

# פתרון 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?

פתרון. נפרק לגורמים ראשוניים  $50 = 2 \cdot 5^2$ , ולכן יש רק  $\rho(1)\rho(2) = 2$  חבורות אבליות מסדר 50, עד כדי איזומורפיזם.

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

פתרון. החבורה  $\mathbb{Z}_2 \times \mathbb{Z}_{12}$  לא ציקלית, ולכן אינה איזומורפית לחבורה כפלית של שדה סופי. החבורה  $\mathbb{Z}_2 \times \mathbb{Z}_{13}$  ציקלית וגם הסדר שלה הוא חזקת ראשוני פחות 1. בפרט,

$$\mathbb{F}_{27}^* \cong \mathbb{Z}_{26} \cong \mathbb{Z}_2 \times \mathbb{Z}_{13}$$

### שאלות להגשה

**שאלה 3.** כתבו את כל החבורות האבליות מסדר  $6! = 720$  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.

פתרון. קל לחשב  $6! = 2^4 \cdot 3^2 \cdot 5$ , ולכן יש  $\rho(4)\rho(2) = 5 \cdot 2 = 10$  חבורות אבליות מסדר

720, עד כדי איזומורפיזם. הרשימה המלאה היא

$$\begin{aligned}
 \mathbb{Z}_{2^4} \times \mathbb{Z}_{3^2} \times \mathbb{Z}_5 &\cong \mathbb{Z}_{720} & * \\
 \mathbb{Z}_{2^4} \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 &\cong \mathbb{Z}_3 \times \mathbb{Z}_{240} \\
 \mathbb{Z}_2 \times \mathbb{Z}_{2^3} \times \mathbb{Z}_{3^2} \times \mathbb{Z}_5 &\cong \mathbb{Z}_2 \times \mathbb{Z}_{360} & * \\
 \mathbb{Z}_2 \times \mathbb{Z}_{2^3} \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 &\cong \mathbb{Z}_6 \times \mathbb{Z}_{120} \\
 \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_{3^2} \times \mathbb{Z}_5 &\cong \mathbb{Z}_4 \times \mathbb{Z}_{180} & * \\
 \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 &\cong \mathbb{Z}_{12} \times \mathbb{Z}_{60} \\
 \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{2^2} \times \mathbb{Z}_{3^2} \times \mathbb{Z}_5 &\cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{180} & * \\
 \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{2^2} \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 &\cong \mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_{60} \\
 \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{3^2} \times \mathbb{Z}_5 &\cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{90} & * \\
 \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 &\cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_{30}
 \end{aligned}$$

כשבאגף ימין מופיעה הצורה הקנונית. בחבורות המסומנות \* יש איבר מסדר 9, כי אפשר להציג אותן כאשר  $\mathbb{Z}_9$  היא אחד מן הגורמים במכפלה הישרה. בחבורות האחרות, איברים מסדר  $3^i$  "מגיעים" רק מהגורמים  $\mathbb{Z}_3 \times \mathbb{Z}_3$ , ולכן אין בהן 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.

פתרון. נחשב  $54 = 2 \cdot 3^3$ . לכן יש  $\rho(1)\rho(3) = 3$  חבורות אבליות מסדר 54, עד כדי איזומורפיזם. את הנימוקים לאיזומורפיזמים נשאיר לכם למלא, עם הרמז שהחבורה השמאלית בכל שורה היא בצורה קנונית:

$$\begin{aligned}
 \mathbb{Z}_{54} &\cong \mathbb{Z}_{27} \times \mathbb{F}_3^* \\
 \mathbb{Z}_3 \times \mathbb{Z}_{18} &\cong \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \cong \mathbb{Z}_{18} \times \mathbb{Z}_3 \cong U_7 \times \mathbb{Z}_9 \\
 \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_6 &\cong \mathbb{F}_9 \times U_{18}
 \end{aligned}$$

**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- $\mathbb{F}_{125}$ .

פתרון.

א. נמצא פולינום אי פריק ממעלה 3 עם מקדמים ב- $\mathbb{F}_5$ . בדיקה מהירה על ידי הצבה מראה כי  $f(x) = x^3 + 3x + 3$  הוא אי פריק, כי פולינומים ממעלה 2 או 3 הם אי פריקים מעל שדה אם אין להם שורשים מעל השדה. ישנם 160 פולינומים אי פריקים ממעלה 3 מעל  $\mathbb{F}_5$ , וכמובן שמתוכם 40 הם מתוקנים. לכן יכולות להיות הרבה תשובות נכונות לסעיף הזה.

ב. ללא תלות בבחירה בסעיף הקודם מתקיים  $x + y = \alpha$ . עבור  $xy$  ישנה תלות בבחירה, במקרה שלנו נקבל

$$xy = (4\alpha^2 + 2)(\alpha^2 + \alpha + 3) = 4\alpha^4 + 4\alpha^3 + 14\alpha^2 + 2\alpha + 6 = 2\alpha^2 + 3\alpha + 4$$

ג. לפי הסעיף הקודם  $x + y = \alpha$ , ולכן מדובר ביוצר של  $\mathbb{F}_{125}^*$ . מפני שזו חבורה ציקלית מסדר 124, אזי  $x + y$  מסדר 124 שם. בחבורה  $\mathbb{F}_{125}$  הסדר של כל האיברים, פרט לאיבר היחידה, הוא 5. מפני ש- $xy \neq 0$ , אז הסדר של  $xy$  הוא בודאי 5.

**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

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

פתרון.

א. לפי הרמז נשים לב כי  $x = 1$  הוא שורש של הפולינום  $x^{2017} - 1$ . בעזרת חלוקת פולינומים נקבל

$$x^{2017} - 1 = (x - 1) \left( \sum_{i=0}^{2016} x^i \right)$$

מכאן נפצל למקרים: אם  $x = 1$  הוא שורש של הפולינום בשאלה, אז  $2017 \cdot x = 0$ , ולכן השדה ממאפיין 2017. אז בהכרח מתקיים  $q \equiv 0 \pmod{2017}$  כי  $q$  יהיה חזקה של 2017. אחרת, אם  $x \neq 1$  הוא שורש של הפולינום בשאלה, אז נקבל  $x^{2017} = 1$ . לכן  $o(x) | 2017$ . כלומר  $o(x) = 1$  או  $o(x) = 2017$ . במקרה של  $o(x) = 1$  כבר טיפלנו. מפני שידוע לנו לפי התרגיל בכיתה ש- $x^{q-1} = 1$ , כמסקנה מלגראנז' עבור החבורה הכפלית  $\mathbb{F}_q^*$ , אז  $2017 | q - 1$ , ולכן  $q \equiv 1 \pmod{2017}$ . בכיוון השני, אם  $q \equiv 0 \pmod{2017}$  נבחר  $x = 1$ , ואם  $q \equiv 1 \pmod{2017}$  נבחר יוצר של  $\mathbb{F}_q^*$ . ודאו שאתם מבינים למה היוצר יהיה שורש של הפולינום בשאלה.

ב. בהוכחה דומה לסעיף הקודם, השדות הסופיים שבהם קיים איבר שהוא שורש של הפולינום בשאלה הם שדות  $\mathbb{F}_q$  שבהם מתקיים  $q \equiv 0 \pmod{7}$  או  $q \equiv 1 \pmod{7}$ . מפני ש- $5 \in U_7$ , אז אין  $n$  עבורו  $5^n \equiv 0 \pmod{7}$ . הסדר של 5 בחבורה  $U_7$  הוא 6, ולכן כמסקנה ממשפט לגראנז' יתקיים  $5^n \equiv 1 \pmod{7}$  אם ורק אם  $6 | n$ .

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

א. בחרו שפת תכנות (לא איזוטריית) 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 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:

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

פתרון.

א. נשמח לשמוע על מימושים מקוריים.

ב. שימו לב שהשגיאה היחידה שיכולה להיות באלגוריתם מילר-רבין היא שהוא יחזיר מספר פריק בתור "כנראה ראשוני". לכן התוצאות להרצות תמיד יהיו מספרים פריקים:

- $first\_mistake(\{3\}) = 121$  •
- $first\_mistake(\{3, 5\}) = 112141$  •
- $first\_mistake(\{4, 5\}) = 5461$  •
- $first\_mistake(\{7, 11\}) = 88831$  •
- $first\_mistake(\{7, 11, 13\}) = 1152271$  •

## 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 ארטסטנס עם מטמון (Cache). לחלק הזה אפשר להשתמש במערכת תוכנה מתמטית.