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

1. (40 נק')

(א) (30 נק')
שיטה 1:
האיבר a של $\mathbb{Z}/n\mathbb{Z}$ יהיה יוצר אם ורק אם $\mathrm{ord}(a) = n$. כעת, ברור ש $na = 0$ בחבורה $\mathbb{Z}/n\mathbb{Z}$. אנו צריכים תנאים על a על מנת ש $a, 2a, \ldots, (n-1)a$ יהיו כולם שונים מ 0 בחבורה $\mathbb{Z}/n\mathbb{Z}$. מצד אחד, אם $\gcd(a,n) = d \geq 2$ אז ניתן לכתוב $n = d\tilde{n}$ ואז $\tilde{n}a = 0$ בחבורה, אבל $n = \tilde{n}d|\tilde{n}a$ לכן $\tilde{n} \leq n-1$ כי $d \geq 2$ ולכן $\mathrm{ord}(a) \leq \tilde{n} \leq n-1$ ו a אינו יוצר של $\mathbb{Z}/n\mathbb{Z}$.
מצד שני, אם $\gcd(a,n) = 1$ יהי $0 < i \leq n-1$. אילו $ia = 0$ ב $\mathbb{Z}/n\mathbb{Z}$ אז $ia \equiv 0 \equiv 0a \mod n$ ב $\mathbb{Z}$. אבל $\gcd(a,n) = 1$ ונובע ש $i \equiv 0 \mod n$ בסתירה לכך ש $0 < i \leq n-1$. לכן $0, a, 2a, \ldots, (n-1)a$ כולם שונים מ 0 ב $\mathbb{Z}/n\mathbb{Z}$. קילבנו שבמקרה ש a, n זרים, $\mathrm{ord}(a) = n$ ו a אכן יוצר של החבורה.

שיטה 2:
קודם נוכיח שאיבר $a \in \mathbb{Z}/n\mathbb{Z}$ יוצר של החבורה אם ורק אם $1 \in \langle a \rangle$. בכיוון אחד, אם a יוצר אז $\langle a \rangle = \mathbb{Z}/n\mathbb{Z}$ אבל $1 \in \mathbb{Z}/n\mathbb{Z}$ לכן $1 \in \langle a \rangle$. בכיוון השני, אם $1 \in \langle a \rangle$ אז

$$\mathbb{Z}/n\mathbb{Z} = \langle 1 \rangle = \{t \cdot 1 \mid t \in \mathbb{Z}\} \subseteq \langle a \rangle \subseteq \mathbb{Z}/n\mathbb{Z}$$

כי תת החבורה $\langle a \rangle$ סגורה ביחס לפעולת חיבור. נובע ש

$$\langle a \rangle = \mathbb{Z}/n\mathbb{Z}$$

כלומר a יוצר של $\mathbb{Z}/n\mathbb{Z}$.

כעת, אם $\gcd(a,n) = 1$ אז לפי הלמה של בזו קיימים $x, y \in \mathbb{Z}$ כך ש $ax + ny = 1$. נובע ש $xa \equiv 1 \mod n$ לכן $\tilde{x}a = 1$ בחבורה $\mathbb{Z}/n\mathbb{Z}$ כאשר $\tilde{x}$ השארית של x מודולו n. נובע ש $1 \in \langle a \rangle$ ולכן a יוצר של $\mathbb{Z}/n\mathbb{Z}$ לפי הדיון הנ"ל.
מצד שני, אם $1 \in \langle a \rangle$ אז קיים $y \in \mathbb{Z}/n\mathbb{Z}$ כך ש $ya = 1$ בחבורה. נובע שב $\mathbb{Z}$ קיים $w \in \mathbb{Z}$ כך ש $ya - 1 = nw$ ב $\mathbb{Z}$. נובע ש

$$ya - nw = 1 \tag{1}$$

ולכן $\gcd(a,n) = 1$ כי $\gcd(a,n)$ מחלק את שני האגפים של (1).
בסיכום, הוכחנו ש a יוצר של $\mathbb{Z}/n\mathbb{Z}$ אם ורק אם $1 \in \langle a \rangle$ אם ורק אם $\gcd(a,n) = 1$.

(ב) (10 נק') אם p ראשוני אז $\gcd(a,p) = 1$ לכל $a = 1, \ldots, p-1$. לפי הסעיף הקודם, כל אחד מהאיברים $1, \ldots, p-1$ של $\mathbb{Z}/p\mathbb{Z}$ יוצר של החבורה. כמובן, 0 אינו יוצר של $\mathbb{Z}/p\mathbb{Z}$.

2. (60 נק')

(א) (5 נק') לפי ההגדרה ברור ש $x \cdot_n y \geq 0$.
יהיו $x, y \in (\mathbb{Z}/n\mathbb{Z})^*$. ניתן לכתוב את $x \cdot_n y$ בצורה של $xy - k_0 n$.
אם $xy - k_0 n \geq n$ אז $xy - (k_0 + 1)n \geq 0$ וזאת סתירה לכך ש $xy - k_0 n$ ביטוי מינימלי תחת האילוץ ש $xy - kn \geq 0$. נובע ש $0 \leq x \cdot_n y = xy - k_0 n \leq n - 1$.

(ב) (5 נק') קודם נוכיח כי $\gcd(xy, n) = 1$. נניח שקיים $t \geq 2$ שהוא מחלק משותף של xy ו n. אז קיים ראשוני p שמחלק את t ואז $p|n, p|xy$. מכיוון ש p ראשוני, נובע ש $p|x$ או $p|y$. זאת סתירה לכך ש x, n זרים או לכך ש y, n זרים. נובע ש $\gcd(xy, n) = 1$.
כעת, קל לראות שלכל $k \in \mathbb{Z}$ מספר t מחלק משותף של xy ו n אם ורק אם t מחלק משותף של $xy - kn$ ו n. נובע שלכל k מתקיים $1 = \gcd(xy, n) = \gcd(xy - kn, n)$. לפי ההגדרה של $x \cdot_n y$ נובע ש $\gcd(x \cdot_n y, n) = 1$.

(ג) (5 נק') לפי סעיפים א' וב' $x \cdot_n y \in \{0, 1, \ldots, n-1\}$ ו $\gcd(x \cdot_n y, n) = 1$ לכן $x \cdot_n y \in (\mathbb{Z}/n\mathbb{Z})^*$. לכן פעולת הכפל $\cdot_n$ מוגדרת היטב.

(ד) (40 נק') **קיבוציות:** יהיו $x, y, z \in (\mathbb{Z}/n\mathbb{Z})^*$. מתקיים

$$(x \cdot_n y) \cdot_n z \equiv (x \cdot_n y)z \equiv (xy)z \mod n$$

לפי ההגדרה של $\cdot_n$. באופן דומה, מתקיים

$$x \cdot_n (y \cdot_n z) \equiv x(y \cdot_n z) \equiv x(yz) \mod n.$$

לכן $(x \cdot_n y) \cdot_n z \equiv x \cdot_n (y \cdot_n z) \mod n$. נובע ששני הביטויים שווים כאיברים של $(\mathbb{Z}/n\mathbb{Z})^*$.
קיום אדיש: ברור ש $1 \in (\mathbb{Z}/n\mathbb{Z})^*$ והוא האדיש.
קיום הופכי כפלי: יהי $x \in (\mathbb{Z}/n\mathbb{Z})^*$. מכיוון ש x, n זרים, לפי הלמה של בזו קיימים מספרים שלמים y, t כך ש $xy + nt = 1$. נובע ש y, n זרים (כל מחלק משותף שלהם מחלק את $xy + nt$ ולכן שווה ל 1). יהי r השארית של y מודולו n. אז קיים $k \in \mathbb{Z}$ כך ש $y = r + kn$. לפי הדיון בפתרון לסעיף ב',

$$\gcd(r, n) = \gcd(y - kn, n) = \gcd(y, n) = 1.$$

לכן $r \in (\mathbb{Z}/n\mathbb{Z})^*$ ו $x \cdot_n r \equiv xr \equiv 1 \mod n$. נובע ש $x \cdot_n r = 1$ בחבורה $(\mathbb{Z}/n\mathbb{Z})^*$ ומצאנו הופכי ל x.
אבליות: ברור שההגדרה של $x \cdot_n y$ סימטרית ב x, y לכן $x \cdot_n y = y \cdot_n x$ לכל $x, y \in (\mathbb{Z}/n\mathbb{Z})^*$.

(ה) (5 נק') בחבורה $(\mathbb{Z}/15\mathbb{Z})^*$ מתקיימים

$$2 \neq 1, \ 2^2 = 4 \neq 1, \ 2^3 = 8 \neq 1, \ 2^4 = 1$$

לכן $\mathrm{ord}(2) = 4$.