שקילות ליניארית

הגדרה: משוואה מהצורה

$$ax \equiv b \ (mod\ m)$$

נקראת *שקילות ליניארית*.

אבחנה: אם $x = x_0 \in \mathbb{Z}$ הינו פתרון למשוואה $ax \equiv b \ (mod\ m)$, אזי כל איבר במחלקת השקילות של x_0 מודולו m הינו פתרון למשוואה.

דוגמה: עבור $x \equiv 1 \ (mod\ 3)$ קל לראות כי הפתרון הוא $x_0 \equiv 1$. כל איבר מאותה מחלקת שקילות גם יפתור את השקילות, כגון $x = 4,7,13,31$.

למה 1: יהיו $x_1 = x_0 + \left(\frac{m}{d}\right)t_1,\ x_2 = x_0 + \left(\frac{m}{d}\right)t_2$ שני פתרונות למשוואה $ax \equiv b \ (mod\ m)$. אזי $x_1 \equiv x_2 \ (mod\ m)$ אם ורק אם $t_1 \equiv t_2 \ (mod\ d)$.

הוכחה:

<u>כיוון ראשון</u>: נניח כי $x_0 + \left(\frac{m}{d}\right)t_1 \ \equiv \ x_0 + \left(\frac{m}{d}\right)t_2 \ (mod\ m)$.

אזי, לפי משפט אריתמטיקה מודולרית נוכל לחסר את x_0 משני האגפים ונקבל

$$\left(\frac{m}{d}\right)t_1 \equiv \ \left(\frac{m}{d}\right)t_2 \ (mod\ m)$$

לפי משפט (משפט 6 מהרצאת שקילויות) נקבל

$$t_1 \equiv \ t_2 \ (mod\ {}^{m}/_{D})$$

כאשר $D = (m, {}^{m}/_{d})$. היות ו- $\frac{m}{d}|m$ נקבל $D = {}^{m}/_{d}$ ולכן $t_1 \equiv t_2 \ (mod\ d)$ כנדרש.

<u>כיוון שני</u>: דומה לכיוון הראשון, רק הולכים מלמטה למעלה. ■

משפט 2: יהי $m \in \mathbb{Z}^+$ ויהיו $a, b \in \mathbb{Z}$, ויהי $d = (a, m)$.

1. אם $d \nmid b$ אזי ל $ax \equiv b \ (mod\ m)$ אין פתרון.
2. אחרת ל- $ax \equiv b \ (mod\ m)$ יש d פתרונות לא שקולים מודולו m.

הוכחה: 1. לפי משפט 1 מההרצאה של שקילויות, פתירת המשוואה שקולה לפתירת משוואה דיאפנטית b=ax-my. לכן, אם $d \nmid b$ למשוואה אין פתרון.

2. אם $d|b$ אז למשוואה הדיאפנטית יש אינסוף פתרונות מהצורה

$$x = x_0 + \left(\frac{m}{d}\right)t, \quad y = y_0 - \left(\frac{a}{d}\right)t, \quad t \in \mathbb{Z}$$

כאשר $x = x_0,\ \ y = y_0$ פתרון למשוואה. הערכים של x שנקבעו על ידי $x = x_0 + \left(\frac{m}{d}\right)t$ כולם מהווים פתרון למשוואה $ax \equiv b \ (mod\ m)$. נותר להראות כי כל הפתרונות האלו מתחלקים בדיוק ל-d מחלקות שקילות מודולו m. לפי למה 1 נזדקק לתת ל-t את כל הערכים של קבוצת השאריות הקנונית מודולו d בשביל לקבל את כל הפתרונות שאינם שקולים מודולו m. כך נקבל קבוצה של d פתרונות עבור x.

מסקנה 3: אם במשוואה $ax \equiv b \ (mod\ m)$ מתקיים $(a, m) = 1$ אזי יש לה פתרון יחיד מודולו m. אמנם יש אינסוף פתרונות, אך כולם נמצאים באותה מחלקת שקילות מודולו m.

דוגמה: עבור השקילות $3x \equiv 17 \ (mod\ 5)$ נקבל $(3,5) = 1$ ולכן קיים פתרון יחיד *מודולו* 5. נפתור בעזרת הכלי של משוואה דיאפנטית:

$$17 = 3x - 5y$$

$$(5,3) \rightarrow 5 = 1 \cdot 3 + 2$$

$$(3,2) \rightarrow 3 = 1 \cdot 2 + 1$$

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

$$1 = 3 - 1 \cdot (5 - 1 \cdot 3)$$

$$1 = 2 \cdot 3 - 1 \cdot 5$$

$$17 = 34 \cdot 3 - 17 \cdot 5$$

ולכן קיבלנו $x = 34 \equiv 4 \ (mod\ 5)$. יש אינסוף פתרונות ממחלקה זו, אך כולם שקולים ל-4 מודולו 5.

לעומת זאת, עבור השקילות $3x \equiv 17 \ (mod\ 6)$ נקבל $(3,6) = 3 \nmid 17$ ולכן לשקילות זו אין פתרון כלל.