

CEVAPLAR

ALIŞTIRMALAR 17

1. $\mathbb{Z}_{24}^* \not\cong \mathbb{Z}_4^* \oplus \mathbb{Z}_6^*$; $|\mathbb{Z}_{24}^*| = 8, |\mathbb{Z}_4^* \oplus \mathbb{Z}_6^*| = 4$. Çelişmez, $(4, 6) \neq 1$.
3. a. $\text{çek}(f_3^*) = \{1, 7, 13, 19\}$, $\text{çek}(f_8^*) = \{1, 17\}$.
b. $\text{çek}(f_4^*) = \{1, 5, 13, 17\}$, $\text{çek}(f_6^*) = \{1, 7, 13, 19\}$ olup buradan görülür ki $\text{çek}(f_4^*) \cap \text{çek}(f_6^*) = \{1, 13\}$ ve $\mathbb{Z}_{24}^* \neq \text{çek}(f_4^*) \times \text{çek}(f_6^*)$.
5. $\mathbb{Z}_{220}^* \cong \mathbb{Z}_4^* \oplus \mathbb{Z}_5^* \oplus \mathbb{Z}_{11}^* \cong \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{10} \cong \mathbb{Z}_{20} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$.
7. $720 = 2^4 \cdot 3^2 \cdot 5$. $\mathbb{Z}_{720}^* \cong \mathbb{Z}_{16}^* \oplus \mathbb{Z}_9^* \oplus \mathbb{Z}_5^* \cong \mathbb{Z}_8 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_4 \cong \mathbb{Z}_{24} \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2$.
 $(a, b, c) \in \mathbb{Z}_{24} \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2$ elemanının mertebesinin 6 olacağı durumlar:
 $|a| = 6$, $b \in \{0, 2\}$, $c \in \{0, 1\}$ olan 8 eleman; $|a| = 3$, $b \in \{0, 2\}$, $c = 1$ olan 4 eleman, $|a| = 3$, $b = 2$, $c = 0$ olan 2 eleman; toplam 14 eleman.
9. $2 < p < q$ kabul edelim.
a. $\mathbb{Z}_{p^m} \oplus \mathbb{Z}_{q^n}$ devirlidir; p^m ve q^n aralarında asal.
b. $\mathbb{Z}_{p^m}^* \oplus \mathbb{Z}_{q^n}^* \cong \mathbb{Z}_{p^{m-1}(p-1)} \oplus \mathbb{Z}_{q^{n-1}(q-1)}$ devirli değil; $p^{m-1}(p-1)$ ve $q^{n-1}(q-1)$ aralarında asal değil.
11. $(\mathbb{Z}_n^*)^2 = \{x^2 : x \in \mathbb{Z}_n^*\} \subseteq \mathbb{Z}_n^*$ olduğu açık. $1 = 1^2 \in (\mathbb{Z}_n^*)^2$. Ayrıca, $x^2, y^2 \in (\mathbb{Z}_n^*)^2 \implies x^2(y^2)^{-1} = (xy^{-1})^2 \in (\mathbb{Z}_n^*)^2$. Dolayısıyla, $(\mathbb{Z}_n^*)^2 \leq \mathbb{Z}_n^*$. Diğer yandan, $n > 1 \implies 1^2 = (n-1)^2$. O nedenle, $(\mathbb{Z}_n^*)^2 < \mathbb{Z}_n^*$.
13. $|\mathbb{Z}_{15}^*| = 8$.
15. $n = 49$. $|9| = 14$.
17. Gauss Teoremi'ne göre, $r \geq 3$ ise, $\mathbb{Z}_{2^r}^* \cong \mathbb{Z}_2^* \oplus \mathbb{Z}_{2^{r-1}}^*$ devirli değildir ve 2^r modunda ilkel kök yoktur. Eğer n sayısının iki veya daha çok

(farklı) tek asal çarpanı varsa, $\mathbb{Z}_n^*$ devirli olmayacağından, n modunda ilkel kök yoktur. Geriye, verilen kümenin elemanları olan n sayıları kalıyor ki, Gauss Teoremi'ne göre bunlar için $\mathbb{Z}_n^*$ devirlidir.

19. p tek asal sayı.

a. x, p^n modunda bir ilkel kök, $x = pa + x_0$, $a \in \mathbb{Z}$, $x_0 \in \mathbb{Z}_p^*$, $|x_0| = k$ olsun. Bu takdirde, $x_0^k \equiv 1 \pmod{p} \implies x^k \equiv 1 \pmod{p}$, buradan $x^{kp} \equiv 1 \pmod{p^2}$ ve tümevarımla, $x^{kp^{n-1}} \equiv 1 \pmod{p^n}$. x, p^n modunda bir ilkel kök olduğundan, $\varphi(p^n) \mid kp^{n-1}$. Böylece, $k = p - 1$ ve x, p modunda ilkel köktür (Sayfa 165 in son paragrafına bakınız).

b. x, p^2 modunda bir ilkel kök ise, $x^{p-1} \not\equiv 1 \pmod{p^2}$; Fermat Teoremi'nden, $x^{p-1} \equiv 1 \pmod{p}$ olur. $x^{p-1} = 1 + pa$, $a \in \mathbb{Z} \setminus \{0\}$ olsun. Buradan, $x^{p(p-1)} \equiv 1 + p^2a \pmod{p^3}$, $x^{p(p-1)} \not\equiv 1 \pmod{p^3}$ ve $x^{p^2(p-1)} \equiv 1 \pmod{p^3}$ olduğu görülür. Tümevarımla, $x^{p^{n-2}(p-1)} \not\equiv 1 \pmod{p^n}$ ve $x^{p^{n-1}(p-1)} \equiv 1 \pmod{p^n}$ olduğu görülür. Bu, x in p^n modunda da ilkel kök olduğunu kanıtlar.

21. a. $\mathbb{Z}_9^*$ in $\varphi(\varphi(9)) = \varphi(6) = 2$ üretici: 2, 2^5 .

b. $\mathbb{Z}_{18}^*$ in $\varphi(\varphi(18)) = \varphi(6) = 2$ üretici: 5, 5^5 .

c. $\mathbb{Z}_{27}^*$ in $\varphi(\varphi(27)) = \varphi(18) = 6$ üretici: 2, 2^5 , 2^7 , 2^{11} , 2^{13} , 2^{17} .

d. $\mathbb{Z}_{81}^*$ in $\varphi(\varphi(81)) = 18$ üretici: $\{2^k : 1 \leq k \leq 53, (k, 54) = 1\}$.

e. $\mathbb{Z}_{162}^*$ in $\varphi(\varphi(162)) = 18$ üretici: $\{5^k : 1 \leq k \leq 161, (k, 162) = 1\}$.

23. $Oto(\mathbb{Z}_{50}) \cong \mathbb{Z}_{50}^* \cong \mathbb{Z}_{25}^* \oplus \mathbb{Z}_2^* \cong \mathbb{Z}_{20}$.

25. $p = 41$, $q = 73$ ve $r = 7$. $n = 41 \cdot 73 = 2993$, $m = okek(40, 72) = 360$, 7 nin $\mathbb{Z}_{360}$ içinde tersi 103.

a. OLUR sözcüğü, 1815 ve 2521 bloklarına karşılık gelir; dolayısıyla bu sözcük şifrelenirken şu işlemler yapılır: $1815^7 \equiv 1511 \pmod{2993}$, $2521^7 \equiv 1812 \pmod{2993}$. Böylece, OLUR sözcüğünün şifrelenmiş biçimi LIOİ bulunur.

b. $2990^{103} \equiv 0806 \pmod{2993}$, $2529^{103} \equiv 1500 \pmod{2993}$. Dolayısıyla, gönderilen mesajın aşı, 0806 1500 bloklarına karşılık gelen GEL sözcüğüdür.