Buna göre, aşağıdaki açıklamaları yapabiliriz.

1. $a \equiv b \pmod m$ ise a ve b aynı kalan sınıfına aittir.
2. $a \equiv b \pmod m$ ise a ile b nin farkı, m ile tam bölünür.
3. $a \equiv k \pmod m$ ve $0 \le k < m$ ise a nın, m ile bölünmesinden kalan k dır.
4. $a \equiv 0 \pmod m$ ise a sayısı m ile tam bölünür.

ÖRNEK 1.46

Tam sayılar kümesinin 3, 4 ve 6 ile bölünmesinden elde edilen kalan sınıflarının kümesini ayrı ayrı yazalım.

$Z / 3 = \{\overline{0}, \overline{1}, \overline{2}\}$ dir.

$Z / 4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ tür.

$Z / 6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$ dir.

ÖRNEK 1.47

Tam sayılarda 2 ile bölündüğünde, elde edilen kalan sınıflarını ve Z / 2 kümesini yazalım.

Kalan sınıfları:

$\overline{0} = \{ ..., -4, -2, 0, 2, 4, ...\}$ ve $\overline{1} = \{ ..., -3, -1, 1, 3,...\}$ dir.

$Z / 2 = \{\overline{0}, \overline{1}\}$ olur.

b. Tam Sayılar Kümesinde Modüle Göre, Kalan Sınıfların Özelikleri

1. Kalan sınıflar tam sayılar kümesinin, ikişer ikişer ayrık alt kümeleridir.

$\overline{0}, \overline{1}, \overline{2}, ..., \overline{(m - 1)}$ kümeleri m modülüne göre, kalan sınıflar olsun.

2. Kalan sınıflarının birleşimi, tam sayılar kümesini verir.

$\overline{0} \cap \overline{1} = \varnothing, ..., \overline{1} \cap \overline{2} = \varnothing, ..., \overline{(m - 2)} \cap \overline{(m - 1)} = \varnothing$ dir.

3. Kalan sınıflarının hiçbiri, boş küme değildir.

$\overline{0} \cup \overline{1} \cup \overline{2} \cup ..., \cup \overline{(m - 1)} = Z$ dir.

c. Teoremler

Her a, b, c, d, x ∈ Z ve m, n ∈ Z^+, m > 1 için;

a ≡ b (mod m) ve c ≡ d (mod m) ise,

1, a ± c ≡ b ± d (mod m)

2. a . c ≡ b . d (mod m)

3. a ± x ≡ b ± x (mod m)

4. a . x ≡ b . x (mod m)

5. $a^n \equiv b^n$ (mod m)

Bu teoremleri ispat etmeden, örneklerle doğruluğunu gösterelim.

ÖRNEK 1.48

54 ≡ 2 (mod 4) ve 69 ≡ 1 (mod 4) ise taraf tarafa toplarsak,

(54 + 69) ≡ (2 + 1) (mod 4)

123 ≡ 3 (mod 4) olur.

ÖRNEK 1.49

29 ≡ 1 (mod 7) ve 33 ≡ 5 (mod 7) ise taraf tarafa çarparsak,

(29. 33) ≡ (1 . 5) (mod 7)

957 ≡ 5 (mod 7) olur.

ÖRNEK 1.50

5^{24} sayısını, 7 ile bölünmesinden elde edilen kalanı bulalım.

$5^2 \equiv 4$ (mod 7)

x $5^4 \equiv 2$ (mod 7) } Taraf tarafa toplarsak

$5^2 . 5^4 \equiv 4 . 2$ (mod 7)

$5^6 \equiv 1$ (mod 7)

$(5^6)^4 \equiv 1^4$ (mod 7)

$5^{24} \equiv 1$ (mod 7)

Buna göre, 5^{24} sayısının 7 ile bölünmesinden kalan 1 dir.

ç. Kalan Sınıflar Kümesinde Toplama ve Çarpma İşlemleri

m, pozitif tam sayı olmak üzere, m modülüne göre, kalan sınıflarının kümesi;

$Z / m = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, ..., \overline{(m-1)}\}$ dir.

Kalan sınıfları kümesinde, toplama işlemi $\oplus$ sembolü ile, çarpma işlemi $\odot$ sembolü ile gösterilir.

$\overline{a}, \overline{b} \in Z / m$ olduğuna göre,

1. Toplama işlemi : $\overline{a} \oplus \overline{b} = \overline{a + b}$ dir.
2. Çarpma işlemi: $\overline{a} \odot \overline{b} = \overline{a \cdot b}$ dir.

ÖRNEK 1.51

$Z / 5$ kümesinde, toplama ve çarpma işlemleri yaparsak, $Z / 5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ dir.

Kalanlar sınıfı kümesindeki, $\overline{2}$ ve $\overline{4}$ sayıları için,

1. Toplama işlemi : $\overline{2} \oplus \overline{4} = \overline{6} = \overline{1}$ olur.
2. Çarpma işlemi: $\overline{2} \odot \overline{4} = \overline{2 \cdot 4} = \overline{8} = \overline{3}$ olur.

ÖRNEK 1.52

$Z / 7$ kümesinde, toplama ve çarpma işlemleri yaparsak,

$Z / 7 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$ dir. Buna göre, bazı sayılar için,

$\overline{3} \oplus \overline{5} = \overline{3 + 5} = \overline{8} = \overline{1}$ dir.

$\overline{6} \oplus \overline{4} = \overline{6 + 4} = \overline{10} = \overline{3}$ tür.

$\overline{3} \odot \overline{6} = \overline{3 \cdot 6} = \overline{18} = \overline{4}$ tür.

$\overline{5} \odot \overline{4} = \overline{5 \cdot 4} = \overline{20} = \overline{6}$ dır.

d. Kalan Sınıflar Kümesinde Toplama ve Çarpma İşleminin Özelikleri

$\bar{a}, \bar{b}, \bar{c} \in Z/m$ olmak üzere, $\oplus$ ve $\odot$ işlemleri için aşağıdaki özelikler vardır.

1. Kapalılık özeliği vardır.

$\bar{a} \oplus \bar{b} = \bar{a} + \bar{b} \in Z/m$

$\bar{a} \odot \bar{b} = \overline{a \cdot b} \in Z/m$

2. Değişme özeliği vardır.

$\bar{a} \oplus \bar{b} = \bar{b} \oplus \bar{a}$

$\bar{a} \odot \bar{b} = \bar{b} \odot \bar{a}$

3. Birleşme özeliği vardır.

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

$\bar{a} \odot (\bar{b} \odot \bar{c}) = (\bar{a} \odot \bar{b}) \odot \bar{c}$

4. Birim (etkisiz) elemanı vardır.

$\bar{0} \oplus \bar{x} = \bar{x} \oplus 0 = \bar{x}$

$\bar{1} \odot \bar{x} = \bar{x} \odot \bar{1} = \bar{x}$

5. Toplama işleminin ters elemanı vardır.

$\bar{x} \oplus (\overline{-x}) = (\overline{-x}) \oplus \bar{x} = \bar{0}$ ($\bar{x}$ in tersi $\overline{-x}$ dir.)

Bu özelliklerden yararlanarak, $(Z/m, \oplus)$ sistemi değişmeli bir gruptur.

6. $\odot$ işleminin $\oplus$ işlemi üzerinde sağdan ve soldan dağılma özeliği vardır.

$\bar{a} \odot (\bar{b} \oplus \bar{c}) = (\bar{a} \odot \bar{b}) \oplus (\bar{a} \odot \bar{c})$

$(\bar{a} \oplus \bar{b}) \odot c = (\bar{a} \odot \bar{c}) \oplus (\bar{b} \odot \bar{c})$

ÖRNEK 1.53

$Z / 5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ kümesinde, toplama ve çarpma işlemlerinin tablosunu yaparak, elemanlarının terslerini bulalım.

$\oplus$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$\odot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Tablodan da görüldüğü gibi,

$\oplus$ işlemine göre,

$\overline{0}$ tersi $\overline{0}$; $\overline{1}$ in tersi $\overline{4}$; $\overline{2}$ in tersi $\overline{3}$; $\overline{3}$ ün tersi $\overline{2}$; $\overline{4}$ ün tersi $\overline{1}$ dir.

$\odot$ işlemine göre,

$\overline{1}$ in tersi $\overline{1}$; $\overline{2}$ in tersi $\overline{3}$; $\overline{3}$ ün tersi $\overline{2}$; $\overline{4}$ ün tersi $\overline{4}$ dür.

Sıfırın çarpma işlemine göre tersi yoktur.

ÖRNEK 1.54

Yukarıdaki Örnek 1.53 de çizdiğimiz $Z / 5$ kalan sınıfları kümesinde, toplama ve çarpma tablosundan faydalanarak, $\overline{2} \odot (\overline{4} \oplus \overline{4})$ ifadesinin sonucunu bulalım.

$Z / 5$ kalan sınıfları kümesinde toplama ve çarpma tablolarına göre,

$\overline{2} \odot (\overline{4} \oplus \overline{4}) = \overline{2} \odot \overline{3} = \overline{\overline{1}}$ olur.

e. Çeşitli Örnekler

ÖRNEK 1.55

3^{76} ın 5 ile bölümünden elde edilecek kalanın kaç olduğunu bulalım.

$3 \equiv 3 \pmod 5$

$3^2 \equiv 4 \pmod 5$

$3^4 \equiv 1 \pmod 5$

$(3^4)^{19} \equiv 1^{19} \pmod 5$

$3^{76} \equiv 1 \pmod 5$

O halde, 3^{76} ın 5 ile bölümünde kalan 1 olur.

ÖRNEK 1.56

7^{124} ın birler basağındaki rakamı bulalım.

$7 \equiv 7 \pmod{10}$

$7^2 \equiv 9 \pmod{10}$

$7^4 \equiv 1 \pmod{10}$

$(7^4)^{31} \equiv 1^{31} \pmod{10}$

$7^{124} \equiv 1 \pmod{10}$

Aynı modüllü iki denklik taraf tarafa çarpılabileceğinden,

$7^{124} \equiv 1 \pmod{10}$

x $\quad 7^2 \equiv 9 \pmod{10}$

$7^{126} \equiv 9 \pmod{10}$

O halde, 7^{126} ın birler basamağındaki rakamı 9 olur.

ÖRNEK 1.57

$Z / 3$ te $(\overline{2} \odot \overline{x}) \oplus \overline{1} = \overline{0}$ denkleminin çözüm kümesini bulalım.

$(\overline{2} \odot \overline{x}) \oplus \overline{1} \oplus \overline{2} = \overline{0} \oplus \overline{2}$ ($Z / 3$ te $\overline{1}$ in toplama işlemine göre ters elemanı $\overline{2}$ dir.)

$\overline{2} \odot \overline{x} \oplus \overline{0} = \overline{2}$ ($Z / 3$ te $\overline{1} \oplus \overline{2} = \overline{0}$ olur.)

$\overline{2} \odot \overline{x} = \overline{2}$ ($Z /3$ te $\overline{0}$ toplama işleminin etkisiz elemanıdır.)

$\overline{2} \odot \overline{2} \odot \overline{x} = \overline{2} \odot \overline{2}$ ($Z / 3$ te $\overline{2}$ nin çarpma işlemine göre ters elemanı $\overline{2}$ dir.)

$1 \odot x = 1$

$x = 1$

O halde, denklemin çözüm kümesi $Ç = \{\overline{1}\}$ dir.

ÖRNEK 1.58

m bir doğal sayı olduğuna göre, 13^{2m+1} sayısının 5 ile bölümündeki kalanı bulalım.

$13 \equiv 3 \pmod 5$

$13^2 \equiv 4 \pmod 5$

$13^4 \equiv 1 \pmod 5$

$(13^4)^{2m} \equiv 1^{2m} \pmod 5$

$13^{8m} \equiv 1 \pmod 5$

x $13 \equiv 3 \pmod 5$

$13^{8m+1} \equiv 3 \pmod 5$

O halde, 13^{8m+1} sayısının 5 ile bölümünde kalan 3 olur.

ÖRNEK 1.59

Z / 6 da karekökü olan sayıları bulalım.

$a \in Z/6$ için, $Z/6=\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$ olduğundan, $b \odot b = b^2 = a$ şartını sağlayan bir $b \in Z / 6$ sayısı bulunuyorsa, $b = \sqrt{a}$ olur.

$\overline{0}$ için, $\overline{0} \odot \overline{0} = \overline{0}$ ise $\sqrt{\overline{0}} = \overline{0}$ dır.

$\overline{1}$ için, $\overline{1} \odot \overline{1} = \overline{1}$ ise $\sqrt{\overline{1}} = \overline{1}$ dir.

$\overline{2}$ için, $\overline{2} \odot \overline{2} = \overline{4}$ ise $\sqrt{\overline{4}} = \overline{2}$ dir.

$\overline{3}$ için, $\overline{3} . \overline{3} = \overline{3}$ ise $\sqrt{\overline{3}} = \overline{3}$ tür.

$\overline{4}$ için, $\overline{4} \odot \overline{4} = \overline{4}$ ise $\sqrt{\overline{4}} = \overline{4}$ dür.

$\overline{5}$ için, $\overline{5} \odot \overline{5} = \overline{1}$ ise $\sqrt{\overline{1}} = \overline{5}$ dir.

ÖZET

- a ve b tam sayıları verilen bir m pozitif tam sayısına bölündüklerinde, aynı kalanı verirse a tam sayısı, b tam sayısına, m modülüne göre denktir. $a \equiv b \pmod m$ şeklinde gösterilir. Biz bunu, $\beta = \{(a, b) \mid a - b, m \text{ ile bölünür}\}$ bağıntısı ile de gösterebiliriz. Bu bağıntı bir denklik bağıntısıdır. β denklik bağıntısı, tam sayılar kümesini denklik sınıflarına ayırır. m modülüne göre, denklik sınıflarının kümesi Z / m ile gösterilir.

- Tam sayılar kümesinde modüle göre, kalan sınıfların özelikleri:

1. Kalan sınıfların tam sayılar kümesinin, ikişer ikişer ayrık alt kümeleridir.
2. Kalan sınıfların birleşimi tam sayılar kümesini verir.
3, Kalan sınıflarının hiçbiri boş küme değildir.

- Modüler aritmetiğe ait aşağıdaki teoremler vardır.

  Her $a, b, c, d, x \in Z$ ve $m, n \in Z^+$, $m > 1$ için;

  $a \equiv b \pmod m$ ve $c \equiv d \pmod m$ ise;

1. $a \pm c \equiv b \pm d \pmod m$
2. $a \cdot c \equiv b \cdot d \pmod m$
3. $a \pm x \equiv b \pm x \pmod m$
4. $a \cdot x \equiv b \cdot x \pmod m$
5. $a^n \equiv b^n \pmod m$

- Kalan sınıflar kümesinde toplama ve çarpma işlemleri için, m pozitif tamsayı olmak üzere, m modülüne göre, kalan sınıflarının kümesi

  $Z / m = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, ..., \overline{(m - 1)}\}$ dir.

  Kalan sınıfları kümesinde, toplama işlemleri $\oplus$ sembolü ile, çarpma işlemleri $\odot$ sembolü ile gösterilir.

1. Toplama işlemi: $\overline{a} \oplus \overline{b} = \overline{a + b}$ dir.
2. Çarpma işlemi: $\overline{a} \odot \overline{b} = \overline{a \cdot b}$ dir.