

# Bölüm 1

## Temel Kavramlar

Bu bölümde bağıntı ve fonksiyon gibi bazı temel kavramlar üzerinde durulacak, tamsayıların bazı özellikleri ele alınacaktır. Bu çalışma boyunca kullanılacak bazı kümelerin gösterimleri aşağıda belirtilmiştir.

- (a) Doğal sayılar kümesi:  $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ .
- (b) Tamsayılar kümesi:  $\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \dots\}$ .
- (c) Sıfırdan farklı tamsayılar kümesi:  $\mathbb{Z}^*$ .
- (d) Pozitif tamsayılar kümesi:  $\mathbb{Z}^+ = \{1, 2, 3, \dots\}$ .
- (e) Her  $n \in \mathbb{Z}^+$  için  $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ .
- (f) Çift tamsayılar kümesi:  $2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\} = \{0, 2, -2, 4, -4, \dots\}$ .
- (g) Tek tamsayılar kümesi:  $T = \{2k + 1 \mid k \in \mathbb{Z}\} = \{1, -1, 3, -3, 5, -5, \dots\}$ .
- (h) Her  $n \in \mathbb{Z}$  için  $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\} = \{n, -n, 2n, -2n, 3n, -3n, \dots\}$ .
- (i) Rasyonel sayılar kümesi:  $\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\}$ .
- (j) Pozitif rasyonel sayılar kümesi:  $\mathbb{Q}^+ = \{r \in \mathbb{Q} \mid r > 0\}$ .
- (k) Sıfırdan farklı rasyonel sayılar kümesi:  $\mathbb{Q}^*$ .
- (l) Reel sayılar kümesi:  $\mathbb{R}$ .
- (m) İrrasyonel sayılar kümesi:  $\mathbb{I}$ .
- (n) Pozitif reel sayılar kümesi:  $\mathbb{R}^+$ .
- (o) Sıfırdan farklı reel sayılar kümesi:  $\mathbb{R}^*$ .
- (p) Kompleks (karmaşık) sayılar kümesi:  $\mathbb{C}$ .
- (r) Sıfırdan farklı kompleks sayılar kümesi:  $\mathbb{C}^*$ .

## 1.1 Bağlılıklar

Bu kısımda “bağlılık” kavramı tanımlanacak ve bağlılıkların yansıma, simetri, ters simetri ve geçişme gibi bazı özellikleri incelenecektir. Ayrıca denklik bağlılıkları ve sıralama bağlılıkları üzerinde durulacaktır.

**Tanım 1.1.1**  $n \geq 2$  bir tamsayı olmak üzere  $A_1, A_2, \dots, A_n$  kümeleri verilsin.  $A_1 \times A_2 \times \dots \times A_n$  kartezyen çarpım kümesinin her bir  $R$  altkümesine  $A_1, A_2, \dots, A_n$  üzerinde bir  **$n$ -li bağlılık** denir. Eğer  $R = \emptyset$  ise o zaman  $R$  ye **boş bağlılık**,  $R = A_1 \times A_2 \times \dots \times A_n$  ise o zaman  $R$  ye **evrensel bağlılık** adı verilir.  $A$  ve  $B$  iki küme olmak üzere  $R \subseteq A \times B$  ise  $R$  ye  **$A$  dan  $B$  ye bir bağlılık**, özel olarak  $R \subseteq A \times A$  ise  $R$  ye  **$A$  üzerinde bir bağlılık** denir.

**Tanım 1.1.2**  $A$  ve  $B$  iki küme olmak üzere  $R \subseteq A \times B$  olsun.

$$\{a \in A \mid (a, b) \in R \text{ olacak şekilde bir } b \in B \text{ vardır}\}$$

kümesine  $R$  nin **tanım kümesi**,

$$\{b \in B \mid (a, b) \in R \text{ olacak şekilde bir } a \in A \text{ vardır}\}$$

kümesine de  $R$  nin **görüntü kümesi** adı verilir. Eğer  $(a, b) \in R$  ise o zaman  **$a$  ile  $b$  bağlılıktır** denir.

**Uyarı 1.1.3**  $A$  ile  $B$  iki küme ve  $A$  dan  $B$  ye bir bağlılık  $R$  olsun. Eğer  $(a, b) \in R$  ise o zaman  $a$  ile  $b$  nin bağlılık olması  $aRb$  şeklinde de gösterilebilir. ♦

**Örnek 1.1.4**  $A = \{1, 2, 3, 4\}$  ve  $B = \{x, y, z, w\}$  olsun.  $R = \{(1, y), (2, x), (2, w), (3, y)\}$  kümesi  $A$  dan  $B$  ye bir bağlılıktır.  $R$  nin tanım kümesi  $\{1, 2, 3\}$  görüntü kümesi  $\{x, y, w\}$  dur. ▲

Şimdi bir küme üzerinde tanımlı bağlılıkların bazı özelliklerini tanımlayalım.

**Tanım 1.1.5**  $R$  bir  $A$  kümesi üzerinde tanımlı bir bağlılık olsun. Eğer

- (1) her  $x \in A$  için  $(x, x) \in R$  ise o zaman  $R$  ye **yansıma özelliğine sahiptir**,
- (2)  $(x, y) \in R$  şartını sağlayan her  $x, y \in A$  için  $(y, x) \in R$  ise o zaman  $R$  ye **simetri özelliğine sahiptir**,
- (3)  $(x, y) \in R$  ve  $(y, x) \in R$  şartlarını sağlayan her  $x, y \in A$  için  $x = y$  oluyorsa  $R$  ye **ters (anti) simetri özelliğine sahiptir**,
- (4)  $(x, y) \in R$  ve  $(y, z) \in R$  şartlarını sağlayan her  $x, y, z \in A$  için  $(x, z) \in R$  ise o zaman  $R$  ye **geçişme özelliğine sahiptir** denir.

**Örnek 1.1.6**  $A = \{a, b, c\}$  üzerinde tanımlı

$$R_1 = \{(a, a), (a, c), (b, b), (c, a), (c, c)\}$$

ve

$$R_2 = \{(a, a), (a, b), (b, b), (b, c)\}$$

bağlıntılarını göz önüne alalım.  $(a, a), (b, b), (c, c)$  sıralı ikilileri  $R_1$  in elemanı olduğundan  $R_1$  yansıyandır. Fakat  $(c, c) \notin R_2$  olduğundan  $R_2$  yansıyan değildir.  $R_1$  bağıntısı simetrik olmasına rağmen  $(a, b) \in R_2$  iken  $(b, a) \notin R_2$  olduğundan  $R_2$  bağıntısı simetrik değildir. Diğer taraftan  $(a, c), (c, a) \in R_1$  şartlarını sağlayan  $a, c \in A$  için  $a = c$  olmadığından  $R_1$  bağıntısı ters simetrik değildir. Fakat  $(x, y) \in R_2$  ve  $(y, x) \in R_2$  şartlarını sağlayan  $x, y \in A$  var olmadığından  $R_2$  bağıntısı ters simetriktir. Benzer şekilde  $R_1$  bağıntısı geçişmeli olmasına rağmen  $(a, b), (b, c) \in R_2$  iken  $(a, c) \notin R_2$  olduğundan  $R_2$  bağıntısı geçişmeli değildir. ▲

### 1.1.1 Denklik Bağlıntıları

Bu kısımda denklik bağıntısı adı verilen ve bir kümenin elemanlarını sınıflandırmaya yarayan bağıntıları ele alacağız. Ayrıca denklik bağıntıları yardımıyla kümelerin parçalanmalarının elde edilmesi üzerinde duracağız.

**Tanım 1.1.7** Bir  $A$  kümesi üzerinde tanımlı bir  $R$  bağıntısı yansıma, simetri ve geçişme özelliklerine sahip ise o zaman  $R$  ye  $A$  üzerinde bir **denklik bağıntısı** denir.

**Örnek 1.1.8**  $A = \{1, 2, 3, 4, 5, 6\}$  kümesi üzerinde tanımlanan

$$R = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (6, 6), (1, 3), (1, 6), (6, 1), (6, 3), (3, 1), (3, 6), (2, 4), (4, 2)\}$$

$A$  üzerinde bir denklik bağıntısıdır. ▲

**Tanım 1.1.9**  $R$  bir  $A$  kümesi üzerinde tanımlı bir denklik bağıntı olsun. Bir  $a \in A$  için

$$[a]_R = \{x \in A : xRa\}$$

kümesine  **$a$  nın  $R$  bağıntısına göre denklik sınıfı** denir.  $A$  üzerinde tanımlı  $R$  denklik bağıntısına göre bütün denklik sınıflarının kümesi

$$A/R = \{[a]_R : a \in A\}$$

şeklinde gösterilir.

**Uyarı 1.1.10**  $\emptyset \neq A$  kümesi üzerinde tanımlı bir denklik bağıntısı  $R$  ve  $a \in A$  olsun.  $R$  nin yansıma özelliği gereğince  $aRa$  dır. Bu sebeple  $a \in [a]_R$  olup  $[a]_R \neq \emptyset$  dir. Ayrıca  $a$  nın denklik sınıfı için eğer  $R$  yi belirtmek gerekmiyorsa  $[a]_R$  yerine  $[a]$  veya  $\bar{a}$  gösterimi kullanılabilir. ◆

**Örnek 1.1.11**  $A = \{1, 2, 3, 4, 5, 6\}$  kümesi üzerinde tanımlı

$$R = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (6, 6), (1, 3), (1, 6), (6, 1), (6, 3), (3, 1), (3, 6), (2, 4), (4, 2)\}$$

denklik bağıntısına göre denklik sınıfları  $\bar{1} = \{1, 3, 6\}$ ,  $\bar{2} = \{2, 4\}$ ,  $\bar{3} = \{1, 3, 6\}$ ,  $\bar{4} = \{2, 4\}$ ,  $\bar{5} = \{5\}$ ,  $\bar{6} = \{1, 3, 6\}$  şeklindedir.  $\bar{1} = \bar{3} = \bar{6}$  ve  $\bar{2} = \bar{4}$  olduğundan  $R$  denklik bağıntısına göre bütün denklik sınıfları  $\bar{1}$ ,  $\bar{2}$  ve  $\bar{5}$  ve böylece  $A/R = \{\bar{1}, \bar{2}, \bar{5}\}$  dir. ▲

**Teorem 1.1.12**  $\emptyset \neq A$  kümesi üzerinde tanımlı bir denklik bağıntısı  $R$  olsun.

(i) Her  $a \in A$  için  $a \in [a]_R$  ve  $A = \bigcup_{a \in A} [a]_R$  dir.

(ii)  $a, b \in A$  olmak üzere  $aRb$  olması için gerek ve yeter şart  $[a]_R = [b]_R$  olmasıdır.

(iii) Eğer  $a, b \in A$  ise o zaman  $[a]_R \cap [b]_R = \emptyset$  ya da  $[a]_R = [b]_R$  dir.

**Teorem 1.1.13**  $\emptyset \neq A$  kümesi üzerinde tanımlı bir denklik bağıntısı  $R$  olsun. Bu durumda  $A/R$  kümesi  $A$  nın bir parçalanmasıdır.

**Örnek 1.1.14**  $A = \{1, 2, 3, 4, 5, 6\}$  kümesi üzerinde tanımlanan

$$R = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (6, 6), (1, 3), (1, 6), (6, 1), (6, 3), (3, 1), (3, 6), (2, 4), (4, 2)\}$$

denklik bağıntısına göre bütün denklik sınıfları  $\bar{1}$ ,  $\bar{2}$  ve  $\bar{5}$  olduğundan  $A/R = \{\bar{1}, \bar{2}, \bar{5}\}$  kümesi  $A$  nın bir parçalanmasıdır. ▲

## 1.1.2 Sıralama Bağlılıkları

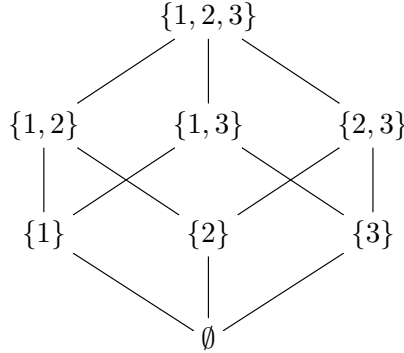
Bu kısımda sıralama bağıntısı adı verilen ve bir kümenin elemanları arasında sıralama yapmaya yarayan bağıntıları inceleyeceğiz.

**Tanım 1.1.15** Bir  $A$  kümesi üzerinde tanımlı  $\preceq$  bağıntısı yansıyan, ters simetrik ve geçişmeli ise o zaman  $\preceq$  bağıntısına  $A$  üzerinde **bir kısmi sıralama bağıntısı** denir ve  $(A, \preceq)$  ikilisine bir **kısmi sıralı küme** adı verilir.

**Örnek 1.1.16**  $A = \{1, 2, 3\}$  olmak üzere  $\mathcal{P}(A)$  üzerinde bir  $\preceq$  bağıntısı “  $B \preceq C$  olması için gerek ve yeter şart  $B \subseteq C$  olmasıdır ” şeklinde tanımlansın. Bu bağıntı  $\mathcal{P}(A)$  kümesi üzerinde yansıyan, ters simetrik ve geçişmeli olduğundan bir kısmi sıralama bağıntısıdır. ▲

$(A, \preceq)$  kısmi sıralı sonlu bir küme ve  $a, b \in A$  olsun.  $a \neq b$  olmak üzere  $a \preceq c$  ve  $c \preceq b$  olacak şekilde bir  $c \in A$  bulunamıyorsa o zaman  **$b$  ye  $a$  nın ardılı** denir.  $A$  nın  $\preceq$  bağıntısına göre ardıl olan elemanlarının doğru parçaları ile birleştirilmesi sonucunda elde edilen diyagramlara  $A$  nın  $\preceq$  bağıntısına göre **Hasse diyagramı** denir.

**Örnek 1.1.17**  $A = \{1, 2, 3\}$  kümesi veriliyor. Bu durumda  $(\mathcal{P}(A), \subseteq)$  kısmi sıralı kümesinin Hasse diyagramı



şeklindedir. ▲

**Tanım 1.1.18**  $(A, \preceq)$  kısmi sıralı bir küme olsun. Eğer  $a, b \in A$  için  $a \preceq b$  veya  $b \preceq a$  ise o zaman  $a$  ve  $b$  elemanları **kıyaslanabilir** denir. Eğer  $A$  nın her eleman çifti kıyaslanabilir ise o zaman  $\preceq$  bağıntısına bir **tam (lineer) sıralama bağıntısı** denir ve  $(A, \preceq)$  ikilisine de bir **tam (lineer) sıralı küme** adı verilir.

**Örnek 1.1.19**  $A = \{1, 2, 3\}$  kümesi veriliyor. Bu durumda  $\subseteq$  bağıntısı  $\mathcal{P}(A)$  üzerinde bir kısmi sıralama bağıntısı olmasına rağmen tam sıralama bağıntısı değildir. Fakat  $\subseteq$  bağıntısı  $\{\emptyset, \{1\}, \{1, 2\}, \{1, 2, 3\}\}$  üzerinde bir tam sıralama bağıntısıdır. ▲

**Tanım 1.1.20**  $(A, \preceq)$  kısmi sıralı bir küme olsun.  $A$  nın tam sıralı her altkümeye bir **zincir** adı verilir.

**Örnek 1.1.21**  $A = \{1, 2, 3, 5, 6, 10, 15, 30\}$  kümesinin  $B = \{1, 2, 6, 30\}$ ,  $C = \{1, 5, 15, 30\}$  ve  $D = \{1, 2, 10, 30\}$  altkümeleri bölünebilme bağıntısına göre birer zincirdir. ▲

**Tanım 1.1.22**  $(A, \preceq)$  kısmi sıralı bir küme,  $B \subseteq A$  ve  $c \in B$  olsun. Eğer  $b \preceq c$  şartını sağlayan her  $b \in B$  için  $b = c$  oluyorsa o zaman  $c$  ye  $B$  nin bir **minimal elemanı** denir. Benzer şekilde  $c \preceq b$  şartını sağlayan her  $b \in B$  için  $c = b$  oluyorsa o zaman  $c$  ye  $B$  nin bir **maksimal elemanı** denir.

**Örnek 1.1.23**  $A = \{2, 3, 4, 5, 6, 7, 8, 9, 10\}$  kümesinde bölünebilme bağıntısına göre minimal elemanların kümesi  $\{2, 3, 5, 7\}$  ve maksimal elemanların kümesi  $\{6, 7, 8, 9, 10\}$  şeklindedir. ▲

**Tanım 1.1.24**  $(A, \preceq)$  kısmi sıralı bir küme,  $B \subseteq A$  ve  $m \in B$  olsun. Eğer her  $b \in B$  için  $m \preceq b$  ise o zaman  $m$  ye  $B$  nin **minimum (en küçük) elemanı** denir. Ayrıca her  $b \in B$  için  $b \preceq m$  ise o zaman  $m$  ye  $B$  nin **maksimum (en büyük) elemanı** denir.

**Örnek 1.1.25**  $A$  herhangi bir küme olmak üzere  $\mathcal{P}(A)$  üzerinde bir  $\preceq$  bağıntısı “ $B \preceq C$  olması için gerek ve yeter şart  $B \subseteq C$ ” ile tanımlansın. Bu durumda  $(\mathcal{P}(A), \subseteq)$  kısmi sıralı bir kümedir.  $\mathcal{P}(A)$  kümesinin  $\preceq$  bağıntısına göre minimumu  $\emptyset$  ve maksimumu  $A$  dır. ▲

**Tanım 1.1.26**  $(A, \preceq)$  kısmi sıralı bir küme olsun. Eğer  $A$  nın boş kümeden farklı her altkümesinin minimumu varsa o zaman  $\preceq$  bağıntısına **iyi sıralama bağıntısı** ve  $(A, \preceq)$  ikilisine de bir **iyi sıralı küme** adı verilir.

**Örnek 1.1.27**  $(\mathbb{N}, \leq)$  iyi sıralı bir kümedir. Fakat negatif tamsayıların kümesi en küçük elemana sahip olmadığından  $(\mathbb{Z}, \leq)$  iyi sıralı bir küme değildir. ▲

**Teorem 1.1.28** İyi sıralı her küme tam sıralıdır.

## 1.2 Fonksiyonlar

Bu kısımda “fonksiyon” kavramını tanımlayıp birebir fonksiyon, örten fonksiyon, birim fonksiyon gibi bazı fonksiyon çeşitlerini ele alacağız. Verilen fonksiyonlardan yeni bir fonksiyon elde etmenin bir yolu olarak bileşke işlemi üzerinde duracağız. Ayrıca bir fonksiyonun tersi kavramını da inceleyeceğiz.

**Tanım 1.2.1**  $A$  ile  $B$  iki küme ve  $A$  dan  $B$  ye bir bağıntı  $f$  olsun. Eğer her  $a \in A$  için  $(a, b) \in f$  olacak şekilde bir tek  $b \in B$  varsa o zaman  $f$  ye  $A$  dan  $B$  ye bir **fonksiyon** denir ve  $f: A \rightarrow B$  ile gösterilir.  $A$  kümesine  $f$  nin **tanım kümesi**,  $B$  kümesine de  $f$  nin **değer kümesi** adı verilir.  $a \in A$  için  $(a, b) \in f$  ise  $b$  ye  $a$  nın  $f$  fonksiyonundaki **görüntüsü** denir ve  $b = f(a)$  şeklinde gösterilir.

**Örnek 1.2.2**  $A = \{1, 2, 3\}$  ve  $B = \{x, y, z, w\}$  olsun.  $f_1 = \{(1, y), (2, w), (3, y)\}$  kümesi  $A$  dan  $B$  ye bir fonksiyondur. Fakat  $f_2 = \{(1, x), (2, z), (3, y), (2, x)\}$  kümesi verildiğinde birinci bileşeni 2 olan birden çok sıralı ikili içerdiğinden  $f_2$  bağıntısı iyi tanımlı değildir. Bu sebeple bir fonksiyon değildir. Diğer taraftan  $f_3 = \{(1, z), (3, x)\}$  kümesinin tanım kümesi  $A$  olmadığından  $f_3$  bir fonksiyon değildir. Fakat  $f_3$  bağıntısı  $A \setminus \{2\}$  den  $B$  ye bir fonksiyondur. ▲

**Tanım 1.2.3**  $A$  ve  $B$  iki küme,  $f: A \rightarrow B$  bir fonksiyon olsun.  $X \subseteq A$  ve  $Y \subseteq B$  olmak üzere

$$f(X) = \{f(x) \mid x \in X\} \text{ ve } f^{-1}(Y) = \{a \in A \mid f(a) \in Y\}$$

kümelerine sırasıyla  $X$  kümesinin  $f$  fonksiyonundaki **görüntüsü** ve  $Y$  kümesinin  $f$  fonksiyonundaki **ters görüntüsü** denir. Özel olarak  $X = A$  ise o zaman  $f(A)$  ya  $f$  nin **görüntü kümesi** denir ve  $\text{Im} f$  ile gösterilir.

**Örnek 1.2.4**  $A = \{a, b, c\}$ ,  $B = \{x, y, z\}$  kümeleri ve  $f = \{(a, x), (b, x), (c, y)\}$  fonksiyonu veriliyor.  $D = \{a, b\} \subseteq A$  için

$$f(D) = \{f(d) \mid d \in D\} = \{x\}$$

ve

$$\text{Im} f = \{f(d) \mid d \in A\} = \{x, y\}$$

şeklindedir. Ayrıca

$$f^{-1}(\{x\}) = \{\alpha \in A \mid (\alpha, x) \in f\} = \{a, b\}$$

ve

$$f^{-1}(\{z\}) = \{\alpha \in A \mid (\alpha, z) \in f\} = \emptyset$$

dir. ▲

**Tanım 1.2.5**  $A$  ve  $B$  iki küme,  $f: A \rightarrow B$  ve  $g: A \rightarrow B$  fonksiyonları verilsin. Eğer her  $a \in A$  için  $f(a) = g(a)$  ise o zaman  $f$  ve  $g$  fonksiyonlarına **eşit fonksiyonlar** denir ve  $f = g$  ile gösterilir.

**Örnek 1.2.6**  $f: \mathbb{R} \rightarrow \mathbb{R}$ ,  $f(n) = n^2 - 1$  ve  $g: \mathbb{R} \rightarrow \mathbb{R}$ ,  $g(k) = (k - 1)(k + 1)$  şeklinde tanımlanan  $f$  ve  $g$  fonksiyonlarını göz önüne alalım. Her  $a \in \mathbb{R}$  için  $f(a) = g(a)$  olup  $f = g$  dir. ▲

### 1.2.1 Birebir ve Örten Fonksiyonlar

Bu kısımda fonksiyonların birebirlik ve örtenlik özellikleri ele alacağız.

**Tanım 1.2.7**  $A$  ile  $B$  iki küme ve  $A$  dan  $B$  ye bir fonksiyon  $f$  olsun. Eğer  $x \neq y$  olacak biçimde her  $x, y \in A$  için  $f(x) \neq f(y)$  ise, denk olarak  $f(x) = f(y)$  şartını sağlayan her  $x, y \in A$  için  $x = y$  ise o zaman  $f$  ye bir **birebir fonksiyon** denir.

**Örnek 1.2.8**  $A = \{a, b, c, d\}$ ,  $B = \{r, s, t, u, v\}$  ve  $C = \{x, y, z\}$  olsun.  $A$  dan  $B$  ye tanımlı  $f_1 = \{(a, s), (b, u), (c, v), (d, r)\}$  fonksiyonunda  $A$  nın farklı elemanlarının görüntüleri de farklı olduğundan  $f_1$  birebirdir. Fakat  $f_2 = \{(a, s), (b, t), (c, s), (d, u)\}$  fonksiyonu için  $a$  ve  $c$  elemanlarının görüntüsü  $s$ , yani  $f_2(a) = f_2(c) = s$  olduğundan  $f_2$  fonksiyonu birebir değildir. Ayrıca  $C$  nin eleman sayısı  $A$  nın eleman sayısından küçük olduğu için  $A$  dan  $C$  ye birebir bir fonksiyon tanımlanamaz. ▲

**Tanım 1.2.9**  $A, B$  iki küme ve  $f: A \rightarrow B$  bir fonksiyon olsun. Eğer  $\text{Im}f = B$ , yani her  $b \in B$  için  $b = f(a)$  olacak şekilde bir  $a \in A$  varsa o zaman  $f$  ye bir **örten fonksiyon** denir.

**Örnek 1.2.10**  $A = \{1, 2, 3\}$ ,  $B = \{x, y, z, w\}$  için  $f = \{(1, y), (2, w), (3, y)\}$  fonksiyonunu göz önüne alalım.  $x, z \in B$  elemanları  $A$  daki elemanların görüntüleri olarak ifade edilemediğinden  $f_1$  örten fonksiyon değildir. Diğer taraftan  $|A| < |B|$  olması sebebiyle  $A$  dan  $B$  ye örten bir fonksiyon tanımlanamaz. Fakat  $g = \{(x, 3), (y, 1), (z, 3), (w, 2)\}$  ile tanımlı  $g: B \rightarrow A$  fonksiyonu için  $\text{Im}g = \{1, 2, 3\} = A$  olduğundan  $g$  örtendir. ▲

**Tanım 1.2.11** Birebir ve örten olan bir fonksiyona **birebir eşleme** denir.

**Teorem 1.2.12**  $A$  ve  $B$  sonlu kümeler,  $|A| = |B|$  ve  $f: A \rightarrow B$  bir fonksiyon olsun.  $f$  nin birebir olması için gerek ve yeter şart örten olmasıdır.

**Tanım 1.2.13**  $\emptyset \neq A$  bir küme olsun. Her  $a \in A$  için  $i_A(a) = a$  şeklinde tanımlı  $i_A: A \rightarrow A$  fonksiyonuna  $A$  üzerinde **birim fonksiyon** denir.

**Örnek 1.2.14**  $S = \{1, 2, 3\}$  üzerinde tanımlı  $i_S = \{(1, 1), (2, 2), (3, 3)\}$  fonksiyonu  $S$  üzerinde birim fonksiyondur. ▲

**Uyarı 1.2.15** Keyfi bir  $A$  kümesi üzerinde tanımlı birim fonksiyon bir birebir eşlemedir. ◆

## 1.2.2 Fonksiyonların Bileşkesi

Bu kısımda verilen fonksiyonlar yardımıyla yeni bir fonksiyon elde etmenin bir yolu olan bileşke işlemini tanımlayacağız.

**Tanım 1.2.16** Boş kümeden farklı  $A, B$  ve  $C$  kümeleri verilsin.  $f: A \rightarrow B$  ve  $g: B \rightarrow C$  fonksiyonları verildiğinde her  $a \in A$  için  $(g \circ f)(a) = g(f(a))$  şeklinde tanımlanan  $g \circ f: A \rightarrow C$  fonksiyonuna  $f$  ve  $g$  nin **bileşkesi** denir.

**Örnek 1.2.17**  $A = \{1, 2, 3, 4\}$ ,  $B = \{a, b, c, d\}$  ve  $C = \{r, s, t, u, v\}$  kümeleri üzerinde  $f: A \rightarrow B$  ve  $g: B \rightarrow C$  fonksiyonları

$$f = \{(1, b), (2, d), (3, a), (4, a)\}, \quad g = \{(a, u), (b, r), (c, r), (d, s)\}$$

şeklinde tanımlı olsun. Bu durumda  $g \circ f = \{(1, r), (2, s), (3, u), (4, u)\}$  dir. ▲



**Uyarı 1.2.18**  $g \circ f$  bileşke fonksiyonunun tanımlı olması her zaman  $f \circ g$  bileşke fonksiyonunun da tanımlı olmasını gerektirmez. Ayrıca  $f: A \rightarrow B$  ve  $g: B \rightarrow C$  fonksiyonları verildiğinde  $g \circ f: A \rightarrow C$  bileşke fonksiyonunu tanımlayabilmek için  $f$  nin değer kümesi ile  $g$  nin tanım kümesinin aynı olması gerekmez. Eğer  $f$  nin görüntü kümesi  $g$  nin tanım kümesinin bir altkümesi ise  $g \circ f: A \rightarrow C$  bileşke fonksiyonu tanımlanabilir.  $\blacklozenge$

**Teorem 1.2.19**  $f: A \rightarrow B$  ve  $g: B \rightarrow C$  iki fonksiyon olsun.

- (i) Eğer  $f$  ve  $g$  birebir ise o zaman  $g \circ f$  birebirdir.
- (ii) Eğer  $f$  ve  $g$  örten ise o zaman  $g \circ f$  örtendir.

**Sonuç 1.2.20**  $f: A \rightarrow B$  ve  $g: B \rightarrow C$  fonksiyonları birebir eşleme ise o zaman  $g \circ f$  bileşke fonksiyonu da bir birebir eşlemedir.

### 1.2.3 Fonksiyonların Tersi

Bu kısımda bir fonksiyonun tersi kavramını tanımlayacağız. Bir fonksiyonun tersinin var olması için gerek ve yeter şartları belirleyeceğiz.

**Tanım 1.2.21**  $R$ ,  $A$  dan  $B$  ye bir bağıntı olsun.  $B$  den  $A$  ya

$$R^{-1} = \{(b, a) : (a, b) \in R\}$$

şeklinde tanımlı  $R^{-1}$  bağıntısına  $R$  nin **tersi** denir.

**Örnek 1.2.22**  $A = \{1, 2, 3\}$  ve  $B = \{4, 5, 6\}$  kümeleri verildiğinde  $A$  dan  $B$  ye bir fonksiyon  $f = \{(1, 5), (2, 4), (3, 5)\}$  olsun. Bu durumda

$$f^{-1} = \{(5, 1), (4, 2), (5, 3)\}$$

$B$  den  $A$  ya bir bağıntı olmasına rağmen bir fonksiyon değildir.  $\blacktriangle$

**Teorem 1.2.23**  $A$  ve  $B$  kümeleri için  $f: A \rightarrow B$  bir fonksiyon olsun.  $f^{-1}$  bağıntısının  $B$  den  $A$  ya fonksiyon olması için gerek ve yeter şart  $f$  nin bir birebir eşleme olmasıdır. Ayrıca  $f$  bir birebir eşleme ise o zaman  $f^{-1}$  de bir birebir eşlemedir.

**Tanım 1.2.24**  $A$  ve  $B$  kümeleri için  $f: A \rightarrow B$  fonksiyonu verilmiş olsun. Eğer  $f$  bir birebir eşleme ise o zaman  $f^{-1}: B \rightarrow A$  fonksiyonuna  $f$  nin **tersi** denir.

**Örnek 1.2.25**  $f: \mathbb{R} \setminus \{2\} \rightarrow \mathbb{R} \setminus \{3\}$ ,  $f(x) = \frac{3x}{x-2}$  şeklinde tanımlı birebir ve örten fonksiyonu veriliyor.  $x \in \mathbb{R} \setminus \{3\}$  için  $f^{-1}(x)$  i belirleyelim.  $x \in \mathbb{R} \setminus \{3\}$  için  $(f \circ f^{-1})(x) = x$  olduğundan

$$(f \circ f^{-1})(x) = f(f^{-1}(x)) = \frac{3f^{-1}(x)}{f^{-1}(x) - 2} = x$$

eşitliği elde edilir. Gerekli hesaplamalar yapılırsa  $f^{-1}(x): \mathbb{R} \setminus \{3\} \rightarrow \mathbb{R} \setminus \{2\}$  fonksiyonu

$$f^{-1}(x) = \frac{2x}{x-3}$$

olarak elde edilir. ▲

### 1.3 Matrisler

Bu kısımda “matris” kavramını tanımlayıp bu kavramın bazı temel özelliklerini vereceğiz.

**Tanım 1.3.1**  $m, n \in \mathbb{Z}^+$  olsun. Bir  $A: \{1, 2, \dots, m\} \times \{1, 2, \dots, n\} \rightarrow \mathbb{R}$  fonksiyonuna  $\mathbb{R}$  üzerinde  $m \times n$  tipinde bir matris denir.  $A$  matrisinin girişleri  $A(i, j) = a_{ij}$  dir. Genellikle  $A$  matrisi için

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}$$

şeklinde  $m$  satır ve  $n$  sütundan oluşan dikdörtgensel gösterim kullanılır. Özel olarak eğer  $n = m$  ise o zaman

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix}$$

matrisine  $n \times n$  tipinde kare matris adı verilir.

**Uyarı 1.3.2**  $n, m \in \mathbb{Z}^+$  olsun.  $1 \leq i \leq m$  ve  $1 \leq j \leq n$  için  $a_{ij} \in \mathbb{R}$  olmak üzere  $m \times n$  tipinde bir  $A$  matrisi  $A = [a_{ij}]_{m \times n}$  ile de gösterilir. ◆

**Tanım 1.3.3**  $n, m, p, q \in \mathbb{Z}^+$  ve  $A = [a_{ij}]_{m \times n}$ ,  $B = [b_{ij}]_{p \times q}$  de  $\mathbb{R}$  üzerinde iki matris olsun. Eğer  $m = p$ ,  $n = q$  ve her  $i, j$  için  $a_{ij} = b_{ij}$  ise  $A$  ile  $B$  matrisleri eşittir denir.

**Uyarı 1.3.4**  $n, m \in \mathbb{Z}^+$  olsun.  $\mathbb{R}$  kümesi üzerinde tanımlı  $m \times n$  tipindeki matrislerin kümesi  $M_{m \times n}(\mathbb{R})$  ile gösterilir. Eğer  $m = n$  ise  $n \times n$  tipindeki matrislerin kümesi  $M_n(\mathbb{R})$  ile gösterilir.  $\blacklozenge$

### 1.3.1 Matrislerde Toplama

**Tanım 1.3.5**  $n, m \in \mathbb{Z}^+$  ve  $A = [a_{ij}]$ ,  $B = [b_{ij}] \in M_{m \times n}(\mathbb{R})$  olsun.  **$A$  ile  $B$  matrislerinin toplamı**  $[a_{ij}]_{m \times n} + [b_{ij}]_{m \times n} = [a_{ij} + b_{ij}]_{m \times n}$  ile tanımlıdır.

**Örnek 1.3.6**  $M_{2 \times 3}(\mathbb{Z})$  kümesi üzerinde

$$\begin{bmatrix} 3 & -2 & 1 \\ 2 & 2 & 5 \end{bmatrix} + \begin{bmatrix} 2 & 1 & 0 \\ 2 & -1 & 7 \end{bmatrix} = \begin{bmatrix} 5 & -1 & 1 \\ 4 & 1 & 12 \end{bmatrix}$$

dir.  $\blacktriangle$

**Teorem 1.3.7**  $n, m \in \mathbb{Z}^+$  ve  $A = [a_{ij}]_{m \times n}$ ,  $B = [b_{ij}]_{m \times n}$ ,  $C = [c_{ij}]_{m \times n} \in M_{m \times n}(\mathbb{R})$  olsun.

- (i)  $(A + B) + C = A + (B + C)$  dir.
- (ii)  $A + 0 = 0 + A = A$  olacak şekilde  $0 = [0_{ij}]_{m \times n} \in M_{m \times n}(\mathbb{R})$  vardır.
- (iii)  $A + (-A) = (-A) + A = 0$  olacak şekilde  $-A = [-a_{ij}]_{m \times n} \in M_{m \times n}(\mathbb{R})$  vardır.
- (iv)  $A + B = B + A$  dır.

### 1.3.2 Matrislerde Çarpma

**Tanım 1.3.8**  $m, n, p \in \mathbb{Z}^+$  olsun.  $\mathbb{R}$  üzerinde tanımlı  $A = [a_{ij}]_{m \times n}$  ve  $B = [b_{ij}]_{n \times p}$  matrisleri için  $(i, j)$ -yinci bileşeni  $\sum_{k=1}^n a_{ik}b_{kj}$  olan  $m \times p$  tipindeki matrise  **$A$  ile  $B$  matrislerinin çarpımı** adı verilir.

**Örnek 1.3.9**  $A = \begin{bmatrix} 3 & -2 \\ 0 & 4 \\ 1 & -3 \\ 5 & 1 \end{bmatrix}$  ve  $B = \begin{bmatrix} 2 & 1 & 0 \\ 4 & -3 & 7 \end{bmatrix}$  matrisleri için

$$A \cdot B = \begin{bmatrix} -2 & 9 & -14 \\ 16 & -12 & 28 \\ -10 & 10 & -21 \\ 14 & 2 & 7 \end{bmatrix}$$

şeklindedir.  $\blacktriangle$

**Teorem 1.3.10**  $m, n, p, q \in \mathbb{Z}^+$  için  $\mathbb{R}$  üzerinde tanımlı  $A = [a_{ij}]_{m \times n}$ ,  $B = [b_{ij}]_{n \times p}$  ve  $C = [c_{ij}]_{p \times q}$  matrisleri verilmiş olsun. Bu durumda  $A \cdot (B \cdot C) = (A \cdot B) \cdot C$  dir.

**Teorem 1.3.11**  $m, n, p, q \in \mathbb{Z}^+$  için  $\mathbb{R}$  üzerinde tanımlı  $A = [a_{ij}]_{m \times n}$ ,  $B = [b_{ij}]_{n \times p}$ ,  $C = [c_{ij}]_{p \times q}$  ve  $D = [d_{ij}]_{p \times q}$  matrisleri verilmiş olsun.

(i)  $A \cdot (B + C) = (A \cdot B) + (A \cdot C)$  dir.

(ii)  $(B + C) \cdot D = (B \cdot D) + (C \cdot D)$  dir.

**Tanım 1.3.12**  $n \in \mathbb{Z}^+$  ve  $1 \leq i, j \leq n$  için

$$\delta_{ij} = \begin{cases} 1, & i = j \text{ ise} \\ 0, & i \neq j \text{ ise} \end{cases}$$

olmak üzere  $I_n = [\delta_{ij}]_{n \times n}$  şeklinde tanımlıdır.  $\delta_{ij}$  ye **Kronecker deltası** adı verilir.

$n \in \mathbb{Z}^+$  olmak üzere  $I_n$  matrislerinin matrislerin çarpımında önemli bir yeri vardır.

**Teorem 1.3.13**  $m, n \in \mathbb{Z}^+$  için  $\mathbb{R}$  üzerinde tanımlı  $A = [a_{ij}]_{m \times n}$  matrisi verilmiş olsun.

(i)  $I_m \cdot A = A$  dir.

(ii)  $A \cdot I_n = A$  dir.

**Tanım 1.3.14**  $n \in \mathbb{Z}^+$  için  $A \in M_n(\mathbb{R})$  olsun.  $A \cdot B = I_n$  olacak şekilde bir  $B \in M_n(\mathbb{R})$  bulunabiliyorsa o zaman  $B$  ye  $A$  nın çarpmaya göre **sağ tersi** denir. Benzer şekilde  $B \cdot A = I_n$  olacak şekilde bir  $B \in M_n(\mathbb{R})$  bulunabiliyorsa o zaman  $B$  ye  $A$  nın çarpmaya göre **sol tersi** denir. Eğer  $A \cdot B = B \cdot A = I_n$  olacak şekilde bir  $B \in M_n(\mathbb{R})$  bulunabiliyorsa o zaman  $B$  ye  $A$  nın çarpmaya göre **tersi**,  $A$  ya **tersinir matris** adı verilir.

**Uyarı 1.3.15**  $n \in \mathbb{Z}^+$  olmak üzere  $\mathbb{R}$  üzerinde tanımlı bütün tersinir matrislerin kümesi  $GL_n(\mathbb{R})$  ile gösterilir.  $A \in M_n(\mathbb{R})$  için  $A$  matrisinin determinantı  $\det(A)$  ise o zaman  $SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) \mid \det(A) = 1\}$  şeklindedir.  $\blacklozenge$

## 1.4 Tamsayılar

Bu kısımda tamsayıların bazı önemli özellikleri verilecektir. Tamsayılarda en büyük ortak bölen kavramı üzerinde durulacaktır.

### 1.4.1 Tamsayıların Temel Özellikleri

**Önerme 1.4.1 (Çarpmanın Sadeleşme Özelliği)**  $x, y, z \in \mathbb{Z}$  ve  $x \neq 0$  olsun. Eğer  $yx = zx$  ise  $y = z$  dir.

**Önerme 1.4.2 (Sıfır Bölensizlik Özelliği)**  $x, y \in \mathbb{Z}$  olsun. Eğer  $xy = 0$  ise  $x = 0$  veya  $y = 0$  dir.

**Önerme 1.4.3**  $\mathbb{Z}$  tamsayılar kümesi üzerinde sadeleşme özelliği ile sıfır bölensizlik özelliği birbirine denktir.

**Tanım 1.4.4**  $n \geq 2$  tamsayısı için  $x_1, x_2, \dots, x_n$  tamsayılarının toplamı

$$x_1 + x_2 + \dots + x_{n-1} + x_n = (x_1 + x_2 + \dots + x_{n-1}) + x_n$$

şeklinde ardışık olarak tanımlıdır.

**Teorem 1.4.5 (Genelleştirilmiş Dağılma Özelliği)**  $n \geq 2$  tamsayısı ve  $x_1, x_2, \dots, x_n, y$  tamsayıları için

$$y(x_1 + x_2 + \dots + x_n) = yx_1 + yx_2 + \dots + yx_n$$

ve

$$(x_1 + x_2 + \dots + x_n)y = x_1y + x_2y + \dots + x_ny$$

dir.

**Teorem 1.4.6 (Genelleştirilmiş Birleşme Özelliği)**  $m, n \in \mathbb{Z}^+$ ,  $n \geq 3$  ve  $1 \leq m < n$  olmak üzere  $x_1, x_2, \dots, x_n$  tamsayıları için

$$(x_1 + x_2 + \dots + x_m) + (x_{m+1} + x_{m+2} + \dots + x_n) = x_1 + \dots + x_m + x_{m+1} + \dots + x_n$$

ve

$$(x_1x_2 \dots x_m)(x_{m+1}x_{m+2} \dots x_n) = x_1 \dots x_mx_{m+1} \dots x_n$$

dir.

**Tanım 1.4.7**  $0 \neq x \in \mathbb{Z}$  için  $x^0 = 1$ , herhangi bir  $x \in \mathbb{Z}$  için  $x^1 = x$  ve  $1 \leq n$  olmak üzere  $x^{n+1} = x^n x$  şeklinde tanımlıdır.

**Teorem 1.4.8**  $m, n \in \mathbb{Z}^+$  ve  $x, y \in \mathbb{Z}$  için

(i)  $x^m x^n = x^{m+n}$

(ii)  $(x^m)^n = x^{mn}$

(iii)  $(xy)^m = x^m y^m$

dir.

### 1.4.2 Tamsayılarda Bölme ve Özellikleri

**Teorem 1.4.9 (Bölüm Algoritması)**  $x, y \in \mathbb{Z}$  ve  $y \neq 0$  olsun. Bu durumda  $x = qy + r$  ve  $0 \leq r < |y|$  olacak şekilde tek türlü belirli  $q, r \in \mathbb{Z}$  vardır.  $x = qy + r$  yazılışında  $q$  ya **bölüm**,  $r$  ye **kalan** adı verilir.

**Örnek 1.4.10** Teorem 1.4.9 da (i)  $x = 13, y = 5$  alınırsa  $13 = 5 \cdot 2 + 3$  ve  $0 \leq 3 < 5$  tir.

(ii)  $x = -13, y = 5$  alınırsa  $-13 = 5 \cdot (-3) + 2$  ve  $0 \leq 2 < 5$  tir.

(iii)  $x = 2, y = 9$  alınırsa  $2 = 9 \cdot 0 + 2$  ve  $0 \leq 2 < 9$  dur. ▲

**Tanım 1.4.11 (Tamsayılarda Bölünebilme)**  $a, b \in \mathbb{Z}$  olsun. Eğer  $a = bc$  olacak şekilde bir  $c \in \mathbb{Z}$  varsa o zaman  $b, a$  yı **böler** ya da  $a, b$  ile **bölünür** denir ve  $b \mid a$  ile gösterilir. Eğer  $b, a$  yı bölmüyorsa bu durum  $b \nmid a$  ile gösterilir.

**Uyarı 1.4.12** Her  $c \in \mathbb{Z}$  için  $0 = 0c$  olduğundan  $0 \mid 0$  dir. Diğer taraftan  $0 \neq a \in \mathbb{Z}$  için  $0 \nmid a$  dir. Eğer  $0 \mid a$  ise  $a = 0$  dir. ◆

**Örnek 1.4.13**  $24 = 3 \cdot 8$  olduğundan  $3 \mid 24$  ve  $54 = (-6)(-9)$  olduğundan  $-6 \mid 54$  tür. Fakat  $3 \nmid 17$  ve  $-6 \nmid (-13)$  tür. ▲

**Teorem 1.4.14**  $a, b, c \in \mathbb{Z}$  için

(i)  $\pm 1 \mid a$  ve  $\pm a \mid a$  dir.

(ii)  $a \mid \pm 1 \Leftrightarrow a = \pm 1$  dir.

(iii) Eğer  $a \mid b$  ve  $b \mid c$  ise o zaman  $a \mid c$  dir.

(iv) Eğer  $a \mid b$  ve  $b \mid a$  ise o zaman  $a = \pm b$  dir.

(v) Eğer  $a \mid b$  ise o zaman  $\pm a \mid \pm b$  dir.

(vi) Eğer  $a \mid b$  ve  $a \mid c$  ise o zaman her  $x, y \in \mathbb{Z}$  için  $a \mid bx + cy$  dir.

**Tanım 1.4.15**  $p \geq 2$  bir tamsayı olsun. Eğer  $p$  nin bölenleri sadece  $\pm 1$  ve  $\pm p$  ise o zaman  $p$  ye bir **asal sayı** denir.

**Tanım 1.4.16**  $a$  ve  $b$  her ikisi birden sıfır olmayan iki tamsayı olsun. Bu durumda

(i)  $d \in \mathbb{Z}^+$ ,

(ii)  $d \mid a$  ve  $d \mid b$ ,

(iii)  $c \in \mathbb{Z}$  için  $c \mid a$  ve  $c \mid b$  ise  $c \mid d$

şartlarını sağlayan  $d$  tamsayısına  $a$  ile  $b$  nin **en büyük ortak böleni** adı verilir ve  $(a, b)$  veya  $\text{ebob}(a, b)$  ile gösterilir.

**Teorem 1.4.17** Her ikisi birden sıfır olmayan  $a$  ve  $b$  tamsayılarının en büyük ortak böleni  $d$  vardır. Ayrıca  $d = am + bn$  olacak şekilde  $m$  ve  $n$  tamsayıları mevcut olup bu yazılışa sahip en küçük pozitif tamsayı  $d$  dir.

**Teorem 1.4.18 (Euclid Algoritması)**  $a, b \in \mathbb{Z}$  ve  $a > 0$  olsun. Eğer  $a \mid b$  ise o zaman  $\text{ebob}(a, b) = a$  dir ve  $\text{ebob}(a, b) = 1 \cdot a + 0 \cdot b$  dir. Eğer  $a \nmid b$  ise o zaman Bölüm Algoritması'nın ard arda uygulanması sonucunda bir  $s \geq 1$  için

$$\begin{aligned} b &= q_1 a + r_1, & 0 < r_1 < a \\ a &= q_2 r_1 + r_2, & 0 < r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3, & 0 < r_3 < r_2 \\ &\vdots & \vdots \\ r_{s-2} &= q_s r_{s-1} + r_s, & 0 < r_s < r_{s-1} \\ & & r_{s-1} = q_{s+1} r_s \end{aligned}$$

eşitlikleri elde edilir.  $\text{ebob}(a, b)$  sıfırdan farklı son kalan olan  $r_s$  ye eşittir.  $r_s = (a, b) = x_0 a + y_0 b$  eşitliğindeki  $x_0$  ve  $y_0$  değerleri her  $1 \leq i \leq s$  için  $r_i$ ,  $a$  ve  $b$  nin lineer kombinasyonu olarak yazılarak elde edilebilir.

**Örnek 1.4.19** Euclid algoritması yardımıyla 1492 ile 1776 nın en büyük ortak bölenini bulalım.

$$\begin{aligned} 1776 &= 1492 \cdot 1 + 284 \\ 1492 &= 284 \cdot 5 + 72 \\ 284 &= 72 \cdot 3 + 68 \\ 72 &= 68 \cdot 1 + 4 \\ 68 &= 4 \cdot 17 \end{aligned}$$

olup sıfırdan farklı son kalan 4 tür. Bu sebeple  $\text{ebob}(1492, 1776) = 4$  tür. Şimdi  $\text{ebob}(1492, 1776) = 1492m + 1776n$  olacak biçimdeki  $m$  ve  $n$  tamsayılarını bulalım. Yukarıdaki eşitliklerden

$$\begin{aligned} 284 &= 1776 \cdot 1 + 1492 \cdot (-1) \\ 72 &= 1492 \cdot 1 + 284 \cdot (-5) \\ 68 &= 284 \cdot 1 + 72 \cdot (-3) \\ 4 &= 72 \cdot 1 + 68 \cdot (-1) \end{aligned}$$

elde edilir. Sıfırdan farklı son kalanı içeren  $72 = 68 \cdot 1 + 4$  eşitliğinden başlayarak  $1776 = 1492 \cdot 1 + 284$  eşitliğine kadar her adımda kalanların yerine yazılmasıyla

$$\begin{aligned} 4 &= 72 \cdot 1 + 68 \cdot (-1) \\ &= 72 \cdot 1 + (284 \cdot 1 + 72 \cdot (-3)) \cdot (-1) \\ &= 72 \cdot 4 + 284 \cdot (-1) \\ &= (1492 \cdot 1 + 284 \cdot (-5)) \cdot 4 + 284 \cdot (-1) \\ &= 1492 \cdot 4 + 284 \cdot (-21) \\ &= 1492 \cdot 4 + (1776 \cdot 1 + 1492 \cdot (-1)) \cdot (-21) \\ &= 1492 \cdot 25 + 1776 \cdot (-21) \end{aligned}$$

$m = 25$  ve  $n = -21$  bulunur. ▲

**Tanım 1.4.20** Eğer sıfırdan farklı  $a$  ve  $b$  tamsayıları için  $\text{ebob}(a, b) = 1$  ise o zaman  $a$  ile  $b$  aralarında asaldır denir.

**Teorem 1.4.21**  $a, b, c \in \mathbb{Z}$  olsun. Eğer  $a \mid bc$  ve  $\text{ebob}(a, b) = 1$  ise o zaman  $a \mid c$  dir.

**Teorem 1.4.22 (Euclid Teoremi)**  $x, y \in \mathbb{Z}$  ve  $p$  bir asal sayı olsun. Eğer  $p \mid xy$  ise o zaman  $p \mid x$  veya  $p \mid y$  dir.

Aşağıdaki teorem gereğince 1 den büyük her tamsayı ya asal ya da asal sayıların sonlu bir çarpımıdır.

**Teorem 1.4.23 (Aritmetiğin Temel Teoremi)** Her  $1 < a \in \mathbb{Z}$  için  $a = p_1 p_2 \dots p_r$  ve  $p_1 \leq p_2 \leq \dots \leq p_r$  olacak biçimde  $p_1, p_2, \dots, p_r$  asal sayıları vardır.

**Uyarı 1.4.24**  $1 < a \in \mathbb{Z}$  olsun. Bu durumda

$$a = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}$$

olacak şekilde  $p_1 < p_2 < \dots < p_k$  asal sayıları ve  $m_1, m_2, \dots, m_k \in \mathbb{Z}^+$  vardır ve bu yazılış çarpanların sırası farkıyla tek türdür. Bu yazılışta  $1 \leq i \leq k$  için  $m_i$  ye  $p_i$  nin **katlılığı** adı verilir. ◆

**Teorem 1.4.25** Sonsuz çoklukta asal sayı vardır.