הופכיים

לפי משפט 2 בהרצאת "שקילות ליניארית", ראינו שלמשוואה $ax \equiv b\ (mod\ m)$ קיים פתרון אם ורק אם $(a,m)|b$. כעת נחקור את המשוואה הזו: $ax \equiv 1\ (mod\ m)\quad (1)$

הגדרה 1: יהיו $a \in \mathbb{Z}, m \in \mathbb{Z}^+$ כך ש-$(a,m) = 1$. אזי הפתרון ל-(1) נקרא *ההופכי המודולרי של* a *מודולו* m.

דוגמה: מהו ההופכי של 7 מודולו 31? נפתור את המשוואה $7x \equiv 1\ (mod\ 31)$.

$$31 = 4 \cdot 7 + 3$$

$$7 = 2 \cdot 3 + 1$$

$$1 = 7 - 2 \cdot 3$$

$$1 = 7 - 2 \cdot (31 - 4 \cdot 7)$$

$$1 = \mathbf{9} \cdot 7 - 2 \cdot 31$$

ולכן הפתרון הוא $x \equiv 9\ (mod\ 31)$, כלומר, 9 הינו ההופכי של 7 במודולו 31.

למה זה מעניין אותנו? אם נדע את ההופכי של a (נקרא לו $\tilde{a}$) נבצע את התהליך הבא:

$$ax \equiv b\ (mod\ m)\ \backslash\cdot\ \tilde{a}$$

$$\tilde{a}ax \equiv\ \tilde{a}b\ (mod\ m)$$

$$x \equiv \tilde{a}b\ (mod\ m)$$

וכך נמצא את הפתרון עבור x.

דוגמה: עבור השקילות $7x \equiv 8\ (mod\ 31)$ ניעזר בדוגמה לעיל ונפתור:

$$7x \equiv 8\ (mod\ 31) \cdot 9$$

$$7 \cdot 9 \cdot x \equiv 8 \cdot 9\ (mod\ 31)$$

$$x \equiv 72\ (mod\ 31)$$

$$\equiv 10\ (mod\ 31)$$

לפי משפט 2 מהרצאת "שקילות ליניארית", נוכל לרשום את המסקנה הבאה:

מסקנה 2: יהי p ראשוני. אזי לכל $a \in [p-1]$ יש הופכי מודולו p.

הוכחה: לפי הגדרה

$$\forall a \in [p-1]: (a,p) = 1. \qquad \blacksquare$$

למה 3: יהיו $a \in \mathbb{Z}$ ו-p ראשוני. אזי a הינו ההופכי של עצמו במודולו p אם ורק אם $a \equiv 1\ (mod\ p)$ או $a \equiv -1\ (mod\ p)$.

הוכחה:

<u>כיוון ראשון</u>: נניח ש-$a \equiv 1 \ (mod\ p)$ או $a \equiv -1 \ (mod\ p)$. כשנציב את a במשוואה $a^2 \equiv 1 \ (mod\ p)$ אכן נקבל שיוויון, ולכן a ההופכי של עצמו לפי הגדרה.

<u>כיוון שני</u>: נניח ש-a ההופכי של עצמו $mod\ p$. לכן נקבל

$$p \mid a^2 - 1$$

$$p|(a+1)(a-1)$$

היות ו-p ראשוני, נקבלכי מתקיימת אחת מהאפשרויות הבאות: או ש $p|a+1$ ואז $a \equiv -1 \ (mod\ p)$

או ש $p|a-1$ ואז $a \equiv 1 \ (mod\ p)$ ■

דוגמה: עבור $4x \equiv 1 \ (mod\ 5)$ נשתמש בלמה (שכן 5 ראשוני) ונקבל $x \equiv 4 \ (mod\ 5)$.