

## Sayılar Teorisi I Vize Soruları

1- a)  $a, b, x \in \mathbb{Z}$  olsun.  $(a, b) = (a, b + ax)$  olduğunu gösteriniz.

b)  $q \geq 5$  ve  $q$  asal sayı olsun.

$6 \cdot (q-4)! \equiv 1 \pmod{q}$  olduğunu gösteriniz.

2- a) Modüler aritmetiği kullanarak 11 ile bölünebilme kuralını bulunuz.

b)  $86x \equiv 17 \pmod{303}$  kongrüansının tüm çözümlerini bulunuz.

3- a)  $7^{5^{2003}}$

sayısının 17 ile bölümünden elde edilen kalanı bulunuz.

b)  $f(x) = 6x^3 + 27x^2 + 17x + 1 \equiv 0 \pmod{15}$

kongrüansının varsa çözümlerini bulunuz.

4-  $x^3 + 4x + 5 \equiv 0 \pmod{125}$  polinom kongrüansının tüm çözümlerini bulunuz.

5-  $\bar{6} \in \mathbb{Z}_{11}^*$  elemanının primitif kök olduğunu gösterip onun yardımıyla

$5x^2 \equiv 2 \pmod{11}$  denkleminin çözümünü bulunuz.

Not: Sorular eşit puanlıdır.

## Cevap Anahitari

1- a)  $(a, b) = d$   $(a, b + ax) = t$  olsun.

$$d|a \wedge d|b \Rightarrow d|b+ax \Rightarrow d|t \quad *$$

$t|a \wedge t|b+ax \Rightarrow t|b$  olup  $t|d$   $**$   $t=d$  bulunur.

$$b) \quad q-1 \equiv -1 (q), \quad q-2 \equiv -2 (q) \quad q-3 \equiv -3 (q)$$

$$(q-1)! = (q-1)(q-2)(q-3)(q-4)! \equiv -1 (mod q) \quad (\text{Wilson})$$

$$(-1)(-2)(-3)(q-4)! \equiv -1 (mod q)$$

$$-6(q-4)! \equiv -1 (mod q) \Rightarrow 6(q-4)! \equiv 1 (mod q)$$

2- a) Defterinizde var.

$$b) \quad 86x \equiv 17 (mod 303) \Rightarrow$$

$$86x - 303y = 17$$

$$303 = 3 \cdot 86 + 45$$

$$86 = 1 \cdot 45 + 41$$

$$45 = 1 \cdot 41 + 4$$

$$41 = 10 \cdot 4 + 1$$

$$4 = 4 \cdot 1 + 0$$

$$1 = 41 - 10 \cdot 4$$

$$= -10 \cdot 45 + 11 \cdot 41$$

$$= 11 \cdot 86 - 21 \cdot 45$$

$$= -21 \cdot 303 + 74 \cdot 86$$

$$17 = -357 \cdot 303 + 1258 \cdot 86$$

$$3- a) \quad x \equiv 46 (mod 303)$$

$$5^{2003} \equiv x (mod 17)$$

$$5^{2003} \equiv x (mod 16)$$

$$5^{2003} \equiv (5^8)^{250} \cdot 5^3 \equiv 13 (mod 16)$$

$$7^{13} \equiv 15 \cdot 7 \equiv (-2)^6 \cdot 7 \equiv 2^6 \cdot 7 \equiv 6 (mod 17)$$

$$(7, 17) = 1 \quad \text{olup}$$

$$7^{16} \equiv 1 (mod 17)$$

$$\varphi(16) = 2^4 \left(1 - \frac{1}{2}\right) = 8$$

$$3- b) f(x) = 6x^3 + 27x^2 + 17x + 1 \equiv 0 \pmod{3.5}$$

$$3 \text{ için } f(1) = 0 \quad b_1 = \bar{1} \quad x \equiv 1 \pmod{3}$$

$$5 \text{ için } f(4) = 0 \quad b_2 = \bar{4} \quad x \equiv 4 \pmod{5}$$

$$x = 1 + 3k \Rightarrow 1 + 3k \equiv 4 \pmod{5} \Rightarrow 3k \equiv 3 \pmod{5}$$

$$k \equiv 1 \pmod{5} \quad k = 1 + 5t \Rightarrow x = 1 + 3(1 + 5t)$$

$$= 4 + 5t$$

$$\boxed{\bar{4}}$$

$$4- x^3 + 4x + 5 \equiv 0 \pmod{125}$$

$$p = p^2 = 5 \text{ için}$$

$$f(x) = \bar{0} \quad b = \bar{1} \quad f(1) = 10$$

$$b = \bar{1}$$

$$f(1) = 10$$

$$f'(1) = 7 \quad x = \bar{30} //$$

$$7k \equiv \frac{-10}{5} \pmod{5}$$

$$k \equiv 4 \pmod{5}$$

$$x = 1 + 4 \cdot 5 = \bar{21}$$

$$b = 21$$

$$f(21) = 9350$$

$$f'(21) = 1327$$

Not:  $f(4) = \bar{0} \pmod{5}$  oluyor  
buradan  $f(4) = 85 \quad f'(4) = 52$

$52k \equiv 3 \pmod{5} \quad k = 4$  oluyor  
 $x = \bar{96}$  oluyor.

$$1327k \equiv -374 \pmod{5}$$

$$2k \equiv 1 \pmod{5}$$

$$k \equiv 3 \pmod{5}$$

$$x = 21 + 3 \cdot 25 \pmod{125}$$

$$x = \bar{96} //$$

$$5- 6^1 = 6$$

$$6^2 = 3$$

$$6^3 = 7$$

$$6^4 = 9$$

$$6^5 = 10$$

$$6^6 = 5$$

$$6^7 = 8$$

$$6^8 = 4$$

$$6^9 = 2$$

$$6^{10} = 1$$

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

$$\text{ind } 5 + 7 \text{ind } x \equiv \text{ind } 2 \pmod{10}$$

$$6 + 7 \text{ind } x \equiv 9 \pmod{10}$$

$$7 \text{ind } x \equiv 3 \pmod{10}$$

$$\text{ind } x \equiv 9 \pmod{10}$$

$$x \equiv 6^9 \pmod{11}$$

$$x \equiv (6^2)^4 \cdot 6 \equiv 3^4 \cdot 6 \equiv 4 \cdot 6 \equiv 2 \pmod{11}$$

$$x = \bar{2}$$