תרגיל 1:

פתרו את המשוואות הבאות בעזרת משפט השאריות הסיני
$4x \equiv 5\ (mod\ 3)$
$49x \equiv 3\ (mod\ 4)$
$4x \equiv -9\ (mod\ 5)$

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:
$$4x\ \equiv\ -9\ (mod\ 5)$$
ולכן:
$$x \equiv -9 \equiv 1\ (\ mod\ 5\ )$$
לחלופין אפשר גם להשתמש בהופכי מודלרי, ידוע כי 4 הוא הופכי עצמי במודלו 5 ולכן ניתן להכפיל את המשוואה ב4, ולקבל כי $x \equiv -9 \cdot 4 \equiv -36 \equiv 1\ (\ mod\ 5\ )$

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

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

<u>נמצא את y_3</u>

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

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:

$$4x \equiv 5 \ (mod\ 3)$$ ✓

$$49x \equiv 3 \ (mod\ 4)$$ ✓

$$11x \equiv -9 \ (mod\ 5)$$ ✓

<u>משפט וילסון</u>

p ראשוני אם"ם $(p-1)! \equiv -1 \ (mod\ p)$

<u>שימושים:</u>

- בעזרת הטענה ניתן לדעת אם מספר $n \in \mathbb{Z}$ הוא **מספר ראשוני**, כל מה שצריך לעשות זה לחשב את $(n-1)!$ ולבדוק אם $(n-1)! \equiv -1 \ (mod\ n)$
- בעזרת הטענה ניתן לדעת אם מספר $n \in \mathbb{Z}$ **אינו מספר ראשוני**.

<u>חסרון:</u> יש קושי לחשב עצרת של מספר גדול.

דוגמא עבור הוכחה ש7 מספר ראשוני:

$$(7-1)! \equiv 6! \equiv 720 \equiv -1 \ (mod\ 7)$$

ולכן 7 מספר ראשוני.

דוגמא עבור הוכחה ש4 אינו מספר ראשוני:

$$(4-1)! \equiv 3! \equiv 6 \equiv 2 \ (mod\ 4)$$

ולכן 4 אינו מספר ראשוני.

<u>הוכחה:</u>

צד ראשון: נניח כי p מספר ראשוני ונוכיח כי $(p-1)! \equiv -1 \ (\ mod\ p\ )$

לפי ההנחה, ידוע כי p מספר ראשוני ולכן מתקיים כי :
$(p-1)! = 1 \cdot 2 \cdot \ldots \cdot (p-2) \cdot (p-1)$

הוכחנו כי 1 ו-$(p-1)$ הינו הופכיים עצמאים במודלו p וכי לכל $a \in [2, p-2]$ קיים $b \in [2, p-2]$ כך ש $a \neq b$ כך ש $ab \equiv 1 \ (\ mod\ p\ )$ ולכן נקבל כי :

$$(p-1)! \equiv 1 \cdot 1 \cdot \ldots .1 \cdot (p-1) \equiv (p-1) \equiv -1 \ (\ mod\ p\ )$$

כנדרש.

צד שני: נניח כי $(p-1)! \equiv -1 \ (\ mod\ p\ )$ ונוכיח כי p ראשוני.

נניח בשלילה כי p אינו ראשוני ולכן p הוא מספר פריק, כלומר $p = a \cdot b$ עבור $1 < a, b < p$ אזי מתקיים כי $a \mid (p-1)!$ ו $a \mid p$ כי $a \in [1, p-1]$, ולכן $a \mid p - (p-1)!$ אזי $a \mid 1$ וזוהי סתירה כי $a > 1$.

טענה: יהי $n > 1$ מספר שלם כלשהו, n הוא מספר ראשוני אם ורק אם $(n-2)! \ \equiv 1 \ (mod\ n)$

הוכחה: לפי משפט וילסון ידוע כי אם n הוא מספר ראשוני אזי מתקיים ש:

$(n-1)! \equiv -1 \equiv n-1 \ (mod\ n)$ ולכן היות ו $(n-1, n) = 1$ ניתן לרשום ש

$$\frac{(n-1)!}{n-1} \equiv \frac{n-1}{n-1} \equiv 1 \ (mod\ n\ )$$

ומכאן נקבל כי $(n-2)! \ \equiv 1\ mod\ (n)$