odot (\bar{4} \oplus \bar{2}) = \bar{5} \odot \bar{6} = \bar{2}$

$(\bar{5} \odot \bar{4}) \oplus (\bar{5} \odot \bar{2}) = \bar{6} \oplus \bar{3} = \bar{2}$

■ $(\bar{4} \odot \bar{3}) \odot \bar{6} = \bar{5} \odot \bar{6} = \bar{2}$

$\bar{4} \odot (\bar{3} \odot \bar{6}) = \bar{4} \odot \bar{4} = \bar{2}$

TANIM: $\mathbb{Z}_m$ de kendileri $\bar{0}$ dan farklı olduğu halde çarpımları $\bar{0}$ olan sınıflara **sıfır bölen sınıflar** denir.

ÖRNEK:$\mathbb{Z}_8 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}\}$ olmak üzere $\mathbb{Z}_8$ in sıfır bölenleri; $\bar{2}, \bar{4}, \bar{6}$ dır.
$\bar{2} \neq \bar{0}$ ve $\bar{4} \neq \bar{0}$ olduğu halde $\bar{2} \odot \bar{4} = \bar{0}$ olur. $\bar{4} \neq \bar{0}\ ve\ \bar{6} \neq \bar{0}$ için $\bar{4} \odot \bar{6} = \bar{0}$ dır.

ÖNERME: $a \equiv b\ (mod\ m) \Rightarrow (a, m) = (b, m)$

İSPAT: $a \equiv b\ (mod\ \ m) \Rightarrow m|a - b \Rightarrow a - b = mk \Rightarrow b = a - mk\ \ , k \in \mathbb{Z}$

$(a, m) = d$ olsun.

$d|a\ , d|m$ olduğundan $d|a - mk = b\ \Rightarrow d|b$ olur. O halde; d, b ile m nin ortak bölenidir.

Kabul edelim ki; t herhangi bir ortak bölen olsun.

$t|b$ ve $t|m \Rightarrow t|b + mk = a$

$\Rightarrow t|a\ \ \Rightarrow t|d = (a, m) \Rightarrow d = (b, m)$

TANIM: $\bar{a} \in \mathbb{Z}_m$ sınıfı için $(a, m) = 1$ ise $\bar{a}$ sınıfına **asal kalan sınıfı** denir. $\mathbb{Z}_m$ nin bütün asal kalan sınıfları $\mathbb{Z}_m^*$ ile gösterilir. Ayrıca m modülü asal ise $\mathbb{Z}_m^* = \mathbb{Z}_m \setminus \{\bar{0}\}$ dır.

ÖRNEK: $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ için $\mathbb{Z}_4^* = \{\bar{1}, \bar{3}\}$ dır.

$\mathbb{Z}_7 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$ için $\mathbb{Z}_7^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$ dır.

TEOREM: İki asal kalan sınıfının çarpımı da bir asal kalan sınıfıdır.

İSPAT: $\bar{a}, \bar{b} \in \mathbb{Z}_m^*$ olsun. $(a,m) = (b,m) = 1$ olduğundan, $xa + ym = 1$ olacak şekilde $\exists x, y \in \mathbb{Z}$ bulunabilir. Bu eşitliğin her iki yanını b ile çarparsak;

$b = xab + ymb$ elde edilir. $(ab,m) = t$ olarak kabul edelim.

$\Rightarrow t|ab$ ve $t|m$ olur

$\Rightarrow t|b$ ve $t|m$

$\Rightarrow (b,m) = 1$ kabul ettiğimizden $t = 1$ olmalıdır. Yani $(ab,m) = 1$ olur.

O halde $\overline{ab} = \bar{a} \odot \bar{b}$ olur. İki asal kalan sınıfının çarpımı da bir asal kalan sınıfıdır.

ÖNERME: $\mathbb{Z}_m$ deki $\bar{0}$ den farklı bir kalan sınıfının sıfır bölen olması için gerek ve yeter koşul asal kalan sınıfı olmamasıdır.

İSPAT: $(\Rightarrow)$ $\bar{0} \neq \bar{a} \in \mathbb{Z}_m$ bir sıfır bölen olsun. O halde $\bar{a}\bar{b} = \bar{0}$ olacak şekilde bir $\bar{b} \in \mathbb{Z}_m$ bulunabilir.

$\bar{a}$ nın bir asal kalan sınıfı olduğunu kabul edelim. Yani $(a,m) = 1$ olsun.

$\bar{a} \odot \bar{b} = \overline{ab} = \bar{0} \Rightarrow m|ab$ ve $(a,m) = 1$ olduğundan, $m|b$ yani $\bar{b} = \bar{0}$ çelişkisi elde edilir.

O halde kabulümüz yanlıştır. $\bar{a}$ bir asal kalan sınıfı değildir.

$(\Leftarrow)$ $\bar{0} \neq \bar{a}$ asal kalan sınıfı olmasın. O halde $(a,m) = d > 1$ dir.

$\bar{a} \neq \bar{0}$ olduğundan, $m \nmid a$ dır. Buradan $d \neq m$ bulunur.

$(a,m) = d \Rightarrow m = dm'$, $a = da'$ ve $(a',m') = 1$, $\exists a', m' \in \mathbb{Z}$ bulunabilir.

$am' = da'\, m' = a'm$ eşitliğinden $\bar{a} \odot \overline{m'} = \bar{0}$ bulunur. $\overline{m'} \neq \bar{0}$ olduğundan, sonuç olarak $\bar{a}$ nın bir sıfır bölen olduğu anlaşılır.

TANIM: $\bar{a} \in \mathbb{Z}_m$ olsun. $\bar{a} \odot \bar{c} = \bar{1}$ olacak şekilde $\exists\, \bar{c} \in \mathbb{Z}_m$ varsa **$\bar{c}$ ye $\bar{a}$ nin tersi** denir.

ÖNERME: $\mathbb{Z}_m$ deki bir kalan sınıfının tersinin olması için gerek ve yeter koşul bir asal kalan sınıfı olmasıdır.

İSPAT: ($\Rightarrow$) $\bar{a} \in \mathbb{Z}_m$ nın tersi var olsun. Yani $\bar{a} \odot \bar{c} = \bar{1}$ olacak şekilde $\exists\, \bar{c} \in \mathbb{Z}_m$ bulunabilsin. $\bar{a}$ nın bir sıfır bölen olmadığını gösterirsek bir önceki önermemize göre bir asal kalan sınıfı olur.

Bir $\bar{0} \neq \bar{b} \in \mathbb{Z}_m$ için, $\bar{a} \odot \bar{b} = \bar{0}$ olduğunu kabul edelim. Bu eşitliğin her iki yanını $\bar{a}$ nın tersi $\bar{c}$ ile çarparsak; $\bar{c} \odot (\bar{a}\bar{b}) = (\bar{c}\bar{a})\bar{b} = \bar{1}\bar{b} = \bar{b} = \bar{0}$ çelişkisi elde edilir.

O halde $\bar{a}$ bir sıfır bölen değildir. Dolayısıyla $\bar{a}$ bir asal kalan sınıfı olur.

($\Leftarrow$) $\bar{a}$ bir asal kalan sınıfı olsun**.** Bu takdirde $(a, m) = 1$ ve $xa + yb = 1$ olacak şekilde $\exists\, x, y \in \mathbb{Z}$ bulunabilir. Buradan, $xa \equiv 1\ (mod\ m)$ veya $\bar{x} \odot \bar{a} = \bar{1}$ elde edilir. O halde $\bar{a}$ nin tersi mevcuttur.

SONUÇ: m asal tam sayı ise $\mathbb{Z}_m$ deki sıfırdan farklı her kalan sınıfının tersi mevcuttur. Yani

m asal tamsayı ise $\mathbb{Z}_m$ bir cisimdir.

ALIŞTIRMALAR

1. $\mathbb{Z}_{11}$ de $\bar{3}\bar{x} + \bar{2} = \bar{6}$ denklemini çözünüz.

ÇÖZÜM: $\bar{3}\bar{x} + \bar{2} = \bar{6} \Rightarrow \bar{3}\bar{x} = \bar{4}$ ve $\mathbb{Z}_{11}$ de $\bar{3}$ sınıfı asal kalan sınıfı ve tersi $\bar{4}$ olup denklemin her iki tarafını $\bar{4}$ ile çarparsak denklemin çözümü $\bar{x} = \bar{4}.\bar{4} = \bar{5}$ olarak bulunur.

2. $a \equiv b\ (mod\ 2n)$ ise $a^2 \equiv b^2 (mod\ 4n)$ olduğunu gösteriniz.

ÇÖZÜM: $a \equiv b\ (mod\ 2n) \Rightarrow 2n \mid a - b \Rightarrow a - b = 2nk\ , k \in \mathbb{Z} \Rightarrow b = a - 2nk$

$$b^2 = (a - 2nk)^2 = a^2 - 4nka + 4n^2a^2$$

$\Rightarrow\ a^2 - b^2 = 4n(ka - na^2)\ \ ,\ ka - na^2 \in \mathbb{Z}$

$\Rightarrow 4n \mid a^2 - b^2$

$\Rightarrow a^2 \equiv b^2\ (mod\ 4n)$

3. $\mathbb{Z}_5$ de $(a + b)^5$ denklemini çözünüz.

ÇÖZÜM: $(a + b)^5 = \binom{5}{0}a^5 + \binom{5}{1}a^4b + \binom{5}{2}a^3b^2 + \binom{5}{3}a^2b^3 + \binom{5}{4}ab^4 + \binom{5}{5}b^5$

$$= a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5$$

olduğundan $\mathbb{Z}_5$ de denklemin çözümü $a^5 + b^5$ dir.

4. $an \equiv bn\ (mod\ m) \Leftrightarrow a \equiv b\ (mod\ \frac{m}{(m,n)})$ olduğunu gösteriniz.

ÇÖZÜM: $(\Rightarrow)\ (m, n) = d$ olsun.

$\Rightarrow d \mid m$ ve $d \mid n$

$\Rightarrow m = dm'\ ve\ n = dn'\ \ ,\ \ m', n' \in \mathbb{Z}$ vardır. Bu takdirde $(m', n') = 1$ olur.

$an \equiv bn\ (mod\ m) \Rightarrow m \mid n(a - b) \Rightarrow\ m' \mid (n'(a - b)) \Rightarrow m' \mid a - b \Rightarrow a \equiv b\ (mod\ m')$

$(\Leftarrow)\ a \equiv b\ (mod\ m') \Rightarrow m' \mid a - b\ \Rightarrow m' \mid n'(a - b)$ olacağından d ile çarparsak,

$m \mid n(a - b) \Rightarrow an \equiv bn\ (mod\ m)$ elde edilir.

KAYNAKÇA

1. Çallıalp, Fethi.: Çözümlü Soyut Cebir Problemleri, İstanbul Teknik Üniv. Fen-Ed. Fak. Yay. 1995.
2. Çallıalp, Fethi.: Örneklerle Soyut Matematik, 1997
3. Hungerferd, T. W.: Absract Algebra, Cleveland State univ. 1997