Bölüm 11

İŞLEM

11.1 İŞLEM KAVRAMI

Sayı kümeleri üzerinde *dört işlem* adıyla anılan *toplama, çıkarma, çarpma* ve *bölme* işlemlerini yapmayı biliyorsunuz. Ayrıca, bu işlemlerin *yer değişme, birleşme, dağılma* özelikleri ile *birim öğe, ters öğe varlığı* kavramlarını, kullanarak işlemler (operatör) yapıyor ve problemler çözüyorsunuz.

Bu bölümde, bu tür işlemleri, soyut bir matematiksel yapı içinde inceleyeceğiz. Bu inceleme sonunda ulaşacağımız genel kurallar, istediğimiz somut duruma kolayca uygulanabilecektir.

11.1.1 Birli İşlemler

Tanım *Bir kümeden kendisine tanımlı olan her fonksiyon, bir* birli işlem'*dir.*

Örnekler

1. $\mathbb{Z}$ Tam Sayılar Kümesi olmak üzere, $\mathbb{Z}$ den $\mathbb{Z}$ ye tanımlı $f(x) = -x$ fonksiyonu birli bir işlemdir.
2. Sıfırdan farklı Rasyonel Sayılar Kümesinden kendisine tanımlı $f(x) = \frac{1}{x}$ fonksiyonu birli bir işlemdir.

11.1.2 İkili İşlemler

Tanım: *$A \neq \emptyset$ ve $A \subset B$ ise, her*

$$f : A \times A \to B$$

fonksiyonu, A üzerinde bir ikili işlem'*dir.*

Birli ve ikili işlemler apaçık belli olacağı için, birli işlem, ikili işlem terimleri yerine, kısaca, *işlem* diyeceğiz. Bu kısaltma bir karışıklık yaratmayacaktır.

İşlemler, fonksiyonların özel bir türüdür. Bir fonksiyonun işlem olduğunu belirtmek için, onları, fonksiyonlar için kullandığımız $f, g, h, \ldots$ gibi harflerle değil; özel simgelerle belirtiyoruz. Bu simgeler, sayı kümelerinde kullandığımız $+$, $-$, $\times$, $\cdot$, $\div$ simgeleri olabileceği gibi, $\star$. $\circ$, $\oplus$, $\ominus$, $\otimes$, $\odot$, $\Box, \cdots$ gibi simgeler olacaktır.

Üzerinde bir ya da daha çok işlem tanımlı bir A kümesi, bir *matematiksel yapı*'dır. Bu yapıyı, $(A, \oplus, \otimes), \cdots)$ biçiminde göstereceğiz.

A üzerinde bir $\star$ işleminin tanımlı olması demek, $\oplus : A \times A \to B$ fonksiyonunun verilmiş olması demektir. Öyleyse, $\star$ işlemi, her $(x, y) \in A \times A$ sıralı çiftini bir tek $z \in B$ ögesine eşleyecektir. Çoğunlukla, z görüntüsünü $x \star y$ simgesiyle göstereceğiz:

$$\star : (x, y) \to x * y = z$$

Bunu *"x işlem y eşit z"* diye okuyacağız..

Örnek

$\mathbb{N}$ Doğal Sayılar kümesi üzerindeki çarpma işlemini $\cdot$ ile gösterelim.

$$\cdot \; : \; \mathbb{N} \times \mathbb{N} \to \mathbb{N}, \quad \cdot \; : \; (m, n) \to m.n$$

dir.

11.1.3 n-li İşlemler

Tanım:

$A \neq \emptyset$ ve $n \in \mathbb{N}$ olmak üzere A nın n kez kendisiyle kartezyen çarpımından A ya tanımlı her fonksiyon bir n-li işlemdir. Bunu simgelerle gösterirsek, her

$$f : A \times A \times \ldots \times A \to A$$

fonksiyonuna, A kümesi üzerinde bir *n-li işlemlem* denilir.

11.2 İŞLEMLERİN ÖZELİKLERİ

Kapalılık

$\star$ fonksiyonunun görüntü kümesi bazan A kümesine eşit olur; bazan da A dan büyük olur. Bu iki durumu birbirinden ayırmak gerekir.

Tanım: $*$, A kümesi üzerinde bir işlem olsun. Eğer $\star$ fonksiyonunun görüntü kümesi, A ise; yani,

$$* : \; A \times A \to A$$

bir fonksiyon ise, "A kümesi $*$ işlemine göre *kapalıdır*" denilir.

Bu durumda,

$$\forall x, y \in A \quad \text{için} \quad x * y = z \in A$$

olur.

Eğer, $\star$ fonksiyonunun görüntü kümesi, A kümesininden büyükse, "A kümesi $*$ işlemine göre *kapalı değildir,*" denilir.

Uyarı 11.2.1. Aslında *işlemin kapalı olması* tanımı, fonksiyon (işlem) tanımımız uyarınca, gereksizdir. Çünkü işlem tanımlı ise, zaten kapalılık özeliği sağlanacaktır. Bu kavram, fonksiyon tanımının iyi yapılmadığı eski zamanlardan kalan bir alışkanlık olarak sürmektedir. Bir çok kaynakta karşılaşıldığı için, bu tanım bilgi amacıyla buraya alınmıştır. Bizim işlem tanımımız kapalılık kavramını kapsamaktadır.

Örnekler

1. Doğal Sayılar Kümesi çarpma işlemine kapalıdır.

   Gerçekten, iki doğal sayının çarpımı gene bir doğal sayıdır. Bunu, simgelerle ifade etmek için, $\mathbb{N}$ Doğal Sayılar Kümesi üzerindeki çarpma işlemini " $\cdot$ " ile gösterelim.

   $$\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, \quad \cdot : (m, n) \to m.n \in \mathbb{N}$$

   olduğundan, $\cdot$ çarpma işlemi Doğal Sayılar Kümesi üzerinde tanımlıdır; yani, $\mathbb{N}$ kümesi çarpma işlemine kapalıdır.

2. Doğal Sayılar Kümesi çıkarma işlemine kapalı değildir.

   Böyle olduğunu örneklerle gösterebiliriz:

   $$7 - 2 = 5 \in \mathbb{N} \quad \text{dir; ama} \quad 2 - 7 = -5 \notin \mathbb{N}$$

   olduğundan, çıkarma işleminin görüntü kümesi, Doğal Sayılar Kümesinden büyüktür. Başka bir deyişle, $- : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ tanımlı değildir; dolayısıyla, Doğal Sayılar Kümesi çıkarma işlemine kapalı değildir. Öte yandan,

   $$- : \mathbb{N} \times \mathbb{N} \to \mathbb{Z}$$

   tanımlıdır.

   Bu tür özelikler, matematiksel yapıların genişletilmesi gerekçesini doğurur.

Yer Değişim

Tanım: Boş olmayan bir A kümesi üzerinde tanımlı $\star$ işlemi verilsin. Her $x, y \in A$ için,

$$x \star y = y \star x$$

oluyorsa, $\star$ işleminin *yer değişim* (takas - komutatiflik) özeliği vardır, denilir.

Örnekler

1. $5.7 = 7.5$ örneğinde olduğu gibi, her m, n doğal sayı çifti için $m.n = n.m$ dir. O halde, Doğal Sayılar Kümesi üzerinde çarpma işlemi yer değişimi özeliğine sahiptir.

2. $9-5 \neq 5-9$ örneğinde olduğu gibi, her m, n dodoğal sayı çifti için $m-n \neq n-m$ dir. O halde, Doğal Sayılar Kümesi üzerinde çıkarma işlemi yer değişimi özeliğine sahip değildir.

Daha genel söylemek gerekirse;

a. Sayı kümeleri üzerinde tanımlı toplama $(+)$ ve çarpma $(.)$ işlemlerinin değişme özeliği vardır.

b. Çıkarma $(-)$ ve bölme $(\div)$ işlemlerinin değişme özeliği yoktur.

Birleşme Özeliği

Birleşme Özeliği

Boş olmayan bir A kümesinde tanımlı bir $\star$ işlemi verilsin. Her $x, y, z \in A$ için,

$$x \star (y \star z) = (x \star y) \star z$$

oluyorsa $\star$ işleminin *birleşme özeliği* vardır, denilir.

Örnekler

1. $2.(3.4) = (2.3).4$ örneğinde olduğu gibi, her m, n, r doğal sayıları için $m.(n.r) = (m.n).r$ dir. O halde, Doğal Sayılar Kümesi üzerinde çarpma işlemi birleşme özeliğine sahiptir.

2. $40 : (20 : 2) = 4 \neq 2 = (40 : 20) : 2$ örneğinde olduğu gibi, her p, q, r rasyonel sayılar için $m : (n : r) \neq (n : m) : r$ dir. O halde, Rasyonel Sayılar Kümesi üzerinde bölme işlemi birleşme özeliğine sahip değildir.

Genel olarak, sayı kümeleri üzerinde toplama ve çarpma işlemleri birleşme özeliğine sahiptir; ama çıkarma ve bölme işlemlerinin birleşme özeliği yoktur.

11.3 Birim Öğe

$\star$ işlemi bir A kümesi üzerinde tanımlı olsun. Her $x \in A$ için,

$$x \star e = x = e \star x$$

eşitliğini sağlayan bir $e \in A$ varsa, e öğesine, $\star$ işlemine göre *birim (etkisiz) öğe,* denilir.

Örnekler

1. $8 + 0 = 8 = 0 + 8$ örneğinde olduğu gibi, her k tam sayısı için $k + 0 = k = 0 + k$ dir. O halde, 0 sayısı, Tam Sayılar Kümesinde üzerinde tanımlı toplama işlemine göre birim öğedir.

2. $A = \{2, 3, 4, \ldots\}$ kümesi üzerinde $\cdot$ çarpma işlemi tanımlıdır; yani,

$$\cdot : A \times A \to A, \qquad \cdot : (m, n) \to m.n$$

bir ikili işlemdir. kapalılık, yer değişimi ve birleşme özelikleri sağlanır. Ama, bir sayının 1 den başka bir sayı ile çarpımı kendisine eşit olamaz. $1 \notin A$ olduğundan, çarpma işlemine göre birim öğe A içinde yoktur.

Q rasyonel sayılar kümesi üzerinde "$*$" işlemi

$$a * b = a + b + ab$$

biçiminde tanımlansın. Bu işlemin, varsa, birim elemanını bulalım.

Tanım gereğince $\forall a \in Q$ için $a * e = e * a = a$ olacak biçiminde bir $e \in Q$ arayacağız.

$$\begin{aligned} a * e = a &\Rightarrow a + e + a.e = a \\ &\Rightarrow e + a.e = 0 \\ &\Rightarrow (1 + a).e = 0 \\ &\Rightarrow (e = 0) \vee (1 + a = 0) \\ &\Rightarrow e = 0 \in Q \end{aligned}$$

olur. $\forall a \in Q$ için,

$$a * 0 = a + 0 + a.0 = a$$

olduğundan *sağdan birim eleman* $e = 0$ dır.

$$\begin{aligned} e * a = a &\Rightarrow e + a + e.a = a \\ &\Rightarrow e + e.a = 0 \\ &\Rightarrow e(1 + a) = 0 \\ &\Rightarrow (e = 0) \vee (1 + a = 0) \\ &\Rightarrow e = 0 \in Q \end{aligned}$$

olur. $\forall a \in Q$ için,

$$0 * a = 0 + a + 0.a = a$$

olduğundan "$*$" işleminin *soldan birim elemanı* $e = 0$ dır.

Q da tanımlı "$*$" işleminin hem sağdan, hem soldan birim elemanı 0 (sıfır) olduğundan, işlemin birim elemanı vardır ve $e = 0 \in Q$ dır.

Birim eleman çoğunlukla e ile gösterilir.

11.4 Ters Öğe

Bir Öğenin Tersi

Tanım: A kümesinde tanımlı bir $\star$ işlemi verilsin ve buna göre birim e birim öğesi var olsun. Her $x \in A$ için,

$$x \star y = e = y \star x$$

eşitliğini sağlayan bir $y \in A$ varsa, y öğesi, $\star$ işlemine göre, x öğesinin *tersi*dir.

Sayı kümeleri üzerinde, toplama işlemine göre, bir x öğesinin tersi $-x$; çarpma işlemine göre $x^{-1} = \frac{1}{x},\ x \neq 0$ dir. Örneğin, 12 nin toplamsal tersi -12; çarpımsal tersi $\frac{1}{12}$ dir. Aynı biçimde, $-(-\frac{5}{3})$ ün toplamsal tersi $-(-\frac{5}{3}) = \frac{5}{3}$; çarpımsal tersi $(-\frac{5}{3})^{-1} = -\frac{3}{5}$ dir.

Sayı kümelerinden edindiğimiz alışkanlıkla, soyut kümeler üzerinde tanımlı olup $+$ işlemine benzeyenlere *toplama işlemi*; $\cdot$ işlemine benzeyenlere de *çarpma işlemi*, diyeceğiz. Dolayısıyla, bir x öğesinin toplamsal tersi $-x$; çarpımsal tersi x^{-1} simgesiyle gösterilecektir.

Dağılma Özeliği

Boş olmayan bir A kümesi üzerinde $\oplus$ ve $\otimes$ işlemleri tanımlı olsun. $\forall a, b, c \in A$ için,

$$a \otimes (b \oplus c) = (a \otimes b) \ \oplus \ (a \otimes c)$$

eşitliği sağlanıyorsa, $\otimes$ işleminin $\oplus$ işlemi üzerine *soldan dağılma* özeliği vardır;

$$(a \oplus b) \otimes c = (a \otimes c) \ \oplus \ (b \otimes c)$$

eşitliği varsa $\otimes$ işleminin $\oplus$ işlemi üzerine *sağdan dağılma* özeliği vardır, denilir.

Hem soldan, hem sağdan dağılma özeliği varsa, $\otimes$ işleminin $\oplus$ işlemi üzerine *dağılma özeliği* vardır.

Sayı kümeleri üzerinde çarpmanın, toplama üzerine dağılma özeliği vardır; ama, toplamanın çarpma işlemi üzerine dağılma özeliği yoktur.

Tanım: A kümesi üzerinde tanımlı bir $\star$ işlemi olsun. Eğer $\forall x \in A$ için,

$$\forall x \in A \quad \text{için} x * u = u * x = u$$

olacak biçimde bir $u \in A$ varsa, u ya $\star$ işleminin *yutak (yutan) öğesi* denilir.

Örnek

Sayı kümeleri üzerinde çarpma işleminin yutak öğesi 0 sayısıdır; çünkü, her x sayısı için,

$$x.0 = 0.x = 0$$

dır.

11.4.1 Çözümlü Örnekler

Örnekler

1. $\mathbb{Q}$ Rasyonel Sayılar Kümesi üzerinde $\oplus$ işlemini aşağıdaki eşitlik ile tanımlayalım: $a+b$ ve $\frac{a}{b}$ işlemleri, $\mathbb{Q}$ üzerindeki toplama ve bölme işlemleri olmak üzere, $\forall x, y \in \mathbb{Q}$ için,

$$x \oplus y = \frac{x + y}{2} \tag{2}$$

diyelim.

Şimdi bu işlemin niteliklerini araştıralım.

(a) $\mathbb{Q}$ kümesi $\oplus$ işlemine göre kapalıdır; çünkü $\forall x, y \in \mathbb{Q}$ için, (2) eşitliğinin sağ yanı daima bir rasyonel sayıdır.

(b) $\oplus$ işleminin yer değişim özeliği vardır; çünkü,

$$x \oplus y = \frac{x+y}{2} = \frac{y+x}{2} = y \oplus x\,.$$

(c) $\oplus$ işleminin birleşme özeliği yoktur; örneğin,

$$2 \oplus (4 \oplus 8) = 2 \oplus 6 = 4 \neq \frac{11}{2} = 3 \oplus 8 = (2 \oplus 4) \oplus 8$$

dir.

(d) 0 sayısı, $\oplus$ işlemine göre, $\mathbb{Q}$ içinde birim öğedir; çünkü,

$$\forall x \left(\frac{x+0}{2} = \frac{x}{2} = \frac{0+x}{2} \right)$$

dir.

(e) Her x rasyonel sayısının, $\oplus$ işlemine göre, $\mathbb{Q}$ içindeki tersi $-x$ sayısıdır; çünkü,

$$x \oplus (-x) = \frac{x-x}{2} = 0$$

dır.

(f) $(\mathbb{Q}, \oplus)$ sistemi yer değişimli bir gruptur.

2. $\mathbb{Q}$ Rasyonel Sayılar Kümesi üzerinde $\otimes$ işlemini aşağıdaki eşitlik ile tanımlayalım: $a+b$ ve $a.b$ işlemleri, $\mathbb{Q}$ üzerindeki toplama ve çarpma işlemleri olmak üzere, $\forall x, y \in \mathbb{Q}$ için,

$$x \otimes y = x + y + x.y \tag{3}$$

diyelim.

Şimdi bu işlemin niteliklerini araştıralım.

(a) $\mathbb{Q}$ kümesi $\otimes$ işlemine göre kapalıdır; çünkü $\forall x, y \in \mathbb{Q}$ için, (3) eşitliğinin sağ yanı daima bir rasyonel sayıdır.

(b) $\otimes$ işleminin yer değişim özeliği vardır; çünkü,

$$x \otimes y = x + y + x.y = y + x + y.x = y \otimes x$$

(c) $\oplus$ işleminin birleşme özeliği vardır; çünkü,

$$\begin{aligned} x \otimes (y \otimes z) &= x \otimes (y + z + y.z) \\ &= x + (y + z + y.z) + x.(y + z + y.z) \\ &= x + y + z + y.z + x.y + x.z + x.(y.z) \\ &= x + y + x.y + z + x.z + y.z + (x.y)z \\ &= (x + y + x.y) + z + (x + y + x.y).z \\ &= (x \times y) \otimes z \end{aligned}$$

dir.

(d) $\otimes$ işlemine göre, $\mathbb{Q}$ içindeki birim öğe 0 dır; çünkü,

$$\forall x \text{için}, (x \otimes 0) = (x + 0 + x.0) \;=\; x \;=\; (0 + x + 0.x) = (0 \otimes x)$$

dir.

(e) Bir $x \neq -1$ sayısının, $\otimes$ işlemine göre, $\mathbb{Q}$ içindeki ters öğesi $\frac{-x}{1+x}$ dir; çünkü,

$$x \otimes \left(\frac{-x}{1+x}\right) = x + \frac{-x}{1+x} + x \cdot \frac{-x}{1+x} = 0$$

dır.

(f) $((\mathbb{Q} \setminus \{1\}), \otimes)$ sistemi yer değişimli bir gruptur.

3. $\mathbb{Q}$ üzerinde tanımlı olan $\otimes$ işleminin, $\oplus$ işlemi üzerine dağılma özeliği vardır:

$$\begin{aligned} x \otimes (y \oplus z) &= x \otimes \left(\frac{y+z}{2}\right) \\ &= x + \frac{y+z}{2} + x \cdot \frac{y+z}{2} \\ &= \frac{x}{2} + \frac{x}{2} + \frac{y+z}{2} + \frac{x.y}{2} + \frac{y+z}{2} + x \cdot \frac{x.z}{2} \\ &= \left(\frac{x}{2} + \frac{y}{2} + \frac{x.y}{2}\right) + \left(\frac{x}{2} + \frac{z}{2} + \frac{x.z}{2}\right) \\ &= \frac{(x + y + x.y) + (x + z + x.z)}{2} \\ &= \frac{(x \otimes y) + (x \otimes z)}{2} \\ &= (x \otimes y) + (x \otimes z) \end{aligned}$$

4. $(\mathbb{Q}, \oplus, \otimes)$ sistemi yer değişimli ve birimli bir halkadır.

Önceki örneklerde gösterilen nitelikler, bu önermenin ispatıdır.

5. $\mathbb{Q}$ üzerinde tanımlı olan $\otimes$ işlemine göre, iki sayının tersleri aşağıda gösterilmiştir.

$$\begin{aligned} 7^{-1} &= \frac{-7}{1+7} \\ &= -\frac{7}{8} \\ (-\frac{5}{4})^{-1} &= \frac{-(-\frac{5}{4})}{1+(-\frac{5}{4})} \\ &= \frac{5}{9} \end{aligned}$$

6. $\mathbb{Q}$ üzerinde tanımlı olan $\otimes$ işlemine göre, -1 sayısının ters öğesinin olmadığını gösteriniz.

$x^{-1} = \frac{-(-1)}{1-1}$ ifadesinin sağ yanı tanımsızdır; çünkü, sayı kümelerinde 0 ile bölme işlemi tanımsızdır. Öyleyse, $\otimes$ işlemine göre -1 in tersi yoktur.

7. Öğe sayısı az olan kümeler üzerinde ikili bir işlem tanımlamak ya da tanımlanmış bir işlemi göstermek için, aşağıdaki gibi *işlem tablosu* düzenlenebilir.

$\star$	a	b	c	d	e	f	
a	a	a	a	a	a	a	
b	a	b	a	b	b	b	
c	a	a	c	a	c	c	
d	a	b	a	d	b	d	
e	a	b	c	b	e	e	
f	a	b	c	d	e	f	
							köşegen

Bu tabloda, ikili işlemin ilk öğesi satırların solundan, ikinci öğesi sütunlardan seçilir. İşlem sonucu, seçilen satır ve sütunun kesiştiği yerdeki öğedir. Örneğin, yukarıdaki tabloda tanımlı işlem için,

$$\begin{aligned} (a,a) &\rightarrow a \star a = a \\ (a,b) &\rightarrow a \star b = a \\ (c,f) &\rightarrow c \star f = c \\ (d,e) &\rightarrow d \star e = b \\ (e,d) &\rightarrow e \star d = b \end{aligned}$$

dir. Diğer sonuçlar da benzer biçimde listelenebilir.

$A = \{a,b,c,d,e,f\}$ için,

1. A kümesinin, $\star$ işlemine göre kapalı olduğu,

2. $\star$ işleminin yer değişim özeliğine sahip olduğu,
3. $\star$ işleminin birleşme özeliğine sahip olduğu,

tablodan kolayca çıkarılabilir.

8. $A = \{1, 2, 3, 4, 5\}$ kümesi üzerinde $\odot$ işlemi,

$$a, b \in A \quad \Rightarrow \quad a \odot b = 3a - 2b$$

biçiminde tanımlanıyor. İşlem tablosunu yapınız ve $\odot$ işleminin özeliklerini inceleyiniz.

$\odot$	1	2	3	4	5	
1	1	-1	-3	-4	-7	
2	4	2	0	-2	-4	
3	7	5	3	1	-1	
4	10	8	6	4	2	
5	13	11	9	7	5	
						köşegen

yukarıdaki tabloda tanımlı işlem için,

$$\begin{aligned}
(1,1) &\rightarrow 1 \odot 1 = 1 \\
(1,2) &\rightarrow 1 \odot 2 = -1 \\
(3,2) &\rightarrow 3 \odot 2 = 5 \\
(4,3) &\rightarrow 4 \odot 3 = 6 \\
(5,5) &\rightarrow 5 \odot 5 = 5
\end{aligned}$$

dir. Diğer sonuçlar da benzer biçimde listelenebilir. Tablodan, $\odot$ işleminin şu özeliklerini görebiliriz.

(a) A kümesi, $\odot$ işlemine kapalı değildir; çünkü, görüntü kümesi

$$B = \{-7, -5, -4, -3, -1, 0, 1, 2, 3, 4, 5, 7, 8, 9, 11, 13\}$$

kümesidir. Bu küme A nın bir has üst kümesidir. Dolayısıyla,

$$\odot : A \times A \rightarrow A$$

işlemi tanımsızdır; bunun yerine

$$\odot : A \times A \rightarrow B$$

işlemi tanımlıdır.

(b) $\odot$ işleminin yer değişim özeliği yoktur; örneğin,

$$3 \odot 2 = 5 \neq 0 = (2, 3)$$

dür.

(c) $\odot$ işleminin birleşim özeliği yoktur; örneğin,

$$3 \odot (4 \odot 5) = 3 \odot 2 = 5$$

olduğu halde,

$$(3 \odot 4) \odot 5 = 1 \odot 5 = -7$$

dir.

(d) A kümesinde, $\odot$ işlemine göre birim öğe yoktur; çünkü,

$$\forall x \in A \quad \Rightarrow \quad x \odot e = x = e \odot x$$

eşitliğini sağlayan bir $e \in A$ öğesi yoktur.

(e) Birim öğe olmadığına göre, A içindeki hiç bir öğenin tersi olamaz.

11.5 ALIŞTIRMALAR

1. İlköğretim çağından bu yana, öğrendiğiniz birli ve ikili işlemleri yazınız.

2. $\mathbb{N} = \{0, 1, 2, 3, \cdots\}$ doğal sayılar kümesi üzerinde $x \odot y = 3x + 2y$ eşitliği ile tanımlanan işlemin tablosunu, ilk 5×5 satır $\times$ sütun için düzenleyiniz. İşlemin özeliklerini araştırınız.

3. $A = \{-i, -1, 0, 1, i\}$ kümesi üzerinde,

$$1 * 1 = 1, (-1) * (-1) = 1, 1 * i = i, i * 1 = i, i * i = -1$$

eşlemeleri ile $*$ işlemi tanımlanıyor. $*$ işleminin tablosunu yapınız; özeliklerini inceleyiniz.

4. 1 sayısı, $\mathbb{R}$ gerçek (reel) sayılar kümesi üzerinde tanımlı bölme işleminin birim öğesi midir? Neden?

5. $\mathbb{Z}$ Tamsayılar Kümesi üzerinde,

$$x, y \in \mathbb{Z} \quad \text{için} \quad x \diamond y = 4x + 3y$$

bağıntısıyla tanımlanan işlemin,

   (a) Yer değişim özeliğine sahip midir?

   (b) Birleşme özeliğine sahip midir?

6. $\mathbb{Q}$ Rasyonel Sayılar Kümesi üzerinde,

$$x, y \in \mathbb{Q} \quad \text{için} \quad x \diamond y = x + y - xy$$

bağıntısıyla tanımlanan işlemin,

   (a) Yer değişim özeliğine sahip midir?

(b) Birleşme özeliğine sahip midir?

(c) Bu işleme göre $\mathbb{Q}$ içinde birim öğe var mıdır?

(d) Bu işleme göre tersi var olan öğeler var mıdır?

7. $A = \{0, 1\}$ kümesi üzerinde $+$ ve $\cdot$ işlemleri veriliyor.

(a) Her iki işlemin tablolarını yapınız.

(b) $+$ işlemine göre, A içinde birim öğe var mıdır?

(c) $\cdot$ işlemine göre, A içinde birim öğe var mıdır?

(d) $+$ işlemine göre, A içindeki her öğenin tersi var mıdır?

(e) $+$ işlemine göre, A içindeki her öğenin tersi var mıdır?

(f) $\cdot$ işleminin $+$ işlemi üzerine dağılma özeliği var mıdır?

8. $\forall x \in \mathbb{R}$ için $x - 0 = x$ dir. 0 sayısı,c$\mathbb{R}$ üzerinde çıkarma $(-)$ işleminin birim elemanı olur mu? İnceleyiniz.

9. Bir işleme göre en çok bir tane birim öğe olabileceğini gösteriniz.

10. Bir işleme göre, bir öğenin en çok bir tane ters öğesinin olabileceğini gösteriniz.

11. $\mathbb{N}$ üzerinde tanımlı $m \diamond n = m^n + 1$ işleminin yer değişme ve birleşme özeliklerinin olup olmadığını araştırınız.

12. $\mathbb{Z}$ üzerinde tanımlı $a \circ b = a^b - ab$ işlemi veriliyor. $(2 \circ 3) \circ 4$ işleminin sonucu nedir?

13. A üzerinde tanımlı bir $\star$ işlemine göre, her öğenin tersi varsa, $(x \star y)^{-1} = y^{-1} \star x^{-1}$ olduğunu gösteriniz.

11.6 MODULAR ARİTMETİK

11.6.1 Farklı Bir Aritmetik

Yılın dokuzuncu ayında açılan okul, beş ay sonra yarıyıl tatiline girmektedir. Yaryıl tatili kaçıncı ayda olmaktadır?

Bu soruyu yanıtlarken, $9 + 5 = 14$ demeyiz; 2 deriz. Çünkü, bir yılda 12 ay vardır. 12 nci aydan sonra 1 nci ay gelir.

Sabah saat dokuzda işbaşı yapan bir işçi, günde sekiz saat çalşmaktadır. Bu işçi, işi bırakırken, saati kaçı gösterir?

Bu sorunun yanıtı, $9 + 8 = 17$ değildir; çünkü saatin göstergesinde, 12 den sonra 1 gelmektedir. Dolayısıyla, yanıt 5 dir.

Yılın birinci mevsimi 21 Mart'ta başlar. Beş mevsim sonra, yılın kaçıncı mevsimi başlar?

Bu sorunun da yanıtı $1+5 = 6$ değil; 2 dir. Çünkü, yılın mevsimleri 4 tanedir, 4 üncüden sonra 1 nci mevsim gelir.

Bunlara benzer problemlerin çözümü, tamsayılardaki aritmetikten farklı bir aritmetiği gerektirir. Buna *Modüler Aritmetik* denilir. Bu bölümde, modüler aritmetiği, kısaca ele alacağız.

Tanım 11.6.1. a tamsayısı b tamsayısını kalansız bölüyorsa (tam bölüyorsa), bu durumu göstermek için $a|b$ simgesini kullanırız. Karşıt olarak, a tamsayısı b tamsayısını kalansız bölmüyorsa (tam bölmüyorsa), bu durumu göstermek için $a \nmid b$ simgesini kullanırız.

Teorem 11.6.1. *$a, b, m \in \mathbb{Z}$, $m > 1$ olmak üzere $\mathbb{Z}$ üzerinde*

$$\beta = \{(a, b) : m \mid (a - b)\}$$

bağıntısı bir denklik bağıntısıdır.

İSPAT: Bir denklik bağıntısı olması için, β bağıntısı *yansımalı, simetrik ve geçişken* olmalıdır.
β Yansımalıdır:
$a - a = 0$ ve $m|0$ olduğundan,

$$a \in \mathbb{Z} \quad \Rightarrow \quad m \mid (a - a) \Rightarrow (a, a) \in \beta$$

çıkar.
β Simetriktir:
$a, b \in \mathbb{Z}$ için,

$$m \mid (a - b) \Rightarrow m \mid (b - a)$$

olduğundan, $[(a, b) \in \beta \Rightarrow (b, a) \in \beta]$ çıkar.
β Geçişkendir :
$a, b, c \in \mathbb{Z}$ için,

$$[m \mid (a - b),\ m \mid (b - c)] \Rightarrow m \mid (a - c)$$

olduğunu gösterirsek,

$$[(a, b) \in \beta,\ (b, c) \in \beta] \Rightarrow (a, c) \in \beta$$

çıkacaktır:

$$\begin{aligned} m \mid (a - b) \quad \text{ve} \quad m \mid (b - c) \quad &\Rightarrow \quad \exists p, q \in \mathbb{Z}, a - b = mp \wedge b - c = mq \\ &\Rightarrow \quad (a - b) + (b - c) = mp + mq \quad \text{dır.} \\ &\Rightarrow \quad a - b + b - c = m(p + q) \\ &\Rightarrow \quad a - c = mk \qquad (p + q = k \in \mathbb{Z}) \\ &\Rightarrow \quad m \mid (a - c) \end{aligned}$$

O halde, β bir denklik bağıntısıdır.

β bağıntısı, $\mathbb{Z}$ kümesini denklik sınıflarına böler. Neden? Şimdi, denklik sınıflarını bulalım.

Bir a tamsayısı, 1 den büyük bir bir m tamsayısına bölünürse, Bölme Algoritmasına göre,

$$a = m.r + k$$

eşitliğini sağlayan r ve k tamsayılarının varlığını söyleyebiliriz. Burada, r bölüm, k kalandır ve $0 \leq k < m$ koşulunu sağlar. Buradan,

$$\begin{aligned} a = m.r + k &\Rightarrow a - k = m.r \\ &\Rightarrow m \mid a - k \\ &\Rightarrow (a, k) \in \beta \end{aligned}$$

yazabiliriz. Bu, a nın k ya denk olduğunu; yani, a ile k nın aynı denklik sınıfında olduğunu söyler.

Bir a tamsayısının k ye denk olması demek, aynı kalan sınıfına ait olmaları demektir. Bu durumu,

$$a \equiv k \pmod{m} \tag{11.1}$$

simgesiyle gösterecek ve "*m modülüne göre, a sayısı, k ya denktir*", ya da "*a denk k modulo m*" diye okuyacağız.

Bu gösterimdeki, k sayısı,a nın m ye bölünmesiyle elde edilen kalandır.

$a \equiv k \ (mod\ m)$ bağıntısının yansıyan, simetrik ve geçişken olduğu apaçıktır.

Bir tam sayı, m ile bölünürse, kalan $0, 1, 2, 3, \cdots, m-1$ sayılarından birisidir. Yukarıdaki anlamda, k ya denk olan bütün a tamsayılarının oluşturduğu denklik sınıfı,

$$\overline{k} = \{a \mid a \equiv k \ (mod\ m) \tag{11.2}$$

dir. Oluşabilen bütün denklik sınıfları,

$$\mathbb{Z}/m = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \cdots, \overline{m-1}\} \tag{11.3}$$

dir. Bu denklik sınıflarının kümesine m nin *kalan sınıflarının kümesi* de denilir ve $\mathbb{Z}/m$ simgesiyle gösterilir.

Öyleyse,

$$\mathbb{Z}/m = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \cdots, \overline{m-1}\}$$

olur.

Bir a tamsayısının b ye denk olmasını

$$a \equiv b \ (mod\ m) \tag{11.4}$$

simgesiyle göstereceğiz.

Bir k tamsayısına denk olan bütün tamsayıların oluşturduğu denklik sınıfı,

$$\overline{k} = \{a \mid a \equiv k \ (mod\ m)\} \tag{11.5}$$

dir. Bu denklik sınıflarının ailesine, *m ye göre kalan sınıflar* da denilir ve $\mathbb{Z}/m$ simgesiyle gösterilir. Bir a tamsayısının b ye denk olması demek, bu sayıların, aynı kalan sınıfına ait olmaları demektir:

Birbirlerinden farklı kalan sınıflar (denklik sınıfları),

$$\mathbb{Z}/m = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \cdots, \overline{m-1}\}$$

dir.

Teorem 11.6.2. *Aşağıdaki ifadeler birbirlerine denktir.*

1. $a \equiv b \,(mod\, m)$
2. $m|(a-b)$
3. a ile b aynı kalan sınıfına aittir.
4. $a \in \overline{b}$
5. $b \in \overline{a}$
6. $a, b \in \overline{c}$
7. $\overline{a} = \overline{b}$

Örnek 11.6.1. 1. $\mathbb{Z}/4$ kalan sınıflarını bulunuz.

Çözüm: 4 ün kalan sınıfları, $\mathbb{Z}/4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ dür. Bunlar,

$$\begin{aligned}
\overline{0} &= \{\ldots, -16, -12, -8, -4, 0, 4, 8, 12, 16, \ldots\} \\
\overline{1} &= \{\ldots, -15, -11, -7, -3, 1, 5, 9, 13, 17, \ldots\} \\
\overline{2} &= \{\ldots, -14, -10, -6, -2, 2, 6, 10, 14, 18, \ldots\} \\
\overline{3} &= \{\ldots, -13, -9, -5, -1, 3, 7, 11, 15, 19, \ldots\}
\end{aligned}$$

dur.

Teorem 11.6.3. *$a, b, c, m \in \mathbb{Z}$ ve $m > 1$ için,*

$$a \equiv b \,(mod\, m) \quad \Rightarrow \quad (a \mp c) \equiv (b \mp c)(mod\, m)$$

olur.

Bunun ispatı tanımdan hemen görülür.

Teorem 11.6.4. *$a, b, c, d, m \in \mathbb{Z}$ ve $m > 1$ için,*

$$(a \equiv b(mod\, m)) \ \wedge \ (c \equiv d(mod\, m)) \ \Rightarrow \ (a \pm c) \equiv (b \pm d)(mod\, m)$$

dir.

İSPAT:

$$\begin{array}{rcl} a \equiv b \pmod{m} & \Rightarrow & m \mid a-b \\ & \Rightarrow & \exists p \in \mathbb{Z}, a-b = mp \end{array}$$

$$\begin{array}{rcl} c \equiv d \pmod{m} & \Rightarrow & m \mid c-d \\ & \Rightarrow & \exists q \in \mathbb{Z}, c-d = mq \end{array}$$

$$\left.\begin{array}{l} a-b=mp \\ c-d=mq \end{array}\right\} \begin{array}{rcl} & \Rightarrow & (a+c)-(b+d) = m(p+q) \\ & \Rightarrow & (a+c)-(b+d) = mk \quad (p+q=k \in \mathbb{Z}) \\ & \Rightarrow & m \mid (a+c)-(b+d) \\ & \Rightarrow & a+c \equiv b+d \pmod{m} \end{array}$$

olur. Buradan,

$$\left.\begin{array}{l} a \equiv b \pmod{m} \\ c \equiv d \pmod{m} \end{array}\right\} \Rightarrow (a+c) \equiv (b+d) \pmod{m}$$

çıkar.

$$\left.\begin{array}{l} a \equiv b \pmod{m} \\ c \equiv d \pmod{m} \end{array}\right\} \Rightarrow (a-c) \equiv (b-d) \pmod{m}$$

olduğu benzer yolla gösterilebilir.

Örnekler

1. $-11 \equiv 9 \pmod 4$ ve $19 \equiv -5 \pmod 4$ için,

$$\left.\begin{array}{l} -11+19 = 8 \equiv 0 \pmod{4} \\ 9-5 = 4 \equiv 0 \pmod{4} \end{array}\right\} \Rightarrow -11+19 \equiv 9-5 \pmod{4}$$

   olur.

2. $-14 \equiv 34 \bmod (12)$ ve $-22 \equiv 26 \pmod{12}$ için,

$$\left.\begin{array}{l} -14-(-22) = 8 \equiv 8 \pmod{12} \\ 34-26 = 8 \equiv 8 \pmod{12} \end{array}\right\} \Rightarrow -14-(-22) \equiv 34-26 \pmod{12}$$

   olur.

   Kalan sınıfları üzerinde toplama işlemini, aşağıdaki gibi tanımlayabiliriz:

   Tanım 11.6.2. $\overline{a}, \overline{b} \in \mathbb{Z}/m$ ise,

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

   dır.

Burada, a ve b yerine, $a_1 \in \overline{a}$ ve $b_1 \in \overline{b}$ olmak üzere herhangi a_1, b_1 sayıları alınabilir. Toplama işlemi, kalan sınıflardan seçilen temsilciye bağlı değildir. Neden?

3. $\overline{11}, \overline{5}, \overline{2} \in \mathbb{Z}/7$ için,

$$\overline{11} \oplus \overline{5} = \overline{11+5} = \overline{16} = \overline{2}, \quad \overline{-17} \oplus \overline{26} = \overline{-17+26} = \overline{9} = \overline{2}$$

olur.

4. $a + b = c$ işlemi doğru ise, eşitliğin iki yanının $(mod\ 9)$ için değerleri de eşit olmalıdır. Bu, 9 atarak sağlama yönteminin dayanağıdır.

5. $\begin{array}{r} 516 \\ +\ \ 92 \\ \hline 608 \end{array}$ $\quad$ $\begin{array}{l} 516 \equiv 3 \pmod 9 \\ 92 \equiv 2 \pmod 9 \\ 3+2 \equiv 5 \pmod 9 \\ 608 \equiv 5 \pmod 9 \end{array}$ $\quad$ $\begin{array}{ccc} & 3 & \\ 5 & & 5 \\ & 2 & \end{array}$

Bu sağlama işleminde, $\mathbb{Z}/9$ içinde,

$$\overline{516} \oplus \overline{92} = \overline{516+92} \quad \Leftrightarrow \quad \overline{3} \oplus \overline{2} = \overline{5}$$

olduğunu göstermiş olduk.

Teorem 11.6.5. *$a, b, c, m \in \mathbb{Z}$, $m > 1$ için,*

$$a \equiv b\ (mod\ m) \quad \Rightarrow \quad ac \equiv bc\ (mod\ m)$$

olur.

Bunun ispatı tanımdan çıkar.

Teorem 11.6.6. *$a, b, c, d, m \in \mathbb{Z}$ ve $m > 1$ için,*

$$[(a \equiv b\ (mod\ m)) \ \wedge\ (c \equiv d\ (mod\ m))] \quad \Rightarrow \quad a.c \equiv b.d\ (mod\ m)$$

dir.

İspat: Aşağıdaki bağıntılardan istenen çıkar.

$$\begin{array}{lll} a \equiv b \pmod m & \Rightarrow & m \mid a-b \\ & \Rightarrow & \exists p \in \mathbb{Z}, a-b = mp \\ & \Rightarrow & a = b+mp \quad \text{dir.} \end{array}$$

$$\begin{array}{lll} c \equiv d \pmod m & \Rightarrow & m \mid c-d \\ & \Rightarrow & \exists q \in \mathbb{Z}, c-d = mq \\ & \Rightarrow & c = d+mq \quad \text{dir.} \end{array}$$

$$\begin{aligned} a = b + mp \wedge c = d + mq &\Rightarrow a.c = (b+mp)(d+mq) \\ &\Rightarrow a.c = bd + mbq + mdp + m^2pq \\ &\Rightarrow ac - bd = m\underbrace{(bq + dp + mpq)}_{k\in\mathbb{Z}} \\ &\Rightarrow ac - bd = mk \\ &\Rightarrow m \mid ac - bd \\ &\Rightarrow ac \equiv bd \pmod{m} \end{aligned}$$

Örnek 11.6.2. $19 \equiv -9 \pmod 7$ ve $-13 \equiv 22 \pmod 7$ için,

$$\left.\begin{array}{l} 19.(-13) = -247 \equiv 2 \pmod 7 \\ (-9).22 = -198 \equiv 2 \pmod 7 \end{array}\right\} \Rightarrow 19.(-13) \equiv (-9).22 \pmod 7$$

olur.

Teorem 11.6.7. *$a, b, m, n \in \mathbb{Z}$, $m > 1$ ve $n > 0$ ise,*

$$[(a \equiv b \ (mod\ m)) \quad \Rightarrow \quad a^n \equiv b^n \ (mod\ m)$$

dir.

Bunun ispatı, verilen bir n için, önceki teormden çıkar. Genel ispatı tümevarım yöntemini gerektirir. Dolayısıyla, teoremin varlığını kabul edeceğiz.

$\mathbb{Z}/m$ üzerinde çarpma işlemi tanımlayabiliriz.

Tanım 11.6.3. $\overline{p}, \overline{q} \in \mathbb{Z}/m$ için

$$\overline{p} \otimes \overline{q} = \overline{p.q} \tag{11.6}$$

dır.

Örnek $\overline{7}, \overline{8} \in \mathbb{Z}/3$ için $\overline{7} \otimes \overline{8} = \overline{7.8} = \overline{56} = \overline{2}$ dır.

$a.b = c$ işlemi doğru ise, eşitliğin iki yanının $(mod\ 9)$ için değerleri de eşit olmalıdır. Çarpmada, 9 atarak sağlama yönteminin dayanağı budur.

Örnekler

1.
$$\begin{array}{rr} & 123 \\ \times & 38 \\ \hline & 184 \\ + & 369 \\ \hline & 4674 \end{array}$$

$123 \equiv 6 \pmod 9$
$38 \equiv 2 \pmod 9$
$6.2 \equiv 3 \pmod 9$
$4674 \equiv 3 \pmod 9$

$$\begin{array}{ccc} & 6 & \\ 3 & & 3 \\ & 2 & \end{array}$$

Bu sağlama işleminde, $\mathbb{Z}/9$ içinde,

$$\overline{123} \otimes \overline{38} = \overline{123.38} \quad \Leftrightarrow \quad \overline{6} \otimes \overline{2} = \overline{3}$$

olduğunu göstermiş olduk.

2. $\mathbb{Z}/5$ de $6.4 + 5^2.4 + 2.8$ işlemini yapınız.

$$\begin{aligned} 6.4 + 5^2.4 + 2.8 &\equiv 1.4 + 0.4 + 2.3 \pmod 5 \\ &\equiv 5 \pmod 5 \\ &\equiv 0 \pmod 5 \end{aligned}$$

3. $\mathbb{Z}/6$ kalan sınıfında toplama ve çarpma tablolarını oluşturunuz.

$\oplus$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\otimes$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

4. $\mathbb{Z}/5$ kümesinde, $(3x - 2)(2x + 1) = 0$ denklemlerinin çözüm kümesini bulunuz.

$$\begin{aligned} (3x-2)(2x+1) = 0 &\Rightarrow (3x - 2 = 0) \vee (2x + 1 = 0) \\ &\Rightarrow (3x - 2 + 2 = 2) \vee (2x + 1 + 4 = 4) \\ &\Rightarrow (3x = 2) \vee (2x = 4) \\ &\Rightarrow (3.2.x = 2.2) \vee (2.3.x = 3.4) \\ &\Rightarrow (x = 4) \vee (x = 2) \end{aligned}$$

$$S = \{1, 2\}$$

olur.

5. $\mathbb{Z}/7$ kalan sınıfları içinde, $2x^2 + 25 = 10$ denkleminin çözümünü bulunuz.

$$\begin{aligned} 2x^2 + 25 = 10 &\Rightarrow 2x^2 + 25 - 25 = 10 - 25 \\ &\Rightarrow 2x^2 = -15 \\ &\Rightarrow 2.x^2 = -1 \\ &\Rightarrow 4.2.x^2 = -4 \\ &\Rightarrow 8.x^2 = -4 \\ &\Rightarrow x^2 = 3 \end{aligned}$$

$\mathbb{Z}/7$ kalan sınıfları içinde karesi 3 olan sayı yoktur; o halde, denklemin çözümü yoktur.

6. $-13 \equiv 12 \pmod 5$ olduğunu gösteriniz.

   1.Çözüm: (mod 5) e göre, -13 ile 12 sayıları aynı denklik sınıfına ait olmalıdır. $12 \div 5$ işleminin kalanı 2 dir; yani $12 \in \overline{2}$ dir. $-13 \div 5$ işleminden kalan -3 dür; yani, $-13 \in \overline{-3}$ dir. Öte yandan, $-3+5=2$ olduğundan, $\overline{-3} = \overline{2}$ yazılabilir. O halde, -13 ile 12 sayıları aynı denklik sınıfındadır.

   2.Çözüm: (mod 5) e göre, -13 ile 12 sayılarının aynı denklik sınıfına ait olması için, farklarının 5 ile tam bölünmesi gerekli ve yeterlidir: $12-(-13)=25$ ve $5|25$ dir.

7. $3^{33} \equiv x \pmod 5$ eşitliğini sağlayan en küçük x sayısını bulunuz.

   Çözüm: Önce aşağıdaki eşitlikleri inceleyelim.

$$\begin{array}{lcrcl} 3 & \equiv & 3 \pmod 5 & \equiv & 3 \pmod 5 \\ 3^2 & \equiv & 3.3 \pmod 5 & \equiv & 4 \pmod 5 \\ 3^3 & \equiv & 3.4 \pmod 5 & \equiv & 2 \pmod 5 \\ 3^4 & \equiv & 3.2 \pmod 5 & \equiv & 1 \pmod 5 \\ 3^5 & \equiv & 3.1 \pmod 5 & \equiv & 3 \pmod 5 \\ \cdots & & & & \end{array}$$

   Buradan görüldüğü gibi, $3^5 \equiv 3 \pmod 5$ olur ve üslü ifadeler, dörderli döngüler halinde aynı sayıya denk olur. Öyleyse,

$$\begin{array}{rcl} 3^{33} = 3^{32+1} = 3^{32}.3 = 3^{4.8}.3 & \equiv & (3^4)^8.3 \pmod 5 \\ & \equiv & [(3^4)^8 \pmod 5].[3 \pmod 5] \\ & \equiv & [(1)^8 \pmod 5].[3 \pmod 5] \\ & \equiv & [1 \pmod 5].[3 \pmod 5] \\ & \equiv & 1.3 \pmod 5 \\ & \equiv & 3 \pmod 5 \end{array}$$

   olur. Son eşitlik, aradığımız sayının 3 olduğunu söyler.

8. 4897^{97} sayısının birler basamağındaki sayı nedir?

   Çözüm: Önce aşağıdaki eşitlikleri inceleyelim.

$$\begin{array}{lcrcl} 4897 & \equiv & 7 \pmod{10} & \equiv & 7 \pmod{10} \\ 4897^2 & \equiv & 7.7 \pmod{10} & \equiv & 9 \pmod{10} \\ 4897^3 & \equiv & 7.9 \pmod{10} & \equiv & 3 \pmod{10} \\ 4897^4 & \equiv & 7.3 \pmod{10} & \equiv & 1 \pmod{10} \\ 4897^5 & \equiv & 7.1 \pmod{10} & \equiv & 7 \pmod{10} \\ \cdots & & & & \end{array}$$

Görüldüğü gibi, $4897^4 \equiv 1 \pmod{10}$ olduğundan,

$$\begin{aligned} 4897^{97} = 4897^{4.24+1} &\equiv (4897^4)^{24}.4897 \pmod{10} \\ &\equiv [(1)^{24} \pmod{10}] . [7 \pmod{10}] \\ &\equiv [1 \pmod{10}] . [7 \pmod{10}] \\ &\equiv 1.7 \pmod{10} \\ &\equiv 7 \pmod{10} \end{aligned}$$

olur. Son eşitlik, aradığımız sayının 7 olduğunu söyler.

11.7 BÖLÜNEBİLME KURALLARI

Teorem 11.7.1. *$a, b \in \mathbb{Z}$, $m, n \in \mathbb{N}^+$ olmak üzere*

$$a \equiv b(\mod m) \Rightarrow a^n \equiv b^n(\mod m) \tag{11.7}$$

olur.

Bu teoremin doğruluğunu seçilecek her n sayısı için sağlamak kolaydır. Ama ispatı tümevarım yöntemine dayanır; dolayısıyla, bu dersin kapsamı dışındadır.

$a, m, p, k \in \mathbb{N}$, $m > 1$, $0 \leq k < m$ olmak üzere a'nın m ye bölünmesinden bulunan bölüm p, kalan k ise bu durumda,

$$a = m.p + k \Leftrightarrow a \equiv k \pmod{m}$$

olduğunu biliyoruz.

Eğer a sayısı m ye tam olarak bölünüyorsa,

$$a \equiv 0 \pmod{m}$$

olur.

Örnek 8^{21} in 5 ile bölünmesinden elde edilen kalanı bulunuz.

Çözüm:

$$\begin{aligned} 8 \equiv 3 \pmod{5} &\Rightarrow 8^{21} \equiv 3^{21} \pmod{5} \\ &\Rightarrow 8^{21} \equiv (3^2)^{10}.3 \pmod{5} \\ &\Rightarrow 8^{21} \equiv 9^{10}.3 \pmod{5} \\ &\Rightarrow 8^{21} \equiv 4^{10}.3 \pmod{5} \\ &\Rightarrow 8^{21} \equiv (4^2)^5.3 \pmod{5} \\ &\Rightarrow 8^{21} \equiv (1)^5.3 \pmod{5} \\ &\Rightarrow 8^{21} \equiv 3 \pmod{5} \end{aligned}$$

O halde, çözüm kümesi, $S = \{\overline{3}\} \in \mathbb{Z}/5$ olur.

Örnek 7^{67} nin 8 ile bölünmesinden elde edilen kalanı bulunuz.
Çözüm:

$$\begin{aligned} 7 \equiv -1 \pmod 8 &\Rightarrow 7^{67} \equiv (-1)^{67} \pmod 8 \\ &\Rightarrow 7^{67} \equiv (-1)^{67} \pmod 8 \\ &\Rightarrow 7^{67} \equiv -1 \pmod 8 \\ &\Rightarrow 7^{67} \equiv 7 \pmod 8 \end{aligned}$$

O halde, çözüm kümesi, $S = \{\overline{7}\} \in \mathbb{Z}/8$ olur.

Teorem 11.7.2. *Bir a doğal sayısının basamaklarındaki rakamlar, soldan sağa doğru, $0 \leq a_n, a_{n-1}, \ldots, a_2, a_1, a_0 \leq 9$ ise, a sayısının, onlu sayı sistemindeki açılımı,*

$$a = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_2 10^2 + a_1.10 + a_0 \tag{11.8}$$

dır.

Örnek

$$7853 = 7.10^3 + 8.10^2 + 5.10 + 3$$

Teorem 11.7.3. *Onlu sayı sistemindeki açılımı (11.8) deki gibi olan bir a doğal sayısı için,*

$$a = [a_n + a_{n-1} + \cdots + a_2 + a_1 + a_0] \pmod 9 \tag{11.9}$$

eşitliği sağlanır.

İSPAT: Ker k doğal sayısı için $10^k \equiv 1 \ (mod\ 9)$ dur. Bu özelik, (11.8) eşitliğinin her terimine uygulanırsa, (11.9) eşitliği elde edilir.

2 ile Bölünebilme Kuralı

Bir tamsayının 2 ile tam bölünebilmesi için, gerekli ve yeterli koşul, birler basamağındaki rakamın çift olmasıdır.
İspat: (1) eşitliğinden,

$$\begin{aligned} \alpha &\equiv a_n.0 + a_{n-1}0 + \cdots + a_3.0 + a_2.0 + a_1.0 + a_0 \pmod 2 \\ &\equiv a_0 \pmod 2 \end{aligned}$$

elde edilir. Öyleyse, $a \equiv 0 \pmod 2$ olması için $a_0 \equiv 0 \pmod 2$ olmalıdır.
Örnekler

1. 17398 sayısının birler basamağındaki rakam 8 dır. $8 \equiv 0 \ (mod\ 2)$ olduğundan $17398 \equiv 0 \ (mod\ 2)$ dir. Öyleyse, 17398 sayısı 2 ile tam bölünür.
2. 5753 sayısının birler basamağındaki rakam 3 dür. $3 \equiv 1 \ (mod\ 2)$ olduğundan $5753 \not\equiv 0 \ (mod\ 2)$ dır. Öyleyse, 5753 sayısı 2 ile tam bölünemez.

3 ile Bölünebilme Kuralı

Bir tamsayının 3 ile tam bölünebilmesi için, gerekli ve yeterli koşul, basamaklarındaki rakamların toplamının 3 ya da 3 ün bir katı olmasıdır.
İspat: Her k doğal sayısı için, $(10)^k \equiv 1 \ (mod\ 3)$ bağıntısı kullanılırsa, (1) eşitliğinden,

$$\begin{aligned} a &\equiv a_n.1 + a_{n-1}.1 + \cdots + a_2.1 + a_1.1 + a_0 \pmod 3 \\ &\equiv a_n + a_{n-1} + \cdots + a_3 + a_2 + a_1 + a_0 \pmod 3 \end{aligned}$$

elde edilir. O halde,
$a \equiv 0 \pmod 3$ olması için, gerekli ve yeterli koşul,

$$a_n + a_{n-1} + \cdots + a_3 + a_2 + a_1 + a_0 \equiv 0(mod 3)$$

olmasıdır.
Örnekler

1. 8931 sayısının basamaklarındaki rakamların toplamı 21 dir. Bu toplam 3 ün bir katıdır;yani, 3 ile tam bölünür. Öyleyse, 8931 sayısı da 3 ile tam bölünür. Bunun, eşdeğerlik bağıntısıyla ifadesi, $8931 \equiv 0 \ (mod\ 3)$ dür.
2. 7451 sayısının basamaklarındaki rakamların toplamı 17 dir. Bu toplam 3 ün bir katı değildir; yani, 3 ile tam bölünemez. $8931 \div 3$ işlemi yapılırsa, elde edilecek kalan,

$$\begin{aligned} 7451 &\equiv 7 + 4 + 5 + 1 \pmod 3 \\ &\equiv 2 \pmod 3 \end{aligned}$$

dir.

4 ile Bölünebilme Kuralı

Bir a tamsayısının birler basamağındaki rakam ile onlar basamağındaki rakamın iki katının toplamı 4 ün bir katı ise, a sayısı 4 e tam bölünür.
İspat: Her $k \geq 2$ doğal sayısı için, $(10)^k \equiv 0 \ (mod\ 4)$ bağıntısı kullanılırsa, (1) eşitliğinden,

$$\begin{aligned} a &\equiv a_n.0 + a_{n-1}.0 + \cdots + a_3.0 + a_2.0 + a_1.10 + a_0 \pmod 4 \\ &\equiv 2a_1 + a_0 \pmod 4 \end{aligned}$$

elde edilir ve ispat biter.
$a_1.10 + a_0 \equiv 2a_1 + a_0 \pmod 4$ olduğundan, yukarıdakine eşdeğer olan şu kuralı söyleyebiliriz.

Kural: Bir a doğal sayısının son iki rakamından oluşan doğal sayı, 4 ün bir katı ise, a sayısı 4 ile tam bölünür.
Örnekler

1. $a = 332456$ sayısının son iki basamağındaki sayı 56 dır. Bu sayı 4 ün bir katıdır. O halde, 332456 sayısı 4 ile tam bölünür.

2. $a = 5738$ sayısının son iki basamağındaki sayı 38 dir. Bu sayı 4 ün bir katı olmadığından, verilen 5738 sayısı 4 ile tam bölünemez. $5738 \div 4$ bölme işleminin kalanı 2 dir; çünkü,

$$5738 \equiv 2.3 + 8 \equiv 6 + 0 \equiv 2 \ (mod\ 4)$$

yazılabilir.

Aşağıdaki kuralların çıkışı, yukarıda yaptıklarımıza benzer.

5 ile Bölünebilme Kuralı

Birler basamağında 0 ya da 5 olan her doğal sayı, 5 ile tam bölünür.

9 ile Bölünebilme Kuralı

Bir tamsayının 9 ile tam bölünebilmesi için, gerekli ve yeterli koşul, basamaklarındaki rakamların toplamının 9 ya da 9 un bir katı olmasıdır.

11 ile Bölünebilme Kuralı

Herhangi bir a tamsayısının basamaklarındaki rakamlar, sağdan sola doğru numaralandığında, tek numaralı basamaklardaki rakamların toplamı ile çift numaralı basamaklardaki rakamların toplamının farkı, 11 in bir katı ise, a sayısı 11 *ile tam bölünür.*
İspat: Her k tamsayısı için,

$$\begin{aligned} a_{2k}.10^{2k} + a_{2k-1}.10^{2k-1} &\equiv [a_{2k}.10 + a_{2k-1}].10^{2k-1} \ (mod\ 11) \\ &\equiv [a_{2k}.(-1) + a_{2k-1}].10^{2k-1} \ (mod\ 11) \\ &\equiv [a_{2k-1} - a_{2k}].10^{2k-1} \ (mod\ 11) \end{aligned}$$

dir. Bunu, (1) eşitliğinde, ardışık terimler için kullanırsak, yukarıdaki kural çıkar.

Örnekler

1. $a = 199617$ sayısının rakamlarını, yukarıda açıklandığı gibi numaralayalım:

$$\begin{array}{lcccccc} a = & 1 & 9 & 9 & 6 & 1 & 7 \\ & 6 & 5 & 4 & 3 & 2 & 1 \end{array}$$

Tek numaralı basamakların toplamı: $7 + 6 + 9 = 22$,

Çift numaralı basamakların toplamı: $1 + 9 + 1 = 11$ dir.

$22 - 11 = 11$ ve $11 \equiv 0 \ (mod\ 11)$ olduğundan, verilen sayı 11 ile tam bölünür; yani,

$$199617 \equiv 0 \ (mod\ 11)$$

dir.

2. $a = 526390$ sayısının basamaklarını, sağdan sola doğru, numaralayalım.

$$\begin{array}{rcccccc} a = & 5 & 2 & 6 & 3 & 9 & 0 \\ & 6 & 5 & 4 & 3 & 2 & 1 \end{array}$$

Tek numaralı basamakların toplamı : $0 + 3 + 2 = 5$,

Çift numaralı basamakların toplamı: $9 + 6 + 5 = 20$

$5 - 20 = -15$ ve $-15 \not\equiv 0 \pmod{11}$ olduğundan, verilen 526390 sayısı 11 e tam bölünemez. $526390 \div 11$ işleminin kalanı,

$$526390 = 11.47853 + 7 \quad \Rightarrow \quad 526390 \equiv 7 \ (mod\ 11)$$

dir.

3. n bir doğal sayı ise, $a = 26.(13)^{4n+3}$ sayısının birler basamağındaki rakamı nedir?

Çözüm: Sayının birler basamağındaki rakam, a nın 10 ile bölünmesinden elde edilecek kalandır. Çünkü, a sayısının, (1) açılımından,

$$\begin{aligned} a &= a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_2 10^2 + a_1.10 + a_0 \equiv a_0 \ (mod\ 10) \\ &= a_0 \ (mod\ 10) \end{aligned}$$

yazılabilir. Şimdi, bu kalanı bulacağız.

$$\begin{aligned} 26.(13)^{4n+3} &\equiv 6.3^{4n+3} (\text{mod} \quad 10) \\ &\equiv 6.3^{4n}.3^3 (\text{mod} \quad 10) \\ &\equiv 2.3.3^{4n}.3^2.3 (\text{mod} \quad 10) \\ &\equiv 2.3^2.3^2.3^{4n} (\text{mod} \quad 10) \\ &\equiv 2.(-1)(-1).3^{4n} (\text{mod} \quad 10) \\ &\equiv 2.3^{4n} (\text{mod} \quad 10) \\ &\equiv 2.(3^2)^{2n} (\text{mod} \quad 10) \\ &\equiv 2.(-1)^{2n} (\text{mod} \quad 10) \\ &\equiv 2.(1) (\text{mod} \quad 10) \\ &\equiv 2 (\text{mod} \quad 10) \end{aligned}$$

olduğundan, $a = 6.3^{4m+3}$ sayısının 10 ile bölünmesinden kalan 2 dir.

11.8 ALIŞTIRMALAR

1. $6, 15, 21, 22, 26, \cdots$ gibi farklı iki asal sayının çarpımı olan bir sayı ile bölünebilme kuralını söyleyiniz.

2. $4346.567 = 2464182$ ve $2513.527 = 1324351$ çarpma işlemlerinin sağlamasını yapınız.

3. Toplama ve çarpma işlemleri için, $[mod\ m)$ yardımıyla yapılan sağlamada, m ve m'in katlarında eşit hatalar görülemez. Neden?

4. Bölme işlemini yapmadan, $5^{256} \div 7$ işleminin kalanını bulunuz.

   Bölme işlemini yapmadan, $13^{12n+1} \div 5$ işleminin kalanını bulunuz ($n \in \mathbb{N}^+$).

5. $\mathbb{Z}_{11}$ kümesinde, $\otimes$ işlemine göre, $\overline{5}$ in tersini bulunuz.

6. $\mathbb{Z}_4$ kümesinde, $\otimes$ işlemine göre, karekökü olmayan sayı nedir?

7. Aşağıdaki denklemleri çözünüz.

   $x + 2 \equiv 3 \pmod 5$ $\quad$ $x - 4 \equiv 2 \pmod 7$
   $x + 1 \equiv 5 \pmod 6$ $\quad$ $5x \equiv 3 \pmod 8$
   $42.76 \equiv x \pmod{100}$ $\quad$ $2x + 8 \equiv 4 \pmod 3$

8. $\mathbb{Z}_{11}$ kümesinde $f(x) = 3x + 1$ ise, $f^{-1}(3)$ nedir?

9. $\mathbb{Z}_6$ kümesinde $x \oplus a = b$ denkleminin bir tek çözümü olduğunu gösteriniz.

10. $\mathbb{Z}_6$ kümesinde $x \otimes a = b$ denkleminin çözümü tek midir? Neden?

11. $(3^{27} + 5^{35} + x \equiv 1 \pmod 8)$ denklemini çözünüz.

12. $(4^{47} + 3^{21}) \div 5$ işleminin kalanını bulunuz.

13. $5^{2k+1} \div 7$ işleminin kalanını bulunuz.

14. Sağlama yapmak için neden *mod 9* seçilir?

15. $\mathbb{Z}_5$ kümesinde $3.2^{17} + 2.4^{24} + 3.2^{436} + 3(5.3^{33})$ işlemini yapınız.

16. $\mathbb{Z}_7$ kümesinde $(3x^2 + 2x + 1)(4x^3 + 2x^2 + x + 3)$ işlemini yapınız.

17. $4.7^{322} + 5.5^{347} + 5.4^{367} + 3.453$ sayısının birler basamağındaki rakamı bulunuz.

18. n bir sayma sayısı olsun. $(53957)^{40n}$ sayısının birler basamağındaki rakamı bulunuz.

19. $\mathbb{Z}_m$ kümesinde x'in toplamaya göre tersi $-x$, çarpmaya göre tersi x^{-1} ile gösteriliyor. $\mathbb{Z}_5$ kümesinde $2(-2)^7 + 4^{-2}.3^{234} + (8^{-1})^6(-3)^7$ işlemini yapınız.

20. Bölme işlemi yapmadan, aşağıdaki önermelerin doğru mu, yoksa yanlış mı, olduğunu belirleyiniz.

    a. $3|37845$ $\quad$ b. $8|6934256$ $\quad$ c. $9|39510454$
    c. $15|54795$ $\quad$ e. $18|5269772$ $\quad$ f. $24|51064948$