<u>שקילות לינארית</u>

הגדרה: משוואה מהצורה $ax \equiv b \ (\,mod\ m\,)$ נקראת שקילות לינארית

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

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

הוכחה: יש צורך להוכיח ע"י גרירה דו כיוונית.
נוכיח כיוון אחד, כיוון שני ישאר תרגיל לבית.
נניח כי $\begin{matrix} x_1 = x_0 + \left(\frac{m}{a,m}\right)t_1 \\ x_2 = x_0 + \left(\frac{m}{a,m}\right)t_2 \end{matrix}$ וכי $x_1 \equiv x_2 \ (\,mod\ m\,)$ ונוכיח כי $t_1 \equiv t_2 \ (\,mod\ (a,m))$
בשביל נוחות נסמן $d = (a,m)$
ידוע כי $x_1 \equiv x_2 \ (\,mod\ m\,)$ ולכן מתקיים כי $x_0 + \left(\frac{m}{d}\right)t_1 \equiv x_0 + \left(\frac{m}{d}\right)t_2 \ (\,mod\ m\,)$
ולכן $\left(\frac{m}{d}\right)t_1 \equiv \left(\frac{m}{d}\right)t_2 \ (\,mod\ m\,)$ ולכן $t_1 \equiv t_2 \ (\,mod\,\frac{m}{D})$ כאשר $D = (m, \frac{m}{d})$
היות ו- $\frac{m}{d} \mid m$ נקבל כי $D = \frac{m}{d}$ ולכן:

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

כנדרש.

טענה 1: למשוואה $ax \equiv b \ (\,mod\ m\,)$ יש פתרון אם"ם $(a,m) \mid b$
טענה 2: אם למשוואה $ax \equiv b \ (\,mod\ m\,)$ יש בדיוק (a,m) פתרונות לא שקולים מודלו m
טענה 3: אם x_0 הוא פתרון למשוואה אזי $t \in [0,d] : t\left(\frac{m}{(a,m)}\right) + x = x_0$ גם כן פתרון למשוואה.
אבחנה: אם למשוואה $ax \equiv b \ (\,mod\ m\,)$ מתקיים $(a,m) = 1$ אזי יש לה פתרון יחיד מודלו m, אומנם יש אינסוף פתרונות אבל כולם נמצאים באותה מחלקת שקילות מודלו m

דרך כללית לפתרון משוואה מהצורה $\boldsymbol{ax \equiv b \ (\,mod\ m\,)}$
שלב 0: נבדוק אם $(a,m) \mid b$
שלב 1: נמיר את המשוואה הלינארית למשוואה מהצורה $ax - my = b$
שלב 2: נבצע את אלגוריתם אוקלידס המורחב עבור הקלט (a,m)
שלב 3: נגיע למשוואה מהצורה $(a,m) = ax' - by'$
שלב 4: נכפיל את המשוואה ב $\frac{b}{(a,m)}$
שלב 5: נקבל כי $b = ax_0 - by_0$ ולכן $x = x_0$ ולבצע בדיקה אם $m \mid ax - b$
שלב 6: נשים לב כי לפי טענה 2 יש בדיוק (a,m) פתרונות לא שקולים מודלו m ולכן נרשום את כולם באופן הבא:

$$x = x_0 + \left(\frac{m}{(a,m)}\right) \cdot t : t \in [0,(a,m)]$$

תרגיל 1:
מצאו את הפתרונות למשוואה הלינארית $7x \equiv 11 \ (\,mod\ 77\,)$

<u>**פתרון:**</u>

שלב 0: נבדוק אם $(a,m) \mid b$
למשוואה אין פתרונות היות ו $(7,77) = 7 \nmid 11$

תרגיל 2:
מצאו את הפתרונות למשוואה הלינארית
$$14x \equiv 42 \ (\ mod\ 22\ )$$

<u>פתרון:</u>
נשים לב כי $(a,m) = (14,22) = 2$ וכי אכן מתקיים $2 \mid 42$ ולכן יש פתרון למשוואה הלינארית
נפתור את המשוואה $14x - 22y = 42$ עבור $y \in \mathbb{Z}$ ע"י אלגוריתם אוקלידס המורחב

$$22 = \underline{14} \cdot 1 + 8 \rightarrow \quad 8 = 22 - \underline{14} \cdot 1$$
$$14 = \underline{8} \cdot 1 + 6 \rightarrow \quad 6 = 14 - \underline{8} \cdot 1$$
$$8 = \underline{6} \cdot 1 + 2 \quad \rightarrow \quad 2 = 8 - \underline{6} \cdot 1$$
$$6 = \underline{2} \cdot 3 + 0$$

ולכן
$$2 = 8 - \underline{6} \cdot 1 = 8 - \left(14 - \underline{8} \cdot 1\right) \cdot 1 = 2 \cdot \underline{8} - 1 \cdot 14 = 2 \cdot \left(22 - \underline{14} \cdot 1\right) - 1 \cdot 14$$
$$= 2 \cdot 22 - 3 \cdot 14$$

ולכן קבלנו כי $2 = 2 \cdot 22 - 3 \cdot 14$
כעת נכפיל את המשוואה ב- $21 = \frac{42}{2} = \frac{42}{(22,14)}$
ולכן נקבל כי $42 = 42 \cdot 22 - 63 \cdot 14$
ולכן $x_0 = -63 \equiv 3 \ (\ mod\ 22\ )$
נשים לב כי אכן מתקיים ש- $22 \mid 14 \cdot 3 - 42 = 0$
כעת נשים לב כי יש בדיוק 2 פתרונות היות ו- $(14,22) = 2$ ולכן:
$$x = x_0 + \left(\frac{m}{(a,m)}\right) \cdot t \ : t \in [0,(a,m)]$$
כלומר $x_0 = 3, x_1 = 14$

- הערה: נשים לב כי אכן $22 \mid 14 \cdot 14 - 42 = 7$

<u>הופכי מודלרי</u>

הגדרה: יהיו $m \in \mathbb{Z}^+$ ו- $a \in \mathbb{Z}$ כך ש- $(a,m) = 1$ אזי הפתרון למשוואה הלינארית
$$ax \equiv 1 \ (\ mod\ m)$$
נקרא הופכי מודלרי של a במודולו m
אבחנה: אם $(a,m) \neq 1$ אז אין פתרון למשוואה.
דוגמא:
מה ההופכי של 7 מודלו 31? נפתור את המשוואה $7x \equiv 1 \ (\ mod\ 31\ )$
$$31 = 4 \cdot 7 + 3$$
$$7 = 2 \cdot 3 + 1$$
$$1 = 7 - 2 \cdot 3$$

$$1 = 7 - 2 \cdot (31 - 4 \cdot 7) = 9 \cdot 7 - 2 \cdot 31$$
ולכן $x \equiv 9 \ (\ mod\ 31\ )$ ואכן $7 \cdot 9 = 63 \equiv 1 \ (mod\ 31)$

טענה: יהי p ראשוני כלשהו, אזי לכל $a \in [1, p-1]$ יש הופכי מודולו p
טענה: יהיו $a \in \mathbb{Z}$ ו-p ראשוני כלשהו, אזי a הינו **<u>הופכי עצמי</u>** במודולו p אם"ם $a \equiv 1 \ (\ mod\ p\ )$ או $a \equiv -1 \ (mod\ p\ )$
הוכחה:
נוכיח ע"י גרירה דו כיוונית
<u>צד ראשון:</u> נניח כי $a \equiv 1 \ (\ mod\ p\ )$ או $a \equiv -1 \ (\ mod\ p)$ ולכן $a^2 \equiv 1 \ (\ mod\ p\ )$ ולכן a הינו הופכי עצמי לפי הגדרה.
<u>צד שני:</u> נניח כי a הופכי עצמי מודלו p ולכן $a^2 \equiv 1 \ \ (\ mod\ p\ )$ ולכן $p \mid a^2 - 1 = (a-1)(a+1)$
בגלל ש-p ראשוני אזי $p \mid (a-1)$ או $p \mid (a+1)$ ולכן $a \equiv 1 \ (\ mod\ p\ )$ או $a \equiv -1 \ (\ mod\ p)$.
לפי טענת עזר: יהי p ראשוני כך ש $p \mid ab$ עבור $a, b \in \mathbb{Z}$ ולכן $p \mid a$ או $p \mid b$

מסקנה: יהי p ראשוני כלשהו, אזי לכל $a \in [2, p-2]$ קיים $b \in [2, p-2]$ כך ש:

$$a \cdot b \equiv 1 \ (\ mod\ p\ )$$

ו- $1, p-1$ הם הופכיים עצמיים.

דוגמא: מה ההופכי העצמי של 6 מודלו 7? **פתרון:** 6

למה זה מעניין אותנו?
זה מעניין אותנו כי אם נשקול את המשוואה הלינארית $ax \equiv b \ (\ mod\ m\ )$ ונסמן ב $\tilde{a}$ את ההופכי של a במודלו m אזי נוכל לבצע את התהליך הבא:

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

וכך נוכל למצוא את הפתרון של x

דוגמאות:

מצאו את הפתרונות למשוואה הלינארית
$$6x \equiv 3 \ (\ mod\ 7\ )$$

פתרון: 6 הינו הופכי עצמי מודלו 7 ולכן אם נכפיל את המשוואה ב-6 נקבל כי $x \equiv 18 \equiv 4 \ (\ mod\ 7)$

מצאו את הפתרונות למשוואה הלינארית
$$14x \equiv 42 \ (\ mod\ 23\ )$$

פתרון:
נמצא את ההופכי מודלרי של 14 במוד 22.
נפתור את המשוואה $14x \equiv 1 \ (\ mod\ 23\ )$
ולכן:

$$\begin{aligned} 23 &= \underline{14} \cdot 1 + 9 \rightarrow \quad 9 = 23 - \underline{14} \cdot 1 \\ 14 &= \underline{9} \cdot 1 + 5 \rightarrow \quad 5 = 14 - \underline{9} \cdot 1 \\ 9 &= \underline{5} \cdot 1 + 4 \rightarrow \quad 4 = 9 - \underline{5} \cdot 1 \\ 5 &= \underline{4} \cdot 1 + 1 \rightarrow \quad 1 = 5 - \underline{4} \cdot 1 \\ 4 &= 1 \cdot 4 + 0 \end{aligned}$$

ולכן:

$$1 = 5 - \underline{4} \cdot 1 = 5 - \left(9 - \underline{5} \cdot 1\right) \cdot 1 = 2 \cdot \underline{5} - 9 \cdot 1 = 2 \cdot \left(14 - \underline{9} \cdot 1\right) - 9 \cdot 1 = 14 \cdot 2 - 3 \cdot \underline{9}$$
$$= 14 \cdot 2 - 3 \cdot \left(23 - \underline{14} \cdot 1\right) = 5 \cdot 14 - 3 \cdot 23$$

ולכן $x = 5$
ולכן נכפיל את המשוואה המקורית

$$14x \equiv 42 \ (\ mod\ 23\ )$$

ב-5 ונקבל $70x \equiv 210 \ (\ mod\ 23\ )$ ולכן $x \equiv 3 \ (mod\ 23)$ ואכן $14 \cdot 3 \equiv 42 \ (\ mod\ 23\ )$

שאלה: שימו לב כי זה אותו התרגיל מסעיף הקודם, אך במקום מודלו 22 מדובר במודלו 23. למה היה צורך לשנות את המודלו בשביל פתרון מהצורה שהוצגה?

מערכת קונגרואנציות בשני משתנים

טענה: יהי $a, b, c, d, r, s \in \mathbb{Z}$ ויהי $n \in \mathbb{Z}^+$.
אזי למערכת הקונגרואנציות :

$$ax + by \equiv r \ (\ mod\ n)$$
$$cx + dy \equiv s \ (\ mod\ n\ )$$

קיים **<u>פתרון יחיד</u>** מודלו n כאשר $(ad - bc, n) = 1$

תרגיל 3:
פתרו את מערכת הקונגרואנציות הבאה:
$$7x + 3y \equiv 10\ (\ mod\ 16)$$
$$2x + 5y \equiv 9\ (\ mod\ 16\ )$$

<u>פתרון:</u>
תחילה נבדוק האם קיים פתרון, נשים לב כי $(7 \cdot 5 - 2 \cdot 3, 16) = (29,16) = 1$
ולכן קיים פתרון למערכת משוואות.
כעת נכפול את המשוואה הראשונה ב-2 ואת המשוואה השנייה ב-7 ונקבל את מערכת המשוואות:
$$14x + 6y \equiv 20\ (\ mod\ 16)$$
$$14x + 35y \equiv 63\ (\ mod\ 16)$$
כעת נוכל לחסר בין המשוואות ולבצע את אוקלידס המורחב על מנת למצוא את y.
לאחר מכן, נציב את y חזרה באחת המשוואות ונפתור אותה שוב עזרת אלגוריתם אוקלידס המורחב,
או לחלופין, נוכל באותה דרך שהעלמנו את x אז להעלים את y.

הפתרון המלא נשאר לקוראים 🙂