תזכורת מתרגול שעבר:

הגדרה: משוואה מהצורה $ax \equiv b\ (\,mod\ m\,)$ נקראת שקילות לינארית
טענה 1: למשוואה $ax \equiv b\ (\,mod\ m\,)$ יש פתרון אם"ם $(a,m)\mid b$ ולכן אם $(a,m)=1$ אזי לכל b יש פתרון למשוואה.

הופכי מודלרי
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

טענה 1: יהיו $m_1, m_2, \dots, m_k \in \mathbb{Z}^+$ אזי אם $a \equiv b\ (\,mod\ m_i)$ עבור כל $i \in [1,k]$ אזי מתקיים:
$a \equiv b\ \left(mod\ lcm\ (m_1, m_2, \dots, m_k)\right)$

אבחנה: אם $m_1, m_2, \dots m_k$ זרים בזוגות אזי $lcm(m_1, \dots m_k) = m_1 \cdot \dots \cdot m_k$

הוכחה: לפי ההנחה מתקיים כי $m_i \mid a-b$ עבור כל $i \in [1,k]$ ולכן $a-b$ הוא מכפלה משותפת של $m_1, m_2, \dots, m_k$ ולכן לפי הגדרה מתקיים כי $lcm(m_1, m_2, \dots m_k) \mid a-b$

טענה 2: יהיו $m_1, m_2 \in \mathbb{Z}$ כך ש $x \equiv r\ (\,mod\ lcm(m_1,m_2))$ אזי $\begin{matrix} x\equiv r\ (\,mod\ m_1) \\ x\equiv r\ (\,mod\ m_2)\end{matrix}$

הוכחה: לפי הגדרה ניתן לקבל כי $lcm(m_1,m_2) \mid x-r$ ולכן $x = lcm(m_1,m_2)\cdot N + r$
בנוסף נשים לב כי $lcm(m_1,m_2) = k_1 m_1 = k_2 m_2$ ולכן :
$$x = lcm(m_1,m_2)\cdot N + r = k_1 m_1 \cdot N + r = k_1 m_1 \cdot N + k_1 l_1 + (r\ mod\ k_1)$$
$$= k_1(m_1 \cdot N + l_1) + (r\ mod\ k_1)$$
כאשר המעבר השני נכון לפי משפט החלוקה.
ולכן מתקיים כי $x \equiv r\ (\,mod\ k_1)$
בנוסף
$$x = lcm(m_1,m_2)\cdot N + r = k_2 m_2 \cdot N + r = k_2 m_2 \cdot N + k_2 l_2 + (r\ mod\ k_2)$$
$$= k_2(m_2 \cdot N + l_2) + (r\ mod\ k_2)$$
ולכן מתקיים כי $x \equiv r\ (\,mod\ k_2)$
כנדרש.

טענה 3: יהי $m_1, \dots m_k$ זרים בזוגות, ויהי $M = \Pi_i m_i$ ויהי $M_k = \frac{M}{n_k}$ אזי $(M_k, n_k) = 1$
הוכחה: היות ו $m_1, \dots m_k$ זרים בזוגות אזי M_k, m_k לא חולקים גורמים ראשוניים משותפים.

משפט השאריות הסיני:

יהיו $m_1, m_2, \dots, m_r \in \mathbb{Z}$ שלמים **זרים אחד לשני**

אזי למערכת:

$$x\ \equiv\ a_1\ (\,mod\ m_1\,)$$

$$x \equiv a_2 \ (mod\ m_2)$$

$$\vdots$$

$$x \equiv a_r \ (mod\ m_r\ )$$

<u>קיים</u> פתרון **<u>יחיד</u>** מודלו M כך ש- $x \in [0, M-1]$

כאשר $M \coloneqq m_1 \cdot m_2, \dots \cdot m_r$

הרעיון:

נסתכל על המערכת משוואות הבאה:

$$x \equiv 1\ (mod\ 2)$$
$$x \equiv 2\ (mod\ 3)$$
$$x \equiv 3\ (mod\ 5)$$

נשים לב כי $(2,3,5) = 1$

נשים לב כי $x = a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3\ (mod\ 2 \cdot 3 \cdot 5)$ הוא פתרון למערכת משוואות כאשר:

$$M_i = \frac{M}{m_i}$$

כאשר m_i הוא המודלו של המשוואה ה-i

כי:

$$x = a_1m_2m_3y_1 + a_2m_1m_3y_2 + a_3m_1m_2y_3 \equiv a_1m_2m_3y_1 \equiv a_1M_1y_1\ (mod\ m_1)$$

היות וכולם כפולות של המודלו.

בנוסף אם נגדיר את y_i להיות ההופכי של M_i במודלו m_i אזי נקבל כי

$$x \equiv a_1M_1y_1 \equiv a_1\ (mod\ m_1)$$

וזה נכון לכל אחת מהמשוואות.

$$x \equiv \underbrace{1}_{a_1} \cdot \underbrace{(3\cdot 5)}_{M_1} \cdot \left(\underbrace{\widetilde{3\cdot 5}}_{y_1}\right) + \underbrace{2}_{a_2} \cdot \left(\underbrace{2\cdot 5}_{M_2}\right) \cdot \left(\underbrace{\widetilde{2\cdot 5}}_{y_2}\right) + \underbrace{3}_{a_3} \cdot \left(\underbrace{2\cdot 3}_{M_3}\right) \cdot \left(\underbrace{\widetilde{2\cdot 3}}_{y_3}\right) \left(mod\ \underbrace{2\cdot 3\cdot 4}_{M}\right)$$

הוא פתרון למערכת (כמובן יש צורך לחשב ולהציג פתרון סופי.)

כאשר y_i הוא בעצם ההופכי של M_i במוד m_i .

<u>משפט שאריות הסיני – הוכחה.</u>

הוכחה: יש צורך להוכיח קיום ויחודיות (**שימו לב כי יכול להיות וההוכחה בשיעור שונה!**)

קיום: נגדיר $M \coloneqq m_1 \cdot m_2, \dots \cdot m_r$ ולכל $k \in [1, r]$ נגדיר $M_k = \frac{M}{m_k}$ ונשים לב כי $(n_k, M_k) = 1$ היות ואין גורם משותף במכפלה, נגדיר לכל M_k, y_k כך ש $y_k \cdot M_k \equiv 1\ (mod\ m_k\ )$, נשים לב כי אכן קיים y_k שכזה היות ו- $(n_k, M_k) = 1$ ולכן נגדיר $x \coloneqq \sum_{i=1}^{r} a_i m_i y_i$ ונשים לב כי x הוא אכן פתרון למערכת במוד M כי:

$$x \equiv \sum_{i=1}^{r} a_i m_i y_i = a_1m_1y_1 + \cdots + a_rm_ry_r \equiv a_k\ (mod\ m_k\ )$$

עבור כל $k \in [1, r]$

<u>יחודיות:</u> יהיו x_2 וx_1 פתרונות למערכת מודלו M. כך ש $x_1 \equiv x_2 \equiv a_k\ (mod\ m_k\ )$ לכל $k \in [1, r]$ אזי $m_k \mid x_1 - x_2$ לכל $k \in [1, r]$ ולכן $M \mid x_1 - x_2$ ולכן $x_1 \equiv x_2\ (mod\ M\ )$

<u>תרגיל 1:</u>

פתרו את המשוואות הבאות בעזרת משפט השאריות הסיני

$$4x \equiv 5\ (mod\ 3)$$
$$49x \equiv 3\ (mod\ 4)$$
$$11x \equiv -9\ (mod\ 5)$$

פתרון:

שלב 1: נבדוק זרות

נבדוק שכל המודולו זרים בזוגות, נשים לב כי 3,5 ראשוניים ולכן $(3,5) = 1$ ובנוסף $(3,4) = (4,5) = 1$

שלב 2: נבודד את x בכל אחת מהמשוואות

משוואה ראשונה:

$$4x \equiv 5 \ (\mod 3)$$

ולכן:

$$x \equiv 2 \ (\mod 3)$$

משוואה שנייה:

$$49x \equiv 3 \ (\mod 4)$$
$$49x = x + 48x \equiv x \equiv 3 \ (\mod 4)$$

משוואה שלישית:

$$11x \equiv -9 \ (\mod 5)$$

ולכן:

$$x \equiv -9 \equiv 1 \ (\mod 5)$$

שלב 3: נגדיר $M = 3 \cdot 4 \cdot 5$

שלב 4: לכל $i \in [1,3]$ נגדיר m_i

$$M_1 = \frac{M}{m_1} = 20$$
$$M_2 = \frac{M}{m_2} = 15$$
$$M_3 = \frac{M}{m_3} = 12$$

שלב 5: לכל $i \in [1,3]$ נגדיר y_i להיות ההופכי של m_i במוד M_i

נמצא את y_1

$$M_1 \cdot y_1 \equiv 1 \ (\mod m_i)$$

כלומר

$$20 \cdot y_1 \equiv 1 \ (\mod 3)$$

ולכן

$$-1 \cdot y_1 \equiv 1 \ (\mod 3)$$

ולכן

$$y_1 \equiv -1 \equiv 2 \ (\mod 3)$$

נמצא את y_2

$$M_2 \cdot y_2 \equiv 1 \ (\mod m_2)$$

כלומר

$$15 \cdot y_2 \equiv 1 \ (\mod 4)$$

ולכן

$$-1 \cdot y_2 \equiv 1 \ (\mod 4)$$

נמצא את y_3

$$M_3 \cdot y_3 \equiv 1 \ (\mod m_3)$$

כלומר

$$12 \cdot y_3 \equiv 1 \ (\mod 5)$$

ולכן

$$24 \cdot y_3 \equiv 2 \ (mod \ 5 \ )$$

ולכן

$$-1 \cdot y_1 \equiv 2 \ (mod \ 5 \ )$$

ולכן

$$y_1 \equiv -2 \equiv 1 \ (mod \ 5 \ )$$

<u>שלב 6: נגדיר את הפתרון כך ש $x = \sum_{i=1}^{3} a_i \cdot M_i \cdot y_i$</u>

ולכן $x = 2 \cdot 20 \cdot 2 + 3 \cdot 15 \cdot 3 + 1 \cdot 12 \cdot 3 = 251$

ולכן $x \equiv 251 \equiv 11 \ (mod \ 3 \cdot 4 \cdot 5 \ ) \equiv 11 \ (mod \ 60 \ )$

נשים לב כי אכן:

$$4x \ \equiv \ 5 \ (mod \ 3) \checkmark$$

$$49x \ \equiv \ 3 \ (mod \ 4) \checkmark$$

$$11x \ \equiv \ -9 \ (mod \ 5) \checkmark$$