

מטלה מס' 2 אלגברה מודרנית להגשה: עד יום ג' 4 בדצמבר

1. (60 נק') נתבונן במשוואה $ax \equiv b \pmod{n}$ כאשר $a, b, n \in \mathbb{N}$ קבועים ו x משתנה. אנו מעוניינים לגלות תנאים על a, b, n על מנת שיהיה פתרון למשוואה. נסמן $d = \gcd(a, n)$.

(א) (15 נק') הראו שאם d אינו מחלק את b אז אין פתרונות למשוואה.

מעטה והלאה נניח ש $d|b$ ונכתוב $a = d\tilde{a}, b = d\tilde{b}, n = d\tilde{n}$

(ב) (15 נק') הראו ש $x \in \mathbb{Z}$ פתרון למשוואה הנ"ל אם ורק אם x פתרון למשוואה $\tilde{a}x \equiv \tilde{b} \pmod{\tilde{n}}$.

(ג) (15 נק') הראו שהמספרים $\tilde{a}0, \tilde{a}1, \dots, \tilde{a}(\tilde{n} - 1)$ הם כולם שונים אחד מהשני מודולו \tilde{n} .

(ד) (15 נק') הראו (עדיין תחת ההנחה ש $d|b$) שקיים פתרון למשוואה $ax \equiv b \pmod{n}$.

2. (40 נק') עבור כל סעיף, הוכיחו או הפריכו אותו.

(א) (20 נק') קיים חבורה לא אבלית G עם תת חבורה אבלית H .

(ב) (20 נק') קיים חבורה אבלית G עם תת חבורה לא אבלית H .

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.