

## תרגיל בית 9 במבנים אלגבריים 89-214 סמסטר א' תשפ"ג

**שאלה 1** (חזרה). מצאו את כל המחלקות השמאליות ב- $\mathbb{Z}_{30}/\langle 3 \rangle$ .

**שאלה 2**. תזכורת: מספר פריק  $n$  נקרא מספר קרמייקל אם ורק אם לכל  $b \leq n$  הזר ל- $n$  מתקיים  $b^{n-1} \equiv 1 \pmod{n}$  (או באופן שקול  $b^n \equiv b \pmod{n}$  לכל  $b$ ). הריצו את אלגוריתם מילר-רבין עבור המספר 29341 והעדים (הפוטנציאליים)  $a, b+2$ , כאשר  $a$  הוא 3 הספרות הראשונות בת"ז שלכם ו- $b$  הוא 2 הספרות האחרונות. כתבו את מסקנתכם מההרצה.

**שאלה 3**. הוכיחו או הפריכו האם  $H \triangleleft G$  עבור החבורות ותת־קבוצות הבאות:

א.  $H = \langle (89)(214) \rangle, G = S_9$ .

ב.  $H = \{\sigma \in S_n \mid \sigma(1) = 1\}, G = S_n$ .

ג.  $H = \{\alpha I \mid \alpha \in F^*\}, G = GL_n(F)$  (כאן  $H$  היא קבוצת המטריצות הסקלריות ההפיכות מעל השדה  $F$ ).

**שאלה 4**. הפריכו את הטענות השגויות הבאות:

א. כל תת־חבורה אבלית היא נורמלית.

ב. כל תת־חבורה נורמלית היא אבלית.

ג. התמונה של כל הומומורפיזם  $f: G \rightarrow H$  היא תת־חבורה נורמלית של  $H$ .

**שאלה 5**. תהי  $G$  חבורה מסדר 46, ותהי  $H$  תת־חבורה לא נורמלית שלה. מצאו את הסדר של  $H$ .

**שאלה 6**. תהי  $H \leq G$ . הוכיחו כי  $H \triangleleft G$  אם ורק אם לכל  $x, y \in G$ ,

$$yx \in H \iff xy \in H$$

**שאלה 7**. חבורה  $G$  נקראת פשוטה אם אין לה תת־חבורות נורמליות לא טריוויאליות (כלומר שונות מ- $\{e\}$  ו- $G$ ).

א. תהי  $G$  חבורה פשוטה ו- $H$  חבורה כלשהי. הוכיחו שאם  $f: G \rightarrow H$  הוא הומומורפיזם לא טריוויאלי, אז  $f$  מונומורפיזם.

ב. הוכיחו שלא קיימת חבורה אבלית פשוטה אינסופית.

ג. תהי  $A$  חבורה אבלית פשוטה. הוכיחו כי  $A$  טריוויאלית או שקיים  $p$  ראשוני כך ש- $A \cong \mathbb{Z}_p$ .

**שאלה 8.** בשאלה הזו תראו שאלגוריתם מילר-רבין הוא דטרמיניסטי למספרים לא כל כך קטנים עבור קבוצת עדים נתונה.

א. חשבו ש-97 הוא עד חזק לראשוניות של 469 ואילו 133 לא. לעומת זאת, חשבו כי 133 הוא עד חזק לראשוניות של 305 ואילו 79 לא. ודאו חישובים אלו בסעיף הבא.

ב. בחרו שפת תכנות כרצונכם וכתבו פונקציה בשם  $\text{millerrabin}(N, W)$  המממשת את אלגוריתם מילר-רבין למספר טבעי  $N$  ולקבוצת עדים נתונה  $W$  (בכיתה במקום  $W$  בחרנו באקראי כמה מספרים). הראו שהעדים החזקים לראשוניות של 505 בקטע [2, 503] הם רק 192, 212, 293, 313.

ג. כתבו פונקציה נוספת  $\text{first\_mistake}(W)$  שמחזירה את המספר  $N \geq 3$  האי זוגי הקטן ביותר שעבורו הפונקציה  $\text{millerrabin}(N, W)$  טועה. כלומר התשובה של  $\text{millerrabin}(N, W)$  שונה מהתשובה של  $\text{is\_prime}(N)$ , המחזירה בודאות האם  $N$  ראשוני. רק עבור המימוש של  $\text{is\_prime}(N)$  אפשר להשתמש בספריות חיצוניות!<sup>1</sup>

דוגמה להרצה היא  $\text{first\_mistake}(\{2\}) = 2047$ . כלומר לכל מספר אי זוגי  $3 \leq N < 2047$  הקריאה  $\text{millerrabin}(N, \{2\})$  מחזירה את התשובה הנכונה, אבל  $\text{millerrabin}(2047, \{2\})$  מחזירה ש-2047 כנראה ראשוני, אבל הוא למעשה פריק:  $2047 = 23 \cdot 89$ . כתבו את התוצאות של הרצת:

- `first_mistake({3})` •
- `first_mistake({3, 5})` •
- `first_mistake({4, 9})` •
- `first_mistake({7, 11})` •
- `first_mistake({7, 11, 13})` •

בהצלחה!

<sup>1</sup>כמובן שאפשר לממש בעצמכם. אפשרות טובה לשאלה הנוכחית היא **הנפה של ארטוסטנס** עם מטמון (Cache). לחלק הזה אפשר להשתמש במערכת תוכנה מתמטית.