Soru 1. *Elementer Sayılar Teorisi dersini alan öğrenciler, Çinli Kalan Teoremini çalışmak üzere gruplara ayrılacaktır. Öğrenciler üçerli gruplara ayrıldığında 1 öğrenci, dörderli gruplara ayrıldığında 2 öğrenci, beşerli gruplara ayrıldığında ise 3 öğrencinin dışarıda kaldığı görülmektedir. Öğrenciler yedişerli gruplara ayrıldığında, eğer Bülent Hoca gruplardan birine girerse, hiç öğrenci açıkta kalmadığına göre dersi alan en az kaç öğrenci vardır? Bulunuz.* [15p]

Çözüm. Dersi alan öğrencilerin sayısı

$$\begin{aligned} X &\equiv 1 \pmod 3 \\ X &\equiv 2 \pmod 4 \\ X &\equiv 3 \pmod 5 \\ X &\equiv 6 \pmod 7 \end{aligned}$$

kongrüens sisteminin bir çözümüdür. Çinli Kalan Teoremini kullanarak problemi çözebiliriz. Teoremin kanıtında kullandığımız gösterimleri kullanırsak yukarıdaki denkleme göre

$$\begin{array}{cccc} a_1 = 1 & a_2 = 2 & a_3 = 3 & a_4 = 6 \\ m_1 = 3 & m_2 = 4 & m_3 = 5 & m_4 = 7 \\ M_1 = 140 & M_2 = 105 & M_3 = 84 & M_4 = 60 \end{array}$$

ifadelerini yazabiliriz. Öte yandan

$$140b_1 \equiv 1 \pmod 3 \Rightarrow 2b_1 \equiv 1 \pmod 3 \Rightarrow b_1 \equiv 2 \pmod 3$$

$$105b_2 \equiv 1 \pmod 4 \Rightarrow b_2 \equiv 1 \pmod 4$$

$$84b_3 \equiv 1 \pmod 5 \Rightarrow 4b_3 \equiv 1 \pmod 5 \Rightarrow b_3 \equiv 4 \pmod 5$$

$$60b_4 \equiv 1 \pmod 7 \Rightarrow 4b_4 \equiv 1 \pmod 7 \Rightarrow b_4 \equiv 2 \pmod 7$$

olduğundan yukarıdaki kongrüens sisteminin çözümü

$$\begin{aligned} X &\equiv \sum_{i=1}^{4} a_i b_i M_i \pmod{420} \\ &\equiv 140.2 + 2.105 + 3.84.4 + 6.60.2 \pmod{420} \\ &\equiv 118 \pmod{420} \end{aligned}$$

olarak bulunur. Dolayısıyla dersi alan en az 118 kişi olmalıdır.

Soru 2.

(a) *2'nin 19'un bir ilkel kökü olduğunu gösteriniz.* [10p]

(b) $X^{24} \equiv 11 \pmod{19}$ *kongrüensini çözünüz.* [15p]

(c) $5X^2 + 4X + 7 \equiv 0 \pmod{19}$ *kongrüensini çözünüz.* [15p]

Çözüm. (a)

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$2k$	0	2	4	6	8	10	12	14	16	18	1	3	5	7	9	11	13	15	17
2^k	1	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1

Yukardaki tabloya göre $2^k \equiv 1 \pmod{19}$ kongrüensini sağlayan en küçük pozitif k tamsayısı 18'dir. Dolayısıyla 2'nin 19 modülüne göre mertebesi $\varphi(19) = 18$ olacağından 2, 18'in bir ilkel köküdür.

(b)

$$\begin{aligned} X^{24} \equiv 11 \pmod{19} &\Rightarrow 24I(X) \equiv 12 \pmod{18} \\ &\Rightarrow 4I(X) \equiv 2 \pmod{3} \\ &\Rightarrow I(X) \equiv 2 \pmod{3} \\ &\Rightarrow I(X) \equiv 2, 5, 8, 11, 14, 17 \pmod{18} \end{aligned}$$

olacağından verilen kongrüensin çözümleri

$$\begin{aligned} X &\equiv 4 \pmod{19} \\ X &\equiv 13 \pmod{19} \\ X &\equiv 9 \pmod{19} \\ X &\equiv 15 \pmod{19} \\ X &\equiv 6 \pmod{19} \\ X &\equiv 10 \pmod{19} \end{aligned}$$

olarak bulunur.

(c) Verilen kongrüensin çözümü

$$Y^2 \equiv 16 - 4.5.7 \equiv -124 \equiv 9 \pmod{19}$$

olmak üzere

$$10X+4 \equiv Y \pmod{19}$$

lineer kongrüensinin çözümüdür. Buna göre önce

$$Y^2 \equiv 9 \pmod{19}$$

kuadratik kongrüensini çözelim. (a) şıkkında yazılan tabloyu kullanarak $9 \equiv 2^8 \pmod{19}$ olduğunu görebiliriz. Buna göre

$$Y \equiv \pm 2^4 \pmod{19}$$

yani

$$Y \equiv 16 \pmod{19}$$

ve

$$Y \equiv 3 \pmod{19}$$

bulunur. Buna göre verilen kongrüensin iki çözümü vardır ve bunlar

$$10X+4 \equiv 16 \pmod{19} \Rightarrow 10X \equiv 12 \pmod{19} \Rightarrow X \equiv 5 \pmod{19}$$

ve

$$10X+4 \equiv 3 \pmod{19} \Rightarrow 10X \equiv 18 \pmod{19} \Rightarrow X \equiv 17 \pmod{19}$$

şeklinde elde edilir.

Soru 3. $X^3+2X^2+7X+2 \equiv 0 \pmod{54}$ *kongrüensini çözünüz.* [20p]

Çözüm. $f(X)=X^3+2X^2+7X+2$ olsun. $f(X) \equiv 0 \pmod{54}$ kongrüensinin çözüm kümesi

$$f(X) \equiv 0 \pmod{27}$$
$$f(X) \equiv 0 \pmod{2}$$

kongrüens sisteminin çözüm kümesi ile aynıdır.

$f(X) \equiv 0 \pmod{3}$ kongrüensinin tek çözümünün $X \equiv 1 \pmod{3}$ olduğunu (0, 1 ve 2 değerlerini 3 modülüne göre deneyerek) kolayca görebiliriz. $f(1)=12$ ve $f'(X)=3X^2+4X+7$

olduğundan $f'(1) = 14$ olur. Buna göre

$$0 \equiv \frac{f(1)}{3} + f'(1)k \equiv 4 + 14k \equiv 1 + 2k \pmod 3$$

yani $k \equiv 1 \pmod 3$ olduğundan $x_1 \equiv 1 + 3k \equiv 4 \pmod 9$, $f(X) \equiv 0 \pmod 9$ kongrüensinin çözümüdür.

$f(4) = 126$ ve $f'(4) = 71$ olduğundan

$$0 \equiv \frac{f(4)}{9} + f'(4)t \equiv 14 + 71t \equiv 2 + 2t \pmod 3$$

yani $t \equiv 2 \pmod 3$ elde edilir. Buna göre $x_2 \equiv 4 + 9.2 \equiv 22 \pmod{27}$, $f(X) \equiv 0 \pmod{27}$ kongrüensinin çözümüdür.

$f(X) \equiv 0 \pmod 2$ kongrüensinin $x \equiv 0 \pmod 2$ ve $X \equiv 1 \pmod 2$ gibi iki tane çözümü olduğundan $f(X) \equiv 0 \pmod{54}$ kongrüensinin çözümleri

$$\begin{cases} X & \equiv 22 \pmod{27} \\ X & \equiv 0 \pmod 2 \end{cases}$$

ve

$$\begin{cases} X & \equiv 22 \pmod{27} \\ X & \equiv 1 \pmod 2 \end{cases}$$

sistemlerinin çözümleridir. Birinci sistemin çözümü $X \equiv 22 \pmod{54}$, ikinci sistemin çözümü ise $X \equiv 24 \pmod{54}$ şeklindedir. Böylece $5X^2 + 4X + 7 \equiv 0 \pmod{19}$ kongrüensinin çözümleri

$$X \equiv 22 \pmod{54}$$

ve

$$X \equiv 24 \pmod{54}$$

olur.

Soru 4.

(a) $X^2 \equiv 713 \pmod{1009}$ *kongrüensinin çözümü olup olmadığını araştırınız. (*$713 = 23 \times 31$ *ve* 1009 *bir asal sayıdır.)* `[10p]`

(b) p *ve* q *iki farklı asal sayı olmak üzere* $p \equiv 3 \pmod 4$ *ve* $q \equiv 3 \pmod 4$ *olsun. Buna göre*

gösteriniz ki $X^2 \equiv p \pmod{q}$ *kongrüensinin bir çözümü vardır ancak ve ancak* $X^2 \equiv q \pmod{p}$ *kongrüensinin hiç çözümü yoktur.* [15p]

Çözüm. (a)

$\left(\frac{713}{1009}\right)$ sembolünün değerini arıyoruz.

$$\left(\frac{713}{1009}\right) = \left(\frac{23}{1009}\right)\left(\frac{31}{1009}\right)$$

olduğundan $\left(\frac{23}{1009}\right)$ ve $\left(\frac{31}{1009}\right)$ sembollerini ayrı ayrı bulalım.

$$\begin{aligned}\left(\frac{23}{1009}\right) &= (-1)^{11\times 504}\left(\frac{1009}{23}\right)\\ &= \left(\frac{20}{23}\right)\\ &= \left(\frac{2}{23}\right)^2\left(\frac{5}{23}\right)\\ &= \left(\frac{5}{23}\right)\\ &= (-1)^{2\times 11}\left(\frac{23}{5}\right)\\ &= \left(\frac{3}{5}\right)\end{aligned}$$

ve

$$3^{\frac{5-1}{2}} \equiv 3^2 \equiv -1 \pmod{5}$$

olduğundan

$$\left(\frac{23}{1009}\right) = \left(\frac{3}{5}\right) = -1$$

bulunur. Diğer taraftan

$$\begin{aligned}\left(\frac{31}{1009}\right) &= (-1)^{15\times 504}\left(\frac{1009}{31}\right)\\ &= \left(\frac{17}{31}\right)\\ &= (-1)^{8\times 15}\left(\frac{31}{17}\right)\\ &= \left(\frac{14}{17}\right)\\ &= \left(\frac{2}{17}\right)\left(\frac{7}{17}\right)\end{aligned}$$

ve $17 \equiv 1 \pmod 8$ olduğundan

$$\left(\frac{31}{1009}\right) = \left(\frac{2}{17}\right)\left(\frac{7}{17}\right) = \left(\frac{7}{17}\right)$$

olur. Fakat

$$\left(\frac{7}{17}\right) = (-1)^{3\times 8}\left(\frac{17}{7}\right) = \left(\frac{3}{7}\right)$$

ve

$$3^{\frac{7-1}{2}} \equiv 3^3 \equiv 27 \equiv -1 \pmod 7$$

olduğundan

$$\left(\frac{31}{1009}\right) = \left(\frac{7}{17}\right) = -1$$

bulunur. Dolayısıyla

$$\left(\frac{713}{1009}\right) = \left(\frac{23}{1009}\right)\left(\frac{31}{1009}\right) = (-1)(-1) = 1$$

bulunur. Buna göre $X^2 \equiv 713 \pmod{1009}$ kongrüensinin çözümü vardır.

(b) $p \equiv 3 \pmod 4$ ve $q \equiv 3 \pmod 4$ ise o zaman $\frac{p-1}{2} \equiv 1 \pmod 2$ ve $\frac{q-1}{2} \equiv 1 \pmod 2$ olur. Buna göre

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = -1$$

olacağından $\left(\frac{p}{q}\right) = 1$ ancak ve ancak $\left(\frac{q}{p}\right) = -1$ olur. Böylece $X^2 \equiv p \pmod q$ çözülebilirdir ancak ve ancak $X^2 \equiv q \pmod p$ çözülebilir değildir.