

תרגילים 4: תמורהות וצופן אניגמה

שאלה 1 הוכחו או הפריכו ע"י דוגמה נגדית: אם π מחזור באורך k אז π^n מחזור באורך k .

שאלה 2 הוכחו או הפריכו ע"י דוגמה נגדית: אם π ו- σ תמורהות מתחלפות, כלומר $\sigma\pi = \pi\sigma$ אז לכל $k \geq 1$ מתקיים $(\pi\sigma)^k = \pi^k\sigma^k$.

שאלה 3 תהי $\Sigma \rightarrow \Sigma$: π תמורה על האלפבית Σ . הוכחו או הפריכו ע"י דוגמה נגדית: אם $\alpha \in \Sigma$ היא נקודת זהה של π אז $\pi^{-1}(\alpha)$ היא נקודת זהה של π .

שאלה 4 נתונות התמורהות הבאות של צופן אניגמה:

$$\Delta_4\Delta_1 = (\text{ZRYS})(\text{JNVU})(\text{GPDOFWHQB})(\text{ACIKETMLX}) ,$$

$$\Delta_5\Delta_2 = (\text{DO})(\text{IA})(\text{STYHJ})(\text{BPMZX})(\text{NWFVLR})(\text{CEUKGQ}) ,$$

$$\Delta_6\Delta_3 = (\text{MOE})(\text{CNK})(\text{WBIZ})(\text{AGLY})(\text{VFPXTJ})(\text{DHRSUQ}) .$$

נתון כי התמורהות הן בסדר ריבסקי. חשבו את הטקסט המקורי של המילים הבאות שהוצפנו ע"י צופן אניגמה:

(א)

KOOSRT

(ב)

QIUTRN

(ג)

JVIGE

(ד)

LLSXRT

פתרונות

שאלה 1

שאלה 2

שאלה 3

שאלה 4

(א)

winner

(ב)

coffee

(ג)

sugar

(ד)

pepper