Bölüm 2

Modüler Aritmetik

Bu bölümde tamsayılar kümesi üzerinde tanımlı önemli bir denklik bağıntısı ele alınacak ve bu bağıntı sonucunda ortaya çıkan denklik sınıflarının kümesi incelenecektir.

2.1 Tamsayı Kongrüansları

Tanım 2.1.1 *$n \in \mathbb{Z}^+$ olsun. $\mathbb{Z}$ üzerinde*

$$\text{“}x \equiv y \pmod{n} \text{ gerek ve yeter şart } n \mid x - y \text{ olmasıdır”}$$

şeklinde tanımlanan bağıntıya $\equiv \pmod{n}$ **bağıntısı** *denir.*

Teorem 2.1.2 *$\equiv (mod\ n)$ bağıntısı $\mathbb{Z}$ üzerinde bir denklik bağıntısıdır.*

Teorem 2.1.3 *$a \equiv b \pmod{n}$ ve $x \in \mathbb{Z}$ ise*

(i) $a + x \equiv b + x \pmod{n}$

(ii) $ax \equiv bx \pmod{n}$

dir.

Teorem 2.1.4 *$a \equiv b \pmod{n}$ ve $c \equiv d \pmod{n}$ ise*

(i) $a + c \equiv b + d \pmod{n}$

(ii) $a \cdot c \equiv b \cdot d \pmod{n}$

dir.

Tanım 2.1.5 *$\mathbb{Z}$ üzerinde tanımlı bir denklik bağıntısı $\approx$ olsun. $a,\ b,\ c,\ d \in \mathbb{Z}$ için $a \approx b$ ve $c \approx d$ iken $(a + c) \approx (b + d)$ ve $(a \cdot c) \approx (b \cdot d)$ ise $\approx$ bağıntısına $\mathbb{Z}$ üzerinde bir* **kongrüans bağıntısı** *adı verilir.*

Teorem 2.1.6 $\equiv \pmod n$ *bağıntısı* $\mathbb{Z}$ *üzerinde bir kongrüans bağıntısıdır.*

Uyarı 2.1.7 "Eğer $ax \equiv ay \pmod n$ ise o zaman $x \equiv y \pmod n$" önermesi doğru değildir. Örneğin $3 \cdot 4 \equiv 3 \cdot 0 \pmod 6$ olmasına rağmen $4 \not\equiv 0 \pmod 6$ dır. ♦

Teorem 2.1.8 (Sadeleşme Kuralı) $ax \equiv ay \pmod n$ *ve* $ebob(a,n) = 1$ *ise o zaman* $x \equiv y \pmod n$ *dir.*

Şimdi $ax \equiv b \pmod n$ kongrüansının $\mathbb{Z}$ içerisinde çözümlerinin hangi şartlar altında var olduğunu belirleyelim.

Teorem 2.1.9 *Eğer* $ebob(a,n) = d$ *ise* $ax \equiv b \pmod n$ *kongrüansının* $\mathbb{Z}$ *içerisinde bir* x *çözümünün olması için gerek ve yeter şart* $d \mid b$ *olmasıdır. Ayrıca bu kongrüansın bir çözümü varsa* $\mathbb{Z}$ *içinde birbirine denk olmayan* d *tane çözüm vardır.*

Örnek 2.1.10 $20x \equiv 14 \pmod{63}$ kongrüansını göz önüne alalım. $\text{ebob}(20, 63) = 1$ olduğundan verilen kongrüansın $\mathbb{Z}$ içerisinde bir çözümü vardır. Euclid algoritması yardımıyla $1 = 20 \cdot (-22) + 63 \cdot 7$ elde edilir. Bu durumda $14 \equiv (20)(-308) \pmod{63}$ olduğundan aranılan çözüm $x \equiv -308 \equiv 7 \pmod{63}$ dir. ▲

2.2 Kongrüans Sınıfları

Bu kısımda $\equiv \pmod n$ denklik bağıntısı sonucunda ortaya çıkan denklik sınıflarının oluşturduğu küme incelenecektir. Bu küme üzerinde toplama ve çarpma işlemleri tanımlanıp özellikleri araştırılacaktır.

Herhangi bir $x \in \mathbb{Z}$ nin $\equiv \pmod n$ bağıntısına göre denklik sınıfı

$$\begin{aligned} \overline{x} &= \{y \in \mathbb{Z} : \ y \equiv x \pmod n\} \\ &= \{y \in \mathbb{Z} : \ y - x = nk \ , \ k \in \mathbb{Z}\} \\ &= \{y \in \mathbb{Z} : \ y = x + nk \ , \ k \in \mathbb{Z}\} \\ &= \{x + nk : \ k \in \mathbb{Z}\} \end{aligned}$$

dir. Bu sebeple $\equiv \pmod n$ bağıntısına göre bütün denklik sınıfları

$$\begin{aligned} \overline{0} &= \{nk : \ k \in \mathbb{Z}\} \\ \overline{1} &= \{nk + 1 : \ k \in \mathbb{Z}\} \\ &\vdots \\ \overline{n-1} &= \{nk + (n-1) : \ k \in \mathbb{Z}\} \end{aligned}$$

dir.

Tanım 2.2.1 $\equiv \pmod n$ *bağıntısına göre denklik sınıflarına* **kongrüans sınıfları** *adı verilir ve bu sınıfların kümesi* $\mathbb{Z}_n$ *ile gösterilir. Bu durumda* $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}$ *dir.*

Şimdi $\mathbb{Z}_n$ kümesi üzerinde toplama ve çarpma işlemlerini tanımlayalım ve özelliklerini verelim.

Teorem 2.2.2 *$n \in \mathbb{Z}^+$ olsun. $\overline{a},\ \overline{b} \in \mathbb{Z}_n$ için*

$$\overline{a} + \overline{b} = \overline{a+b}$$

ile tanımlı $+$ aşağıdaki özelliklere sahiptir.

(i) *$+$ işlemi $\mathbb{Z}_n$ üzerinde birleşme özelliğine sahiptir.*

(ii) *$+$ işlemi $\mathbb{Z}_n$ üzerinde değişme özelliğine sahiptir.*

(iii) *$\mathbb{Z}_n$ kümesinde $+$ işlemine göre birim eleman vardır.*

(iv) *$\mathbb{Z}_n$ kümesinde her elemanın $+$ işlemine göre tersi vardır.*

Teorem 2.2.3 *$n \in \mathbb{Z}^+$ olsun. $\overline{a},\ \overline{b} \in \mathbb{Z}_n$ için*

$$\overline{a} \cdot \overline{b} = \overline{a.b}$$

ile tanımlı $\cdot$ aşağıdaki özelliklere sahiptir.

(1) *$\cdot$ işlemi $\mathbb{Z}_n$ üzerinde birleşme özelliğine sahiptir.*

(2) *$\cdot$ işlemi $\mathbb{Z}_n$ üzerinde değişme özelliğine sahiptir.*

(3) *$\mathbb{Z}_n$ kümesinde $\cdot$ işlemine göre birim eleman vardır.*

(4) *$\mathbb{Z}_n$ kümesinde $\cdot$ işleminin $+$ işlemi üzerine dağılma özelliği vardır.*

Örnek 2.2.4 $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ kümesinin $+$ ve $\cdot$ işlemlerine göre tabloları

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Tablo 2.1: $\mathbb{Z}_4$ ün $+$ ve $\cdot$ İşlem Tabloları

şeklindedir. Tablo 2.1 den görüleceği gibi $\mathbb{Z}_4$ te $\overline{0}$ ve $\overline{2}$ nin çarpımsal tersi yoktur. ▲

$\mathbb{Z}_n$ de çarpımsal tersi mevcut olan ve olmayan elemanlar aşağıdaki teoremle belirlenebilir.

Teorem 2.2.5 *$\overline{0} \neq \overline{a} \in \mathbb{Z}_n$ nin çarpımsal tersinin var olması için gerek ve yeter şart $ebob(a, n) = 1$ olmasıdır.*

Örnek 2.2.6 Teorem 2.2.5 gereğince $\mathbb{Z}_{15}$ içerisinde çarpımsal tersi mevcut olan elemanlar

$$\overline{1}, \overline{2}, \overline{4}, \overline{7}, \overline{8}, \overline{11}, \overline{13}, \overline{14}$$

ve $\mathbb{Z}_{15}$ içerisinde sıfırdan farklı çarpımsal tersi mevcut olmayan elemanlar

$$\overline{3}, \overline{5}, \overline{6}, \overline{9}, \overline{10}, \overline{12}$$

dir. ▲

Örnek 2.2.7 $\text{ebob}(13, 191) = 1$ olduğundan Teorem 2.2.5 gereğince $\mathbb{Z}_{191}$ içerisinde $\overline{13}$ nin çarpımsal tersi vardır. Tersini bulmak için $13x \equiv 1 \pmod{191}$ kongrüansın bir çözümünü bulalım. Euclid Algoritması yardımıyla $13(-44) \equiv 1 \pmod{191}$ olduğu görülebilir. Dolayısıyla

$$x = \overline{13}^{-1} = \overline{-44} = \overline{147}$$

dir. ▲