

## תרגיל בית 8 במבנים אלגבריים 89-214 סמסטר א' תשע"ט

**שאלה 1.** תהי  $G = GL_2(\mathbb{Z}_2)$ . מצאו את תמונת כל האיברים בשיכון קיילי  $\Phi: G \rightarrow S_6$ . רמז: שאלה 4 בתרגיל בית 6 ואפשר להעזר במחשב.

**שאלה 2.** תהי  $G$  חבורה מסדר  $n$  ויהי  $\Phi: G \rightarrow S_n$  שיכון קיילי. הוכיחו שאיבר  $g \in G$  הוא מסדר  $m$  אם ורק אם  $\Phi(g) \in S_n$  הוא מכפלה של  $\frac{n}{m}$  מחזורים זרים מאורך  $m$ .

**שאלה 3.** חשבו בשיטה של ריבועים בעזרת חזקה חישוב את הביטויים הבאים. מותר להשתמש במחשב (כולל בפונקציית המודולו) לחישובי הביניים, שאותם תפרטו:

א.  $2790^{2753} \in \mathbb{Z}_{3233}$ . רמז: בתרגול ראיתם שהתוצאה הסופית היא ההודעה שבו רצה לשלוח לאליס.

ב.  $\begin{pmatrix} 8 & 9 \\ 1 & 1 \end{pmatrix}^{214} \in GL_2(\mathbb{Z}_{1000})$ .

**שאלה 4.** חשבו בעזרת משפט אוילר:

א. שתי הספרות האחרונות של  $543^{3838}$ .

ב.  $89^{214} \pmod{91}$ .

**שאלה 5.** בשאלה הזו תראו שאלגוריתם רבין-מילר הוא דטרמיניסטי למספרים לא כל כך קטנים עבור קבוצת עדים נתונה.

א. חשבו ש-99 הוא עד חזק לראשוניות של 377 ואילו 110 לא. לעומת זאת, חשבו כי 110 הוא עד חזק לראשוניות של 289 ואילו 99 לא. ודאו חישובים אלו בסעיף הבא.

ב. בחרו שפת תכנות כרצונכם וכתבו פונקציה בשם `rabinmiller(N, W)` המממשת את אלגוריתם רבין-מילר למספר טבעי  $N$  ולקבוצת עדים נתונה  $W$  (בכיתה במקום  $W$  בחרנו באקראי כמה מספרים).

הראו שהעדים החזקים לראשוניות של 689 בקטע [2, 687] הם רק 83, 242, 447, 606.

ג. כתבו פונקציה נוספת `first_mistake(W)` שמחזירה את המספר  $N \geq 3$  האי זוגי הקטן ביותר שעבורו הפונקציה `rabinmiller(N, W)` טועה. כלומר התשובה של `rabinmiller(N, W)` שונה מהתשובה של `is_prime(N)`, המחזירה בודאות האם  $N$  ראשוני. רק עבור המימוש של `is_prime(N)` אפשר להשתמש בספריות חיצוניות<sup>1</sup>.

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

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

- first\_mistake({3}) •
- first\_mistake({3,5}) •
- first\_mistake({4,5}) •
- first\_mistake({7,11}) •
- first\_mistake({7,11,13}) •

**שאלה 6** (רשות). חשבו האם ניתן לממש את אלגוריתם RSA באמצעות חבורה לא אבלית (כמו  $S_n$ )? מה משתבש?

**שאלה 7** (רשות). הראו שכאשר  $n = pq$  והראשוניים  $p, q$  "קרובים יחסית", אפשר לתקוף די בקלות את RSA.

שימו לב שמתקיים:  $n = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2$ , ואז  $\frac{p+q}{2}$  יחסית קרוב למספר  $\sqrt{n}$ . סמנו:  $t = \frac{p+q}{2}, s = \frac{p-q}{2}$  והסבירו למה במצב כזה יחסית קל למצוא את  $t, s$  (ובאמצעותם את  $p, q$  בהינתן  $n$ ).  
הדגימו זאת על  $n = 23360947609$ .

בהצלחה!