

# תרגיל בית 10 במבנים אלגבריים

## 89-214 סמסטר א' תשע"ז

**הוראות** בהגשת הפתרון יש לרשום בכל דף שם מלא, מספר ת"ז ומספר קבוצת תרגול. תאריך הגשת התרגיל הוא בתאריך י"ב שבט ה'תשע"ז, 8.2.2017, לתא של המתרגל.

הערה: נסמן את השדה הסופי בן  $q$  איברים ב- $\mathbb{F}_q$ .

### שאלות חימום

שאלות החימום הן שאלות שאינן להגשה, והן בדרך כלל קלות יותר. אבל כדאי מאוד לוודא שיודעים איך לפתור אותן, אפילו בעל פה.

**שאלה 1.** כמה חבורות אבליות יש מסדר 50?

**שאלה 2.** האם  $\mathbb{Z}_2 \times \mathbb{Z}_{12}$  איזומורפית לחבורה כפלית של שדה כלשהו? האם  $\mathbb{Z}_2 \times \mathbb{Z}_{13}$ ?

### שאלות להגשה

**שאלה 3.** כתבו את כל החבורות האבליות מסדר  $720 = 6!$  בצורה קנונית. כלומר עליכם לרשום רשימה של חבורות מן הצורה

$$\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_r}$$

ושמתקיים  $d_i | d_{i+1}$  לכל  $1 \leq i \leq r-1$ . סמנו את החבורות שבהן קיים איבר מסדר 9.

**שאלה 4.** נתונות שש חבורות מסדר 54. זהו ונמקו אילו חבורות איזומורפיות זו לזו:

$$U_7 \times \mathbb{Z}_9, \quad \mathbb{Z}_{27} \times \mathbb{F}_3^*, \quad \mathbb{F}_9 \times U_{18}, \quad \mathbb{Z}_{18} \times \mathbb{Z}_3, \quad \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_9, \quad \mathbb{Z}_{54}$$

כאשר  $\mathbb{F}_9$  זו החבורה החיבורית של השדה מסדר 9 ו- $\mathbb{F}_3^*$  זו החבורה הכפלית של השדה מסדר 3.

**שאלה 5.** הזכרו שהרחבת שדות של  $\mathbb{F}_p$  מדרגה  $n$  מתקבלת על ידי סיפוח שורש  $\alpha$  של פולינום אי פריק ממעלה  $n$  מעל  $\mathbb{F}_p$ . השדה המתקבל  $\mathbb{F}_p[\alpha]$  איזומורפי ל- $\mathbb{F}_{p^n}$ .

א. הציגו את  $\mathbb{F}_{125}$  כהרחבה של  $\mathbb{F}_5$ . כלומר מצאו  $\alpha$  מתאים כך ש- $\mathbb{F}_{125} \cong \mathbb{F}_5[\alpha]$ .

ב. נסמן שני איברים לפי הבניה מהסעיף הקודם:

$$x = 4\alpha^2 + 2, \quad y = \alpha^2 + \alpha + 3$$

הציגו את  $x+y$  ואת  $xy$  כפולינומים ב- $\alpha$ .

ג. מצאו את הסדר (הכפלי) של  $x+y$  ב- $\mathbb{F}_{125}^*$ , ואת הסדר (החיבורי) של  $xy$  ב- $\mathbb{F}_{125}$ .

**שאלה 6.** רמז: המספרים 7 ו-2017 ראשוניים.

א. הוכיחו שקיים  $x \in \mathbb{F}_q$  המקיים

$$\sum_{i=0}^{2016} x^i = 1 + x + \dots + x^{2016} = 0$$

אם ורק אם  $q \equiv 0 \pmod{2017}$  או  $q \equiv 1 \pmod{2017}$ . רמז: קודם מצאו שורש של הפולינום  $x^{2017} - 1$ .

ב. מצאו עבור אילו מספרים טבעיים  $n$  השדה  $\mathbb{F}_{5^n}$  מכיל איבר  $x$  המקיים

$$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = 0$$

**שאלה 7.** בשאלה הזו תראו שאלגוריתם רבין-מילר הוא דטרמיניסטי למספרים לא כל כך קטנים עבור קבוצת עדים נתונה.

א. בחרו שפת תכנות (לא איזוטרית) 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).

ב. 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 חישוביות.<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:

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

## שאלות רשות

את שאלות הרשות אין חובה לפתור, אבל אם פתרתם אותן, בבקשה צרפו את הפתרון שלהן.

**שאלה 8.** הוכיחו את משפט וילסון בעזרת שדות סופיים: מספר  $n \in \mathbb{N}$  ראשוני אם ורק אם

$$(n-1)! \equiv -1 \pmod{n}$$

**שאלה 9.** כתבו תוכנה שתמצא את כל החבורות האבליות מסדר  $n$ . מהו המספר הגדול ביותר שהתוכנה שלכם עובדת עבורו בפחות מדקה?

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.