תרגול-9

תרגיל 1: פתרו את המערכת הבאה:

$$x \equiv 3(mod\ 4)$$
$$\mathrm{x} \equiv 0\ (mod\ 6)$$

פתרון 1: לא קיים פתרון למערכת הנ"ל. (זה לא סותר את משפט השאריות הסיני כי 4 ו-6 לא זרים.)

נכתוב את x בצורה הבאה:

$$.x = 3 + 4t$$

כאשר נציב את הביטוי במשוואה השנייה נקבל:

$$.3 + 4t \equiv 0(mod\ 6)$$
$$.4\mathrm{t} \equiv -3(mod\ 6)$$

לקונגרואנציה הזו לא קיים פתרון מאחר ו- $d = gcd(4,6)$ אינו מחלק את 3-.
למעשה במקרה הזה, ישנה דרך פשוטה יותר לראות שלא קיים פתרון, נוכל לראות לפי הקונגרואנציה הראשונה ש-x הינו אי-זוגי, אבל לפי הקונגרואנציה השנייה x הינו מספר זוגי, סתירה.

תרגיל 2: השתמש במשפט השאריות הסיני בכדי לפתור את מערכת המשוואות הבאה:

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

פתרון 2: נמצא מערכת משוואות השקולה למערכת הנ"ל מהצורה הנתונה במשפט השאריות הסיני:

$$4 \equiv 1(mod\ 3)$$
$$5 \equiv 2(mod\ 3)$$
$$49 \equiv 1(mod\ 4)$$
$$11 \equiv 1(mod\ 5)$$
$$-9 \equiv 1(mod\ 5)$$

קיבלנו כעת:

$$x \equiv 2(mod\ 3)$$
$$x \equiv 3(mod\ 4)$$
$$x \equiv 1(mod\ 5)$$

נקבע את $n_1 = 3, n_2 = 4, n_3 = 5$. ואת $a_1 = 2, a_2 = 3, a_3 = 1$
מאחר ושני שלמים עוקבים הינם זרים וכאן שניים מהם ראשוניים, נקבל ש 3,4,5 הינם זרים אחד לשני. לכן לפי משפט השאריות הסיני למשוואה הזו יש פתרון ייחודי מודולו

$$M = 3 \cdot 4 \cdot 5 = 60.$$

נשתמש במשפט השאריות הסיני ונקבע:

$$M_1 = \frac{M}{3} = 20, M_2 = \frac{M}{4} = 15, M_3 = \frac{M}{5} = 12.$$

בצעד הבא נמצא את y_1, y_2, y_3 כאשר y_i הינו ההופכי של M_i מודולו n_i עבור כל $i \in [3]$.
מכאן, אנו נדרשים לפתור עבור כל אחד מהקונגרואנציות:

$$20y_1 \equiv 1\ (mod\ 3)$$
$$15y_2 \equiv 1\ (mod\ 4)$$
$$12y_3 \equiv 1\ (mod\ 5)$$

כדי למצוא את y_1 נבחין כי $20 \equiv -1\ (mod\ 3)$, לכן $y_1 \equiv -1\ (mod\ 3)$ כלומר $y_1 \equiv 2\ (mod\ 3)$.
עבור y_2 נבחין כי $15 \equiv -1\ (mod\ 4)$, לכן $y_2 \equiv -1\ (mod\ 4)$ כלומר $y_2 \equiv 3\ (mod\ 4)$.
עבור y_3 נבחין כי $12 \equiv 2(mod\ 5)$, ומאחר ו-3 הינו ההופכי המודולרי ל-2 במודולו 5 נובע כי $y_3 \equiv 3\ (mod\ 5)$. כעת ניגש לחישוב הפתרון, בעזרת משפט השאריות הסיני:

$$x = 2 \cdot 20 \cdot 2 + 3 \cdot 15 \cdot 3 + 1 \cdot 12 \cdot 3 = 251 \equiv 11\ (mod\ 60)$$

תרגיל 3:
השתמשו במשפט הקטן של פרמה, במשפט אוילר, ובמשפט שאריות הסיני על מנת לפתור את מערכת המשוואות הבאה:

$$x7 \equiv 11 \pmod{51}$$
$$x8 \equiv 21 \pmod{61}$$
$$9x \equiv 31 \pmod{71}$$

<u>פתרון 3:</u>

<u>שלב ראשון – בדיקה האם קיים פתרון:</u>

נשים לב כי $51 = 3 \cdot 17$; 61 הוא ראשוני (כי אין לו מחלקים ראשוניים עד $\lceil\sqrt{61}\rceil$) ו-71 גם כן ראשוני מאותה סיבה, ולכן $n_1 = 51, n_2 = 61, n_3 = 71$ זרים בזוגות. לפיכך לאחר שנצליח להעביר כל משוואה לצורה $x \equiv \mathrm{a_i} (mod\ n_i)$ (וזאת נעשה בשלב השני) מובטח פתרון יחיד מודולו $51 \cdot 61 \cdot 71$ לפי משפט שאריות הסיני.

<u>שלב שני – בידוד המשוואות: (נבצע כל בידוד בשיטה אחרת כדי לתרגל שיטות שונות.)</u>

1. עבור המשוואה $7x \equiv 11\ (mod\ 51)$, נחפש את $t =$ ההופכי של 7 במודולו 51, בכדי לבודד את x.

נשים לב כי 51 אינו ראשוני ולכן לא נוכל להשתמש בפרמה, אולם כן נוכל להשתמש במשפט אוילר היות ו-$(7,51) = 1$.

לפי משפט אוילר מתקיים: $7^{\varphi(51)} = 1\ (mod\ 51)$

$$\varphi(51) = \varphi(3 \cdot 17) \underbrace{=}_{\substack{\varphi(nm)=\varphi(n)\varphi(m):(n,m)=1 \text{ עבור} \\ \varphi(p)=p-1: \text{עבור כל } p \text{ ראשוני}}} 2 \cdot 16 = 32$$

ולכן $7^{32} \equiv 1\ (mod\ 51)$ ולכן ההופכי של 7 במודולו 51, הינו 7^{31}.

נשים לב כי

$$\begin{aligned} 7^{31} &\equiv 7(7^5)^6 \\ &\equiv 7(28)^6 \\ &\equiv 7(28^2)^3 \\ &\equiv 7 \cdot 19^3 \end{aligned}$$

$$\equiv 7 \cdot 25$$
$$\equiv 22\ (mod\ 51)$$

ולכן

$$t\ \equiv 22(mod\ 51)$$

ונובע

$$x\ \equiv 22 \cdot 11 \equiv 38\ (mod\ 51)$$

2. עבור המשוואה $8x\ \equiv 21\ (mod\ 61)$, נחפש את ההופכי של 8 במודולו 61.

היות ו-61 הינו מספר ראשוני, ו-$(8,61) = 1$ אזי לפי המשפט הקטן של פרמה מתקיים

$$8^{60} \equiv 1(mod\ 61)$$

ולכן $8 \cdot 8^{59} \equiv 1\ (mod\ 61)$

ולכן ההופכי של 8 הינו 8^{59} במודולו 61.

ולכן

$$x\ \equiv 8^{59} \cdot 21(mod\ 61)$$

נשים לב כי

$$\begin{aligned} x &\equiv (8^2)^{29} \cdot 8 \cdot 21 \\ &\equiv (3)^{29} \cdot 8 \cdot 21 \\ &\equiv (3^5)^5 \cdot 3^4 \cdot 8 \cdot 21 \\ &\equiv -1 \cdot 3^4 \cdot 8 \cdot 3 \cdot 7 \\ &\equiv 8 \cdot 7 \\ &\equiv 56\ (mod\ 61) \end{aligned}$$

ולכן:

$$x\ \equiv 56\ (mod\ 61)$$

3. עבור המשוואה $9x\ \equiv 31\ (\ mod\ 71)$, נשתמש באוקלידס המורחב עבור המשוואה הדיאופנטית $9 \cdot x - 71 \cdot y = 31$.

$$71 = 7 \cdot 9 + 8$$
$$9 = 1 \cdot 8 + 1$$
$$1 = 1 \cdot 9 - 1 \cdot 8$$

$$= 1 \cdot 9 - 1 \cdot (71 - 7 \cdot 9)$$
$$= 8 \cdot 9 - 1 \cdot 71$$

כלומר קיבלנו

$$1 = 8 \cdot 9 - 1 \cdot 71$$

נכפיל פי 31 ונקבל

$$31 = 248 \cdot 9 - 31 \cdot 71$$

כלומר

$$x \equiv 248 \equiv 35 \ (mod\ 71)$$

ולכן

סה"כ נקבל כי :

$$\begin{cases} x \equiv 38\ (mod\ 51) \\ x \equiv 56\ (mod\ 61) \\ x \equiv 35\ (mod\ 71) \end{cases}$$

מכאן נפעיל את משפט השאריות הסיני.

הפעלת המשפט נשארת כתרגיל בית.

אוניברסיטת אריאל

תרגילי בית

תרגיל 1. הפעילו את משפט השאריות הסיני על המערכת שקיבלנו בסוף התרגיל הקודם,

$$\begin{cases} x \equiv 38 \ (mod\ 51) \\ x \equiv 56 \ (mod\ 61) \\ x \equiv 35 \ (mod\ 71) \end{cases}$$

פתרון:

נתון כי $n_1 = 51, n_2 = 61, n_3 = 71$, וכי $a_1 = 38, a_2 = 56, a_3 = 35$.

מאחר ו- 71,61,51 הם מספרים שלמים זרים אזי לפי משפט השאריות הסיני למשוואה הזו יש פתרון ייחודי מודולו

$$M = 51 \cdot 61 \cdot 71 = 220881.$$

נשתמש במשפט השאריות הסיני ונקבע:

$$M_1 = \frac{M}{51} = 61 \cdot 71 = 4331, M_2 = \frac{M}{61} = 51 \cdot 71 = 3621,$$

$$M_3 = \frac{M}{71} = 61 \cdot 51 = 3111$$

בצעד הבא נמצא את y_1, y_2, y_3 כאשר y_i הינו ההופכי של M_i מודולו n_i עבור כל $i \in [3]$.

מכאן, אנו נדרשים לפתור כל אחת מהקונגרואנציות הבאות:

$$4331y_1 \equiv 1 \ (mod\ 51)$$
$$3621y_2 \equiv 1 \ (mod\ 61)$$
$$3111y_3 \equiv 1 \ (mod\ 71)$$

כדי למצוא את y_1 נתחיל בצמצום:

$$4331 = 84 * 51 + 47$$

ולכן

$$4331y_1 \equiv 47y_1 \equiv 1 \ (mod\ 51)$$

ולכן נותר למצוא את ההופכי של 47 במודולו 51. נשתמש באוקלידס המורחב ונקבל

$$51 = 47 \cdot 1 + 4$$
$$47 = 11 \cdot 4 + 3$$
$$4 = 1 \cdot 3 + 1$$

ולכן קיבלנו כי

$$
\begin{aligned}
1 &= 4 - 1 \cdot 3 \\
&= 4 - 1 \cdot (47 - 11 \cdot 4) \\
&= 4 + 11 \cdot 4 - 1 \cdot 47 \\
&= 12 \cdot 4 - 1 \cdot 47 \\
&= 12 \cdot (51 - 1 \cdot 47) - 1 \cdot 47 \\
&= 12 \cdot 51 - 13 \cdot 47
\end{aligned}
$$

ולכן -13 הינו ההופכי של 47 במודולו 51. כלומר

$$y_1 \equiv -13 \ (mod\ 51)$$

כדי למצוא את y_2 גם נתחיל בצמצום:

$$3621 = 61 \cdot 59 + 22$$

ולכן

$$3621y_2 \equiv 22y_2 \equiv 1 \ (mod\ 61)$$

ולכן נותר למצוא את ההופכי של 22 במודולו 61. היות ו-61 ראשוני, נפעיל את משפט פרמה הקטן ונקבל

$$22^{60} \equiv 1 \ (mod\ 61)$$

ולכן ההופכי הוא 22^{59}.

$$
\begin{aligned}
22^{59} &\equiv 22^3 \cdot (22^4)^{14} \\
&\equiv 22^3 \cdot 16^{14} \\
&\equiv 22^3 \cdot (16^2)^7 \\
&\equiv 22^3 \cdot 12^7 \\
&\equiv 34 \cdot 42 \\
&\equiv 25 \ (mod\ 61)
\end{aligned}
$$

(מעברים בעזרת המחשבון, במודולו 61 בכל פעם)

כדי למצוא את y_3 גם נתחיל בצמצום:

$$3111 = 43 \cdot 71 + 58$$

ולכן

$$3111y_3 \equiv 58y_3 \equiv 1 \ (mod\ 71)$$

נשתמש שוב במשוואה דיאופנטית בשביל למצוא את ההופכי של 58 במודולו 71.

$$71 = 1 \cdot 58 + 13$$
$$58 = 4 \cdot 13 + 6$$
$$13 = 2 \cdot 6 + 1$$

ולכן

$$\begin{aligned} 1 &= 13 - 2 \cdot 6 \\ &= 13 - 2 \cdot (58 - 4 \cdot 13) \\ &= 9 \cdot 13 - 2 \cdot 58 \\ &= 9 \cdot (71 - 1 \cdot 58) - 2 \cdot 58 \\ &= 9 \cdot 71 - 11 \cdot 58 \end{aligned}$$

ולכן -11 הינו ההופכי של 58 במודולו 71.

ניזכר בנתונים שאספנו בדרך:

$$\mathrm{a}_1 = 38, \mathrm{a}_2 = 56, \mathrm{a}_3 = 35$$
$$M_1 = 4331, M_2 = 3621, M_3 = 3111$$
$$y_1 = -13, y_2 = 25, y_3 = -11$$

כעת ניגש לחישוב הפתרון, בעזרת משפט השאריות הסיני:

$$\begin{aligned} x \equiv \sum_{i=1}^{3} a_i M_i y_i &= 38 \cdot 4331 \cdot -13 \\ &\quad +56 \cdot 3621 \cdot 25 + 35 \cdot 3111 \cdot -11 \\ &\equiv 185984 (mod\ 51 \cdot 61 \cdot 71) \end{aligned}$$