ALIŞTIRMALAR 17

1. $\mathbb{Z}_{24}^* \cong \mathbb{Z}_4^* \oplus \mathbb{Z}_6^*$ mıdır? Yanıtınız, konu içindeki Teorem 1 ile çelişir mi?

2. n ve s doğal sayılar, $s \mid n$ ise, $\mathbb{Z}_n$ den $\mathbb{Z}_s$ ye $(mod\ s)$ indirgeme homomorfizmi f_s nin, $\mathbb{Z}_n^*$ grubuna kısıtlanışını f_s^* ile gösterelim.

a. $f_s^* : \mathbb{Z}_n^* \longrightarrow \mathbb{Z}_s^*$ ın bir örten grup homomorfizmi olduğunu gösteriniz.

b. s ve $\frac{n}{s} = t$, aralarında asal ise, $çek\ (f_s^*) \cong \mathbb{Z}_t^*$ ve $çek\ (f_t^*) \cong \mathbb{Z}_s^*$ olduğunu gösteriniz.

c. s ve $\frac{n}{s} = t$, aralarında asal ise, $\mathbb{Z}_n^* = (çek\ (f_s^*)) \times (çek\ (f_t^*))$ olduğunu gösteriniz.

3. Bundan önceki alıştırmanın gösterimleriyle, $\mathbb{Z}_{24}^*$ içinde

a. $çek\ (f_3^*)$ ve $çek\ (f_8^*)$ ı bulunuz ve $\mathbb{Z}_{24}^* = (çek\ (f_3^*)) \times (çek\ (f_8^*))$ olduğunu gözlemleyiniz.

b. $çek\ (f_4^*)$ ve $çek\ (f_6^*)$ ı bulunuz. $\mathbb{Z}_{24}^* = (çek\ (f_4^*)) \times (çek\ (f_6^*))$ doğru mudur? Neden?

4. $\mathbb{Z}_{220}^*$ ı, üç farklı biçimde, özaltgruplarının iç dolaysız çarpımı olarak ifade ediniz.

5. $\mathbb{Z}_{220}^*$ ı devirli grupların ($\mathbb{Z}_n$ lerin) dış dolaysız çarpımı olarak ifade ediniz.

6. $\mathbb{Z}_{27}^*$ ın kaç altgrubu vardır? Açıklayınız.

7. $\mathbb{Z}_{720}^*$ ın, mertebesi 6 olan kaç elemanı bulunduğunu, fazla hesaba girişmeden, belirleyiniz.

8. $\mathbb{Z}_{900}^*$ ın bir elemanının mertebesi en çok kaç olabilir? Açıklayınız.

9. p ve q iki farklı asal sayı, m ve n iki pozitif tamsayı ise,

a. $\mathbb{Z}_{p^m} \oplus \mathbb{Z}_{q^n}$ devirli midir? Neden ?

b. $\mathbb{Z}^*_{p^m} \oplus \mathbb{Z}^*_{q^n}$ devirli midir? Neden ?

10. $\mathbb{Z}^*_{55} \cong \mathbb{Z}^*_{75}$ ve $\mathbb{Z}^*_{144} \cong \mathbb{Z}^*_{140}$ olduğunu kanıtlayınız.

11. Her $n > 2$ için $(\mathbb{Z}^*_n)^2 = \{x^2 : x \in \mathbb{Z}^*_n\} < \mathbb{Z}^*_n$ olduğunu kanıtlayınız.

12. $(\mathbb{Z}^*_{55})^3 = \{x^3 : x \in \mathbb{Z}^*_{55}\} = \mathbb{Z}^*_{55}$ olduğunu gösteriniz.

13. $|\mathbb{Z}^*_n| = 8$ olacak biçimde bir n var mıdır?

14. $|\mathbb{Z}^*_n| = 14$ olacak biçimde bir n var mıdır?

15. Öyle bir n doğal sayısı bulunuz ki $\mathbb{Z}^*_n$ içinde mertebesi 14 olan bir eleman bulunsun.

16. $\mathbb{Z}^*_n \cong \mathbb{Z}_4 \oplus \mathbb{Z}_4$ olacak biçimde bir n var mıdır?

17. n modunda ilkel kök bulunan n doğal sayılarının kümesinin

$$\{1, 2, 4\} \cup \{p^r : p, r \in \mathbb{N}, p \text{ asal}, \ p > 2\} \cup \{2p^r : p, r \in \mathbb{N}, p \text{ asal}, \ p > 2\}$$

olduğunu gösteriniz.

18. 25 ve 26 modunda tüm ilkel kökleri bulunuz.

19. p bir tek asal sayı ve n herhangi bir doğal sayı olsun. Aşağıdakileri kanıtlayınız.

a. p^n modunda her ilkel kök p modunda da ilkel köktür.

b. p^2 modunda her ilkel kök p^n modunda da ilkel köktür.

20. p bir tek asal sayı, r bir doğal sayı ve x, p^r modunda bir ilkel kök olsun. x in $2p^r$ modunda da bir ilkel kök olması için gerek ve yeter koşul, x in tek olmasıdır; kanıtlayınız.

21. Aşağıdaki n sayılarından her biri için $\mathbb{Z}_n^*$ içinde n modunda ilkel kökleri belirleyiniz.

a. $n = 9$ **b.** $n = 18$ **c.** $n = 27$ **d.** $n = 81$ **e.** $n = 162$

22. *Oto* $(\mathbb{Z}_{20}) \cong \mathbb{Z}_{20}^*$ olduğunu kullanarak, *Oto* $(\mathbb{Z}_{20})$ nin mertebesi 4 olan kaç elemanı bulunduğunu belirleyiniz. *Oto* $(\mathbb{Z}_{20})$ nin, mertebesi 2 olan kaç elemanı vardır?

23. *Oto* $(\mathbb{Z}_{50})$ nin devirli grup olduğunu gösteriniz.

24. *Oto* $(\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5)$ grubunu, $\mathbb{Z}_n$ tipinde grupların dış dolaysız çarpımı olarak ifade ediniz.

25. *RSA* sistemi ile haberleşen bir grupta bir alıcı için, $p = 41$, $q = 73$ ve $r = 7$ seçilmiş olsun.

a. Bu alıcıya gönderilmek üzere *OLUR* sözcüğünü şifreleyiniz.

b. Bu alıcıya, 29902529 şifreli mesajı geliyor. Mesajı çözünüz(deşifre ediniz).