4.5 – Modüler Aritmetik

Etkinlik 4 –145

a. Saat 17'den 7 saat sonra saat 24 (ya da sıfır) olur. Geriye $153-7=146$ saat kalır. Bundan sonraki her 24 saatte bir saat 0'i gösterecektir.

$146=24\cdot 6+2$ olduğundan, saatin 0'ı gösterdiği andan 146 saat sonra saat 2'yi gösterir.

b. Salı gününden 1 gün sonrasının çarşamba olduğuna dikkat ediniz. 7 gün sonrası da yine salı olur.

$45=7\cdot 6+3$ olduğundan, 45 gün sonrası aynı gündür. Bu da cuma'dır.

c. İlk nöbetini tuttuğu günden başlarsak, 9. nöbetine kadar $8\cdot 4=32$ gün geçmiş olur.

$32=7\cdot 4+4$ olduğundan, çarşamba gününden 32 gün sonrası ile 4 gün sonrası aynı gündür. Bu da pazar'dır.

d. 7^1 in birler basamağı 7,
7^2 nin birler basamağı 9,
7^3 ün birler basamağı 3,
7^4 ün birler basamağı 1,
7^5 in birler basamağı 7,
7^6 nın birler basamağı 9,
7^7 nin birler basamağı 3,
7^8 in birler basamağı 1
⋮

7'nin ilk dört kuvvetinin birler basamakları, 7'nin artan kuvvetlerinde periyodik olarak tekrar edilmektedir. 7'nin, 4'ün katı olan kuvvetlerinin birler basamakları 1'dir.

$97=4\cdot 24+1$ olduğundan 7^{96} nın birler basamağı 1, 7^{97} nin birler basamağı 7 olur.

Etkinlik 4 –146

$a, b\in Z$ ve $m\in Z^+$ olsun.

Önce; $a-b$ m ile bölünüyorsa, a ile b'nin m ile bölünmesinde kalanların aynı olacağını gösterelim:

$a=mk_1+r_1,\ \ b=mk_2+r_2$ ve $m\mid a-b$

$\Rightarrow a-b=mk_1+r_1-mk_2-r_2$
$\Rightarrow a-b=m(k_1-k_2)+r_1-r_2$
$\Rightarrow m\mid r_1-r_2$ olur.

$0\le r_1<m$ ve $0\le r_2<m$
$\Rightarrow 0\le r_1<m$ ve $-m<-r_2\le 0$
$\Rightarrow -m<r_1-r_2<m$
$\Rightarrow m\cdot(-1)<r_1-r_2<m\cdot 1$
$\Rightarrow r_1-r_2=m\cdot 0$
$\Rightarrow r_1-r_2=0$
$\Rightarrow r_1=r_2$ bulunur.

Karşıt olarak;

$a=mk_1+r$ ve $b=mk_2+r$
$\Rightarrow a-b=mk_1+r-mk_2-r$
$\Rightarrow a-b=(k_1-k_2)$
$\Rightarrow m\mid a-b$ bulunur.

Teorem – 4.65'e dayanılarak,

$\mathbf{a\equiv b\ (mod\ m)\Leftrightarrow a-b\equiv 0\ (mod\ m)}$ yazılabilir.

Etkinlik 4 –147

1 $a\equiv b\ (mod\ m)$ ve $c\equiv d\ (mod\ m)$
$\Rightarrow m\mid a-b$ ve $m\mid c-d$
$\Rightarrow a-b=m\cdot x$ ve $c-d=my,\ \ x,y\in Z$
$\Rightarrow (a-b)+(c-d)=mx+my$
$\Rightarrow (a+c)-(b+d)=m(x+y)$
$\Rightarrow m\mid (a+c)-(b+d)$
$\Rightarrow (a+c)\equiv (b+d)\ (mod\ m)$

2 $a\equiv b\ (mod\ m)$ ve $c\equiv d\ (mod\ m)$
$\Rightarrow a-b=mx$ ve $c-d=my$
$\Rightarrow (a-b)-(c-d)=mx-my$
$\Rightarrow (a-c)-(b-d)=m(x-y)$
$\Rightarrow m\mid (a-c)-(b-d)$
$\Rightarrow (a-c)\equiv (b-d)\ (mod\ m)$

3 $a\equiv b\ (mod\ m)$ ve $c\equiv d\ (mod\ m)$
$\Rightarrow a-b=mx$ ve $c-d=my$

$\Rightarrow a = b + mx \text{ ve } c = d + my$
$\Rightarrow a \cdot c = (b + mx) \cdot (d + my)$
$\Rightarrow a \cdot c = b \cdot d + mby + mdx + m^2xy$
$\Rightarrow a \cdot c - b \cdot d = m(by + dx + mxy)$
$\Rightarrow m \mid a \cdot c - b \cdot d$
$\Rightarrow a \cdot c \equiv b \cdot d \pmod{m}$

Etkinlik – 4.148

a. $47 \equiv 5 \pmod 7$
$\Rightarrow 47^{74} \equiv 5^{74} \pmod 7$ olur.
$5 \equiv 5 \pmod 7$
$\Rightarrow 5^2 \equiv 4 \pmod 7$
$\Rightarrow 5^3 \equiv -1 \pmod 7$
$\Rightarrow \left(5^3\right)^{24} \equiv (-1)^{24} \pmod 7$
$\Rightarrow 5^{72} \equiv 1 \pmod 7$
$\Rightarrow 5^{72} \cdot 5^2 \equiv 1 \cdot 4 \pmod 7$
$\Rightarrow 5^{74} \equiv 4 \pmod 7 \Rightarrow 47^{74} \equiv 4 \pmod 7$
bulunur.

b. $8 \equiv 2 \pmod 6$
$\Rightarrow 8^2 \equiv 4 \pmod 6$
$\Rightarrow 8^3 \equiv 2 \pmod 6$
$\Rightarrow 8^4 \equiv 4 \pmod 6$
$\vdots$
$\Rightarrow 8^{87} \equiv 2 \pmod 6$ bulunur.

c. $11 \equiv 11 \pmod{13}$
$\Rightarrow 11^2 \equiv 4 \pmod{13}$
$\Rightarrow 11^4 \equiv 3 \pmod{13}$
$\Rightarrow 11^6 \equiv -1 \pmod{13}$
$\Rightarrow \left(11^6\right)^{22} \equiv (-1)^{22} \pmod{13}$
$\Rightarrow 11^{132} \equiv 1 \pmod{13}$
$\Rightarrow 11^{132} \cdot 11^3 \equiv 1 \cdot 5 \pmod{13}$
$\Rightarrow 11^{135} \equiv 5 \pmod{13}$ bulunur.

d. $10 \equiv 10 \pmod{17}$
$\Rightarrow 10^2 \equiv -2 \pmod{17}$
$\Rightarrow 10^4 \equiv 4 \pmod{17}$
$\Rightarrow \left(10^8\right) \equiv -1 \pmod{17}$
$\Rightarrow \left(10^8\right)^{34} \equiv (-1)^{34} \pmod{17}$
$\Rightarrow 10^{272} \equiv 1 \pmod{17}$
$\Rightarrow 10^{272} \cdot 10^7 \equiv 1 \cdot 5 \pmod{17} \quad \left[10^7 \equiv (-7) \cdot (-2) \cdot 4\right]$
$\Rightarrow 10^{279} \equiv 5 \pmod{17}$ bulunur.

e. $2006^{2007} + 2007^{2006}$ toplamının 10 modülüne göre dengini bulacağız.
$2006 \equiv 6 \pmod{10}$
$\Rightarrow 2006^{2007} \equiv 6^{2007} \pmod{10}$ olur.
$6 \equiv 6 \pmod{10}$
$\Rightarrow 6^2 \equiv 6 \pmod{10}$
$\vdots$
$\Rightarrow 6^{2007} \equiv 6 \pmod{10}$
$\Rightarrow 2006^{2007} \equiv 6 \pmod{10}$ bulunur.
$2007 \equiv 7 \pmod{10}$ dir.
$7 \equiv 7 \pmod{10}$
$\Rightarrow 7^2 \equiv 9 \pmod{10}$
$\Rightarrow 7^4 \equiv 1 \pmod{10}$
$\Rightarrow 7^{2004} \equiv 1 \pmod{10}$
$\Rightarrow 7^{2006} \equiv 9 \pmod{10}$
$\Rightarrow 2007^{2006} \equiv 9 \pmod{10}$ olur.
$2006^{2007} \equiv 6 \pmod{10}$ ve
$2007^{2006} \equiv 9 \pmod{10}$
$\Rightarrow 2006^{2007} + 2007^{2006} \equiv 5 \pmod{10}$ bulunur.

f. $23 \equiv 1 \pmod{11}$, $83^{83} \equiv 7 \pmod{11}$
$37 \equiv 4 \pmod{11}$ ve $73^{73} \equiv 2 \pmod{11}$
olduğunu bulunuz.
$23 \cdot 83^{83} + 37 \cdot 73^{73}$ toplamında her sayı yerine 11 modülüne göre dengi konulursa,
$23 \cdot 83^{83} + 37 \cdot 73^{73} \equiv 1 \cdot 7 + 4 \cdot 2 \pmod{11}$
$\equiv 4 \pmod{11}$
bulunur.

Etkinlik – 4.149

a. $17+153=170$ olup saat 170'in 24 modülüne göre dengini, yani 2'yi gösterir.

$170 \equiv 2 \pmod{24}$

b. $45 \equiv 3 \pmod 7$ olduğundan 45 gün sonrası ile 3 gün sonrası aynı gündür ve bu cuma'dır.

$0 \to$ Salı $\quad 1 \to$ Çarşamba

$2 \to$ Perşembe $\quad 3 \to$ Cuma

c. 9. nöbetini çarşamba gününden itibaren $4 \cdot 8 = 32$ gün sonra tutar.

$32 \equiv 4 \pmod 7$ olduğundan, o gün pazar'dır.

$0 \to$ Çarşamba $\quad 1 \to$ Perşembe

$2 \to$ Cuma $\quad 3 \to$ Cumartesi

$4 \to$ Pazar

d. $7 \equiv 7 \pmod{10}$

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

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

$\Rightarrow 7^{96} \equiv 1 \pmod{10}$

$\Rightarrow 7^{97} \equiv 7 \pmod{10}$

7^{97} nin birler basamağı 7'dir.

Etkinlik – 4.150

$a, b, x \in Z;\ x \neq 0,\ m \in Z^+$ ve $OBEB(|x|, m) = d$ olsun.

Farklı iki durum mümkündür.

1. $x \in Z^+$ ise;

$|x| = x = dx_1$ ve $m = dm_1$ diyebiliriz.

Burada, x_1 ve m_1 aralarında asaldır.

$a \cdot x \equiv b \cdot x \pmod m$

$\Rightarrow m \mid ax - bx$

$\Rightarrow (a-b) \cdot x = m \cdot k \quad (k \in Z)$

$\Rightarrow (a-b) \cdot d \cdot x_1 = d \cdot m_1 \cdot k \quad (x = dx_1, m = dm_1)$

$\Rightarrow (a-b)x_1 = m_1 \cdot k \quad (ÇS)$

$\Rightarrow m_1 \mid (a-b) \quad [OBEB(m_1, x_1) = 1]$

$\Rightarrow a \equiv b \pmod{m_1}$

$\Rightarrow a \equiv b \pmod{\frac{m}{d}} \quad \left(m_1 = \frac{m}{d}\right)$

2. $x \in Z^-$ ise $x = -y,\ y \in Z^+$ vardır.

$|x| = |-y| = y$ olur.

$a \cdot x \equiv b \cdot x \pmod m$

$\Rightarrow a \cdot (-y) \equiv b \cdot (-y) \pmod m$

$\Rightarrow (-a) \cdot y \equiv (-b) \cdot y \pmod m$

$\Rightarrow -a \equiv -b \pmod m \quad [OBEB(m, y) = 1]$

$\Rightarrow a \equiv b \pmod m \quad [-1 \equiv -1 \pmod m]$

Etkinlik –4.151

Önce; $a \equiv b \pmod m$ denkliğinde a, b, m sayılarının bir ortak bölenleri ile bölünebileceğini gösterelim:

$x \in Z$ olmak üzere;

$a = a' \cdot x,\ b = b' \cdot x,\ m = m' \cdot x$ olsun.

$a \equiv b \pmod m$

$\Rightarrow a - b = k \cdot m \quad (k \in Z, k \neq 0)$

$\Rightarrow a'x - b'x = k \cdot m'x$

$\Rightarrow x(a' - b') = k \cdot m'x$

$\Rightarrow a' - b' = k \cdot m' \quad (ÇS)$

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

Şimdi de; $a \equiv b \pmod m$ denkliğinde a, b, m sayılarının bir $y \in Z^+$ ile çarpılabileceğini gösterelim.

$a \equiv b \pmod m$

$\Rightarrow a - b = km \quad (k \in Z, k \neq 0)$

$\Rightarrow y \cdot (a-b) = k \cdot m \cdot y \quad (ÇS)$

$\Rightarrow ay - by = k(my)$

$\Rightarrow ay \equiv by \pmod{my}$

Etkinlik –4.152

$\forall x \in Z$ için $(x, x) \in \beta$ mı?

$5 \mid x - x$ olduğundan $(x, x) \in \beta$ olup β yansıyandır.

$\forall (x, y) \in \beta$ için $(y, x) \in \beta$ mı?

$(x, y) \in \beta \Rightarrow 5 \mid x - y$

$\Rightarrow x - y = 5k, \quad k \in Z$

$\Rightarrow y - x = 5 \cdot (-k)$

$\Rightarrow 5 \mid y - x$

$\Rightarrow (y, x) \in \beta$

olduğundan β simetriktir.

$\forall (x,y) \in \beta$ ve $(y,z) \in \beta$ için $(x,z) \in \beta$ mı?

$(x,y) \in \beta$ ve $(y,z) \in \beta$

$\Rightarrow x - y = 5k$ ve $y - z = 5p$

$\Rightarrow (x-y)+(y-z) = 5k + 5p$

$\Rightarrow x - z = 5(k+p)$

$\Rightarrow 5 \mid x - z$

$\Rightarrow (x,z) \in \beta$

olduğundan β geçişkendir.

Öyleyse, β bir denklik bağıntısıdır.

Etkinlik – 4.153

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

$a+b \in Z$ olduğundan $\overline{a+b} \in Z/m$ dir.

Z/m kümesi $\oplus$ işlemine göre kapalıdır.

2. $(\bar{a} \oplus \bar{b}) \oplus \bar{c} = (\overline{a+b}) \oplus \bar{c}$

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

$= \overline{a+(b+c)}$

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

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

$\oplus$ işleminin birleşme özeliği vardır.

3. $\bar{a} \oplus \bar{b} = \overline{a+b}$

$= \overline{b+a}$

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

$\oplus$ işleminin değişme özeliği vardır.

4. $\forall \bar{a} \in Z/m$ için $\bar{a} \oplus \bar{x} = \bar{a} = \bar{x} \oplus \bar{a}$ eşitliğini sağlayan $\bar{x} \in Z/m$ in varlığını göstereceğiz.

$\oplus$ işleminin değişme özeliği olduğundan $\bar{a} \oplus \bar{x} = \bar{a}$ eşitliğini sağlayan $\bar{x} \in Z/m$ in varlığını göstermek yeter.

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

$\Rightarrow \overline{a+x} = \bar{a}$

$\Rightarrow a + x \equiv a \pmod{m}$

$\Rightarrow a + x \equiv a + 0 \pmod{m}$

$\Rightarrow x \equiv 0 \pmod{m}$

$\Rightarrow \bar{x} = \bar{0}$ olur.

Z/m de toplama işlemine göre etkisiz eleman $\bar{0}$ dır.

5. $\forall \bar{a} \in Z/m$ için $\bar{a} \oplus \bar{x} = \bar{0} = \bar{x} + \bar{a}$ eşitliğini sağlayan $\bar{x} \in Z/m$ in varlığını göstereceğiz.

$\oplus$ işleminin değişme özeliği olduğundan $\bar{a} \oplus \bar{x} = \bar{0}$ eşitliğini sağlayan $\bar{x} \in Z/m$ in varlığını göstermek yeter.

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

$\Rightarrow \overline{a+x} = \bar{0}$

$\Rightarrow a + x \equiv 0 \pmod{m}$

$\Rightarrow x \equiv -a \pmod{m}$

$\Rightarrow x \equiv m - a \pmod{m}$ $\quad (0 \le m-a < m)$

$\Rightarrow \bar{x} = \overline{m-a}$ bulunur.

$\bar{a} \in Z/m$ in toplama işlemine göre tersi $\overline{-a}$ (ya da $\overline{m-a}$) dır.

Etkinlik – 4.154

İlk beş önermenin doğruluğunu,
Etkinlik – 4.153 deki gibi gösteriniz.

6. $\forall \bar{a}, \bar{b}, \bar{c} \in Z/m$ için;

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

$= \overline{a \cdot (b+c)}$

$= \overline{(a \cdot b) + (a \cdot c)}$

$= \overline{(a \cdot b)} \oplus \overline{(a \cdot c)}$

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

Sağdan dağılma özeliğini siz gösteriniz.

Etkinlik – 4.155

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

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

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

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

a. Tablo ile verilmiş bir işlemde bir elemanın tersi, o elemanın bulunduğu satırdaki birim elemanın bulunduğu sütunun başındaki elemandır. (Neden?)

$\bar{a}$ nın toplamaya göre tersini $-\bar{a}$; çarpmaya göre tersini $(\bar{a})^{-1}$ ile gösterelim.

Z/5 te $-\bar{0}=0,\ -\bar{1}=\bar{4},\ -\bar{2}=\bar{3},\ -\bar{3}=\bar{2},\ -\bar{4}=\bar{1}$ dir.

$(\bar{0})^{-1}$ yoktur. $(\bar{1})^{-1}=1,\ (\bar{2})^{-1}=3,\ (\bar{3})^{-1}=\bar{2}$,

$(\bar{4})^{-1}=4$ tür.

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

$(\bar{0})^{-1}$, $(\bar{2})^{-1}$, $(\bar{3})^{-1}$, $(\bar{4})^{-1}$ yoktur.

$(\bar{1})^{-1}=\bar{1},\ (\bar{5})^{-1}=\bar{5}$ tir.

b. Z/6 da,

$\bar{4}\oplus\bar{3}\odot(\bar{5}\oplus\bar{2})\oplus\bar{3}\odot\bar{4}$
$=\bar{4}\oplus\bar{3}\odot\bar{1}\oplus\bar{0}$
$=\bar{4}\oplus\bar{3}\oplus\bar{0}$
$=\bar{1}$ bulunur.

c. Z/5 te,

$2x+3=4$
$\Rightarrow 2x+3+2=4+2$
$\Rightarrow 2x=1$
$\Rightarrow 2^{-1}\cdot 2\cdot x=2^{-1}\cdot 1$
$\Rightarrow x=3\cdot 1$
$\Rightarrow x=3$ olur.
$Ç=\{\bar{3}\}$ dir.

d. Z/6 da,

$3x+5=2$
$\Rightarrow 3x+5+1=2+1$
$\Rightarrow 3x=3$ olur.

Z/6 da 3^{-1} yoktur.

Çarpım tablosunda 3'ün bulunduğu satırda, 3'ü veren $x\in Z/6$ lar seçilir.

$3\cdot 1=3,\ 3\cdot 3=3$ ve $3\cdot 5=3$ olduğundan

$Ç=\{\bar{1},\bar{3},\bar{5}\}$ dir.

Etkinlik – 4.156

$\bar{b}=\bar{c}\Rightarrow\bar{a}\odot\bar{b}=\bar{a}\odot\bar{c}$ olacağı açıktır.

$\bar{a}\odot\bar{b}=\bar{a}\odot\bar{c}\Rightarrow\bar{b}=\bar{c}$ olduğunu ispatlayalım:

Z/m de, m asal ve

$\bar{a}\odot\bar{b}=\bar{a}\odot\bar{c}$
$\Rightarrow\overline{a\cdot b}=\overline{a\cdot c}$
$\Rightarrow a\cdot b\equiv a\cdot c\pmod m$
$\Rightarrow b\equiv c\pmod m$ (m asal)
$\Rightarrow\bar{b}=\bar{c}$ bulunur.

Etkinlik – 4.157

$\oplus$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$\odot$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

a. Z/7 de, $\bar{3}\odot\bar{x}\odot\bar{6}=\bar{5}$
$\Rightarrow\bar{x}\odot(\bar{3}\odot\bar{6})=\bar{5}$ (Değ. ve Bir.)
$\Rightarrow\bar{x}\odot\bar{4}=\bar{5}$
$\Rightarrow\bar{x}\odot\bar{4}\odot\bar{2}=\bar{5}\odot\bar{2}$
$\Rightarrow\bar{x}=\bar{3}$

b. Z/7 de, $\bar{4}\odot\bar{x}\odot\bar{3}=\bar{0}$
$\Rightarrow\bar{x}\odot(\bar{4}\odot\bar{3})=\bar{0}$
$\Rightarrow\bar{x}\odot\bar{5}=\bar{0}$
$\Rightarrow\bar{x}\odot\bar{5}\odot\bar{3}=\bar{0}\odot\bar{3}$
$\Rightarrow\bar{x}=\bar{0}$

c. Çarpım tablosunda, köşegen üzerinde bulunmayan sayıların Z/7 de karekökleri yoktur. Bunlar da $\bar{3}$, $\bar{5}$ ve $\bar{6}$ dır.

d. Z/7 de, $\bar{0}^3=\bar{0},\ \bar{1}^3=\bar{1},\ \bar{2}^3=\bar{1},\ \bar{3}^3=\bar{6},$
$\bar{4}^3=\bar{1},\ \bar{5}^3=\bar{6},\ \bar{6}^3=\bar{6}$ dır.

Buna göre; $\bar{2}$, $\bar{3}$, $\bar{4}$ ve $\bar{5}$ in küpkökü yoktur.

e. Z/7 de, $3x^2+2=1$
$\Rightarrow 3x^2+2+5=1+5$
$\Rightarrow 3x^2=6$
$\Rightarrow 5\cdot 3\cdot x^2=5\cdot 6$
$\Rightarrow x^2=2$ olur.

Çarpım tablosundan $3 \odot 3 = 2$ ve $4 \odot 4 = 2$ olduğu görülür.

$Ç = \{\overline{3}, \overline{4}\}$ dir.

f. Z/7 de, $2x^2 + 6 = 5$

$\Rightarrow 2x^2 + 6 + 1 = 5 + 1$

$\Rightarrow 2x^2 = 6$

$\Rightarrow 4 \cdot 2 \cdot x^2 = 4 \cdot 6$

$\Rightarrow x^2 = 3$ olur.

Z/7 de karesi 3 olan sayı yoktur. $Ç = \varnothing$ dir.

Etkinlik –4.158

Z/m de $\overline{a} \odot \overline{x} = \overline{b}$ denkleminde, b sayısı $OBEB(a,m)$ ile bölünüyorsa, denklemin kökü vardır.

İspatlayalım:

$OBEB(a,m) = d$, $a = a' \cdot d$, $m = m' \cdot d$ ve $b = b' \cdot d$ olsun.

Z/m de $\overline{a} \odot \overline{x} = \overline{b}$

$\Rightarrow a \cdot x = b \pmod{m}$

$\Rightarrow ax - b = k \cdot m \quad (k \in Z)$

$\Rightarrow a' \cdot d \cdot x - b' \cdot d = k \cdot m' \cdot d$

$\Rightarrow a'x - b' = k \cdot m' \quad$ (ÇS)

$\Rightarrow a'x \equiv b' \pmod{m'}$

$\Rightarrow Z/m'$ de $\overline{a'} \odot \overline{x} = \overline{b'}$ olur.

a' ve m' aralarında asal olduklarından $\overline{a'} \odot \overline{x} = \overline{b'}$ denkleminin bir tane kökü vardır. (Teorem – 4.71) Bu kök, Z/m de $\overline{a} \odot \overline{x} = \overline{b}$ denkleminin köklerinden biridir.

Z/m'de $\overline{a} \odot \overline{x} = \overline{b}$ denkleminin kökü varsa, b sayısı $OBEB(a,m)$ ile bölünür.

İspatlayalım:

$OBEB(a,m) = d$, $a = a'd$, $m = m'd$ ve denklemin kökü $\overline{x_0}$ olsun.

Z/m de $\overline{a} \odot \overline{x_0} = \overline{b}$

$\Rightarrow a \cdot x_0 = b \pmod{m}$

$\Rightarrow ax_0 - b = km$

$\Rightarrow b = ax_0 - km$

$\Rightarrow b = a' \cdot d \cdot x_0 - k \cdot m' \cdot d$

$\Rightarrow b = d(a'x_0 - km')$

$\Rightarrow d \mid b$

Z/m de $\overline{a} \odot \overline{x} = \overline{b}$ denkleminde b sayısı $OBEB(a,m)$ ile bölünüyorsa, denklemin $OBEB(a,m)$ tane kökü vardır.

İspatlayalım:

$OBEB(a,m) = d$; $a = a'd$; $b = b'd$ ve $m = m'd$ olsun.

Z/m de, $\overline{a} \odot \overline{x} = \overline{b}$

$\Rightarrow Z/m'$ de $\overline{a'} \odot \overline{x} = \overline{b'}$ olup bu denklemin bir tane kökü vardır. (Teorem – 4.71)

Bu kök x_0 olsun.

$x_0 \equiv x_0 + m' \equiv x_0 + 2m' \equiv \ldots \equiv x_0 + (d-1)m' \pmod{m}$

$x_0 < m'$

$\Rightarrow x_0 + (d-1)m' < m' + (d-1)m'$

$\Rightarrow x_0 + (d-1)m' < m' \cdot d$

$\Rightarrow x_0 + (d-1)m' < m$ olur.

Buna göre,

$x_0, x_0 + m', x_0 + 2m', \ldots, x_0 + (d-1)m'$ değerleri Z/m' de $\overline{a'} \odot \overline{x} = \overline{b'}$ denkleminin aynı $\overline{x_0}$ kökünü belirtirken, Z/m de $\overline{a} \odot \overline{x} = \overline{b}$ denkleminin d tane [$OBEB(a,m) = d$] farklı köklerini belirtirler.

Etkinlik – 4.159

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

$\Rightarrow 2x = 2$ olur.

$OBEB(2,4) = 2$ ve $2 \mid 2$ olduğundan denklemin çözüm kümesi 2 elemanlıdır.

$2x = 2 \pmod{4}$

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

$\Rightarrow x_1 = 1$ ve $x_2 = 1 + 2 = 3$

$\Rightarrow Ç = \{1, 3\}$ bulunur.

b. $m = 7$ asal olduğundan çözüm kümesi 1 elemanlıdır.

Z/7 de $4x + 6 = 5$

$\Rightarrow 4x+6+1=5+1 \pmod 7$

$\Rightarrow 4x=6 \pmod 7$

$\Rightarrow 2\cdot 4\cdot x=2\cdot 6 \pmod 7$

$\Rightarrow x=5 \pmod 7$

$\Rightarrow Ç=\{\bar{5}\}$ olur.

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

$\Rightarrow 5x=4$ olur.

$OBEB(8,5)=1$ olduğundan, denklemin çözüm kümesi 1 elemanlıdır.

$5x=4 \pmod 8$

$\Rightarrow 5\cdot 5\cdot x=5\cdot 4 \pmod 8$

$\Rightarrow x=4 \pmod 8$

$\Rightarrow Ç=\{4\}$ bulunur.

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

$\Rightarrow 3x=7$ olur.

$OBEB(3,9)=3$ tür. 7, 3 ile bölünmediğinden $Ç=\varnothing$ dir.

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

$\Rightarrow 6x=4$ olur.

$OBEB(6,12)=6$ dır. 4, 6 ile bölünmediğinden $Ç=\varnothing$ dir.

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

$\Rightarrow 5x=10$ olur.

$OBEB(5,15)=5$ tir. $5|10$ olduğundan çözüm kümesi 5 elemanlıdır.

$5x=10 \pmod{15}$

$\Rightarrow x=2 \pmod 3$

$\Rightarrow x_1=2,\ x_2=5,\ x_3=8,\ x_4=11,\ x_5=14$

$\Rightarrow Ç=\{2,5,8,11,14\}$ bulunur.

Etkinlik – 4.160

a. Z/8 de, $3x+4y=5$

$\Rightarrow 3x=5-4y$

$\Rightarrow 3x=5+4y$ olur.

$OBEB(3,8)=1$ olduğundan Z/8 de 3'ün çarpma işlemine göre tersi vardır ve bu 3'tür.

$3x\equiv 5+4y \pmod 8$

$\Rightarrow 3\cdot 3x\equiv 3\cdot(5+4y) \pmod 8$

$\Rightarrow x=7+4y \pmod 8$ bulunur.

Eşitliği sağlayan $(\bar{x},\bar{y})$ ikililerinin kümesi

$\{(\bar{7},\bar{0}),(\bar{3},\bar{1}),(\bar{7},\bar{2}),(\bar{3},\bar{3}),(\bar{7},\bar{4}),(\bar{3},\bar{5}),(\bar{7},\bar{6}),(\bar{3},\bar{7})\}$ olur.

b. Z/7 de $5x+3y=4$

$\Rightarrow 3y\equiv -5x+4 \pmod 7$

$\Rightarrow 3y\equiv 2x+4 \pmod 7$

$\Rightarrow 5\cdot 3\cdot y=5\cdot 2\cdot x+5\cdot 4 \pmod 7$

$\Rightarrow y\equiv 3x+6 \pmod 7$

$\Rightarrow Z/7$ de $y=3x+6$ bulunur.

c. $f(x)=y$ diyerek, x'i y türünden yazacağız.

Z/7 de $y=3x+1$

$\Rightarrow 3x\equiv y-1 \pmod 7$

$\Rightarrow 5\cdot 3\cdot x\equiv 5y-5 \pmod 7$

$\Rightarrow x\equiv 5y+2 \pmod 7$

$\Rightarrow f^{-1}(y)\equiv 5y+2 \pmod 7$

$\Rightarrow Z/7$ de $f^{-1}(y)=5x+2$ bulunur.

d. $f: Z/5-\{\bar{2}\}\to Z/5,\ f\left(x=\dfrac{3x+2}{x-2}\right)$ ise

$f(\bar{0})=-\bar{1}=\bar{4},\ f(\bar{1})=-\bar{5}=\bar{0},\ f(\bar{3})=\overline{11}=\bar{1},$

$f(\bar{4})=\bar{6}=\bar{1}$ olur.

Etkinlik –4.161

m asal ise, Z/m de çarpım tablosundaki sıfırdan farklı her $\bar{a}$ satırında farklı sıra ile 0, 1, 2, …, $m-1$ sayıları bulunur.

Bu sayılar a'nın yine farklı sıra ile 0, 1, 2, …, $m-1$ katlarıdır. Burada $\bar{a}\cdot\bar{0}=\bar{0}$ olup a'nın sıfırdan farklı katları sıfırdan farklıdır.

Buna göre, aşağıdaki denkliklerin her birinin sağ yanında 1, 2, …, $m-1$ sayılarından yalnız biri bulunur.

Bu denklikler taraf tarafa çarpılırsa;

$a\cdot 1\equiv ? \pmod m$

$a\cdot 2\equiv ? \pmod m$

$\vdots$

$$\underline{\times\ a\cdot(m-1)\equiv ?\pmod m}$$

$a^{m-1}\cdot 1\cdot 2\cdot\ldots\cdot(m-1)\equiv 1\cdot 2\cdot\ldots\cdot(m-1)\pmod m$

$\Rightarrow a^{m-1}\equiv 1\pmod m$ bulunur.

Etkinlik –4.162

a. $5^{10}\equiv 1\pmod{11}$ (Fermat'ın küçük teo.)

$\left.\begin{array}{l}\Rightarrow 5^{120}\equiv 1\pmod{11}\\ 5\equiv 5\pmod{11}\\ \Rightarrow 5^{2}\equiv 3\pmod{11}\end{array}\right\}$ Taraf tarafa çarparsak

$5^{123}\equiv 4\pmod{11}$ bulunur.

b. $15^{16}\equiv 1\pmod{17}$ (Fermat'ın küçük teo.)

$\Rightarrow 15^{132}\equiv 1\pmod{17}$ dir.

$15\equiv -2\pmod{17}$

$\Rightarrow 15^{2}\equiv 4\pmod{17}$

$\Rightarrow 15^{4}\equiv -1\pmod{17}$

$\Rightarrow 15^{8}\equiv 1\pmod{17}$

$\Rightarrow 15^{11}\equiv 9\pmod{17}$ olur.

$\left.\begin{array}{l}15^{132}\equiv 1\pmod{17}\\ 15^{11}\equiv 9\pmod{17}\end{array}\right\}$ Taraf tarafa çarpılırsa

$15^{143}\equiv 9\pmod{17}$ bulunur.

c. $28^{22}\equiv 1\pmod{23}$ (Fermat'ın küçük teo.)

$\Rightarrow 28^{88}\equiv 1\pmod{23}$ tür.

$28\equiv 5\pmod{23}$

$\Rightarrow 28^{2}\equiv 2\pmod{23}$

$\Rightarrow 28^{90}\equiv 2\pmod{23}$ bulunur.

Etkinlik –4.163

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

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

a. $1\cdot a_0\equiv 1\cdot a_0\pmod 3$

$10\cdot a_1\equiv 1\cdot a_1\pmod 3$

$10^2a_2\equiv 1\cdot a_2\pmod 3$

$\vdots$

$+\ \underline{10^n a_n\equiv 1\cdot a_n\pmod 3}$

$a\equiv(a_0+a_1+a_2+\ldots+a_n)\pmod 3$

b. $1\cdot a_0\equiv 1\cdot a_0\pmod 4$

$10\cdot a_1\equiv 2\cdot a_1\pmod 4$

$10^2a_2\equiv 0\pmod 4$

$\vdots$

$+\ \underline{10^n\cdot a_n\equiv 0\pmod 4}$

$a\equiv(a_0+2a_1)\pmod 4$

a sayısının birler basamağındaki rakamı ile onlar basamağındaki rakamının 2 katının toplamının 4 ile bölünmesindeki kalan, a sayısının 4 ile bölünmesindeki kalana eşittir.

c. a'daki gibi yapınız.

d. $1\cdot a_0\equiv 1\cdot a_0\pmod{11}$

$10\cdot a_1\equiv -1\cdot a_1\pmod{11}$

$10^2\cdot a_2\equiv 1\cdot a_2\pmod{11}$

$10^3\cdot a_3\equiv -1\cdot a_3\pmod{11}$

$+\ \vdots$

$a\equiv a_0-a_1+a_2-a_3+\ldots\pmod{11}$

e. $1\cdot a_0\equiv 1\cdot a_0\pmod{13}$

$10\cdot a_1\equiv -3\cdot a_1\pmod{13}$

$10^2\cdot a_2\equiv -4\cdot a_2\pmod{13}$

$10^3\cdot a_3\equiv -1\cdot a_3\pmod{13}$

$10^4\cdot a_4\equiv 3\cdot a_4\pmod{13}$

$10^5\cdot a_5\equiv 4\cdot a_5\pmod{13}$

$10^6\cdot a_6\equiv -1\cdot a_6\pmod{13}$

$+\ \vdots$

$a\equiv a_0-3a_1-4a_2-a_3+3a_4+4a_5-\ldots\pmod{13}$

(10'un kuvvetlerinin 13 modülüne göre denklerini yazarken, mutlak değerce en küçük olanlarını seçtiğimize dikkat ediniz.)

Bir örnek verelim;

235147 sayısının 13 ile bölünmesindeki kalanı bulalım:

$\begin{array}{cccccc}2&3&5&1&4&7\\ \uparrow&\uparrow&\uparrow&\uparrow&\uparrow&\uparrow\\ 4&3&-1&-4&-3&1\end{array}\rightarrow 8+9-5-4-12+7=3$

Verilen sayının 13 ile bölünmesinde kalan 3'tür.

f. e'deki gibi yapınız.

(10'un, en az 10^8 'e kadar olan kuvvetlerinin 17 modülüne göre denklerini bulmanız gerekecektir.)

Etkinlik –4.164

$a = a_n a_{n-1}...a_3a_2a_1a_0$

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

$\Rightarrow a = 10\left(\frac{1}{10}a_0 + \underbrace{a_1 + 10a_2 + 10^2a_3 + ... + 10^{n-1}a_n}_{a_n a_{n-1}...a_3a_2a_1}\right)$

$\Rightarrow a \equiv 10\left(\frac{1}{10}a_0 + a_n a_{n-1}...a_3a_2a_1\right) \pmod{13}$

Z/13 te, $\left(\frac{\bar{1}}{10}\right) = \left(\frac{\overline{1+39}}{10}\right) = \bar{4}$ olduğundan

$a \equiv 10(4a_0 + a_n a_{n-1}...a_3a_2a_1) \pmod{13}$ bulunur.

$4a_0 + a_n a_{n-1}...a_3a_2a_1 = b$ diyelim.

b sayısı 13 ile bölünürse $a = 10b$ sayısının da 13 ile bölüneceği açıktır. b'nin 13 ile bölünmesinde kalan r ise, a'nın 13 ile bölünmesindeki kalan $10 \cdot r$ nin 13 modülüne göre dengi olur.

a. Aşağıda alt alta yazılmış sayılardan her biri, bir üstteki sayının birler basamağının 4 katının geriye kalan sayıya eklenmesiyle elde edilmişlerdir.

	13 ile böl. kalan
2345654	$10 \cdot 9 \equiv 12 \pmod{13}$
234581	$10 \cdot 10 \equiv 9 \pmod{13}$
23462	$10 \cdot 1 \equiv 10 \pmod{13}$
2354	$10 \cdot 4 \equiv 1 \pmod{13}$
251	$10 \cdot 3 \equiv 4 \pmod{13}$
29	3

29 sayısı 13 ile bölünmediğinden 2345654 sayısı 13 ile bölünmez.

29'un 13 ile bölünmesinde kalan 3;

251'in 13 ile bölünmesinde kalan $10 \cdot 3 \equiv 4$;

2354'ün 13 ile bölünmesinde kalan $10 \cdot 4 \equiv 1$;

⋮

2345654'ün 13 ile bölünmesinde kalan 12'dir.

b. $\frac{Z}{17}$ de $\left(\frac{\bar{1}}{10}\right) = \left(\frac{\overline{1+7\cdot17}}{10}\right) = \overline{12} = \overline{-5}$ dir.

$a = a_n a_{n-1}...a_3a_2a_1a_0$

$\Rightarrow a = 10\left(\frac{1}{10}a_0 + a_1 + 10a_2 + 10^2a_3 + ... + 10^{n-1}a_n\right)$

$\Rightarrow a \equiv 10(-5a_0 + a_n a_{n-1}...a_3a_2a_1) \pmod{17}$

bulunur.

Buna göre; bir doğal sayının birler basamağının 5 katı geriye kalan sayıdan çıkarıldığında elde edilen sayı 17 ile bölünürse, verilen sayı 17 ile bölünür.

Elde edilen sayının 17 ile bölünmesinde kalan r ise, verilen sayının 17 ile bölünmesinde kalan $10 \cdot r$ 'nin 17 modülüne göre dengi olur.

Örneğin; 57143 sayısının 17 ile bölünmesinde kalanı bulalım:

	17 ile böl. kalan
57143	$10 \cdot 4 \equiv 6 \pmod{17}$
5699	$10 \cdot 14 \equiv 4 \pmod{17}$
524	$10 \cdot 15 \equiv 14 \pmod{17}$
32	15

32 sayısı 17 ile bölünmediğinden 57143 sayısı 17 ile bölünmez.

32'nin 17 ile bölünmesinde kalan 15,

524'ün 17 ile bölünmesinde kalan 14,

⋮

57143'ün 17 ile bölünmesinde kalan 6'dır.

c. Z/19'da $\left(\frac{\bar{1}}{10}\right) = \left(\frac{\overline{1+19}}{10}\right) = \bar{2}$ dir.

Bir doğal sayının birler basamağının 2 katı geriye kalan sayıya eklendiğinde elde edilen sayı 19 ile bölünürse verilen sayı 19 ile bölünür.

d. Z/23 te $\left(\frac{\bar{1}}{10}\right) = \left(\frac{\overline{1+69}}{10}\right) = \bar{7}$ dir.

Bir doğal sayının birler basamağının 7 katı geriye kalan sayıya eklendiğinde elde edilen sayı 23 ile bölünürse, verilen sayı 23 ile bölünür.

Etkinlik –4.165

a. $108x - 34y = 90$

$\Rightarrow 54x - 17y = 45$

$\Rightarrow 54x - 17y \equiv 45 \pmod{17}$

$\Rightarrow 3x \equiv -6 \pmod{17}$

$\Rightarrow x \equiv -2 \pmod{17}$

$\Rightarrow x = 17k - 2 \quad (k \in Z)$ olur.

Bu değer, sadeleştirilmiş denklemde yerine konulursa;

$54(17k - 2) - 17y = 45$

$\Rightarrow 54 \cdot 17k - 108 - 17y = 45$

$\Rightarrow 54 \cdot 17k - 17y = 17 \cdot 9$

$\Rightarrow 54k - y = 9$

$\Rightarrow y = 54k - 9$ bulunur.

$Ç = \{(x,y) | x = 17k - 2,\ y = 54k - 9,\ k \in Z\}$ dir.

$(-2,-9)$, $(15,45)$, $(32,99)$,... birer çözümdür.

b. $12x + 17y = 30$

$\Rightarrow 12x + 17y \equiv 30 \pmod{17}$

$\Rightarrow 12x \equiv 13 \pmod{17}$

$\Rightarrow 12x \equiv -4 \pmod{17}$

$\Rightarrow 12x \equiv -4 - 68 \pmod{17}$

$\Rightarrow x \equiv -6 \pmod{17}$

$\Rightarrow x = 17k - 6$ olur.

Bu değer denklemde yerine konulursa,

$12(17k - 6) + 17y = 30$

$\Rightarrow 12 \cdot 17k - 72 + 17y = 30$

$\Rightarrow 12k + y = 6$

$\Rightarrow y = 6 - 12k$ bulunur.

$Ç = \{(x,y) | x = 17k - 6,\ y = 6 - 12k,\ k \in Z\}$ dir.

c. $9x + 4y = 15$

$\Rightarrow 9x + 4y \equiv 15 \pmod{4}$

$\Rightarrow x \equiv 3 \pmod{4}$

$\Rightarrow x = 4k + 3$ olur.

$9(4k + 3) + 4y = 15$

$\Rightarrow 9 \cdot 4k + 27 + 4y = 15$

$\Rightarrow 9k + y = -3$

$\Rightarrow y = -9k - 3$ bulunur.

$Ç = \{(x,y) | x = 4k + 3,\ y = -9k - 3,\ k \in Z\}$ dir.

Etkinlik –4.166

$\left.\begin{matrix} x + y + z = 30 \\ 2x + 5y - 3z = 50 \end{matrix}\right\}$ sisteminde ilk denklemi 2 ile çarpıp taraf tarafa çıkaralım:

$$\begin{array}{r} 2x + 2y + 2z = 60 \\ 2x + 5y - 3z = 50 \\ \hline -3y + 5z = 10 \end{array}$$ olur.

$-3y + 5z = 10$

$\Rightarrow -3y + 5z \equiv 10 \pmod{3}$

$\Rightarrow z = 2 \pmod{3}$

$\Rightarrow z = 3k + 2 \quad (k \in Z)$ bulunur.

z'nin bu değerini $-3y + 5z = 10$ denkleminde yerine koyalım:

$-3y + 5(3k + 2) = 10$

$\Rightarrow -3y + 4 \cdot 3k = 0$

$\Rightarrow y = 4k$ olur.

$y = 4k$ ve $z = 3k + 2$ değerleri $x + y + z = 30$ denkleminde yerlerine konulursa $x = 28 - 7k$ bulunur.

x, y, z nin pozitif olması istendiğinden,

$28 - 7k > 0$, $4k > 0$ ve $3k + 2 > 0 \Rightarrow 0 < k < 4$ olmalıdır.

$x = 28 - 7k$, $y = 4k$ ve $z = 3k + 2$ eşitliklerinde k yerine 1, 2, 3 değerleri konulursa, pozitif tam sayı çözümlerinin kümesi

$Ç = \{(21,4,5),(14,8,8),(7,12,11)\}$ olur.

Etkinlik –4.167

a. <u>I. yol</u> (Çin kalan teoremi ile)

$\left.\begin{matrix} x \equiv 1 \pmod{3} \\ x \equiv 3 \pmod{5} \end{matrix}\right\}$

$5x_1 \equiv 1 \pmod{3} \Rightarrow x_1 \equiv 2 \pmod{3}$

$3x_2 \equiv 1 \pmod{5} \Rightarrow x_2 \equiv 2 \pmod{5}$

$x \equiv \frac{m}{m_1} x_1 a_1 + \frac{m}{m_2} x_2 a_2 \pmod{m}$

$\Rightarrow x \equiv 5 \cdot 2 \cdot 1 + 3 \cdot 2 \cdot 3 \pmod{15}$

$\Rightarrow x \equiv 13 \pmod{15}$ bulunur.

II. yol

$x \equiv 1 \pmod 3$

$\Rightarrow x = 3k+1$ olur. $(k \in Z)$

$x \equiv 3 \pmod 5$

$\Rightarrow 3k+1 \equiv 3 \pmod 5$

$\Rightarrow k \equiv 4 \pmod 5$

$\Rightarrow k = 5p+4 \quad (p \in Z)$

$x = 3k+1$ ve $k = 5p+4$

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

$\Rightarrow x = 13+15p$

$\Rightarrow x \equiv 13 \pmod{15}$ bulunur.

III. yol

$$\left.\begin{array}{l} x \equiv 1 \pmod 3 \\ x \equiv 3 \pmod 5 \end{array}\right\}$$

$$\left.\begin{array}{l} \Rightarrow x+2 \equiv 0 \pmod 3 \\ x+2 \equiv 0 \pmod 5 \end{array}\right\}$$

$x+2$ sayısı hem 3'ün hem de 5'in katı olduğundan, $OKEK(3,5)$ in de katıdır.

$x+2 \equiv 0 \pmod{15}$

$\Rightarrow x \equiv -2 \pmod{15}$

$\Rightarrow x \equiv 13 \pmod{15}$ bulunur.

b.
$$\left.\begin{array}{l} x \equiv 2 \pmod 3 \\ x \equiv 1 \pmod 5 \\ x \equiv 3 \pmod 7 \end{array}\right\}$$

$$\left.\begin{array}{l} x \equiv 2 \pmod 3 \Rightarrow x+4 \equiv 0 \pmod 3 \\ x \equiv 1 \pmod 5 \Rightarrow x+4 \equiv 0 \pmod 5 \\ x \equiv 3 \pmod 7 \Rightarrow x+4 \equiv 0 \pmod 7 \end{array}\right\}$$

$x+4$ sayısı 3'ün, 5'in ve 7'nin katı olduğundan $OKEK(3,5,7) = 105$ in de katıdır.

$x+4 \equiv 0 \pmod{105}$

$\Rightarrow x \equiv 101 \pmod{105}$ bulunur.

Diğer yollarla da çözünüz.

c. $x-3$ sayısı 12'nin ve 40'ın katı olduğundan, $OKEK(12,40) = 120$ nin de katıdır.

$x-3 \equiv 0 \pmod{120}$

$x \equiv 3 \pmod{120}$

d. 1. $x \equiv 2 \pmod 5$

2. $x \equiv 1 \pmod 6$

3. $x \equiv 7 \pmod 8$

Modül sayıları ikişer ikişer aralarında asal olmadıklarından, Çin kalan teoremi kullanılamaz.

I. yol

$$\left.\begin{array}{l} x \equiv 2 \pmod 5 \\ x \equiv 1 \pmod 6 \\ x \equiv 7 \pmod 8 \end{array}\right\} \Rightarrow \left.\begin{array}{l} x \equiv 7 \pmod 5 \\ x \equiv 7 \pmod 6 \\ x \equiv 7 \pmod 8 \end{array}\right\}$$

$x-7$ sayısı $OKEK(5,6,8) = 120$ nin katı olur.

$x-7 \equiv 0 \pmod{120}$

$\Rightarrow x \equiv 7 \pmod{120}$ bulunur.

II. yol

$x \equiv 2 \pmod 5 \Rightarrow x = 5k+2$ dir. $(k \in Z)$

$x \equiv 1 \pmod 6$

$\Rightarrow 5k+2 \equiv 1 \pmod 6$

$\Rightarrow k \equiv 1 \pmod 6$

$\Rightarrow k = 6p+1$ olur. $(p \in Z)$

$x = 5k+2$

$\Rightarrow x = 5(6p+1)+2$

$\Rightarrow x = 30p+7$ olur.

$x \equiv 7 \pmod 8$

$\Rightarrow 30p+7 \equiv 7 \pmod 8$

$\Rightarrow p \equiv 0 \pmod 4$

$\Rightarrow p = 4t$ olur.

$x = 30p+7$ ve $p = 4t$

$\Rightarrow x = 30(4t)+7$

$\Rightarrow x = 120t+7$

$\Rightarrow x \equiv 7 \pmod{120}$ bulunur.

e. $x-2$ sayısı $OKEK(8,9,12) = 72$ nin katıdır.

$x-2 \equiv 0 \pmod{72}$

$\Rightarrow x \equiv 2 \pmod{72}$ olur.

f.
$$\left.\begin{array}{l} x \equiv 1 \pmod 3 \\ x \equiv 1 \pmod 4 \\ x \equiv 1 \pmod 5 \end{array}\right\} \Rightarrow x \equiv 1 \pmod{60} \text{ olur.}$$

$x \equiv 0 \pmod 7 \Rightarrow x = 7k \ (k \in Z)$ dir.

$x \equiv 1 \pmod{60}$ ve $x = 7k$

$\Rightarrow 7k \equiv 1 \pmod{60}$

$\Rightarrow 7k \equiv 301 \pmod{60}$

$\Rightarrow k \equiv 43 \pmod{60}$

$\Rightarrow k = 43 + 60p \; (p \in Z)$ olur.

$x = 7k$ ve $k = 43 + 60p$

$\Rightarrow x = 7 \cdot (43 + 60p)$

$\Rightarrow x = 301 + 420p$

$\Rightarrow x \equiv 301 \pmod{420}$ bulunur.

Etkinlik –4.168

a. $A = 5x - 1 = 7y + 3$ eşitliğini sağlayan A sayıları

$\left.\begin{array}{l} x \equiv -1 \pmod{5} \\ x \equiv 3 \pmod{7} \end{array}\right\}$ sisteminin çözümleridir.

Örnek-4.102'deki yöntemlerle çözebilirsiniz.

Biz, problemi diofant denklemi olarak çözelim:

$5x - 1 = 7y + 3$

$\Rightarrow 5x - 1 \equiv 7y + 3 \pmod{7}$

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

$\Rightarrow x \equiv 5 \pmod{7}$

$\Rightarrow x = 7k + 5 \; (k \in Z)$ olur.

x'in bu değerleri için y de tam sayı olacaktır.

$A = 5x - 1$ ve $x = 7k + 5$

$\Rightarrow A = 5(7k + 5) - 1$

$\Rightarrow A = 35k + 24$

$\Rightarrow A \equiv 24 \pmod{35}$ bulunur.

A'nın üç basamaklı en küçük değeri

$24 + 3 \cdot 35 = 129$ dur.

b. $A = 4x + 1 = 6y + 1 = 7z + 1$ ise $A - 1$ sayıları $OKEK(4,6,7) = 84$ ün katları olurlar.

$A - 1 \equiv 0 \pmod{84}$

$\Rightarrow A \equiv 1 \pmod{84}$ bulunur.

A'nın üç basamaklı en küçük değeri,

$1 + 2 \cdot 84 = 169$ dur.

c. $A = 5x + 4 = 8y - 1 = 9z + 3$ eşitliklerini sağlayan A sayıları

$\left.\begin{array}{l} x \equiv 4 \pmod{5} \\ x \equiv -1 \pmod{8} \\ x \equiv 3 \pmod{9} \end{array}\right\}$ sisteminin çözümleridir.

Örnek – 4.102'deki yöntemlerle çözebilirsiniz.

Biz problemi aşağıdaki yöntemlerle çözelim:

I. yol (Kalanları eşitleme yöntemi)

$x \equiv 4 \pmod{5}$ denkliğinde 4'e 5'in katları eklenirse denklik bozulmaz. Kalanlara modüllerin katlarını ekleme işlemini, ilk eşitlikler üzerinde yapalım:

$A = 5x + 4 = 8y - 1 = 9z + 3$

9	7	12
14	15	21
19	23	30
24	31	39
34	39	
39		

Buna göre; verilen eşitlikler,

$A = 5x' + 39 = 8y' + 39 = 9z' + 39$ biçiminde yazılabilir.

$A - 39 \equiv 0 \pmod{360}$

$\Rightarrow A \equiv 39 \pmod{360}$ bulunur.

A'nın üç basamaklı en küçük değeri

$39 + 360 \cdot 1 = 399$ 'dur.

II. yol (Diofant denklemi olarak çözüm)

$5x + 4 = 8y - 1$

$\Rightarrow 5x + 4 \equiv 8y - 1 \pmod{8}$

$\Rightarrow 5x + 4 \equiv -1 \pmod{8}$

$\Rightarrow x \equiv -1 \pmod{8}$

$\Rightarrow x = 8k - 1$ olur. $(k \in Z)$

x'in $8k - 1$ biçimindeki değerleri için y de tam sayı olur.

$5x + 4 = 9z + 3$ ve $x = 8k - 1$

$\Rightarrow 5(8k - 1) + 4 = 9z + 3$

$\Rightarrow 40k - 1 \equiv 9z + 3 \pmod{9}$

$\Rightarrow 4k - 1 \equiv 3 \pmod{9}$

$\Rightarrow k \equiv 1 \pmod{9}$

$\Rightarrow k = 9p + 1$ olur.

$x = 8k - 1$ ve $k = 9p + 1$

$\Rightarrow x = 8(9p + 1) - 1$

$\Rightarrow x = 72p + 7$ olur.

$A = 5x + 4$ ve $x = 72p + 7$

$\Rightarrow A = 5(72p + 7) + 4$

$\Rightarrow A = 360p + 39$

$\Rightarrow A \equiv 39 \pmod{360}$ bulunur.

d. $A = 3x - 2 = 5y + 1 = 8z + 0$

1	6	8
4	11	16
7	16	
10		
13		
16		

$A - 16 \equiv 0 \pmod{120}$

$\Rightarrow A \equiv 16 \pmod{120}$

Üç basamaklı en küçük A, 136'dır.

Öğrendiğiniz diğer yöntemlerle de çözünüz.