

תזכורת: יהיו m, n מספרים זרים. לכל שני מספרים a, b קיים x כך ש:

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

בשיעור הקודם הוכחנו את קיום x , והערנו שהוא יחיד עד כדי מודולו mn . ניזכר בהוכחת הקיום: $(m, n) = 1$ שקול לכך שיש צירוף לינארי ששווה 1. כלומר, קיימים $\alpha, \beta \in \mathbb{Z}$ כך ש:

$$\alpha m + \beta n = 1$$

נקח

$$x = \alpha mb + \beta na$$

דוגמא:

$$\begin{cases} x \equiv 1 \pmod{7} \\ x \equiv 3 \pmod{9} \end{cases}$$

פתרון:

$$9 = 7 + 2 \implies 2 = 9 - 7$$

$$7 = 3 \cdot 2 + 1 \implies 1 = 7 - 3 \cdot 2 = 7 - 3(9 - 7) = 4 \cdot 7 - 3 \cdot 9$$

$$x = 4 \cdot 7 \cdot 3 - 3 \cdot 9 = 57$$

“יחידות”:

הכיוון הקל: ברור שאם $y \equiv x \pmod{mn}$ הוא גם יענה על התנאים. כי בפרט $y \equiv x \pmod{m}$ וגם $y \equiv x \pmod{n}$.
 כעת, נניח ש x עונה על התנאים, וגם y . המטרה היא להראות ש $y \equiv x \pmod{mn}$.
 זה אומר

$$x \equiv y \pmod{m}$$

וגם

$$x \equiv y \pmod{n}$$

כלומר,

$$m, n | (x - y)$$

בש"ב הגדרתם lcm של שני מספרים. שזה המספר הכי קטן ששניהם מחלקים. אפשר להוכיח שאם m, n מחלקים מספר אז $lcm(m, n)$ מחלק את המספר. ובנוסף אפשר להראות שאם m, n זרים אז $lcm(m, n) = |mn|$ ולכן

$$mn | (x - y)$$

כלומר,

$$x \equiv y \pmod{mn}$$

דרך שניה: כמה תנאים שונים אפשר לדרוש מודולו m ומודולו n ? כלומר, כמה משוואות כאלה קיימות?

מספיק לקחת $0 \leq a \leq m - 1$ ו $0 \leq b \leq n - 1$. כלומר, יש mn משוואות. ראינו שלכל משוואה יש פתרון, ושכל שני מספרים ששקולים מודולו mn הם פתרונות של אותה משוואה.

כמה מחלקות שקילות יש מודולו mn ? בדיוק mn . לסיכום: יש mn משוואות. הפתרונות שלהם הם בעצם מחלקות שקילות ביחס מודולו mn . לכן יש mn מחלקות שקילות. ראינו שלכל משוואה יש פתרון, כלומר יש מחלקת שקילות שפותרת אותה.

מחלקת שקילות לא יכולה לפתור 2 משוואות שונות, כי המשמעות שמחלקת שקילות פותרת זה שכל נציג בה פותר. אבל כל מספר שקול רק למספר יחיד בין 0 ל $m - 1$ מודולו m , וכן לגבי n . ולכן לא יכולות להיות שתי מחלקות שונות שפותרות את אותה משוואה. דוגמא נגדית כאשר m, n לא זרים:

$$x \equiv 1 \pmod{2}$$

$$x \equiv 2 \pmod{4}$$

למערכת משוואות הזאת אין פתרון.

הכללה של משפט השאריות הסיני: יהיו m_1, \dots, m_n מספרים זרים בזוגות. אז לכל מערכת משוואות

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

יש פתרון. (הוא גם יהיה יחיד עד כדי $m_1 \cdot \dots \cdot m_n$).

הוכחה: נציג אלגוריתם רקורסיבי שמצמצם את מספר המשוואות בכל שלב. לוקחים את שתי המשוואות הראשונות בכל שלב, ומחליפים אותם במשוואה אחת ששקולה לשניהם.

כלומר:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}$$

למערכת יש פתרון x' עד כדי מודולו $m_1 m_2$, כלומר, המערכת של שתי המשוואות שקולה למערכת של משוואה אחת:

$$x \equiv x' \pmod{m_1 m_2}$$

צריך להוכיח ש $m_1 m_2$ זר לכל המספרים האחרים. נוכיח שהוא זר ל m_i עבור $i = 1, 2$ כמובן. צריך להוכיח ש $(m_i, m_1 m_2) = 1$.

$$\alpha_1 m_i + \beta_1 m_1 = 1$$

$$\alpha_2 m_1 + \beta_2 m_2 = 1$$

$$\begin{aligned} 1 &= (\alpha_1 m_i + \beta_1 m_1)(\alpha_2 m_i + \beta_2 m_2) = \\ &= (\alpha_1 \alpha_2 m_i + \alpha_1 \beta_2 m_2 + \beta_1 \alpha_2 m_1) m_i + \beta_1 \beta_2 m_1 m_2 \end{aligned}$$

כלומר 1 הוא צירוף לינארי ל m_i ו $m_1 m_2$.
דוגמא:

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases}$$

פתרון: את שתי המשוואות הראשונות פתרנו בתרגול הקודם, ולכן אנחנו כבר יודעים שזה שקול למשוואה:

$$x \equiv 7 \pmod{15}$$

כלומר, עכשיו צריך לפתור מערכת של שתי משוואות:

$$\begin{cases} x \equiv 7 \pmod{15} \\ x \equiv 3 \pmod{7} \end{cases}$$

צירוף לינארי שיוצא 1:

$$15 - 2 \cdot 7$$

ולכן הפתרון הוא :

$$x = 3 \cdot 15 - 7 \cdot 2 \cdot 7$$

תזכורת: פעולות כפל וחיבור שומרות על מודולו. כלומר, אם

$$a \equiv b \pmod{n}$$

$$c \equiv d \pmod{n}$$

אז :

$$a + c \equiv b + d \pmod{n}$$

$$ac \equiv bd \pmod{n}$$

תזכורת: לכל a קיים מספר יחיד בטווח בין 0 ל- $n-1$ ששקול ל- a מודולו n . למספר הזה נקרא $a \pmod{n}$.
למשל:

$$5 \pmod{3} = 2$$

תרגיל: מצאו את הספרה האחרונה של המספר 333^{333}
פתרון: ספרה אחרונה של מספר זה פשוט למה המספר שקול מודולו 10. בעצם אנחנו רוצים למצוא

$$333^{333} \pmod{10} = (333 \pmod{10})^{333} \pmod{10} =$$

$$(3 \pmod{10})^{333} \pmod{10} = 3^{333} \pmod{10} = 3^{4 \cdot 83 + 1} \pmod{10} =$$

$$3^{4 \cdot 83} \pmod{10} \cdot 3 \pmod{10} = 81^{83} \pmod{10} \cdot 3 \pmod{10} =$$

$$(81 \pmod{10})^{83} \cdot 3 \pmod{10} = (1 \pmod{10})^{83} \cdot 3 \pmod{10} = 3 \pmod{10}$$

כלומר, הספרה האחרונה היא 3.

מבנים אלגבריים

הגדרה: תהי S קבוצה. פעולה על S היא פונקציה

$$f : S \times S \rightarrow S$$

מקובל לסמן את $f(a, b)$ ב

$$a \cdot b$$

או $a * b$

או ab .

פעולה נקראת "אסוציאטיבית" אם לכל $a, b, c \in S$ מתקיים:

$$(ab)c = a(bc)$$

קבוצה עם פעולה אסוציאטיבית נקראת "חבורה למחצה". (אגודה).

דוגמאות:

1. $\mathbb{N}, a \cdot b = a^b$. האם זאת חבורה למחצה?

תשובה: לא, כי הפעולה אינה אסוציאטיבית. למשל

$$(2 \cdot 2) \cdot 3 \neq 2 \cdot (2 \cdot 3)$$

2. \mathbb{N} , עם הפעולה: $a \cdot b = \max\{a, b\}$ - זאת כן חבורה למחצה. יש אסוציאטיביות. למעשה,

$$(ab)c = a(bc) = \max\{a, b, c\}$$

3. $(a * b) = ab + 1$. זאת לא פעולה לא אסוציאטיבית, אבל היא כן חלופית.

הגדרה: תהי $(S, *)$ חבורה למחצה. איבר $e \in S$ נקרא "איבר יחידה" אם הוא נטרלי לפעולה.

כלומר, לכל $a \in S$

$$a * e = e * a = a$$

לדוגמא: (\mathbb{N}, \max) 1 הוא איבר יחידה.

תכונה: הוכחתם בהרצאה שאם יש איבר יחידה אז הוא יחיד.

הגדרה: חבורה למחצה שיש בה איבר יחידה נקראת מונואיד. (M, \cdot, e)

למשל (\mathbb{N}, \max) הוא מונואיד.

הגדרה: יהי M מונואיד, איבר $a \in M$ נקרא הפיך אם קיים $b \in M$ כך ש

$$ab = ba = e$$

תכונה: אם a הפיך, יש לו הופכי יחיד.

הגדרה: מונואיד שבו כל איבר הפיך נקרא חבורה.

דוגמאות ודוגמאות נגדיות:

1. $(\{0, \dots, n-1\}, \min)$. הפעולה אסוציאטיבית ולכן זאת חבורה למחצה. $n-1$ נטרלי

לפעולה ולכן הוא איבר יחידה. אבל $n-1$ הוא האיבר ההפיך היחיד. כי לכל $a \neq n-1$ ולכל b ,

$$\min\{a, b\} \leq a < n-1$$

2. $(P(X), \cap)$ - X הוא איבר יחידה. X הוא האיבר ההפיך היחיד. כי אם $A \neq X$ אז $A \subsetneq X$, ואז לכל B

$$A \cap B \subseteq A \subsetneq X$$

3. $(P(X), \cup)$ - \emptyset היא איבר היחידה. והיא האיבר ההפיך היחיד. כי לכל $A \neq \emptyset$, ולכל B , $A \cup B \neq \emptyset$.

4. $(P(X), \Delta)$ - \emptyset היא איבר היחידה. כל איבר הפיך, ההופכי שלו זה הוא בעצמו כי לכל A

$$A \Delta A = \emptyset$$

אז 4 היא חבורה.

5. (\mathbb{Z}_n, \cdot) האם היא החבורה?

איבר היחידה - 1.

0 לא הפיך.

$(\mathbb{Z}_n \setminus \{0\}, \cdot)$ - תלוי. למשל עבור $n = 4$. נישאר עם $\{1, 2, 3\}$ ופעולות כפל מודולו 4. זה אפילו לא מאגמה! כי $2 \cdot 2 = 0 \pmod{4}$. אז אין לנו בכלל פעולה על הקבוצה.

הגדרה: חבורה נקראת "אבלית" אם לכל a, b , $ab = ba$.

תרגיל: תהי G חבורה כך שלכל $a \in G$, מתקיים:

$$a^2 = e$$

הוכיחו ש G אבלית.

הוכחה: אם $a^2 = e$ זה אומר שההופכי של a הוא a . נתון שהמשוואה הזאת נכונה לכל איבר בחבורה, לכן לכל איבר בחבורה, הוא ההופכי של עצמו. כלומר,

$$a^{-1} = a$$

$$b^{-1} = b$$

$$(ab)^{-1} = ab$$

כמו כן, בהרצאה הוכחתם ש

$$(ab)^{-1} = b^{-1}a^{-1}$$

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba$$

דרך נוספת:

$$ba/e = (ab)^2 = abab$$

$$ba = (ba)(abab) = b(aa)(bab) = be(bab) = (bb)ab = eab = ab$$

הגדרה: תהי G חבורה. ותהי $H \subseteq G$. נקראת תת חבורה של G אם H בעצמה חבורה ביחס לאותה פעולה.
סימון:

$$H \leq G$$

קריטריון מקוצר: בשביל להוכיח ש $H \subseteq G$ היא תת חבורה של G , מספיק להוכיח:

1. $e \in H$ (שקול: $H \neq \emptyset$)

2. סגירות לפעולה

3. סגירות להופכי.

דוגמאות:

1. $G = GL_n(\mathbb{F})$ כל המטריצות ההפיכות מעל השדה \mathbb{F} מגדול $n \times n$. זאת חבורה ביחס לפעולת כפל מטריצות.

נסמן $\{A \in GL_n(\mathbb{F}) : |A| = 1\} = SL_n(\mathbb{F})$. הוכיחו ש

$$SL_n(\mathbb{F}) \leq GL_n(\mathbb{F})$$

ראשית נשים לב שזאת אכן תת קבוצה כי לכל המטריצות בה יש דטרמיננטה 1, ולכן הדורמיננטה היא לא 0, לכן המטריצות הפיכות.

איבר יחידה: $|I| = 1$.

סגירות לכפל: יהיו $A, B \in SL_n(\mathbb{F})$. כלומר $|A| = 1, |B| = 1$.

$$|AB| = |A||B| = 1 \cdot 1 = 1$$

לכן $AB \in SL_n(\mathbb{F})$

סגירות להופכי: תהי $A \in SL_n(\mathbb{F})$. כלומר $|A| = 1$. ידוע ש $|A^{-1}| = \frac{1}{|A|}$ ולכן $|A^{-1}| = 1$

לכן $A^{-1} \in \mathbb{F}$.