

## I. MODÜLER ARİTMETİK

$a, b, m$  birer tamsayı ve  $m > 1$  olmak üzere, tamsayılar kümesi üzerinde tanımlanan

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

bir denklik bağıntısıdır.

$\beta$  denklik bağıntısı olduğundan

$\forall (a, b) \in \beta$  için,

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

biçiminde yazılır. "**m modülüne göre a sayısı b ye denktir**" denir.

Burada;

$$\begin{array}{r|l} a & m \\ \hline = & k \\ b & \end{array} \text{ dir.}$$

$k$  bir tamsayı olmak üzere,

$$a = b + m \cdot k \text{ dir.}$$

Örnek:

$A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$  kümesinde

$$\beta = \{(x, y) : 3 \mid (x - y)\}$$

denklik bağıntısıdır.

$(7, 1) \in \beta$  olduğu için  $7 \equiv 1 \pmod{3}$

$(7, 10) \in \beta$  olduğu için  $7 \equiv 10 \pmod{3}$

$(1, 4) \in \beta$  olduğu için  $1 \equiv 4 \pmod{3}$

$(8, 5) \in \beta$  olduğu için  $8 \equiv 5 \pmod{3}$  olur.

Örnek:

$$\begin{array}{r|l} 29 & 3 \\ \hline = 27 & 9 \\ 2 & \end{array}$$

29 un 3 ile bölümünden kalan 2 olduğu için

$$29 \equiv 2 \pmod{3}$$

yazılabilir. Ancak bu denklik istenildiği kadar uzatılabilir.

$$\dots \equiv 32 \equiv 29 \equiv 26 \equiv 23 \equiv 20 \equiv \dots \pmod{3}$$

Örnek:

**Aşağıdakilerden hangisi yanlıştır?**

A)  $57893 \equiv 3 \pmod{10}$

B)  $6796 \equiv 1 \pmod{5}$

C)  $2438 \equiv 2 \pmod{3}$

D)  $1574 \equiv 0 \pmod{2}$

E)  $5163 \equiv 1 \pmod{3}$

Örnek:

$$5 - x \equiv 4 \pmod{7}$$

**olduğuna göre, x in alabileceği en küçük pozitif iki farklı tamsayının toplamı kaçtır?**

A) 1      B) 4      C) 8      D) 9      E) 10

Örnek:

$$15 \equiv 3 \pmod{m}$$

**olduğuna göre, m nin alabileceği değerlerin toplamı kaçtır?**

A) 29      B) 28      C) 27      D) 26      E) 25

Örnek:

$$a \equiv 2 \pmod{5}$$

**olduğuna göre, a nın alabileceği değerlerin kümesini bulalım.**

**Kural:**

Tamsayıların  $m$  sayma sayısı ile bölünmesiyle elde edilen kalanlar:

$$0, 1, 2, 3, \dots, (m - 1) \text{ dir.}$$

Her tamsayı  $m$  ile bölündüğünde hangi kalana veriyorsa o kalana denktir. Bu kalanların her biri belirlediği denklik sınıfının temsilci elemanı olarak alınır, denklik sınıfları,

$$\bar{0}, \bar{1}, \bar{2}, \bar{3}, \dots, (\overline{m-1}) \text{ olur.}$$

Bu denklik sınıflarının kümesine  $m$  nin kalan sınıflarının kümesi de denir ve  $Z / m$  biçiminde gösterilir.

Buna göre,  $Z / m = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \dots, \overline{m-1}\}$  olur.

**ÖZELLİKLER**

$n$  bir sayma sayısı ve  $k$  bir tamsayı

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

$$x \equiv y \pmod{m}$$

olmak üzere,

$$1) a + x \equiv b + y \pmod{m}$$

$$2) a - x \equiv b - y \pmod{m}$$

$$3) a \cdot x \equiv b \cdot y \pmod{m}$$

$$4) x^n \equiv y^n \pmod{m}$$

$$5) k \cdot a \equiv k \cdot b \pmod{m} \text{ olur.}$$

Örnek:

$$2^{73}$$

sayısının 5 ile bölünmesiyle elde edilen kalan kaçtır?

- A) 0      B) 1      C) 2      D) 3      E) 4

Örnek:

$$3^{47}$$

sayısının birler basamağındaki rakam kaçtır?

- A) 2      B) 3      C) 6      D) 7      E) 8

Örnek:

$$16^{2003} \equiv x \pmod{7}$$

olduğuna göre,  $x$  aşağıdakilerden hangisidir?

- A) 1      B) 2      C) 3      D) 4      E) 5

Örnek:

$$(1991)^{2002} \equiv x \pmod{5}$$

olduğuna göre,  $x$  kaçtır?

- A) 0      B) 1      C) 2      D) 3      E) 4

Örnek:

$$(2003)^x \equiv 2 \pmod{5}$$

olduğuna göre,  $x$  in en küçük doğal sayı değeri kaçtır?

- A) 0      B) 1      C) 3      D) 7      E) 10

Örnek:

$$(102)^{25}$$

sayısının 8 ile bölünmesiyle elde edilen kalan kaçtır?

- A) 0      B) 1      C) 2      D) 3      E) 6

Örnek:

$$(2000)^{48}$$

sayısının 6 ile bölünmesiyle elde edilen kalan kaçtır?

- A) 0      B) 1      C) 2      D) 3      E) 4

Örnek:

$$3^{45} + 2^{38} - 5^{24}$$

sayısının 8 ile bölümünden kalan kaçtır?

- A) 0      B) 1      C) 2      D) 3      E) 4

Örnek:

$$6^{2000} \equiv x \pmod{7}$$

olduğuna göre, x kaçtır?

- A) 0      B) 1      C) 2      D) 3      E) 5

Örnek:

n bir sayma sayısıdır.

$$(2n + 1)^2 \equiv x \pmod{8}$$

olduğuna göre, x kaçtır?

- A) 0      B) 1      C) 2      D) 3      E) 4

Örnek:

n bir doğal sayıdır.

$$3^{2n} + 7$$

sayısının 8 ile bölümünden kalan kaçtır?

- A) 0      B) 1      C) 2      D) 3      E) 6

### ÖZELLİK

$x$ ,  $m$  nin tam katı olmayan pozitif bir tamsayı ve  $m$  bir asal sayı ise,

$$x^{m-1} \equiv 1 \pmod{m} \text{ dir.}$$

$x$  in  $(m - 1)$  den daha küçük kuvvetinde de 1 bulunabilir.

Örnek:

$$3^6 \equiv 1 \pmod{7}$$

$$4^6 \equiv 1 \pmod{7}$$

$$7^{10} \equiv 1 \pmod{11}$$

$$2^3 \equiv 1 \pmod{7}$$

$$2^6 \equiv 1 \pmod{7}$$

Örnek:

 $x$  bir sayma sayısıdır.

$$3^x \equiv 1 \pmod{19}$$

olduğuna göre,  $x$  in en küçük değeri kaçtır?

- A) 1 B) 5 C) 7 D) 10 E) 18

Örnek:

$$22^{16} + 4^{15} + 6^{14} \equiv x \pmod{11}$$

olduğuna göre,  $x$  kaçtır?

- A) 0 B) 2 C) 5 D) 9 E) 10

Uyarı: $Z / m$  deki işlemler (mod  $m$ ) ye göre yapılır.

Örnek:

 $Z / 5$  te,

$$\bar{4} \cdot (\bar{2} + \bar{4}) + \bar{3}$$

işleminin sonucu kaçtır?

- A)
- $\bar{0}$
- B)
- $\bar{1}$
- C)
- $\bar{2}$
- D)
- $\bar{3}$
- E)
- $\bar{4}$

Örnek:

 $Z / 5$  te,

$$3x + 4 \equiv 2$$

önermesinin doğruluk kümesi aşağıdakilerden hangisidir?

- A)
- $\{\bar{0}\}$
- B)
- $\{\bar{1}\}$
- C)
- $\{\bar{0}, \bar{1}\}$
- D)
- $\{\bar{2}, \bar{1}\}$
- E)
- $\{\bar{0}, \bar{2}\}$

Örnek:

 $Z / 7$  de,  $5x = 2$  denkleminin kökü aşağıdakilerden hangisidir?

- A)
- $\bar{0}$
- B)
- $\bar{1}$
- C)
- $\bar{2}$
- D)
- $\bar{3}$
- E)
- $\bar{6}$

Örnek:

$$f(x) = 3x + 1$$

olduğuna göre,  $Z / 4$  de  $f^{-1}(x)$  aşağıdakilerden hangisine eşittir?

- A)
- $\bar{3} \cdot x + \bar{2}$
- B)
- $\bar{3} \cdot x + \bar{1}$
- C)
- $\bar{2} \cdot x + \bar{1}$
- 
- D)
- $\bar{2} \cdot x + \bar{2}$
- E)
- $\bar{1} \cdot x + \bar{3}$

Örnek:

$$f(x) = 2 \cdot x$$

olduğuna göre,  $(f \circ f)(x)$  işleminin  $Z / 3$  deki sonucu aşağıdakilerden hangisidir?

- A)
- $\bar{2} \cdot x + \bar{1}$
- B)
- $\bar{2} \cdot x + \bar{2}$
- C)
- $\bar{1} \cdot x$
- 
- D)
- $\bar{1} \cdot x + \bar{1}$
- E)
- $\bar{1} \cdot x + \bar{2}$

Örnek:

$$f(x) = \frac{1}{x}$$

olduğuna göre,  $Z / 5$  de  $f(2) + f(3) + f(4)$  kaçtır?

- A)  $\bar{0}$       B)  $\bar{1}$       C)  $\bar{2}$       D)  $\bar{3}$       E)  $\bar{4}$

Örnek:

$Z / 7$  de  $x^2 = 2$  açık önermesinin doğruluk kümesi aşağıdakilerden hangisidir?

- A)  $\{\bar{1}, \bar{2}\}$       B)  $\{\bar{1}, \bar{3}\}$       C)  $\{\bar{3}\}$   
 D)  $\{\bar{3}, \bar{4}\}$       E)  $\{\bar{4}\}$

Örnek:

Bir asker 5 günde bir nöbet tutmaktadır.

**Bu asker ilk nöbetini pazartesi günü tuttuğuna göre, 58. nöbetini hangi gün tutar?**

- A) Pazartesi      B) Salı      C) Perşembe  
 D) Cuma      E) Cumartesi

Örnek:

Bugün günlerden salıdır.

**460 gün önce doğan bir çocuk hangi gün doğmuştur?**

- A) Salı      B) Çarşamba      C) Perşembe  
 D) Cuma      E) Cumartesi

Örnek:

**Tam 12 yi gösterirken çalıştırılan bir saatin akrebi, 2006 saatlik süre dolduğu anda kaç gösterir?**

- A) 2      B) 3      C) 4      D) 5      E) 6

Örnek:

**Saat şu anda 13:30 olduğuna göre, 2410 saat sonra, saat kaçtır?**

- A) 10:00      B) 10:30      C) 11:30  
 D) 19:30      E) 23:30