

מטלה מס' 3 אלגברה מודרנית להגשה: עד יום ג' 18 בדצמבר

1. (40 נק') יהי $n \in \mathbb{N}$ ותהי $\mathbb{Z}/n\mathbb{Z} = \{0, 1, \dots, n-1\}$. נגדיר על הקבוצה פעולת חיבור ע"י

$$x +_n y = \begin{cases} x + y & x + y \leq n - 1 \\ x + y - n & x + y \geq n \end{cases}$$

ראינו בתרגול ש $(\mathbb{Z}/n\mathbb{Z}, +_n)$ חבורה אבלית הנקראת "חבורת השאריות מודולו n". לשם פשטות, מעתה והלאה נכתוב + במקום $+_n$.

(א) (30 נק') הראו שאיבר $a \in \mathbb{Z}/n\mathbb{Z}$ יוצר של החבורה אם ורק אם $\gcd(a, n) = 1$.

(ב) (10 נק') אם p מספר ראשוני מצאו כל איבר שיוצר את החבורה $(\mathbb{Z}/p\mathbb{Z}, +)$.

2. (60 נק') יהי $n \in \mathbb{N}$. נגדיר קבוצה על ידי

$$(\mathbb{Z}/n\mathbb{Z})^* = \{a \in \{0, 1, \dots, n-1\} \mid \gcd(a, n) = 1\}.$$

נגדיר על הקבוצה פעולת כפל על ידי

$$x \cdot_n y = \min\{xy - kn \mid k \in \mathbb{N} \cup \{0\}, xy - kn \geq 0\}.$$

(א) (5 נק') וודאו ש $x \cdot_n y \in \{0, 1, 2, \dots, n-1\}$ לכל $x, y \in (\mathbb{Z}/n\mathbb{Z})^*$.

(ב) (5 נק') וודאו ש $\gcd(x \cdot_n y, n) = 1$ לכל $x, y \in (\mathbb{Z}/n\mathbb{Z})^*$.

(ג) (5 נק') הסברו מדוע פעולת הכפל שהגדרנו על $(\mathbb{Z}/n\mathbb{Z})^*$ מוגדרת היטב.

(ד) (40 נק') הוכיחו ש $((\mathbb{Z}/n\mathbb{Z})^*, \cdot_n)$ חבורה אבלית.

(ה) (5 נק') חשבו את $\text{ord}(2)$, הסדר של 2 ב $((\mathbb{Z}/15\mathbb{Z})^*, \cdot_{15})$.

הוראות:

- יש להגיש את התרגיל **בזוגות**. מותר להגיש לבד.
- חובה לכתוב את מספרי ת.ז. של שני הסטודנטים.
- ניתן לכתוב פתרונות בכל צבע פרט לאדום.
- יש להגיש את העבודה למרצה בקורס (מרק ברמן). ישנן 2 אופציות:
 - להגיש לו ישירות (ידנית)
 - לשים את העבודה בתא דואר שלו (565) שנמצא על יד חדר EM429
- אין להגיש במייל אלקטרוני.
- יש להקפיד על מועד ההגשה. עבודה שמוגשת באיחור ללא סיבה מוצדקת ובלי קבלת אישור מראש לא בהכרח תיבדק.