4.5 – Modüler Aritmetik

4.5.1 – Tam Sayıların Bir Modüle Göre Denkliği

Etkinlik – 4.145

Aşağıdaki problemleri çözünüz.

a. Saatin 17 olduğu andan 153 saat sonra saat kaç olur?

b. Bir salı gününden 45 gün sonra, günlerden ne olur?

c. Dört günde bir nöbet tutacak olan bir doktor ilk nöbetini çarşamba günü tutarsa, 9. nöbetini hangi gün tutar?

d. 7^{97} sayısı rakamları ile yazılsa, birler basamağı kaç olur?

Etkinlik–4.145'teki problemler, bir tam sayının bir sayma sayısıyla bölünmesindeki kalanın, bu tam sayı yerine konulabildiği durumlarla ilgilidir.

Örneğin; pazartesi gününden 17 gün sonrası ile 3 gün sonrası aynı gündür. ($17 = 7 \cdot 2 + 3$) Saatin 13 olduğu andan 86 saat sonra da, 14 saat sonra da saat 3'ü gösterir. ($86 = 24 \cdot 3 + 14$)

Bu bölümde, kalanların aritmetiğinin kurallarını ortaya koyacağız. Bu yeni aritmetik, *Etkinlik–1.145*'teki türden problemlerin çözümlerini kolaylaştıracağı gibi, bize yeni matematiksel olanaklar da sağlayacaktır.

Teorem – 4.64

$\mathbf{m} \in \mathbf{Z^+}$ *olmak üzere; tam sayılarda,*

$\beta = \{(\mathbf{x}, \mathbf{y}) |$ **x ile y, m ile bölündüğünde aynı kalanı verirler.**$\}$

bağıntısı bir denklik bağıntısıdır.

Gerçekten;

$\forall x \in Z$ için $(x, x) \in \beta$ olacağından β yansıyandır.

$\forall (x, y) \in \beta$ için $(y, x) \in \beta$ olacağından β simetriktir.

$\forall (x, y) \in \beta$ ve $(y, x) \in \beta$ için $(x, z) \in \beta$ olacağından β geçişkendir.

Öyleyse; β bir denklik bağıntısıdır.

β bir denklik bağıntısı ve $(x, y) \in \beta$ ise $\mathbf{x \equiv y}$ denildiğini biliyorsunuz.

Tanım – 4.31

a *ve* ***b*** *tam sayıları,* ***modül*** *adı verilen bir* ***m*** *sayma sayısına bölündüklerinde aynı kalanı veriyorlarsa,* ***m modülüne göre; a, b'ye denktir****, denir.*

Bu denklik, $\boldsymbol{a \equiv b \pmod m}$ *biçiminde gösterilir;* ***a denk b modülo m*** *diye okunur.*

Örneğin; 14 ve -22 tam sayılarının 6 ile bölünmesindeki kalanlar aynı olup 2'dir.

$(-22 = -4 \cdot 6 + 2)$

Öyleyse; 14 ve -22 sayıları 6 modülüne göre denktirler. $14 \equiv -22 \pmod 6$ yazılabilir.

Teorem – 4.65

a *ve* ***b*** *tam sayılarının* ***m*** *sayma sayısı ile bölünmesinde kalanların aynı olması için gerekli ve yeterli koşul,* $\boldsymbol{a - b}$ *'nin* ***m*** *ile bölünmesidir.*

Etkinlik – 4.146

Teorem – 4.65'i ispatlayınız.

Teorem–4.64, *Tanım–4.31* ve *Teorem–4.65*' ten şu sonuçlar çıkarılır:

1. Bir **a** tam sayısı bir **m** sayma sayısına bölünüyorsa; **a** sayısı **m** modülüne göre **sıfır**a denktir.

   $\mathbf{m} \mid \mathbf{a} \Rightarrow \mathbf{a \equiv 0 \pmod m}$ dir.

   Örneğin; $21 \equiv 0 \pmod 7$ dir.

2. Bir **a** tam sayısının bir **m** sayma sayısına bölünmesinde kalan **r** ise, **a** sayısı **m** modülüne göre **r**'ye denktir. a, k, r $\in Z$ ve $m \in Z^+$ olmak üzere,

   $\mathbf{a = m \cdot k + r}$ **ve** $\mathbf{0 \le r < m}$ **ise** $\mathbf{a \equiv r \pmod m}$ dir.

   Örneğin; $35 \equiv 3 \pmod 8$ dir. $(35 = 4 \cdot 8 + 3)$

3 a, b $\in Z$ ve $m \in Z^+$ olmak üzere,

$\mathbf{a \equiv b \pmod m \Leftrightarrow a - b \equiv 0 \pmod m}$ dir.

Örnek – 4.85

a. $23 \equiv 11 \pmod 3$ **b.** $23 \equiv 11 \pmod 5$

c. $47 \equiv 32 \pmod 5$ **d.** $18 \equiv -6 \pmod 6$

e. $-53 \equiv 42 \pmod{19}$ **f.** $-27 \equiv 0 \pmod 9$

Teorem – 4.66

Aynı modüllü denklikler taraf tarafa toplanır, çıkarılır ya da çarpılırsa aynı modüllü denklikler elde edilir.

Teorem – 4.66'nın sembollerle ifadesi şöyledir:

1 $\mathbf{a \equiv b \pmod m}$ ve $\mathbf{c \equiv d \pmod m}$

$\mathbf{\Rightarrow a + c \equiv b + d \pmod m}$ 'dir.

2 $\mathbf{a \equiv b \pmod m}$ ve $\mathbf{c \equiv d \pmod m}$

$\mathbf{\Rightarrow a - c \equiv b - d \pmod m}$ 'dir.

3 $\mathbf{a \equiv b \pmod m}$ ve $\mathbf{c \equiv d \pmod m}$

$\mathbf{\Rightarrow a \cdot c \equiv b \cdot d \pmod m}$ 'dir.

Etkinlik – 4.147

Teorem – 4.66'yı ispatlayınız.

Teorem – 4.66'dan şu sonuçlar çıkarılır:

1 Bir modüle göre denkliğin iki tarafına, aynı tam sayı eklenir ya da çıkarılırsa denklik bozulmaz.

$\mathbf{a \equiv b \pmod m}$ **ve** $\mathbf{k \in Z}$

$\mathbf{\Leftrightarrow a \mp k \equiv b \mp k \pmod m}$ olur.

$[k \equiv k \pmod m$ olduğundan$]$

2 Bir modüle göre denkliğin iki tarafı aynı tam sayı ile çarpılırsa denklik bozulmaz.

$\mathbf{a \equiv b \pmod m}$ **ve** $\mathbf{k \in Z}$

$\mathbf{\Rightarrow a \cdot k \equiv b \cdot k \pmod m}$ olur.

$[k \equiv k \pmod m$ olduğundan$]$

3 Bir modüle göre denkliğin bir tarafına modülün tam katları eklenirse ya da çıkarılırsa denklik bozulmaz.

$\mathbf{a \equiv b \pmod m}$ **ve** $\mathbf{c \in Z}$

$\mathbf{\Leftrightarrow a + m \cdot c \equiv b \pmod m}$ olur.

$[m \cdot c \equiv 0 \pmod m$ olduğundan$]$

4 Her $n \in N^+$ için,

$\mathbf{a \equiv b \pmod m}$ **ise** $\mathbf{a^n \equiv b^n \pmod m}$ dir.

$a \equiv b \pmod m$ denkliği alt alta n kere yazılır ve bu denklikler taraf tarafa çarpılırsa, $a^n \equiv b^n \pmod m$ denkliği elde edilir.

Örnek – 4.86

15^{87} nin 4 ile bölünmesinde kalan kaçtır?

Çözüm

15^{87} nin 4 modülüne göre dengini bulacağız.

$15 \equiv 3 \pmod 4$

$\Rightarrow 15^{87} \equiv 3^{87} \pmod 4$ olur.

$3 \equiv 3 \pmod 4$

$\Rightarrow 3^2 \equiv 9 \pmod 4$ (Teo. 4.66; sonuç 4)

$\Rightarrow 3^2 \equiv 1 \pmod 4$

$\Rightarrow \left(3^2\right)^{43} \equiv 1^{43} \pmod 4$ (Teo. 4.66; sonuç 4)

$\Rightarrow 3^{86} \equiv 1 \pmod 4$

$\Rightarrow 3 \cdot 3^{86} \equiv 3 \cdot 1 \pmod 4$ (Teo. 4.66; sonuç 2)

$\Rightarrow 3^{87} \equiv 3 \pmod 4$

$\Rightarrow 15^{87} \equiv 3 \pmod 4$ bulunur.

✚ Bir tam sayının büyük kuvvetlerinin bir modüle göre dengini bulmak için; bu sayının önce 1, 0 ya da -1'e denk olan kuvveti (varsa) bulunur. 1, 0 ve -1 sayıları büyük kuvvete ulaşmada kolaylık sağlarlar.

Örnek – 4.87

7^{77} nin 11 ile bölünmesinde kalan kaçtır?

Çözüm

$7 \equiv 7 \pmod{11}$

$\Rightarrow 7^2 \equiv 5 \pmod{11}$

$\Rightarrow 7^3 \equiv 2 \pmod{11}$

$\Rightarrow 7^3 \cdot 7^2 \equiv 2 \cdot 5 \pmod{11}$

$\Rightarrow 7^5 \equiv -1 \pmod{11}$

$\Rightarrow \left(7^5\right)^{15} \equiv (-1)^{15} \pmod{11}$

$\Rightarrow 7^{75} \equiv -1 \pmod{11}$

$\Rightarrow 7^{75} \cdot 7^2 \equiv (-1) \cdot (5) \pmod{11}$

$\Rightarrow 7^{77} \equiv -5 \pmod{11}$

$\Rightarrow 7^{77} \equiv 6 \pmod{11}$

7^{77} nin 11 ile bölünmesinde kalan 6'dır.

Örnek – 4.88

554^{554} sayısı onluk sistemde yazılırsa, birler basamağındaki rakam kaç olur?

Çözüm

Onluk sayma sisteminde bir sayının birler basamağındaki rakam, o sayının 10 ile bölünmesindeki kalandır.

$554 \equiv 4 \pmod{10}$

$\Rightarrow 554^{554} \equiv 4^{554} \pmod{10}$ olur.

$4 \equiv 4 \pmod{10}$

$4^2 \equiv 6 \pmod{10}$

$4^3 \equiv 4 \pmod{10}$

$4^4 \equiv 6 \pmod{10}$

$\vdots$

Görüldüğü gibi; 10 modülüne göre 4'ün tek kuvvetleri 4'e, çift kuvvetleri 6'ya denk olmaktadır.

O hâlde;

$4^{554} \equiv 6 \pmod{10}$

$\Rightarrow 554^{554} \equiv 6 \pmod{10}$ bulunur.

Örnek – 4.89

$m \in Z^+$ olmak üzere, $62 \equiv 6 \pmod{m}$ denkliğini sağlayan m değerlerini bulunuz.

Çözüm

$62 \equiv 6 \pmod{m}$ ise $m \mid (62-6)$ dır.

$m \mid 56$ ve $m \in Z^+$ ise m değerlerinin kümesi $\{1,2,4,7,8,14,28,56\}$ olur.

Örnek – 4.90

$43x + 31 \equiv 13 \pmod{11}$ denkliğini sağlayan üç basamaklı en küçük x pozitif tam sayısını bulunuz.

Çözüm

$43x + 31 \equiv 13 \pmod{11}$

$\Rightarrow 10x + 9 \equiv 2 \pmod{11}$

$\Rightarrow 10x + 7 \equiv 0 \pmod{11}$

$\Rightarrow x \equiv 7 \pmod{11}$ olur.

x sayıları $7 + 11k (k \in Z)$ biçimindedir.

$7 + 11k \geq 100$

$\Rightarrow 11k \geq 93$

$\Rightarrow k \geq 9$ olacağından üç basamaklı en küçük x tam sayısı, $x = 7 + 11 \cdot 9 \Rightarrow x = 106$ olur.

Örnek – 4.91

$23^x \equiv 3 \pmod{7}$ denkliğini sağlayan iki basamaklı en büyük x tam sayısını bulunuz.

Çözüm

$23 \equiv 2 \pmod{7}$ olduğundan $23^x \equiv 2^x \pmod{7}$ olur.

$2^0 \equiv 1 \pmod{7}$

$2 \equiv 2 \pmod{7}$

$2^2 \equiv 4 \pmod{7}$

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

2'nin 2^3'ten sonra gelen ardışık pozitif tam kuvvetleri, 7 modülüne göre 2, 4 ve 1'e periyodik olarak denk olacaklardır. Öyleyse,

$23^x \equiv 3 \pmod 7$ denkliğini sağlayan bir $x \in Z^+$ yoktur.

Etkinlik – 4.148

a. 47^{74} ün 7 ile bölünmesinde kalan kaçtır?

b. 8^{87} nin 6 ile bölünmesinde kalan kaçtır?

c. 11^{135} in 13 ile bölünmesinde kalan kaçtır?

d. 10^{279} un 17 ile bölünmesinde kalan kaçtır?

e. $2006^{2007} + 2007^{2006}$ toplamı 10'luk sayma düzeninde yazılsa birler basamağı kaç olur?

f. $23 \cdot 83^{83} + 37 \cdot 73^{73}$ toplamının 11 ile bölümündeki kalan kaçtır?

Etkinlik – 4.149

Etkinlik – 4.145'te çözdüğünüz problemleri, bir de modül kavramı ile çözünüz.

✚ Bir modüle göre denkliğin iki tarafı bir tam sayı ile bölündüğünde denklik bozulabilir.

Örneğin; $9 \cdot 4 \equiv 7 \cdot 4 \pmod 8$ olduğu hâlde $9 \not\equiv 7 \pmod 8$ dir.

Teorem – 4.67, hangi durumlarda bir modüle göre denkliğin bir tam sayı ile bölünebileceğini ortaya koyar.

Teorem – 4.67

$a, b, x \in Z$; $x \neq 0$ ve $m \in Z^+$ olmak üzere,

$a \cdot x \equiv b \cdot x \pmod m$ ve $OBEB(|x|, m) = d$ ise

$a \equiv b \left(mod\ \frac{m}{d}\right)$ dir.

Örneğin; $12 \cdot a \equiv 12 \cdot b \pmod{20}$ ise,

$OBEB(12, 20) = 4$ olduğundan

$\frac{12}{4} a \equiv \frac{12}{4} b \left(\text{mod } \frac{20}{4}\right) \Rightarrow 3a \equiv 3b \pmod 5$ dir.

$OBEB(3, 5) = 1$ olduğundan

$\Rightarrow a \equiv b \pmod 5$ olur.

Etkinlik – 4.150

Teorem – 4.67'yi ispatlayınız.

✚ Teorem – 4.67'den şu sonuç çıkarılır.

"a, b, $x \in Z$; $x \neq 0$; $m \in Z^+$ ve $|x|$ ile m aralarında asal olmak üzere,

$a \cdot x \equiv b \cdot x \pmod m$ ise $a \equiv b \pmod m$ dir."

Örneğin; $12 \cdot a \equiv 6b \pmod{25}$ ise

$2 \cdot a \equiv b \pmod{25}$ olur.

Bu sonuca dayanarak da şunu söyleyebiliriz:

m asal ise, m modülüne göre denkliğin iki tarafı bunları bölen her tam sayı ile bölünebilir.

Teorem – 4.68

$a \equiv b \pmod m$ denkliğinde a, b ve m sayıları bunları bölen bir pozitif tam sayı ile bölündüğünde ya da bir pozitif tam sayı ile çarpıldığında denklik bozulmaz.

Örneğin; $6x \equiv 12 \pmod{24}$ denkliği

$3x \equiv 6 \pmod{12}$;

$2x \equiv 4 \pmod 8$;

$x \equiv 2 \pmod 4$;

$12x \equiv 24 \pmod{48}$;

…

denkliklerini çift gerektirir.

Etkinlik – 4.151

Teorem – 4.68'i ispatlayınız.

Teorem – 4.67 ve Teorem – 4.68 modüler denklemlerin çözümünde işimizi kolaylaştıracaktır.

Kalan Sınıfları

Etkinlik – 4.152

Tam sayılarda, $\beta = \{(x,y)|x-y,\ 5 \text{ ile bölünür.}\}$ bağıntısının bir denklik bağıntısı olduğunu gösteriniz.

Etkinlik – 4.152'de verilen bağıntı

$\beta = \{(x,y)|x \text{ ile } y\text{'nin 5 ile bölünmesinde kalanlar aynıdır.}\}$

biçiminde yazılabilir. (Teorem – 4.65)

Bir tam sayının 5 ile bölünmesinde kalan 0, 1, 2, 3 ya da 4'tür. Öte yandan, β bir denklik bağıntısıdır.

$(0,5) \in \beta$ ve $(5,10) \in \beta$ olduğundan

$0 \equiv 5 \equiv 10 \pmod 5$ olur.

Böyle denklik zincirleri en uzun biçimiyle yazılırsa, tam sayılar aşağıdaki denklik sınıflarına ayrılır:

$0 \equiv 5 \equiv 10 \equiv ... \equiv -5 \equiv -10 \equiv ... \pmod 5$

$1 \equiv 6 \equiv 11 \equiv ... \equiv -4 \equiv -9 \equiv ... \pmod 5$

$2 \equiv 7 \equiv 12 \equiv ... \equiv -3 \equiv -8 \equiv ... \pmod 5$

$3 \equiv 8 \equiv 13 \equiv ... \equiv -2 \equiv -7 \equiv ... \pmod 5$

$4 \equiv 9 \equiv 14 \equiv ... \equiv -1 \equiv -6 \equiv ... \pmod 5$

Sıfıra denk olan sayıların kümesi $\overline{0}$, 1'e denk olan sayıların kümesi $\overline{1}$, … ile gösterilirse,

$\overline{0} = \{0,5,10,15,...,-5,-10,-15,...\}$;

$\overline{1} = \{1,6,11,16,...,-4,-9,-14,...\}$;

$\overline{2} = \{2,7,12,17,...,-3,-8,-13,...\}$;

$\overline{3} = \{3,8,13,18,...,-2,-7,-12,...\}$;

$\overline{4} = \{4,9,14,19,...,-1,-6,-11,...\}$ olur.

$\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$ kümelerinden her birine **Z'nin 5 modülüne göre kalan sınıfı** denir.

Bu kalan sınıflarının kümesi "***Z/5***" ile gösterilir ve "***Z bölü 5***" diye okunur.

Buna göre,

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

Tanım – 4.32

m, 1'den büyük bir tam sayı olmak üzere; ***m*** *ile bölündüğünde aynı* ***r*** *kalanını veren tam sayıların kümesine,* ***r****'nin* ***m*** *modülüne göre* ***kalan sınıfı*** *denir.*

Bir tam sayının m ile bölünmesinde kalan 0, 1, 2, 3, …, $m-2$ ya da $m-1$'dir.

Demek ki; m modülüne göre m tane kalan sınıfı vardır.

0'ın kalan sınıfı $\overline{0}$,

1'in kalan sınıfı $\overline{1}$,

⋮

$m-1$'in kalan sınıfı $\overline{m-1}$ ile gösterilir.

Tanım – 4.33

m modülüne göre kalan sınıflarının oluşturduğu kümeye ***m'nin kalan sınıfları kümesi*** *denir. Bu küme "****Z/m****" ile gösterilir ve "****Z bölü m****" diye okunur.*

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

Genellikle, her denklik sınıfı o sınıfın negatif olmayan en küçük elemanı ile temsil edilerek, Z/m kümeleri şöyle gösterilirler:

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

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

$Z/m = \{0,1,2,3,4,...,m-1\}$

Z/m kümesinin elemanları ikişer ikişer ayrık kümelerdir. Birleşimleri Z'dir.

$\mathbf{\overline{0} \cup \overline{1} \cup \overline{2} \cup ... \cup \overline{m-1} = Z}$

4.5.2 – Modüler Aritmetik

Z/m de Toplama ve Çarpma

Tanım – 4.34

*Z/m kümesinde iki kalan sınıfının **toplamı**, bu kalan sınıflarından seçilmiş iki tam sayının toplamının kalan sınıfıdır.*

Toplamı bulma işlemi "$\oplus$" sembolü ile gösterilir.

$\forall \bar{a}, \bar{b} \in Z/m$ *için,* $\bar{a} \oplus \bar{b} = \overline{a+b}$ *dir.*

Örneğin, Z/7'de

$\bar{4} \oplus \bar{5} = \overline{4+5} = \bar{9} = \bar{2}$ olur.

Teorem – 4.69

1. *Z/m kümesi toplama işlemine göre **kapalı**dır.*
2. *Z/m de toplama işleminin **birleşme** özeliği vardır.*
3. *Z/m de toplama işleminin **değişme** özeliği vardır.*
4. *Z/m de toplama işlemine göre **etkisiz eleman** vardır ve bu $\bar{0}$ dır.*
5. *Z/m de her elemanın toplama işlemine göre **tersi** vardır.*
   $\bar{a}$ nın tersi $-\bar{a}$, $\overline{-a}$ ya da $\overline{m-a}$ ile gösterilir.

Etkinlik – 4.153

Teorem – 4.69'u ispatlayınız.

Örnek – 4.92

Toplama işleminin özeliklerinden yararlanarak, Z/7 de $\bar{4} \oplus \bar{x} = \bar{2}$ denklemini çözelim:

$\bar{4}$ ün toplama işlemine göre tersi $\bar{3}$ tür. Eşitliğin iki tarafına ekleyelim.

$\bar{4} \oplus \bar{x} = \bar{2}$

$\Rightarrow \bar{3} \oplus (\bar{4} \oplus \bar{x}) = \bar{3} \oplus \bar{2}$ (TS)

$\Rightarrow (\bar{3} \oplus \bar{4}) \oplus \bar{x} = \bar{5}$ (Birleşme öz.)

$\Rightarrow \bar{x} = \bar{5}$ bulunur. $(\bar{3} + \bar{4} = \bar{0},\ \bar{0} + \bar{x} = \bar{x})$

$\bar{4} \oplus \bar{x} = \bar{2}$ denklemi, aynı anlama gelmek üzere, $4 + x = 2$ biçiminde yazılabilir:

Z/7 de $\bar{4} \oplus \bar{x} = \bar{2}$

$\Rightarrow 4 + x = 2$

$\Rightarrow 3 + (4 + x) = 3 + 2$

$\Rightarrow (3 + 4) + x = 5$

$\Rightarrow x = 5$

Denklem aşağıdaki gibi de çözülebilir:

Z/7 de, $4 + x = 2$

$\Rightarrow 4 + x = 2 \pmod 7$

$\Rightarrow x \equiv 2 - 4 \pmod 7$

$\Rightarrow x \equiv -2 \pmod 7$

$\Rightarrow x \equiv -2 + 7 \pmod 7$

$\Rightarrow x \equiv 5 \pmod 7$

Tanım – 4.35

*Z/m kümesinde iki kalan sınıfının **çarpımı**, bu kalan sınıflarından seçilmiş iki tam sayının çarpımının kalan sınıfıdır.*

Çarpımı bulma işlemi "$\odot$" sembolü ile gösterilir.

$\forall \bar{a}, \bar{b} \in Z/m$ *için,* $\bar{a} \odot \bar{b} = \overline{a \cdot b}$ *dir.*

Örneğin, Z/5'te

$\bar{3} \odot \bar{4} = \overline{3 \cdot 4} = \overline{12} = \bar{2}$ olur.

Teorem – 4.70

1. *Z/m kümesi çarpma işlemine göre **kapalı**dır.*
2. *Z/m de çarpma işleminin **değişme** özeliği vardır.*
3. *Z/m de çarpma işleminin **birleşme** özeliği vardır.*
4. *Z/m de çarpma işlemine göre **etkisiz eleman** vardır ve bu $\bar{1}$ dir.*
5. *Z/m de çarpma işlemine göre **yutan eleman** vardır ve bu $\bar{0}$ dır.*
6. *Z/m de çarpma işleminin toplama işlemi üzerine **dağılma** özeliği vardır.*

Etkinlik – 4.154

Teorem – 4.70'i ispatlayınız.

Etkinlik – 4.155

Z/5 ve Z/6 kümelerinde, aşağıda verilen toplam ve çarpım tablolarını tamamlayınız.

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

$\odot$	0	1	2	3	4
0				0	
1				3	
2				1	
3				4	
4				2	

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

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

İşlem tablolarından yararlanarak;

a. Z/5 ve Z/6 kümelerinin elemanlarının toplama ve çarpma işlemlerine göre terslerini (varsa) bulunuz.

b. Z/6 da, $\bar{4} \oplus \bar{3} \odot (\bar{5} \oplus \bar{2}) \oplus \bar{3} \odot \bar{4}$ işlemini yapınız.

c. Z/5 te, $2x + 3 = 4$ denkleminin çözüm kümesini bulunuz.

d. Z/6 da, $3x + 5 = 2$ denkleminin çözüm kümesini bulunuz.

(İşlem tablolarında ve denklemlerde gördüğünüz her **a** sayısının $\bar{a}$ anlamında olduğunu unutmayınız.)

Teorem – 4.71

$\bar{a}$ ve m aralarında asal olmak üzere, Z/m de $\bar{a} \odot \bar{b} = \bar{a} \odot \bar{c} \Leftrightarrow \bar{b} = \bar{c}$ *dir.*

Etkinlik – 4.156

Teorem – 4.71'i ispatlayınız.

Teorem – 4.70'ten şu sonuçlar çıkarılır:

1 a ve m aralarında asal olmak üzere, Z/m deki çarpım tablosunda $\bar{a}$ nın satırında –sıra gözetilmeksizin– $\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{m-1}$ elemanları bulunur.

Gerçekten; Z/m kümesi çarpma işlemine göre kapalı olup $\bar{a}$ nın, farklı $\bar{b}$ ile $\bar{c}$ sayıları ile çarpımları farklı olacağından $\bar{a} \neq 0$ satırında Z/m in m tane elamanı bulunacaktır.

2 **a ve m aralarında asal ise Z/m in her $\bar{a}$ elemanının çarpma işlemine göre tersi vardır**.

Gerçekten; Z/m deki çarpım tablosunda $\bar{a}$ nın satırında 1 bulunacağından $\bar{a} \odot \bar{x} = \bar{1}$ olacak biçimde bir $\bar{x} \in$ Z/m vardır.

"$\odot$" işleminin değişme özeliği olduğundan $\bar{a} \odot \bar{x} = \bar{x} \odot \bar{a} = \bar{1}$ olur.

Buna göre; $\bar{x} = a^{-1}$ dir.

3 a ve m aralarında asal ise $\forall \bar{a}, \bar{b} \in Z$ için $\bar{a} \odot \bar{x} = \bar{b}$ denkleminin yalnız bir çözümü vardır.

Gerçekten; Z/m de $\bar{a} \odot \bar{x} = \bar{b}$

$\Rightarrow \bar{a}^{-1} \odot \bar{a} \odot \bar{x} = \bar{a}^{-1} \odot \bar{b}$

$\Rightarrow \bar{x} = \bar{a}^{-1} \odot \bar{b}$ olur.

$\bar{a} \odot \bar{x} = \bar{b} \Rightarrow \bar{x} = \bar{a}^{-1} \odot \bar{b}$ dir.

Örnek – 4.93

Z/7 de, $\bar{3} \odot x \oplus \bar{2} = \bar{4}$ denkleminin çözüm kümesini bulunuz.

Çözüm

Z/7 de, $\bar{3} \odot x \oplus \bar{2} = \bar{4}$

$\Rightarrow \bar{3} \odot x \oplus \bar{2} \oplus \bar{5} = \bar{4} \oplus \bar{5}$ $\quad (-\bar{2} = \bar{5})$

$\Rightarrow \bar{3} \odot x = \bar{2}$ $\quad (\bar{2} \oplus \bar{5} = \bar{0})$

$\Rightarrow \bar{5} \odot \bar{3} \odot \bar{x} = \bar{5} \odot \bar{2}$ $\quad (\bar{3}^{-1} = \bar{5})$

$\Rightarrow \bar{x} = \bar{3}$ $\quad (\bar{5} \odot \bar{3} = \bar{1})$

$\Rightarrow Ç = \{\bar{3}\}$ bulunur.

✚ Z/m de

$\bar{a} \odot \bar{a} = \bar{a}^2$

$\bar{a} \odot \bar{a} \odot \bar{a} = \bar{a}^3$

⋮

.

$\underbrace{\bar{a}\odot\bar{a}\odot\ldots\bar{a}}_{n\ tane}=\bar{a}^{n}$ dir.

$\bar{x}^{2}=\bar{a}$ ise $\bar{x}$ e $\bar{a}$ nın **karekök**ü,

$\bar{x}^{3}=\bar{a}$ ise $\bar{x}$ e $\bar{a}$ nın **küpkök**ü denir.

Etkinlik – 4.157

Z/7 de toplam ve çarpım tablolarını yaparak aşağıdaki soruları yanıtlayınız.

a. Z/7 de, $\bar{3}\odot\bar{x}\odot\bar{6}=\bar{5}$ ise $\bar{x}$ kaçtır?

b. Z/7 de, $\bar{4}\odot\bar{x}\odot\bar{3}=\bar{0}$ ise $\bar{x}$ kaçtır?

c. Z/7 de karekökü olmayan sayıları bulunuz.

d. Z/7 de küpkökü olmayan sayıları bulunuz.

e. Z/7 de $3x^2+2=1$ denkleminin çözüm kümesini bulunuz.

f. Z/7 de $2x^2+6=5$ denkleminin çözüm kümesini bulunuz.

Teorem – 4.72

Z/m de, $\bar{a}\odot\bar{x}=\bar{b}$ denkleminin kökünün olması için, $\bar{b}$ nin OBEB(a, m) ile bölünmesi gerekli ve yeterlidir.

$\bar{b}$ nin OBEB(a, m) ile bölünmesi durumunda, denklemin OBEB(a, m) tane farklı kökü bulunur.

Etkinlik – 4.158

Teorem – 4.72'yi ispatlayınız.

Örnek – 4.94

Z/10 kümesinde, aşağıdaki denklemlerin çözüm kümelerini bulunuz.

a. $\bar{4}\odot\bar{x}=\bar{5}$ **b.** $\bar{6}\odot\bar{x}=\bar{4}$

c. $\bar{7}\odot\bar{x}=\bar{3}$ **d.** $\bar{5}\odot\bar{x}=\bar{5}$

e. $\bar{3}\odot\bar{x}\oplus\bar{6}=\bar{5}$ **f.** $\bar{2}\odot\bar{x}\oplus\bar{8}=\bar{4}$

Çözüm

Z/10 da, çarpım tablosunu yapalım. Böylece, Teorem – 4.72'ye dayanarak bulacağımız çözümleri tablodan da doğrulayabileceğiz.

⊙	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

a. $\bar{5}$, $OBEB(4,10)=2$ ile bölünmez.

$Ç=\varnothing$ dir.

Gerçekten; çarpım tablosunda $\bar{4}$ satırında $\bar{5}$ yoktur. $\bar{4}$ ün hiçbir sayı ile çarpımı $\bar{5}$ i vermez.

b. $\bar{4}$, $OBEB(6,10)=2$ ile bölünür. Çözüm kümesi 2 elemanlıdır.

Z/10 da $\bar{6}\odot\bar{x}=\bar{4}$

$\Rightarrow 6x=4\pmod{10}$

$\Rightarrow 3x=2\pmod{5}$ (Teorem – 4.67)

$\Rightarrow x=4\pmod{5}$ olur.

Toplam 10'dan küçük kalacak biçimde, 4'e 5'in katları eklenirse, $x_1=\bar{4}$ ve $x_2=\bar{9}$ bulunur.

$Ç=\{\bar{4},\bar{9}\}$ dir.

Gerçekten; çarpım tablosunda $\bar{6}$ satırında $\bar{4}$ ün bulunduğu sütunlar, $\bar{4}$ ve $\bar{9}$ sütunlarıdır.

$\bar{6}\odot\bar{4}=\bar{4}$ ve $\bar{6}\odot\bar{9}=\bar{4}$ tür.

c. $\bar{3}$, $OBEB(7,10)=1$ ile bölünür. Çözüm kümesi 1 elemanlıdır.

Z/10 da $\bar{7}\odot\bar{x}=\bar{3}$

$\Rightarrow x=\bar{9}$ olur. $Ç=\{\bar{9}\}$ dir.

Gerçekten; çarpım tablosundan $\bar{7}\odot\bar{9}=\bar{3}$ olduğu görülür.

d. $\bar{5}$, $OBEB(5,10)=5$ ile bölünür. Çözüm kümesi 5 elemanlıdır. Z/10 da $\bar{5}\odot\bar{x}=\bar{5}$

$\Rightarrow 5x=5\pmod{10}$

$\Rightarrow x=1\pmod{2}$ olur.

Toplam 10'dan küçük kalacak biçimde, 1'e 2'nin katları eklenirse $x_1 = \bar{1}$, $x_2 = \bar{3}$, $x_3 = \bar{5}$, $x_4 = \bar{7}$, $x_5 = \bar{9}$ bulunur. $Ç = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}, \bar{9}\}$ dur.

Gerçekten; çarpım tablosundan $\bar{5} \odot \bar{1} = \bar{5}$, $\bar{5} \odot \bar{3} = \bar{5}$, $\bar{5} \odot \bar{5} = \bar{5}$, $\bar{5} \odot \bar{7} = \bar{5}$ ve $\bar{5} \odot \bar{9} = \bar{5}$ olduğu görülür.

e. Z/10 da $\bar{3} \odot \bar{x} \oplus \bar{6} = \bar{5}$

$\Rightarrow 3x + 6 = 5 \pmod{10}$

$\Rightarrow 3x + 6 + 4 = 5 + 4 \pmod{10}$

$\Rightarrow 3x = 9 \pmod{10}$

$OBEB(3,10) = 1$ olduğundan çözüm kümesi 1 elemanlıdır.

$3x = 9 \pmod{10}$

$\Rightarrow x = 3 \pmod{10}$

$\Rightarrow Ç = \{\bar{3}\}$ dir.

f. Z/10'da, $\bar{2} \odot \bar{x} \oplus \bar{8} = \bar{4}$

$\Rightarrow 2x + 8 = 4 \pmod{10}$

$\Rightarrow 2x = 6 \pmod{10}$

$OBEB(2,10) = 2$ olup çözüm kümesi 2 elemanlıdır.

$2x = 6 \pmod{10}$

$\Rightarrow x = 3 \pmod{5}$

$\Rightarrow x_1 = \bar{3}$ ve $x_2 = \bar{8}$

$\Rightarrow Ç = \{\bar{3}, \bar{8}\}$ dir.

Etkinlik – 4.159

Aşağıdaki denklemlerin, önce çözüm kümelerinin eleman sayılarını; sonra çözüm kümelerini bulunuz.

a. Z/4 te, $2x + 1 = 3$

b. Z/7 de, $4x + 6 = 5$

c. Z/8 de, $5x + 1 = 5$

d. Z/9 da $3x + 6 = 4$

e. Z/12 de $6x + 4 = 8$

f. Z/15 de $5x + 9 = 4$

Z/m de Çıkarma ve Bölme

Z/m de **çıkarma işlemi** Z'deki çıkarma işlemi gibi tanımlanır:

$\bar{a} \oplus \bar{b} = \bar{c}$ ise $\bar{a}$ ya, $\bar{c}$ nin $\bar{b}$ den farkı denir ve bu $\bar{c} \ominus \bar{b} = \bar{a}$ ile gösterilir.

Örneğin; Z/8 de $\bar{6} \oplus \bar{5} = \bar{3}$ olup

$\bar{6} = \bar{3} \ominus \bar{5}$ ve $\bar{5} = \bar{3} \ominus \bar{6}$ dır.

$\bar{c} \ominus \bar{b} = \bar{c} \oplus (-\bar{b})$ olduğu da tam sayılar kümesindeki gibi ispatlanır. Buna göre; Z/m de çarpma işleminin çıkarma işlemi üzerine dağılma özeliği vardır. Z/m kümesi çıkarma işlemine göre kapalıdır.

Örnek – 4.95

Aşağıdaki işlemleri yapınız.

a. Z/9 da, $\bar{6} \ominus \bar{8}$

b. Z/7 de, $(\bar{3} \ominus \bar{6}) \oplus \bar{4}$

c. Z/10 da, $(\bar{7} \ominus \bar{9}) \ominus \bar{4}$

Çözüm

a. Z/9 da, $\bar{6} \ominus \bar{8} = \bar{6} \oplus (-\bar{8})$

$= \overline{6 + (-8)}$

$= -\bar{2}$

$= \bar{7}$

b. Z/7 de, $(\bar{3} \ominus \bar{6}) \oplus \bar{4} = \bar{3} \oplus (-\bar{6}) \oplus \bar{4}$

$= (-\bar{3}) \oplus \bar{4}$

$= \bar{1}$

c. Z/10 da, $(\bar{7} \ominus \bar{9}) \ominus \bar{4} = \bar{7} \oplus (-\bar{9}) \oplus (-\bar{4})$

$= (-\bar{2}) \oplus (-\bar{4})$

$= -\bar{6}$

$= \bar{4}$

✚ Z/m de $\bar{a} \oplus \bar{b} = \bar{c}$

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

$\Rightarrow \bar{a} = \bar{c} \oplus (-\bar{b})$ olur.

Demek ki, Z/m de bir eşitliğin bir yanındaki terim diğer yana işareti değiştirilerek geçirilir.

Örnek – 4.96

Aşağıdaki denklemleri çözünüz.

a. Z/7 de, $\bar{2} \odot \bar{x} \ominus \bar{3} = \bar{5}$

b. Z/8 de, $\bar{3} \odot \left(\bar{5} \odot \bar{x} \ominus \bar{2}\right) \ominus \bar{7} = \bar{4}$

Çözüm

a. Z/7 de, $\bar{2} \odot \bar{x} \ominus \bar{3} = \bar{5}$

$\Rightarrow \bar{2} \odot \bar{x} = \bar{5} \oplus \bar{3}$

$\Rightarrow \bar{2} \odot \bar{x} = \bar{1}$

$\Rightarrow \bar{4} \odot \bar{2} \odot \bar{x} = \bar{4} \odot \bar{1}$

$\Rightarrow \bar{x} = \bar{4}$

b. Z/8 de, $\bar{3} \odot \left(\bar{5} \odot \bar{x} \ominus \bar{2}\right) \ominus \bar{7} = \bar{4}$

$\Rightarrow \overline{15} \odot \bar{x} \ominus \bar{6} \ominus \bar{7} = \bar{4}$

$\Rightarrow \bar{7} \odot \bar{x} = \bar{4} \oplus \bar{6} \oplus \bar{7}$

$\Rightarrow \bar{7} \odot \bar{x} = \bar{1}$

$\Rightarrow \bar{7} \odot \bar{7} \odot \bar{x} = \bar{7} \odot \bar{1}$

$\Rightarrow \bar{x} = \bar{7}$

Bunu bir de şöyle çözelim:

Z/8 de $\bar{3} \odot \left(\bar{5} \odot \bar{x} \ominus \bar{2}\right) \ominus \bar{7} = \bar{4}$

$\Rightarrow 3(5 \cdot x - 2) - 7 = 4 \pmod 8$

$\Rightarrow 15x - 13 = 4 \pmod 8$

$\Rightarrow 15x = 17 \pmod 8$

$\Rightarrow -x = 1 \pmod 8$

$\Rightarrow x = -1 \pmod 8$

$\Rightarrow x = 7 \pmod 8$

✚ Z/m de **bölme işlemi**ni de tam sayılardaki gibi tanımlayacağız.

Z/m de $\bar{a} \odot \bar{x} = \bar{b}$ eşitliğini sağlayan bir ve yalnız bir $\bar{x}$ sayısı varsa, $\bar{x}$ e $\bar{b}$ nin $\bar{a}$ ile bölümü denir ve bu $\bar{b}/\bar{a}$ ya da $\bar{b} : \bar{a}$ biçiminde gösterilir.

Teorem-4.72ye göre, Z/m de m ile a aralarında asal iken $\bar{a} \odot \bar{x} = \bar{b}$ denkleminin bir ve yalnız bir kökünün bulunduğunu biliyorsunuz. Buna göre; m ile a aralarında asal ise $\bar{b}/\bar{a}$ tanımlıdır.

Z/m de m ile a aralarında asal iken, bölme tanımına göre,

$\bar{a} \odot \bar{x} = \bar{b} \Rightarrow x = \bar{b}\!\not/\bar{a}$ dır. (1)

Teorem-4.70'e göre,

$\bar{a} \odot \bar{x} = \bar{b} \Rightarrow \bar{a}^{-1} \odot \bar{a} \odot x = \bar{a}^{-1} \odot \bar{b}$

$\Rightarrow \bar{x} = \bar{a}^{-1} \odot \bar{b}$

$\Rightarrow \bar{x} = \bar{b} \odot \bar{a}^{-1}$ dir. (2)

(1) ve (2)'den, $\dfrac{\bar{b}}{\bar{a}} = \bar{b} \odot \bar{a}^{-1}$ yazılır.

Örneğin,

Z/7 de $\dfrac{\bar{6}}{\bar{4}} = \bar{6} \odot \bar{4}^{-1} = \bar{6} \odot \bar{2} = \bar{5}$;

Z/8 de $\dfrac{\bar{3}}{\bar{5}} = \bar{3} \odot \bar{5}^{-1} = \bar{3} \odot \bar{5} = \bar{7}$;

Z/9 da $\dfrac{\bar{5}}{\bar{8}} = \bar{5} \odot \bar{8}^{-1} = \bar{5} \odot \bar{8} = \bar{4}$ tür.

Z/m de m ile a aralarında asal değil iken, b sayısı OBEB(m,a) ile bölünmüyorsa denklemin kökü yoktur. Bu durumda $\bar{b}/\bar{a}$ **tanımsız**dır. b sayısı OBEB(m,a) ile bölünüyorsa denklemin OBEB(m,a) tane kökü vardır. Bu durumda da $\bar{b}/\bar{a}$ **belirsiz** olur.

Örnekler verelim

Z/m de $\bar{b} \neq \bar{0}$ iken $\bar{0} \odot \bar{x} = \bar{b}$ denkleminin kökü olmadığından $\bar{b} \neq \bar{0}$ için $\bar{b}/\bar{0}$ tanımsızdır.

Yine Z/m de, her x için $\bar{0} \odot \bar{x} = \bar{0}$ denklemi sağlanacağından $\bar{0}/\bar{0}$ belirsizdir.

Z/8 de $\bar{6} \odot \bar{x} = \bar{4}$ denkleminde $\text{OBEB}(8,6) = 2$ ve $2|4$ olduğundan, denklemin iki kökü vardır. Bu durumda, $\bar{4}/\bar{6}$ belirsizdir.

Gerçekten; $\bar{6} \odot \bar{2} = \bar{4}$ ve $\bar{6} \odot \bar{6} = \bar{4}$ olup $\bar{4}/\bar{6}$ nın $\bar{2}$ ye mi, $\bar{6}$ ya mı eşit sayılacağı belli değildir.

Özetlersek; Z/m de a^{-1} varsa, $\bar{b}$ nin $\bar{a}$ ya bölümü $\bar{b}\!\not/\bar{a} = \bar{b} \odot \bar{a}^{-1}$ olarak tanımlıdır. a^{-1} yoksa bölüm ya tanımsız ya da belirsiz olur.

Bunun sonucu olarak;

m asal ise; $\bar{a} \neq \bar{0}$ olmak üzere, Z/m in her $\bar{a}$ ve $\bar{b}$ değeri için $\bar{b}/\bar{a}$ bölümü tanımlıdır. Z/m $-\{\bar{0}\}$ kümesi bölme işlemine göre kapalıdır.

Örnek – 4.97

Aşağıdaki ifadelerden hangileri tanımlı, hangileri tanımsız, hangileri belirsizdir?

a. Z/7 de, $\bar{5}/\bar{3}$ **b.** Z/8 de, $\bar{4}/\bar{2}$

c. Z/9 da, $\bar{2}/\bar{3}$ **d.** Z/10 da $\bar{5}/\bar{7}$

Çözüm

a. Z/7 de, 7 asal olduğundan 3^{-1} vardır ve $\bar{5}/\bar{3}$ tanımlıdır.

$\frac{\bar{5}}{\bar{3}} = \bar{5} \odot \bar{3}^{-1} = \bar{5} \odot \bar{5} = \bar{4}$ olur.

b. $OBEB(2,8) = 2$ ve $2|4$ olduğundan $\frac{\bar{4}}{\bar{2}}$ iki değerlidir. Diğer bir deyişle; $\frac{\bar{4}}{\bar{2}}$ belirsizdir.

c. $OBEB(3,9) = 3$ ve 2, 3'ü bölmediğinden $\frac{\bar{2}}{\bar{3}}$ tanımsızdır.

d. 7 ile 10 aralarında asal olduğundan, Z/10 da 7^{-1} vardır ve $\bar{5}/\bar{7}$ tanımlıdır.

$\frac{\bar{5}}{\bar{7}} = \bar{5} \odot \bar{7}^{-1} = \bar{5} \odot \bar{3} = \bar{5}$ olur.

Etkinlik – 4.160

a. Z/8 de $3x + 4y = 5$ eşitliğini sağlayan $(\bar{x}, \bar{y})$ ikililerinin kümesini yazınız.

b. Z/7 de $5x + 3y = 4$ ise y'nin x türünden değerini bulunuz.

c. $f : Z/7 \to Z/7,\ f(x) = 3x + 1$ fonksiyonunun tersini bulunuz.

d. $f : Z/5 - \{\bar{2}\} \to Z/5,\ f(x) = \frac{3x+2}{x-2}$ fonksiyonu verildiğine göre; $f(\bar{0})$, $f(\bar{1})$, $f(\bar{3})$, $f(\bar{4})$ değerlerini bulunuz.

Fermat'ın Küçük* Teoremi

Fransız matematikçisi Pierre de Fermat (1601-1665), modern sayılar kuramının kurucusu olarak kabul edilir.

Teorem – 4.73

m asal olmak üzere, Z/m in sıfırdan farklı her $\bar{a}$ *elemanı için*

$\mathbf{a^{m-1} \equiv 1 \pmod{m}}$ *dir.*

Örneğin; $6^{10} \equiv 1 \pmod{11}$, $9^{12} \equiv 1 \pmod{13}$, $24^{16} \equiv 1 \pmod{17}$, … olur.

Etkinlik – 4.161

Fermat'ın küçük teoremini ispatlayınız.

* Fermat'ın büyük teoremi "x, y, z, n $\in N^+$ ve $n > 2$ olmak üzere,

$x^n + y^n = z^n$ eşitliği sağlanamaz." teoremidir.

Etkinlik – 4.162

a. 5^{123} ün 11 ile bölünmesinde kalan kaçtır?

b. 15^{143} ün 17 ile bölünmesinde kalan kaçtır?

c. 28^{90} ın 23 ile bölünmesinde kalan kaçtır?

4.5.3 – Bölünebilme Kuralları

Bölünebilme kurallarından bazılarını kalanlı bölme tanımından yararlanarak ortaya koymuştuk.

Bazı bölünebilme kurallarını da bölünebilme kısmında vermiş, ancak ispatlamakta zorlanmıştık. Burada bölünebilme kurallarını modüler aritmetik yöntemleriyle ele alacağız.

Örnek – 4.98

7 ile bölünebilme kuralını bulunuz.

Çözüm

10 tabanındaki a doğal sayısı

$a = (a_n a_{n-1} \ldots a_5 a_4 a_3 a_2 a_1 a_0)_{10}$

$\Rightarrow a = 1 \cdot a_0 + 10 \cdot a_1 + 10^2 \cdot a_2 + 10^3 a_3 + \ldots + 10^n a_n$ dir.

$1a_0 \equiv 1 \cdot a_0 \pmod 7$

$10 \cdot a_1 \equiv 3a_1 \pmod 7$

$10^2 \cdot a_2 \equiv 2a_2 \pmod 7$

$10^3 \cdot a_3 \equiv -1a_3 \pmod 7$

$10^4 \cdot a_4 \equiv -3a_4 \pmod 7$

$10^5 \cdot a_5 \equiv -2a_5 \pmod 7$

$10^6 \cdot a_6 \equiv 1a_6 \pmod 7$

…

Yukarıdaki denklikler taraf tarafa toplanırsa;

$a \equiv 1a_0 + 3a_1 + 2a_2 - 1a_3 - 3a_4 - 2a_5 + \ldots \pmod 7$ elde edilir.

Demek ki; a'nın 7 ile bölünmesinden elde edilen kalan ile, a'nın rakamlarının birler basamağından başlanarak sıra ile $1, 3, 2, -1, -3, -2, 1, \ldots$ sayıları ile çarpımlarının toplamının 7 ile bölünmesindeki kalan aynı olacaktır.

Etkinlik – 4.163

a. 3 ile bölünebilme kuralını bulunuz.
b. 4 ile bölünebilme kuralını bulunuz.
c. 9 ile bölünebilme kuralını bulunuz.
d. 11 ile bölünebilme kuralını bulunuz.
e. 13 ile bölünebilme kuralını bulunuz.
f. 17 ile bölünebilme kuralını bulunuz.

Etkinlik – 4.164

"*Verilen bir doğal sayının birler basamağı ayrılıp bu basamaktaki rakam 4 ile çarpılarak geride kalan sayıya eklendiğinde elde edilen sayı 13 ile bölünüyorsa, verilen sayı da 13 ile bölünür.*"

İspatlayınız.

Bundan yararlanarak;

a. 2345654 sayısının 13 ile bölünmesindeki kalanı bulunuz.
b. 17 ile bölünebilme kuralını bulunuz.
c. 19 ile bölünebilme kuralını bulunuz.
d. 23 ile bölünebilme kuralını bulunuz.

4.5.4 – Modüler Aritmetiğin Diofant Denklemlerine Uygulanması

Birden çok bilinmeyenli denklemlerin tam sayı çözümlerinin incelendiği denklemlere –Eski Yunanlı metamatikçi Diophantos'un anısına– **Diofant denklemleri** denir.

Örneğin; "$19x + 13y = 5$ *denklemini sağlayan iki basamaklı en büyük x sayısı kaçtır*?" türünden sorularla sık sık karşılaşırsınız. Böyle soruların modüler aritmetik yöntemleri ile çözümleri oldukça kolaydır.

Görelim:

Örnek – 4.99

$19x + 13y = 5$ denklemini sağlayan (x, y) tam sayı ikililerinin kümesini bulunuz.

Çözüm

Denklemi, x'in ya da y'nin kat sayısını sıfır yapan bir modüle göre çözeceğiz.

$19x + 13y = 5$

$\Rightarrow 19x + 13y \equiv 5 \pmod{13}$

$\Rightarrow 6x \equiv 5 \pmod{13}$

$\Rightarrow x \equiv \frac{5}{6} \pmod{13}$

$\Rightarrow x \equiv \frac{5+13}{6} \pmod{13}$

$\Rightarrow x \equiv 3 \pmod{13}$ bulunur.

Buna göre, x'in tam sayı değerleri

$x = 3 + 13k \,(k \in Z)$ biçimindedir. Bu değer verilen denklemde yerine konulursa

$19(3 + 13k) + 13y = 5$

$\Rightarrow 57 + 19 \cdot 13k + 13y = 5$

$\Rightarrow 52 + 19 \cdot 13k + 13y = 0$

$\Rightarrow 4 + 19k + y = 0$

$\Rightarrow y = -4 - 19k$ bulunur.

Denklemin tam sayı ikililerinden oluşan çözüm kümesi

$Ç = \{(x,y) \mid x = 3 + 13k,\ y = -4 - 19k,\ k \in Z\}$ olur.

Örneğin; $(3,-4)$, $(16,-21)$, $(-10,15)$,... ikilileri birer çözümdür.

Örnek – 4.100

$231x + 36y = 19$ denkleminin tam sayı çözümlerini bulunuz.

Çözüm

I. yol

12 modülüne göre hesap yapalım:

$231x + 36y = 19$

$\Rightarrow 231x + 36y = 19 \pmod{12}$

$\Rightarrow 3x = 7 \pmod{12}$ bulunur.

$OBEB(3,12) = 3$ olup 7, 3 ile bölünmez.

Denklemi sağlayan hiçbir (x,y) tam sayı ikilisi yoktur.

II. yol

231 ve 36 sayıları 3 ile bölünür, ancak 19 bölünmez.

$231x + 36y = 19$

$\Rightarrow 3(77x + 12y) = 19$ olup hiç bir (x,y) tam sayı ikilisi için eşitlik sağlanamaz.

Etkinlik – 4.165

Aşağıdaki denklemlerin tam sayılardaki çözüm kümelerini yazınız. Çözümlere örnekler veriniz.

a. $108x - 34y = 96$

b. $12x + 17y = 30$

c. $9x + 4y = 15$

Etkinlik – 4.166

$$\left.\begin{aligned} x + y + z &= 30 \\ 2x + 5y - 3z &= 50 \end{aligned}\right\}$$

Denklem sisteminin pozitif tam sayı çözümlerinin kümesini yazınız.

4.5.5 – Çin Kalan Teoremi

"*Bir sepetteki yumurtalar 3'er 3'er sayıldığında 2, 4'er 4'er sayıldığında 3, 5'er 5'er sayıldığında 1 yumurta artmaktadır.*

Sepette kaç yumurta olabilir?" problemini ele alalım.

Problemin; modüler aritmetik diliyle,

"$x \equiv 2 \pmod{3}$

$x \equiv 3 \pmod{4}$

$x \equiv 1 \pmod{5}$

denkliklerini aynı zamanda sağlayan x sayılarını bulunuz." anlamında olduğu açıktır.

Burada 3, 4 ve 5'in ikişer ikişer aralarında asal olduklarına dikkat ediniz.

$80 + 135 + 36$ toplamı problemin bir çözümüdür.

Şöyle ki;

80'in 3 ile bölünmesinde kalan 2'dir. 135 ve 36, 3'e bölünür. Bunların 3 ile bölünmesinde kalanlar sıfır olur.

135'in 4 ile bölünmesinde kalan 3'tür. 80 ve 36 nın 4 ile bölünmesinde kalanlar sıfır olur.

36'nın 5 ile bölünmesinde kalan 1'dir. 80 ve 135'in 5 ile bölünmesinde kalanlar sıfır olur.

Buna göre; $80 + 135 + 36$ toplamı 3 ile bölündüğünde 2, 4 ile bölündüğünde 3, 5 ile bölündüğünde 1 kalanını verir. Öyleyse; bu toplam problemin bir çözümüdür.

Bu toplama, $OKEK(3,4,5) = 60$'ın katlarını ekleyip çıkararak diğer çözümleri elde ederiz. Buna göre; $x \equiv 80 + 135 + 36 \pmod{60}$ denkliğini yazabiliriz.

Şimdi 80, 135 ve 36 gibi sayıları nasıl bulabileceğimizi araştıralım:

80; 4 ve 5'in (ya da $4 \cdot 5$'in), 3 ile bölündüğünde 2 kalanını veren bir katıdır.

135; 3 ve 5'in (ya da $3 \cdot 5$'in), 4 ile bölündüğünde 3 kalanını veren bir katıdır.

36; 3 ve 4'ün (ya da $3 \cdot 4$'ün), 5 ile bölündüğünde 1 kalanını veren bir katıdır.

Demek ki; örneğin 80 sayısını bulmak için, $4 \cdot 5$ in, 3 ile bölündüğünde 2 kalanını veren bir katını aramalıymışız. Bunu deneme-yanılma yoluyla yaparız.

$80+135+36$ toplamındaki terimleri daha ayrıntılı inceleyelim:

80 sayısı, 4 ve 5 modül sayılarının bir katı olduğu gibi, $x \equiv 2 \pmod 3$ denkliğindeki 2'nin de bir katıdır.

Demek ki; 80 ya da bunun yerine alacağımız sayılar $4 \cdot 5 \cdot (?) \cdot 2$ biçiminde olmalıdır.

Verdiğimiz toplam her üç denkliği de sağlayacağına göre, ilk denkliği de sağlar.

$4 \cdot 5 \cdot (?) \cdot 2 + 135 + 36 \equiv 2 \pmod 3$

$\Rightarrow 4 \cdot 5 \cdot (?) \cdot 2 \equiv 2 \pmod 3$

$\Rightarrow 4 \cdot 5 \cdot (?) \equiv 1 \pmod 3$ bulunur.

Burada "?" işareti yerine 2, 5, 8, … konulabilir. 80 sayısını elde etmek için (2) konulmuştur.

Aynı şekilde;

135 ya da bunun yerine alınacak sayılar

$3 \cdot 5 \cdot (?) \cdot 3$ biçiminde;

$\left[3 \cdot 5 \cdot (?) \equiv 1 \pmod 4\right]$

36 ya da bunun yerine alınacak sayılar

$3 \cdot 4 \cdot (?) \cdot 1$ biçiminde

$\left[3 \cdot 4 \cdot ? \equiv 1 \pmod 5\right]$ olmalıdır.

Bu çözümlemelere dayanarak, 3 denklikten oluşan bir sistemin çözümünü aşağıdaki gibi genelleştirebiliriz:

m_1, m_2, m_3 ikişer ikişer aralarında asal olmak üzere,

$x \equiv a_1 \pmod{m_1}$

$x \equiv a_2 \pmod{m_2}$

$x \equiv a_3 \pmod{m_3}$

sisteminin çözümü,

$m_2 \cdot m_3 \cdot x_1 \equiv 1 \pmod{m_1}$

$m_1 \cdot m_3 \cdot x_2 \equiv 1 \pmod{m_2}$

$m_1 \cdot m_2 \cdot x_3 \equiv 1 \pmod{m_3}$

olmak üzere,

$x = m_2m_3x_1a_1 + m_1m_3x_2a_2 + m_1m_2x_3a_3 \pmod{m_1 \cdot m_2 \cdot m_3}$ tür.

İfadeyi sadeleştirmek için

$m_1 \cdot m_2 \cdot m_3 = m$ diyelim.

$m_2 \cdot m_3 = \dfrac{m}{m_1}$, $m_1 \cdot m_3 = \dfrac{m}{m_2}$, $m_1 \cdot m_2 = \dfrac{m}{m_3}$ olur.

Buna göre,

$$x = \frac{m}{m_1}x_1a_1 + \frac{m}{m_2}x_2a_2 + \frac{m}{m_3}x_3a_3 \pmod m$$

bulunur.

Bu son çözümü de k tane denklikten oluşan bir sistem için genelleştirebiliriz:

Teorem – 4.74

(Çin Kalan Teoremi)

$m_1, m_2, ..., m_k$ *ikişer ikişer aralarında asal iken*

$x \equiv a_1 \pmod{m_1}$

$x \equiv a_2 \pmod{m_2}$

$\vdots$

$x \equiv a_k \pmod{m_k}$

sisteminin bir çözümü vardır.

$m_1 \cdot m_2 \cdot ... \cdot m_k = m$, $\dfrac{m}{m_1}x_1 \equiv 1 \pmod{m_1}$

$\dfrac{m}{m_2}x_2 \equiv 1 \pmod{m_2}, ..., \dfrac{m}{m_k}x_k \equiv 1 \pmod{m_k}$

olmak üzere

$$\mathbf{x = \frac{m}{m_1}x_1a_1 + \frac{m}{m_2}x_2a_2 + ... + \frac{m}{m_k}x_ka_k \pmod m}$$ *dir.*

Örnek – 4.101

$x \equiv 3 \pmod 4$

$x \equiv 2 \pmod 5$

$x \equiv 4 \pmod 7$

denkliklerini aynı zamanda sağlayan pozitif x tam sayılarını bulunuz.

Çözüm

I. yol

Çin Kalan Teoremi'nde ifade edilen çözümden yararlanalım:

$a_1 = 3$, $m_1 = 4$, $a_2 = 2$, $m_2 = 5$, $a_3 = 4$, $m_3 = 7$ dir.

$5 \cdot 7 \cdot x_1 \equiv 1 \pmod 4 \Rightarrow x_1 \equiv 3 \pmod 4$

$4\cdot 7\cdot x_2 \equiv 1 \pmod 5 \Rightarrow x_2 \equiv 2 \pmod 5$

$4\cdot 5\cdot x_3 \equiv 1 \pmod 7 \Rightarrow x_3 \equiv 6 \pmod 7$ olur.

Buna göre,

$x \equiv 5\cdot 7\cdot 3\cdot 3 + 4\cdot 7\cdot 2\cdot 2 + 4\cdot 5\cdot 6\cdot 4 \pmod{140}$

$\Rightarrow x \equiv 907 \pmod{140}$

$\Rightarrow x \equiv 67 \pmod{140}$ bulunur.

Denklikleri sağlayan pozitif x tam sayıları

$x = 67 + 140\cdot k \ (k \in N)$ biçimindedir.

II. yol

$\boxed{1}$. $x \equiv 3 \pmod 4$

$\boxed{2}$. $x \equiv 2 \pmod 5$

$\boxed{3}$. $x \equiv 4 \pmod 7$

$\boxed{1}$ 'den $x = 3 + 4k \ (k \in Z)$ yazılabilir.

Bu değer $\boxed{2}$'de yerine konulursa

$3 + 4k \equiv 2 \pmod 5$

$\Rightarrow k \equiv 1 \pmod 5$

$\Rightarrow k = 1 + 5p$ bulunur. $(p \in Z)$

$x = 3 + 4k$

$\Rightarrow x = 3 + 4(1 + 5p)$

$\Rightarrow x = 7 + 20p$ olur.

Bu değer de $\boxed{3}$'te yerine konulursa,

$7 + 20p \equiv 4 \pmod 7$

$\Rightarrow p \equiv 3 \pmod 7$

$\Rightarrow p = 3 + 7t$ bulunur. $(t \in Z)$

$x = 7 + 20p$

$\Rightarrow x = 7 + 20(3 + 7t)$

$\Rightarrow x = 67 + 140t$

$\Rightarrow x \equiv 67 \pmod{140}$ olur.

! Bu yöntemi, modüllerin ikişer ikişer aralarında asal olmadığı durumlarda da kullanabiliriz.

III. yol (Kalanları eşitleme yöntemi)

Çin Kalan Teoreminden çözümün
$x \equiv a \pmod{4\cdot 5\cdot 7}$
biçiminde olacağını biliyoruz.

Önce, $\left.\begin{matrix} x \equiv 3 \pmod 4 \\ x \equiv 2 \pmod 5 \end{matrix}\right\}$ sistemini çözelim:

4 ile bölündüğünde 3 kalanını veren sayılar $4\cdot 5 = 20$ ile bölündüğünde 3, 7, 11, 15 19 kalanlarını verebilirler.

Bunlardan 7'nin 5 ile bölümündeki kalan 2'dir. Öyleyse, ikili sistemin çözümü $x \equiv 7 \pmod{20}$ dir.

Böylece, verilen üçlü sistem,

$\left.\begin{matrix} x \equiv 7 \pmod{20} \\ x \equiv 4 \pmod 7 \end{matrix}\right\}$ sistemine dönüşür.

20 ile bölündüğünde 7 kalanını veren sayılar $20\cdot 7 = 140$ ile bölündüğünde 7, 27, 47, 67, 87, 107, 127 kalanlarını verebilirler. Bunlardan 67'nin 7 ile bölümündeki kalan 4'tür.

O hâlde, verilen sistemin çözümü:
$x \equiv 67 \pmod{140}$'tır.

! Kalanları eşitleme yöntemi, modüllerin aralarında asal olmadığı durumlarda da kullanılabilir. Bu durumda; çözümdeki modül, denkliklerdeki modüllerin OKEK'i olarak alınır. Ancak, bu durumda sistem çözümsüz olabilir.

Örnek – 4.102

$x \equiv 1 \pmod 4$

$x \equiv 4 \pmod 5$

$x \equiv 1 \pmod 6$

denkliklerini aynı zamanda sağlayan x tam sayılarını bulunuz.

Çözüm

4 ile bölündüğünde 1 kalanını veren sayılar $4\cdot 5 = 20$ ile bölündüğünde 1, 5, 9, 13, 17 kalanlarını verebilir. Bunlardan 9'un 5 ile bölünündeki kalan 4'tür.

Öyleyse, $x \equiv 9 \pmod{20}$'dir.

20 ile bölündüğünde 9 kalanını veren sayılar $OKEK(20;6) = 60$ ile bölündüğünde 9, 29, 49 kalanlarını verebilirler. Bunlardan 49'un 6 ile bölümündeki kalan 1'dir.

O hâlde sistemin çözümü, $x \equiv 49 \pmod{60}$'tır.

Etkinlik – 4.167

Aşağıda verilen denklik sistemlerini çözünüz.

a. $x \equiv 1 \pmod 3$
$x \equiv 3 \pmod 5$

b. $x \equiv 2 \pmod 3$
$x \equiv 1 \pmod 5$
$x \equiv 3 \pmod 7$

c. $x \equiv 3 \pmod{12}$
$x \equiv 3 \pmod{40}$

d. $x \equiv 2 \pmod 5$
$x \equiv 1 \pmod 6$
$x \equiv 7 \pmod 8$

e. $x \equiv 2 \pmod 8$
$x \equiv 2 \pmod 9$
$x \equiv 2 \pmod{12}$

f. $x \equiv 1 \pmod 3$
$x \equiv 1 \pmod 4$
$x \equiv 1 \pmod 5$
$x \equiv 0 \pmod 7$

Etkinlik – 4.168

Aşağıdaki eşitlikleri sağlayan üç basamaklı en küçük A tam sayılarını bulunuz. ($x, y, z \in Z^+$)

a. $A = 5x - 1 = 7y + 3$
b. $A = 4x + 1 = 6y + 1 = 7z + 1$
c. $A = 5x + 4 = 8y - 1 = 9z + 3$
d. $A = 3x - 2 = 5y + 1 = 8z$

Alıştırmalar ve Problemler – 4.6

1. Aşağıdaki sayıların, yanlarında verilen sayılarla bölünmesindeki kalanları bulunuz.

a. -371 'in 6 ile **b.** 783'ün 8 ile
c. -517 'nin 12 ile **d.** 2007'nin 19 ile

2. Aşağıdaki denkliklerden hangileri doğrudur?

a. $-13 \equiv 17 \pmod 5$
b. $45 \equiv -83 \pmod 8$
c. $-27 \equiv 83 \pmod{22}$
d. $52 \equiv -13 \pmod{26}$
e. $2837 \equiv -3647 \pmod 9$
f. $33335 \equiv -11115 \pmod{11}$

3. Aşağıdaki denklikleri sağlayan en küçük x doğal sayılarını bulunuz.

a. $5x + 4 \equiv 3 \pmod 7$
b. $27 - x \equiv 7 \pmod 9$
c. $3x - 1 \equiv 1 - x \pmod 8$
d. $2x^2 + 4 \equiv x \pmod 5$

4. Aşağıdaki sayıların 5, 6, 7, 8, 9 ve 11 ile bölünmesindeki kalanları bulunuz.

a. 23^{43} **b.** 77^{88} **c.** $49 \cdot 29^{129}$
d. $2^{93} \cdot 4^{39}$ **e.** $9^{99} + 13^{99}$
f. $25^{50} \cdot 69^{70} + 32^{81} \cdot 35^{82}$
g. $13^{125} \cdot 11^{57} - 14^{86} \cdot 9^{59}$
h. $87^{86} \cdot 86^{87} + 73^{72} \cdot 72^{73}$

5. Aşağıdaki sayıların, yanlarında verilen sayılarla bölünmesindeki kalanları bulunuz. ($n \in N$)

a. 3^{4n+3} ün 5 ile **b.** 4^{12n+5} in 7 ile
c. 7^{24n+2} nin 13 ile **d.** 9^{5n+1} in 6 ile
e. 14^{7n+3} ün 6 ile **f.** 17^{36n+2} nin 19 ile

6. 4. alıştırmada verilen sayılar onluk yazma düzeninde yazıldığında, birler basamaklarına hangi rakamlar gelir?

7. Z/m de a'nın çarpma işlemine göre tersi a^{-1} ile gösterildiğine göre, aşağıda istenenleri bulunuz.

a. Z/5 te 2^{-1}, 3^{-1} ve 4^{-1}
b. Z/6 da 3^{-1}, 4^{-1} ve 5^{-1}
c. Z/7 de 3^{-1}, 5^{-1} ve 6^{-1}
d. Z/8 de 5^{-1}, 6^{-1} ve 7^{-1}
e. Z/9 da 4^{-1}, 6^{-1} ve 8^{-1}

f. Z/17 de 7^{-1}, 10^{-1} ve 12^{-1}

g. Z/23 te 9^{-1}, 13^{-1} ve 17^{-1}

8. Z/m de $a^{-n} = \left(a^{-1}\right)^n$ olduğuna göre, aşağıdaki sayıların Z/5, Z/7, Z/8, Z/9, Z/11 ve Z/13 kümelerindeki denklerini bulunuz.

a. 3^{-13} **b.** 4^{-27} **c.** 5^{-43} **d.** 6^{-17}

e. 7^{-15} **f.** 9^{-19} **g.** 14^{-14} **h.** 17^{-17}

9. $30 \cdot x \equiv 45y \pmod{48}$ denkliğini sağlayan her x ve y tam sayıları için, aşağıdaki denklikle-rin hangileri geçerlidir.

a. $6x \equiv 9y \pmod{48}$

b. $2x \equiv 3y \pmod{48}$

c. $10x \equiv 15y \pmod{16}$

d. $8x \equiv 12y \pmod{16}$

e. $60x \equiv 90y \pmod{48}$

f. $60x \equiv 90y \pmod{96}$

10. Z/m de $x^2 = a$ ise x'e a'nın karekökü ve $x^3 = b$ ise x'e b'nin küpkökü denir. Buna göre; Z/5, Z/6, Z/7 ve Z/9 da aşağıdaki sa-yıları bulunuz.

a. 3'ün karekökü **b.** 3'ün küpkökü

c. 4'ün karekökü **d.** 4'ün küpkökü

11. Aşağıdaki sayıların Z/5, Z/6, Z/7 ve Z/9 daki denklerini bulunuz.

a. $\left(\frac{3}{4}\right)^{57}$ **b.** $\left(\frac{5}{3}\right)^{-19}$ **c.** $\left(\frac{4}{5}\right)^{43}$ **d.** $\left(\frac{-3}{8}\right)^{-27}$

12. Aşağıdaki denklemlerin Z/5, Z/6, Z/7 ve Z/9 daki çözüm kümelerini bulunuz.

a. $2x + 3 = 1$ **b.** $4x - 1 = 2$

c. $3(2x - 1) = x + 2$ **d.** $(3x - 4)(5x + 1) = 0$

e. $3x^2 = 2$ **f.** $x^2 - 2x - 2 = 0$

13. Z/5, Z/6, Z/7 ve Z/9 kümelerinde, aşağıdaki bağıntıları sağlayan $y = f(x)$ fonksiyonlarını (varsa) bulunuz.

a. $2x - 3y = 4$ **b.** $3x + 4y = 1$

c. $4x - 2y = 0$ **d.** $xy + 2x - 3y = 1$

14. Aşağıdaki fonksiyonlar, ayrı ayrı Z/5, Z/6, Z/7 ve Z/9 da en geniş tanım kümelerinde tanımlandığına göre, bunların terslerinin $f^{-1}(x)$ kurallarını bulunuz.

a. $f(x) = 2x - 3$ **b.** $f(x) = 4x + 1$

c. $f(x) = \frac{2x+1}{3x+1}$ **d.** $f(x) = \frac{4x-3}{3x+2}$

15. a ve b tam sayılarının 35 ile bölünmesinde kalanlar, sırasıyla 17 ve 23'tür. Aşağıdaki sayıların, yanlarında verilen sayılarla bölün-mesindeki kalanları bulunuz.

a. $a + b$ nin 35 ile

b. $a \cdot b$ nin 5 ile

c. $17a + 23b$ nin 7 ile

d. $a^2 + b^2$ nin 7 ile

16. 1 Ocak 2007 günü pazartesi olduğuna göre;

a. 13 Nisan 2007 hangi güne gelir?

b. 1 Ocak 2009 hangi güne gelir?

17. Bir usta, aralıksız 70 günde bitirebileceği bir işi 2 gün çalışıp 1 gün dinlenerek yapacaktır.

23 Ocak 2007 Salı günü işe başlarsa, işi hangi gün bitirir?

18. $f : Z/7 \to Z/7,\ 3x + 4$

$g : Z/7 \to Z/7,\ 2x - 5$

olduğuna göre, aşağıdaki fonksiyonların ku-rallarını bulunuz.

a. $f \circ g$ **b.** $g \circ f$ **c.** $g \circ f^{-1}$ **d.** $g^{-1} \circ f$

19. $f : Z \to Z,\ f(x) = \begin{cases} 3x - 1 & x \equiv 0 \pmod 2 \\ 2x + 3 & x \equiv 1 \pmod 2 \end{cases}$

$g : Z \to Z,\ g(x) = \begin{cases} 2x - 3 & x \equiv 0 \pmod 3 \\ 3x + 2 & x \equiv 1 \pmod 3 \\ x^2 + 1 & x \equiv 2 \pmod 3 \end{cases}$

olduğuna göre, aşağıdakileri bulunuz.

a. $(f \circ g)(3)$ **b.** $(g \circ f)(-1)$ **c.** $(f \circ g \circ f)(2)$

d. $(f \circ g \circ g)(-2)$ **e.** $(g \circ f)(x)$ **f.** $(f \circ g)(x)$

20. Aşağıda verilen denklemlerin Z/7, Z/8, Z/9 ve Z/12 deki çözüm kümelerinin eleman sayılarını bulunuz.

a. $4x+3=1$ **b.** $5x-3=4$

c. $6x+1=4$ **d.** $10x-2=5$

21. Aşağıdaki denklem sistemlerinin Z/7, Z/8 ve Z/9 daki çözüm kümelerini bulunuz.

a. $\begin{matrix}5x-6y=3\\2x+y=4\end{matrix}$ **b.** $\begin{matrix}2x-3y=5\\6x+5y=1\end{matrix}$

c. $\begin{matrix}4y=3x+1\\6x=2y-1\end{matrix}$ **d.** $\begin{matrix}12x-15y=21\\17x+23y=19\end{matrix}$

22. Aşağıdaki sayıların 11, 13, 17 ve 19 ile bölünmelerindeki kalanları bulunuz.

a. 6^{73} **b.** 18^{81} **c.** 23^{123} **d.** 26^{62}

23. "*Verilen bir doğal sayının birler basamağı ayrılıp bu basamaktaki rakam 4 ile çarpılarak geride kalan sayıya eklendiğinde elde edilen sayı 13 ile bölünüyorsa, verilen sayı da 13 ile bölünür.*" teoremini Etkinlik – 4.164'te ispatlamıştınız.

Aynı yöntemle;

a. 29 ile bölünebilme kuralını bulunuz.

b. 31 ile bölünebilme kuralını bulunuz.

24. Aşağıdaki denklemlerin tam sayılardaki çözüm kümelerini yazınız.

Çözümlere örnekler veriniz.

a. $12x+19y=21$;

b. $13x-23y=73$

c. $27x+24y=33$

d. $41x-7y=29$

25. Aşağıdaki denklem sistemlerinin pozitif tam sayı çözümlerinin kümelerini yazınız.

a. $\begin{matrix}x+y+z=18\\3x+5y-2z=28\end{matrix}$ **b.** $\begin{matrix}x+2y-z=8\\2x+3y-3z=1\end{matrix}$

26. Aşağıdaki denklikleri aynı zamanda sağlayan x tam sayılarını bulunuz.

a. $\begin{matrix}x\equiv 2\pmod 3\\x\equiv 1\pmod 4\end{matrix}$ **b.** $\begin{matrix}x\equiv 1\pmod 3\\x\equiv 1\pmod 5\\x\equiv 0\pmod 7\end{matrix}$

c. $\begin{matrix}x\equiv 2\pmod 3\\x\equiv 1\pmod 4\\x\equiv 5\pmod 8\end{matrix}$ **d.** $\begin{matrix}x\equiv 1\pmod 5\\x\equiv 3\pmod 6\\x\equiv 2\pmod 7\end{matrix}$

27. $x,y,z\in Z$ olmak üzere; aşağıdaki eşitlikleri sağlayan üç basamaklı en küçük A tam sayılarını bulunuz.

a. $A=3x+1=11y-3$

b. $A=4x+1=5y-2=7z+2$

c. $A=5x-3=7y+2=8z-1$

d. $A=4x=5y+2=6z-2$

28. Aşağıdaki sayıların 35, 45, 60 ve 100 ile bölünmelerindeki kalanları bulunuz.

a. 3^{143} **b.** 7^{86} **c.** 29^{47} **d.** 37^{75}

29. Aşağıdaki denklik sistemlerini sağlayan x tam sayılarını bulunuz.

a. $216\cdot x\equiv 1(\mathrm{mod}\,385)$

b. $\left.\begin{matrix}21\cdot x\equiv 1(\mathrm{mod}\,34)\\34\cdot x\equiv 1(\mathrm{mod}\,55)\end{matrix}\right\}$

c. $\left.\begin{matrix}24\cdot x\equiv 1(\mathrm{mod}\,77)\\37\cdot x\equiv 1(\mathrm{mod}\,91)\end{matrix}\right\}$

d. $\left.\begin{matrix}23\cdot x\equiv 56(\mathrm{mod}\,65)\\45\cdot x\equiv 44(\mathrm{mod}\,143)\end{matrix}\right\}$

e. $\left.\begin{matrix}5\cdot x\equiv 13(\mathrm{mod}\,14)\\3\cdot x\equiv 3(\mathrm{mod}\,15)\\7\cdot x\equiv 15(\mathrm{mod}\,17)\end{matrix}\right\}$

30. $a,b \in Z$ ve m asal ise
$(a+b)^m = a^m + b^m \pmod m$
olduğunu ispatlayınız.

31. **a.** Z/4'te x^2+3'ü çarpanlara ayırınız.
b. Z/5'te x^2+1'I çarpanlara ayırınız.
c. Z/5'te x^2+3x-3'ü çarpanlara ayırınız.
d. Z/7'de x^2+2x+4'ü çarpanlara ayırınız.

32. **a.** $\forall n \in N^+$ için $n\left(n^2+5\right)$ in 6 ile bölünebileceğini gösteriniz.
b. $\forall n \in N^+$ için, $n(n+1)(2n+1)$ in 6 ile bölünebileceğini gösteriniz.

33. **a.** $\forall n \in N^+$ için, $3^{2n+1}+2^{n+2}$ nin 7 ile bölünebileceğini gösteriniz.
b. $\forall n \in N^+$ için, $3^{2n+2}+2^{6n+1}$ in 11 ile bölünebileceğini gösteriniz.

34. Aşağıda verilen eşitliklerden yararlanarak, bir doğal sayının bu eşitliklerde geçen asal sayılarla bölünebilme kurallarını bulunuz.
a. $10^2-1=9\cdot 11$ **b.** $10^2+1=101$
c. $10^3-1=27\cdot 37$ **d.** $10^3+1=7\cdot 11\cdot 13$
e. $10^4-1=9\cdot 11\cdot 101$ **f.** $10^4+1=73\cdot 137$