Kryptografia z elementami algebry

grupy, notacja wielkie-O, funkcje jednokierunkowe

1. Sprawdź czy H jest podgrupą G, gdzie
   (a) $G = \mathbb{Z}_9^+$, $H = \{0, 5, 7\}$,
   (b) $G = \Phi(20)$, $H = \{1, 9\}$,
2. Wyznacz warstwy grupy G względem podgrupy H oraz oblicz index $(G : H)$, gdzie
   (a) $G = \mathbb{Z}_{12}^+$, $H = \{0, 4, 8\}$
   (b) $G = \mathbb{Z}^+$, $H = 3\mathbb{Z}^+$
   (c) $G = \Phi(13)$, $H = \{1, 3, 9\}$
3. Wyznacz elementy grupy ilorazowej $\Phi(21)/H$, gdzie $H = \{1, 8, 13, 20\}$. Utwórz tabelkę działań w tej grupie.
4. Sprawdź, które grupy są cykliczne?
   (a) $\mathbb{Z}_9^+$,
   (b) $\Phi(13)$,
   (c) $\Phi(12)$.
5. Wyznacz rząd elementu $a \in G$, gdzie
   (a) $a = 0$, $G = \mathbb{Z}^+$,
   (b) $a = -1$, $G = \mathbb{Z}^+$,
   (c) $a = 5$, $G = \mathbb{Z}_{50}^+$,
   (d) $a = 3$, $G = \Phi(7)$,
   (e) $a = 2$, $G = \Phi(11)$,
6.
7. Sprawdź czy odwzorowanie $f : \mathbb{Z}^+ \to \mathbb{Z}_8^+$ takie, że $f(n) = 2n \pmod 7$ jest homomorfizmem grup. Wyznacz jądro i obraz tego homomorfizmu.
8. Sprawdź czy odwzorowanie $f : \mathbb{Z}^+ \to \Phi(7)$ takie, że $f(n) = 3^n \pmod 7$ jest homomorfizmem grup. Wyznacz jądro i obraz tego homomorfizmu.
9. Sprawdź czy odwzorowanie $f : \mathbb{Z}^+ \to \Phi(7)$ takie, że $f(n) = 3^n \pmod 8$ jest homomorfizmem grup. Wyznacz jądro i obraz tego homomorfizmu.
10. Sprawdź czy odwzorowanie $f : \mathbb{Z}_2^+ \to \{-1, 1\}$ takie, że $f(0) = 1$ i $f(1) = -1$ jest homomorfizmem grup. Wyznacz jądro i obraz tego homomorfizmu.
11. Sprawdź czy odwzorowanie $f : \Phi(8) \to \Phi(4)$ takie, że $f(n) = n$ jest homomorfizmem grup. Wyznacz jądro i obraz tego homomorfizmu.

12. Sprawdź czy odwzorowanie $f : \mathbb{Z}^+ \to \mathbb{Z}^+$ takie, że $f(n) = 6n$ jest homomorfizmem grup. Wyznacz jądro i obraz tego homomorfizmu.

13. Znajdź homomorfizm $f : \mathbb{Z}_{12}^+ \to \mathbb{Z}_{12}^+$ taki, że $\ker(f) = \{0, 3, 6, 9\}$.