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

1. (60 נק')

(א) (15 נק') נניח שקיים פתרון x_0 למשוואה. אז

$$ax \equiv b \mod n \implies n|(ax-b).$$

אבל $d|n$, לכן $d|(ax-b)$. מכיוון ש $d|a$, נובע ש $d|b$. לכן, על מנת שיהיה פתרון למשוואה הנתונה חייב להתקיים ש $d|b$. (בשלב זה אנו רק יודעים שזה תנאי הכרחי. אנו עדיין לא ידועים שהתנאי הזה גם מספיק.)

(ב) (15 נק') מתקיים ש x פתרון למשוואה אם ורק אם

$$ax \equiv b \mod n \iff n|(ax-b) \iff d\tilde{n}|(d\tilde{a}x - d\tilde{b}) \iff \tilde{n}|(\tilde{a}x-\tilde{b})$$
$$\iff \tilde{a}x \equiv \tilde{b} \mod \tilde{n}$$

כלומר x פתרון למשוואה $\tilde{a}x \equiv \tilde{b} \mod \tilde{n}$.

(ג) (15 נק') השאלה לא תקינה. ניסוח תקין הוא "הראו שהמספרים $\tilde{a}0, \tilde{a}1, \ldots, \tilde{a}(\tilde{n}-1)$ הם כולם שונים אחד מהשני מודולו $\tilde{n}$."
פתרון:
לפי הנתון, אם t מחלק גם את $\tilde{a}$ וגם את $\tilde{n}$ אז dt מחלק גם את $a = d\tilde{a}$ וגם את $n = d\tilde{n}$. אבל נתון ש $d = \gcd(a,n)$ לכן בהכרח $t = 1$. נובע ש $\gcd(\tilde{a},\tilde{n}) = 1$. כעת, יהיו $0 \le i \le j \le \tilde{n}-1$ כך ש

$$\tilde{a}i \equiv \tilde{a}j \mod \tilde{n}.$$

נובע ש $\tilde{n}|\tilde{a}(j-i)$. מכיוון ש $\tilde{a}$ זר מ $\tilde{n}$, נובע ש $\tilde{n}|(j-i)$. אבל $0 \le j-i < \tilde{n}$ מכיוון ש $0 \le i \le j \le \tilde{n}-1$. נובע ש $j-i = 0$ כלומר $i = j$. לכן לכל $i < j$ המספרים $\tilde{a}i$ ו $\tilde{a}j$ שונים זה מזה מודולו $\tilde{n}$.

(ד) (15 נק') לפי הסעיף הקודם, $\tilde{a}0, \tilde{a}1, \ldots, \tilde{a}(\tilde{n}-1)$ שונים זה מזה מודולו $\tilde{n}$. נובע שישנו שוויון קבוצות

$$\{\tilde{a}0, \tilde{a}1, \ldots, \tilde{a}(\tilde{n}-1)\} = \{0,1,\ldots,\tilde{n}-1\}$$

$b \in \{0,1,\ldots,\tilde{n}-1\}$ מודולו $\tilde{n}$ כי יש רק $\tilde{n}$ שאריות מודולו $\tilde{n}$. כמובן, לכן קיים $0 \le x \le \tilde{n}-1$ כך ש $b \equiv \tilde{a}x \mod \tilde{n}$. לפי סעיף ב', אותו x מהווה פתרון למשוואה המקורית $ax \equiv b \mod n$.

2. (40 נק')

(א) (20 נק') הטענה נכונה. למשל לכל חבורה לא אבלית G ניתן לקחת $H = \{e\}$ כאשר e האדיש. ישנן גם דוגמאות יותר מעניינות. למשל, אם $G = \mathrm{GL}_2(\mathbb{R})$, חבורת המטריצות ההפיכות מסדר 2×2, ניתן לקחת $H = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} | a \in \mathbb{R} \right\}$. כאן H אפילו תת חבורה אינסופית של G. ניתן לוודא ש H אבלית.

(ב) (20 נק') הטענה אינה נכונה. בעצם, לכל חבורה אבלית G עם תת חבורה H, לכל $x,y \in H$ מתקיים $xy = yx$ כי $x,y \in G$ ו G אבלית. נובע ש H גם אבלית.