Alıştırmalar ve Problemler – 4.6

1. **a.** 1 **b.** 5 **c.** 11 **d.** 12

2. **a.** D **b.** D **c.** D **d.** Y **e.** Y **f.** Y

3. Denkliklerdeki bilinmeyenleri bulmak için ya Z/m kümesindeki işlemlerin özeliklerinden yararlanılır ya da Z/m in elemanları tek tek denenir.
a. 4 **b.** 2 **c.** $Ç = \varnothing$ **d.** 1

4. Toplam veya çarpım olarak verilen bir sayının, örneğin 5 ile bölünmesindeki kalanı bulmak için; o sayıdaki her toplanan veya çarpanın yerine, o toplanan veya çarpanın 5 modülüne göre dengini koyunuz.

Sayıların 5, 6, 7, 8, 9 ve 11 ile bölünmesindeki kalanlar aşağıda sırasıyla verilmiştir.

a. 2, 5, 2, 7, 5, 1 **b.** 1, 1, 0, 1, 4, 0
c. 1, 5, 1, 5, 5, 7 **d.** 3, 2, 1, 0, 8, 2
e. 1, 4, 0, 6, 1, 0 **f.** 0, 5, 2, 1, 8, 8
g. 4, 5, 6, 7, 2, 7 **h.** 1, 0, 4, 0, 0, 0

5. **a.** 2 **b.** 2 **c.** 10 **d.** 3 **e.** 2 **f.** 4

6. **a.** 7 **b.** 1 **c.** 1 **d.** 8
e. 6 **f.** 5 **g.** 9 **h.** 6

7. **a.** $2^{-1} = 3,\ 3^{-1} = 2,\ 4^{-1} = 4$

b. 3^{-1} ve 4^{-1} yoktur. $5^{-1} = 5$

c. $3^{-1} = 5,\ 5^{-1} = 3,\ 6^{-1} = 6$

d. $5^{-1} = 5,\ 7^{-1} = 7,\ 6^{-1}$ yoktur.

e. $4^{-1} = 7,\ 8^{-1} = 8,\ 6^{-1}$ yoktur.

f. $7^{-1} = 5,\ 10^{-1} = 12,\ 12^{-1} = 10$

g. Modüller küçük olduğunda Z/m de bir a elemanının tersi, Z/m in elemanları tek tek denenerek bulunabilir.

Modüler büyük olduğunda bu denemeler zaman alır.

Z/23 te 9^{-1} i şöyle bulalım:

$9^{22} \equiv 1 \pmod{23}$ (Fermat teo.)

$\Rightarrow 9 \cdot 9^{21} \equiv 1 \pmod{23}$ olur.

Demek ki; $9^{-1} \equiv 9^{21} \pmod{23}$ dir.

$9 \equiv 9 \pmod{23}$

$\Rightarrow 9^2 \equiv 5 \pmod{23}$

$\Rightarrow 9^4 \equiv 2 \pmod{23}$

$\Rightarrow 9^{20} \equiv 9 \pmod{23}$

$\Rightarrow 9^{21} \equiv 12 \pmod{23}$

O hâlde; Z/23 te $9^{-1} = 12$ dir.

Aynı yolla, $13^{-1} = 16$ ve $17^{-1} = 19$ bulunur.

8. Verilen sayıların Z/5, Z/7, Z/8, Z/9, Z/11 ve Z/13 kümelerindeki denkleri, aşağıda sırasıyla verilmiştir.

a. 2, 5 ,3, tanımsız, 9, 9
b. 4, 1, tanımsız, 1, 9, 12
c. Tanımsız, 3, 5, 2, 3, 5
d. 1, 6, tanımsız, tanımsız, 7, 7
e. 2, tanımsız, 7, 1, 2, 8
f. 4, 4, 1, tanımsız, 9, 3
g. 1, tanımsız, tanımsız, 4, 3, 1
h. 3, 3, 1, 8, 7, 4

9. Bir denkliğin iki tarafı, modül ile aralarında asal olan bir sayıyla çarpılabilir ve bölünebilir. Ancak, denkliğin iki tarafı ile modülün 1'den büyük bir ortak böleni varsa, denkliğin iki tarafını bu ortak bölen ile bölerken modülü de bölmelidir. Hem modül, hem de denkliğin iki tarafı bir pozitif tam sayı ile çarpılabilir.
Buna göre;
a. D **b.** Y **c.** D **d.** D **e.** D **f.** D olur.

10. **a.** Z/6 da 3'ün karekökü 3'tür.
Z/5, Z/7 ve Z/9 da 3'ün kürekökü yoktur.

b. 3'ün küpkökü Z/5 te 2 ve Z/6 da 3'tür.
Z/7 ve Z/9 da 3'ün küpkökü yoktur.

c. Z/5 te 4'ün karekökleri 2 ve 3'tür.
Z/6 da 4'ün karekökleri 2 ve 4'tür.
Z/7 de 4'ün karekökleri 2 ve 5'tir.
Z/9 de 4'ün karekökleri 2 ve 7'dir.

d. Z/5 te 4'ün küpkökü 4'tür.
Z/6 da 4'ün küpkökü 4'tür.
Z/7 ve Z/9 da 4'ün küpkökü yoktur.

11. Verilen sayıların Z/5, Z/6, Z/7 ve Z/9 daki denkleri aşağıda aynı sırada verilmiştir.

a. 3, tanımsız, 6, 0

b. Tanımsız, tanımsız, 2, tanımsız

c. Tanımsız, 2, 4, 8

d. Z/5 te $\left(\frac{\overline{-3}}{8}\right)^{-27} = \left(\frac{\overline{-3}}{3}\right)^{-27}$

$= \left(\overline{-1}\right)^{-27}$

$= \left(\overline{4}\right)^{-27}$

$= \left(\overline{4}\right)^{27} \quad \left[4^{-1} \equiv 4 \pmod 5\right]$

$= \left(\overline{-1}\right)^{27} \quad \left[4 \equiv -1 \pmod 5\right]$

$= \overline{-1}$

$= \overline{4}$ bulunur.

Z/6 da $\left(\frac{\overline{-3}}{8}\right)^{-27} = \left(\frac{3}{2}\right)^{-27}$ olur.

$\text{OBEB}(2,6) = 2$ olup 3, 2 ile bölünmez.

Z/6 da $\frac{3}{2}$ tanımsızdır.

Gerçekten $2x = 3 \pmod 6$ eşitliğini sağlayan $x \notin Z/6$ yoktur.

Z/7 de $\left(\frac{\overline{-3}}{8}\right)^{-27} = \left(\frac{\overline{-3+7}}{1}\right)^{-27} = \left(\overline{4}\right)^{-27}$

$= \overline{2}^{27}$

$= \overline{1}$ bulunur.

Z/9 da $\left(\frac{\overline{-3}}{8}\right)^{-27} = \left(\frac{\overline{-3}}{\overline{-1}}\right)^{-27} = \left(\overline{3}\right)^{-27}$ olur.

$= \left(\overline{3}^{-1}\right)^{27}$

Z/9 da $\left(\overline{3}\right)^{-1}$ yoktur. $\left(\frac{-3}{8}\right)^{-27}$ tanımsızdır.

12. Verilen denklemlerin Z/5, Z/6, Z/7 ve Z/9 daki çözüm kümeleri, aşağıda aynı sırada verilmiştir.

a. $\{\overline{3}\}, \{\overline{2},\overline{5}\}, \{\overline{6}\}, \{\overline{8}\}$ **b.** $\{\overline{2}\}, \varnothing, \{\overline{6}\}, \{\overline{3}\}$

c. $Z/5, \varnothing, \{\overline{6}\}, \{\overline{3}\}$ **d.** $\{\overline{3}\}, \{\overline{1}\}, \{\overline{4},\overline{6}\}, \{\overline{8}\}$

e. $\{\overline{2},\overline{3}\}, \varnothing, \varnothing, \varnothing$ **f.** $\varnothing, \{\overline{4}\}, \varnothing, \varnothing$

($x^2 - 2x - 2 = 0$ denkleminin Z/m'deki çözüm kümelerini, Z/m'nin elemanlarını tek tek deneyerek bulabilirsiniz.)

13. a. Z/5 te $2x - 3y = 4$

$\Rightarrow 2x - 3y \equiv 4 \pmod 5$

$\Rightarrow -3y \equiv -2x + 4 \pmod 5$

$\Rightarrow 2y \equiv 3x + 4 \pmod 5$

$\Rightarrow 3 \cdot 2y \equiv 3(3x + 4) \pmod 5$

$\Rightarrow y \equiv 4x + 2 \pmod 5$ bulunur.

Z/5 te, verilen bağıntıyı sağlayan ikililer $f : Z/5 \to Z/5, \; f(x) = 4x + 2$ fonksiyonunun elemanlarıdır.

Z/m de $ay = bx$ eşitliğinde m asal değilse ve $a^{-1} \in Z/m$ yoksa, x'in bazı değerleri için ya $y \in Z/m$ yoktur ya da $y \in Z/m$ değerleri birden fazla olur. Bu durumda, $f = \{(x,y) | ay = bx, \; x, y \in Z/m\}$ bağıntısı bir fonksiyon değildir.

Buna göre;

Z/6 da $2x - 3y = 4$

$\Rightarrow 2x - 3y \equiv 4 \pmod 6$

$\Rightarrow -3y \equiv -2x + 4 \pmod 6$

$\Rightarrow 3y \equiv 4x + 4 \pmod 6$ olur.

Z/6 da 3^{-1} olmadığından bu bağıntı $y = f(x)$ biçiminde bir fonksiyon belirtmez. $f = \{(x,y) | 3y \equiv 4x + 4, \; x, y \in Z/6\}$ bağıntısında; örneğin $(2,0) \in f$ ve $(2,2) \in f$ tir.

Z/7 de $2x - 3y = 4$

$\Rightarrow y \equiv 3x + 1 \pmod 7$ olur.

Z/7 de, verilen bağıntıyı sağlayan ikililer $\Rightarrow f : Z/7 \to Z/7, \; f(x) = 3x + 1$ fonksiyonunun elemanlarıdır.

Z/9 da 3^{-1} olmadığından verilen bağıntı bir fonksiyon belirtmez.

b. Z/5 te $3x + 4y = 1$ bağıntısını sağlayan ikililer $\Rightarrow f : Z/5 \to Z/5, \; f(x) = 3x + 4$ fonksiyonunun elemanlarıdır.

Z/6 da, verilen bağıntı bir fonksiyon belirtmez.

Z/7 de $3x+4y=1$ bağıntısını sağlayan ikililer $\Rightarrow f: Z/7 \to Z/7,\ f(x)=x+2$ fonksiyonunun elemanlarıdır.

Z/9 da $3x+4y=1$ bağıntısını sağlayan ikililer $\Rightarrow f: Z/9 \to Z/9,\ f(x)=6x+7$ fonksiyonunun elemanlarıdır.

c. Z/5 te, $f=\{(x,y)|4x-2y=0,\ x,y\in Z/5\}$ bağıntısı $\Rightarrow f: Z/5 \to Z/5,\ f(x)=2x$ fonksiyonudur.

Z/7 de, $f=\{(x,y)|4x-2y=0,\ x,y\in Z/7\}$ bağıntısı $\Rightarrow f: Z/7 \to Z/7,\ f(x)=2x$ fonksiyonudur.

Z/9 da, $f=\{(x,y)|4x-2y=0,\ x,y\in Z/9\}$ bağıntısı $\Rightarrow f: Z/9 \to Z/9,\ f(x)=2x$ fonksiyonudur.

$4x-2y=0$

Z/6 da $\Rightarrow 4x-2y\equiv 0 \pmod 6$

$\Rightarrow 2y\equiv 4x \pmod 6$ olur.

Z/6 da 2^{-1} olmadığından verilen bağıntı bir fonksiyon belirtmez.

$2y\equiv 4x \pmod 6$ denkliğine dayanarak,

$y\equiv 2x \pmod 6$ yazmak akla gelebilir. (?) Ancak 2 ile 6 aralarında asal olmadığından, denkliğin iki tarafının 2 ile bölünmesi, modülün de bölünmesini gerektirir.

$2y\equiv 4x \pmod 6 \Rightarrow y\equiv 2x \pmod 3$ tür.

d. $xy+2x-3y=1$

$\Rightarrow y(x-3)=-2x+1$ olur.

Z/5 te $x-3\neq 0$ olmak üzere,

$(x-3)^{-1}\in Z/5$ tir.

Buna göre; $x\neq 3$ iken verilen bağıntıyı sağlayan ikililer,

$f: Z/5-\{3\} \to Z/5,\ f(x)=\dfrac{-2x+1}{x-3}$ ya da

$f: Z/5-\{3\} \to Z/5,\ f(x)=\dfrac{3x+1}{x+2}$

fonksiyonunun elemanlarıdır.

Z/7 de, verilen bağıntı

$f: Z/7-\{3\} \to Z/7,\ f(x)=\dfrac{5x+1}{x+4}$

fonksiyonunu belirtir.

Z/6 da 0^{-1}, 2^{-1}, 3^{-1} ve 4^{-1} yoktur.

$x-3=0,\ x-3=2,\ x-3=3,\ x-3=4$ iken bağıntı bir fonksiyon belirtmez.

$f: \{2,4\} \to Z/6,\ f(x)=\dfrac{4x+1}{x+3}$ bir fonksiyondur.

Z/9 da 0^{-1}, 2^{-1}, 3^{-1}, 6^{-1} yoktur.

$x-3=0,\ x-3=2,\ x-3=3$ ve $x-3=6$ iken bağıntı bir fonksiyon belirtmez.

$f: \{1,2,4,7,8\} \to Z/9,\ f(x)=\dfrac{7x+1}{x+6}$ bir fonksiyondur.

14. a. $f^{-1}: Z/5 \to Z/5,\ f^{-1}(x)=3x+4$;

$f^{-1}: Z/7 \to Z/7,\ f^{-1}(x)=4x+5$;

$f^{-1}: Z/9 \to Z/9,\ f^{-1}(x)=5x+6$ olur.

Z/6 da f bire bir olmadığından f^{-1} fonksiyon değildir.

b. $f^{-1}: Z/5 \to Z/5,\ f^{-1}(x)=4x+1$;

$f^{-1}: Z/7 \to Z/7,\ f^{-1}(x)=2x+5$;

$f^{-1}: Z/9 \to Z/9,\ f^{-1}(x)=7x+2$ olur.

Z/6 da f bire bir olmadığından, f^{-1} fonksiyon değildir.

c.

$f^{-1}: Z/5-\{3\} \to Z/5-\{4\},\ f^{-1}(x)=\dfrac{4x+1}{3x+3}$;

$f^{-1}: Z/7-\{2\} \to Z/7-\{5\},\ f^{-1}(x)=\dfrac{6x+1}{3x+5}$;

$f^{-1}: Z/9 \to Z/9,\ f^{-1}(x)=\dfrac{7x+1}{3x+7}$;

$f^{-1}: Z/6-\{0,2,4\} \to Z/6-\{1,3,5\}$,

$f^{-1}(x)=\dfrac{5x+1}{3x+4}$ dir.

d.

$f^{-1}: Z/5-\{3\} \to Z/5-\{1\},\ f^{-1}(x)=\dfrac{3x+2}{3x+1}$;

$f^{-1}: Z/7-\{6\} \to Z/7-\{4\},\ f^{-1}(x)=\dfrac{5x+4}{3x+3}$;

$f^{-1}: Z/9 \to Z/9,\ f^{-1}(x)=\dfrac{7x+6}{3x+5}$

$f^{-1}: Z/6-\{0,2,4\} \to Z/6-\{1,3,5\}$,

$f^{-1}(x)=\dfrac{4x+3}{3x+2}$ dir.

15. $a \equiv 17 \pmod{35}$ ve $b \equiv 23 \pmod{35}$ dir.
$a \equiv 2 \pmod 5$, $a \equiv 3 \pmod 7$,
$b \equiv 3 \pmod 5$ ve $b \equiv 2 \pmod 7$ olur.

a. $a+b \equiv 13 \pmod{35}$

b. $a \cdot b \equiv 2 \cdot 3 \pmod 5 \Rightarrow a \cdot b \equiv 1 \pmod 5$ olur.

c. $17a + 23b \equiv 3 \cdot 3 + 2 \cdot 2 \pmod 7$
$\Rightarrow 7a + 23b \equiv 6 \pmod 7$ olur.

d. $a^2 + b^2 \equiv 3^2 + 2^2 \pmod 7$
$\Rightarrow a^2 + b^2 \equiv 6 \pmod 7$ olur.

16. a. Cumartesi **b.** Perşembe

17. 6 Mayıs 2007, Pazartesi

18. a. $(fog)(x) = 6x + 3$ **b.** $(gof)(x) = 6x + 3$
c. $\left(gof^{-1}\right)(x) = 3x + 4$ **d.** $\left(g^{-1}of\right)(x) = 5x + 1$

19. a. 9 **b.** 5 **c.** 77 **d.** 37

e.
$$(gof)(x) = \begin{cases} (3x-1)^2 + 1 & x \equiv 0 \pmod 2 \text{ ise} \\ 4x + 3 & x \equiv 3 \pmod 6 \text{ ise} \\ 6x + 11 & x \equiv 5 \pmod 6 \text{ ise} \\ (2x+3)^2 + 1 & x \equiv 1 \pmod 6 \text{ ise} \end{cases}$$

f.
$$(fog)(x) = \begin{cases} 4x - 3 & x \equiv 0 \pmod 2 \text{ ise} \\ 6x + 7 & x \equiv 1 \pmod 6 \text{ ise} \\ 2x^2 + 5 & x \equiv 2 \pmod 6 \text{ ise} \\ 9x + 5 & x \equiv 4 \pmod 6 \text{ ise} \\ 3x^2 + 2 & x \equiv 5 \pmod 6 \text{ ise} \end{cases}$$

20. Verilen denklemlerin Z/7, Z/8, Z/9, Z/12 deki çözüm kümelerinin eleman sayıları aşağıda aynı sırada verilmiştir.

a. 1, 0, 1, 0 **b.** 1, 1, 1, 1
c. 1, 0, 3, 0 **d.** 1, 0, 1, 0

21. Verilen denklemlerin Z/7, Z/8, Z/9 daki çözüm kümeleri aşağıda aynı sırada verilmiştir.

a. $\{(\bar 2, \bar 0)\}$, $\{(\bar 3, \bar 6)\}$, $\{(\bar 0, \bar 4)\}$

b. $\{(x,y) | y = 3x + 3;\ x, y \in Z/7\}$,
$\{(\bar 1, \bar 7)\}$, $\{(\bar 5, \bar 7)\}$, $\{(\bar 1, \bar 8)\}$

c. $\{(\bar 3, \bar 6)\}$, $\varnothing$, $\varnothing$

d. $\{(\bar 2, \bar 3)\}$, $\{(\bar 0, \bar 5)\}$, $\varnothing$

22. Verilen sayıların 11, 13, 17 ve 19 ile bölünmelerindeki kalanlar, aşağıda aynı sıra ile verilmiştir.

a. 7, 6, 11, 6 **b.** 7, 5, 1, 18
c. 1, 12, 5, 11 **d.** 5, 0, 4, 11

23. a. Z/29 da $\left(\frac{\bar 1}{10}\right) = \left(\frac{\overline{1+29}}{10}\right) = \bar 3$ olduğundan, verilen sayının birler basamağının 3 katı geride kalan sayıya eklendiğinde elde edilen sayı 29 ile bölünürse, verilen sayı da 29 ile bölünür.

b. Z/31 de $\left(\frac{\bar 1}{10}\right) = \left(\frac{\overline{1+9\cdot 31}}{10}\right) = \overline{28} = \overline{-3}$ olduğundan, verilen sayının birler basamağının 3 katı geride kalan sayıdan çıkarıldığında elde edilen sayı 31 ile bölünürse, verilen sayı da 31 ile bölünür.

24. a.
$Ç = \{(x,y) | x = 16 + 19k,\ y = -9 - 12k,\ k \in Z\}$

b.
$Ç = \{(x,y) | x = 23k - 5,\ y = 13k - 6,\ k \in Z\}$

c.
$Ç = \{(x,y) | x = 8k + 3,\ y = -9k - 2,\ k \in Z\}$

d.
$Ç = \{(x,y) | x = 7k + 6,\ y = 41k + 31,\ k \in Z\}$
Z'de,
$Ç = \{(x,y,z) | x = 7k + 3,\ y = 7 - 5k,\ z = 8 - 2k\}$

25. a. Z^+ da, $Ç = \{(3,7,8), (10,2,6)\}$ dir.

b. Z de,
$Ç = \{(x,y,z) | x = -22 + 3k,\ y = 15 - k,\ z = k\}$;
Z^+ da, $Ç = \{(2,7,8), (5,6,9), (8,5,10), (11,4,11), (14,3,12), (17,2,13), (20,1,14)\}$ dir.

26. a. $x \equiv 5 \pmod{12}$ **b.** $x \equiv 91 \pmod{105}$

c. $x \equiv 5 \pmod{24}$ **d.** $x \equiv 51 \pmod{210}$

27. a. 118 **b.** 233 **c.** 247 **d.** 112

28. 3^{143} ün 45 ile bölünmesindeki kalanı bulalım:

45 in, aralarında asal olan çarpanları 5 ve 9 dur.

$3^{143} \equiv 2 \pmod 5$ ve $3^{143} \equiv 0 \pmod 9$

olduğundan $3^{143} \equiv 27 \pmod{45}$ olur.

Verilen sayıların 35, 45, 60, 100 ile bölünmelerindeki kalanlar, aşağıda aynı sırada verilmiştir.

a. 12, 27, 27, 27 **b.** 14, 4, 49, 49

c. 29, 14, 29, 9 **d.** 8, 28, 13, 73

29. a. 216 ile 385 aralarında asal olduğundan, Z/385 te çözüm vardır ve bir tanedir.

$385 = 5 \cdot 7 \cdot 11$ olduğundan, verilen denklik daha küçük modüllü denklikleden oluşan bir sisteme dönüştürülebilir.

$$\left.\begin{array}{l} 216 \cdot x \equiv 1 \pmod 5 \\ 216 \cdot x \equiv 1 \pmod 7 \\ 216 \cdot x \equiv 1 \pmod{11} \end{array}\right\}$$

$$\left.\begin{array}{l} x \equiv 1 \pmod 5 \\ x \equiv 6 \pmod 7 \\ x \equiv 8 \pmod{11} \end{array}\right\}$$

Elde ettiğimiz denklik sistemini Çin Kalan Teoreminden yararlanarak çözelim:

$$\left.\begin{array}{l} 7 \cdot 11 \cdot x_1 \equiv 1 \pmod 5 \Rightarrow x_1 \equiv 3 \pmod 5 \\ 5 \cdot 11 \cdot x_2 \equiv 1 \pmod 7 \Rightarrow x_2 \equiv 6 \pmod 7 \\ 5 \cdot 7 \cdot x_3 \equiv 1 \pmod{11} \Rightarrow x_3 \equiv 6 \pmod{11} \end{array}\right\}$$

$$x \equiv 7 \cdot 11 \cdot 3 \cdot 1 + 5 \cdot 11 \cdot 6 \cdot 6 + 5 \cdot 7 \cdot 6 \cdot 8 \pmod{385}$$

$$\Rightarrow x \equiv 3891 \pmod{385}$$

$\Rightarrow x \equiv 41 \pmod{385}$ bulunur.

b. a'daki gibi çözeceğiz:

$$\left.\begin{array}{l} 21 \cdot x \equiv 1 \pmod{34} \\ 34 \cdot x \equiv 1 \pmod{55} \end{array}\right\} \Rightarrow \left.\begin{array}{r} x \equiv 1 \pmod 2 \\ x \equiv 13 \pmod{17} \\ x \equiv 4 \pmod 5 \\ x \equiv 1 \pmod{11} \end{array}\right\}$$

$$\left.\begin{array}{l} 17 \cdot 5 \cdot 11 \cdot x_1 \equiv 1 \pmod 2 \Rightarrow x_1 \equiv 1 \pmod 2 \\ 2 \cdot 5 \cdot 11 \cdot x_2 \equiv 1 \pmod{17} \Rightarrow x_2 \equiv 15 \pmod{17} \\ 2 \cdot 17 \cdot 11 \cdot x_3 \equiv 1 \pmod 5 \Rightarrow x_3 \equiv 4 \pmod 5 \\ 2 \cdot 17 \cdot 5 \cdot x_4 \equiv 1 \pmod{11} \Rightarrow x_4 \equiv 9 \pmod{11} \end{array}\right\}$$

$$x \equiv 17 \cdot 5 \cdot 11 \cdot 1 \cdot 1 + 2 \cdot 5 \cdot 11 \cdot 15 \cdot 13 + 2 \cdot 17 \cdot 11 \cdot 4 \cdot 4 + 2 \cdot 17 \cdot 5 \cdot 9 \cdot 1 \pmod{1870}$$

$$\Rightarrow x \equiv 1849 \pmod{1870}$$

c. $$\left.\begin{array}{l} 24 \cdot x \equiv 1 \pmod{77} \\ 37 \cdot x \equiv 1 \pmod{91} \end{array}\right\} \Rightarrow \left.\begin{array}{r} x \equiv 5 \pmod 7 \\ x \equiv 6 \pmod{11} \\ x \equiv 4 \pmod 7 \\ x \equiv 6 \pmod{13} \end{array}\right\}$$

$x \equiv 5 \pmod 7$ ve $x \equiv 4 \pmod 7$ denklikleri birlikte sağlanamaz. Verilen sistemi sağlayan bir x doğal sayısı yoktur.

d. $$\left.\begin{array}{l} 23x \equiv 56 \pmod{65} \\ 45x \equiv 44 \pmod{143} \end{array}\right\} \Rightarrow \left.\begin{array}{r} x \equiv 2 \pmod 5 \\ x \equiv 3 \pmod{13} \\ x \equiv 0 \pmod{11} \end{array}\right\}$$

$\Rightarrow x \equiv 627 \pmod{715}$ bulunur.

e. $x \equiv 1061 \pmod{1190}$

30. $(a+b)^{m-1} \equiv 1 \pmod m$ (Fermat teo.)

$\Rightarrow (a+b)^m \equiv a+b \pmod m$ dir. ①

$a^{m-1} \equiv 1 \pmod m$ (Fermat teo.)

$\Rightarrow a^m \equiv a \pmod m$;

$b^{m-1} \equiv 1 \pmod m$

$\Rightarrow b^m \equiv b \pmod m$ dir.

$a^m \equiv a \pmod m$ ve $b^m \equiv b \pmod m$

$\Rightarrow a^m + b^m \equiv a+b \pmod m$ olur. ②

① ve ② den

$(a+b)^m \equiv a^m + b^m \pmod m$ bulunur.

31. a. $x^2+3 \equiv x^2-1 \pmod 4$

$\Rightarrow x^2+3 \equiv (x-1)(x+1) \pmod 4$

$\Rightarrow x^2+3 \equiv (x+3)(x+1) \pmod 4$

b. $x^2+1 \equiv x^2-4 \pmod 5$

$\Rightarrow x^2+1 \equiv (x-2)(x+2) \pmod 5$

$\Rightarrow x^2+1 \equiv (x+3)(x+2) \pmod 5$

c. $x^2+3x-3 \equiv x^2+3x+2 \pmod 5$

$\Rightarrow x^2+3x-3 \equiv (x+1)(x+2) \pmod 5$

d. $x^2+2x+4 \equiv x^2+2x-3 \pmod 7$

$\Rightarrow x^2+2x+4 \equiv (x+3)(x-1) \pmod 7$

$\Rightarrow x^2+2x+4 \equiv (x+3)(x+6) \pmod 7$

32. a. $A = n\left(n^2+5\right) \equiv n\left(n^2-1\right) \pmod 6$

$\Rightarrow n\left(n^2+5\right) = n(n-1)(n+1) \pmod 6$ dır.

$n-1$, n, $n+1$ ardışık üç tam sayı olup en az biri çifttir ve en az biri 3'ün katıdır.

Buna göre, A sayısı hem 2'ye hem 3'e bölünebileceğinden 6'ya bölünür.

b. $A = n(n+1)(2n+1)$ olsun.

$n \equiv 0 \pmod 2 \Rightarrow 2 \mid A$;

$n \equiv 1 \pmod 2 \Rightarrow n+1 \equiv 0 \pmod 2$

$\Rightarrow 2 \mid A$ dır.

Buna göre; A sayısı 2 ile bölünür.

$n \equiv 0 \pmod 3 \Rightarrow 3 \mid A$;

$n \equiv 1 \pmod 3 \Rightarrow 2n+1 \equiv 0 \pmod 3$

$\Rightarrow 3 \mid A$;

$n \equiv 2 \pmod 3 \Rightarrow n+1 \equiv 0 \pmod 3$

$\Rightarrow 3 \mid A$ dır.

Buna göre; A sayısı 3 ile bölünür. A sayısı hem 2'ye hem 3'e bölündüğünden 6 ile de bölünür.

33. a. $3^{2n+1}+2^{n+2} = 3^{2n}\cdot 3 + 2^n \cdot 4$

$\Rightarrow 3^{2n+1}+2^{n+2} \equiv 9^n \cdot 3 + 2^n \cdot 4 \pmod 7$

$\Rightarrow 3^{2n+1}+2^{n+2} \equiv 2^n \cdot 3 + 2^n \cdot 4 \pmod 7$

$\Rightarrow 3^{2n+1}+2^{n+2} \equiv 7 \cdot 2^n \cdot 4 \pmod 7$

$\Rightarrow 3^{2n+1}+2^{n+2} \equiv 0 \pmod 7$

b. $3^{2n+2}+2^{6n+1} = 9^n \cdot 9 + 64^n \cdot 2$

$\Rightarrow 3^{2n+2}+2^{6n+1} \equiv 9^n \cdot 9 + 64^n \cdot 2 \pmod{11}$

$\Rightarrow 3^{2n+2}+2^{6n+1} \equiv 9^n \cdot 9 + 9^n \cdot 2 \pmod{11}$

$\Rightarrow 3^{2n+2}+2^{6n+1} \equiv 11 \cdot 9^n \pmod{11}$

$\Rightarrow 3^{2n+2}+2^{6n+1} \equiv 0 \pmod{11}$

34. a, b, e, f'yi siz yapınız.

c. $10^3-1 = 27\cdot 37$ eşitliği

$10^3 \equiv 1 \pmod{27}$ ve $10^3 \equiv 1 \pmod{37}$

denkliklerini gerektirir.

Buna göre; bir doğal sayının 37ile (ya da 27 ile) bölünmesindeki kalan, bu sayının 1000'in kuvvetlerine göre çözümlenmiş biçiminde 1000 yerine 1 konulmasıyla elde edilen sayının 37 ile (ya da 27 ile) bölünmesindeki kalana eşittir.

Örneğin; 2536748'in 37 ile bölünmesindeki kalanı bulalım:

$2\,536\,748$

$= 2\cdot 1000^2 + 536\cdot 1000 + 748$

$\equiv 2\cdot 1^2 + 536\cdot 1 + 748 \pmod{37}$

$\equiv 1\cdot 1000 + 286 \pmod{37}$

$\equiv 1\cdot 1 + 286 \pmod{37}$

$\equiv 287 \pmod{37}$

$\equiv 28 \pmod{37}$ bulunur.

d. $10^3+1 = 7\cdot 11\cdot 13$ eşitliği

$10^3 \equiv -1 \pmod 7$, $10^3 \equiv -1 \pmod{11}$ ve

$10^3 \equiv -1 \pmod{13}$ denkliklerini gerektirir.

Buna göre; bir doğal sayının 7, 11 ya da 13 ile bölünmesindeki kalan, bu sayının 1000'in kuvvetlerine göre çözümlenmiş biçiminde 1000 yerine -1 konulmasıyla elde edilen sayının 7, 11 ya da 13 ile bölünmesindeki kalana eşittir.

Örneğin; 2536748'in 13 ile bölünmesindeki kalanı bulalım:

$2\,536\,748$

$= 2\cdot 1000^2 + 536\cdot 1000 + 748$

$\equiv 2\cdot (-1)^2 + 536\cdot (-1) + 748 \pmod{13}$

$\equiv 214 \pmod{13}$

$\equiv 6 \pmod{13}$ bulunur.