שיעור 2
חוגים מתמטיים

2.1 החוג $\mathbb{Z}_m$

הגדרה 2.1 קבוצת השארית בחלוקה ב-m $\mathbb{Z}_m$

נגדיר $\mathbb{Z}_m$ להיות הקבוצה של מספרים שלמים

$$\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$$

יחד עם הפעולות $\oplus$ ו- $\odot$ המוגדרות כך:

לכל $a, b \in \mathbb{Z}_m$,

$$a \oplus b = (a+b) \ \% \ m \ , \qquad a \odot b = ab \ \% \ m \ .$$

מכאן ואילך נסמן חיבור וכפל ב- $\mathbb{Z}_m$ עם הסימנים הרגילים $+$ ו- $\times$ או $\cdot$.

דוגמה 2.1

חשבו את 11×13 ב- $\mathbb{Z}_{16}$.

פתרון:
$11 \times 13 = 143$. נמצא את השארית בחלוקה ב- 16:

$$(11 \times 13) \ \% \ 16 = 143 \ \% \ 16 = 15 \ .$$

לפיכך $11 \times 13 = 15$ ב- $\mathbb{Z}_{16}$.

■

משפט 2.1 תכונות של הקבוצה השארית $\mathbb{Z}_m$

לכל $a, b, c \in \mathbb{Z}_m$ התנאים הבאים מתקיימים.

1. סגירה תחת חיבור:
$$a + b \in \mathbb{Z}_m \ .$$
2. חוק החילוף לחיבור:
$$a + b = b + a \ .$$
3. חוק הקיבוץ לחיבור:
$$(a + b) + c = a + (b + c) \ .$$
4. קיום איבר הניטרלי ביחס לחיבור:
$$a + 0 = 0 + a = a \ .$$
5. האיבר הנגדי של a הוא $m - a$, ז"א $-a = m - a$. הסבר:
$$a + (m - a) = (m - a) + a = m = 0$$
ב- $\mathbb{Z}_m$.

6. סגירה תחת כפל:

$$ab \in \mathbb{Z}_m \ .$$

7. חוק החילוף לכפל:

$$ab = ba \ .$$

8. חוק הקיבוץ לכפל:

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

9. קיום איבר הניטרלי ביחס לכפל:

$$a \times 1 = 1 \times a = a \ .$$

10. חוק הפילוג:

$$(a+b)c = (ac) + (bc) \ .$$

תכונות 1, 3-5 אומרות כי $\mathbb{Z}_m$ הינו "חבורה מתמטית". יחד עם תכונה 2, $\mathbb{Z}_m$ הוא חבורה אָבֶלִית. כל התכונות 1-10 אומרות כי $\mathbb{Z}_m$ הוא חוג מתמטי.

הגדרה 2.2 איבר ההופכי ב- $\mathbb{Z}_m$

נניח כי $a \in \mathbb{Z}_m$. האיבר ההופכי הוא האיבר $a' \in \mathbb{Z}_m$ עבורו

$$a'a \equiv a'a \equiv 1 \mod m \ .$$

כלל 2.1

האיברים ההופכיים של האיברים $1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25$ של $\mathbb{Z}_{26}$ הם:

$$\begin{aligned}
1^{-1} &= 1 \ , \\
3^{-1} &= 9 \ , \\
5^{-1} &= 21 \ , \\
7^{-1} &= 15 \ , \\
9^{-1} &= 3 \ , \\
11^{-1} &= 19 \ , \\
15^{-1} &= 7 \ , \\
17^{-1} &= 23 \ , \\
19^{-1} &= 11 \ , \\
21^{-1} &= 5 \ , \\
23^{-1} &= 17 \ , \\
25^{-1} &= 25 \ .
\end{aligned}$$

משפט 2.2

נתון היחס שקילות

$$ax \equiv y \mod m \ .$$

יש פתרון יחיד $x \in \mathbb{Z}_m$ לכל $y \in \mathbb{Z}_m$ אם ורק אם $\gcd(a, m) = 1$.

הוכחה:

ללא הגבלת כלליות נניח כי $a > m$.

נניח כי יש פתרון יחיד. נוכיח דרך השלילה כי ו- $\gcd(a, m) = 1$.

נניח כי $\gcd(a, m) = d > 1$.

אם $x_1 = a^{-1}y \mod m$ פתרון ל- $ax \equiv y \mod m$, אז גם $x_1 + \frac{m}{d}$ פתרון, מכיוון ש-
$ax_1 + \frac{am}{d} = ax_1 + km \equiv ax_1 \mod m$, כאשר $k = \frac{a}{d}$ שלם.

שימו לב, כיוון ש- $d > 1$ אז $x_1 + \frac{m}{d} \not\equiv x_1 \mod m$, ז"א קיימים שני פתרונות שונים, בסתירה לכך כי הפתרון יחיד.

נניח כי $\gcd(a, m) = 1$. נוכיח בשלילה כי הפתרון יחיד.
נניח כי קיים שני פתרונות שונים: $x_1 \not\equiv x_2 \mod m$.

ז"א

$$ax_1 \equiv y \mod m \ , \quad ax_2 \equiv y \mod m \ .$$

לכן

$$ax_1 \equiv ax_2 \mod m \ .$$

לכן

$$m \mid ax_1 - ax_2 \ .$$

$\gcd(a, m) = 1$ לפיכך

$$m \mid x_1 - x_2 \ ,$$

ז"א

$$x_1 \equiv x_2 \mod m \ ,$$

בסתירה לכך ש- $x_1 \not\equiv x_2 \mod m$.

■

מסקנה 2.1

יהי $a \in \mathbb{Z}_m$. קיים איבר $a^{-1} \in \mathbb{Z}_m$ יחיד כך ש-

$$aa^{-1} \equiv 1 \mod m$$

אם ורק אם $\gcd(a, m) = 1$.
נקרא a^{-1} האיבר ההו]כי של a ב- $\mathbb{Z}_m$.

דוגמה 2.2

הוכיחו שקיים איבר הופכי ל- 11 ב- $\mathbb{Z}_{26}$ ואם כן מצאו אותו.

פתרון:
קיים איבר הופכי של a ב- $\mathbb{Z}_m$ אם ורק אם $\gcd(a, m) = 1$. לכן נבדוק את ה- $\gcd(26, 11)$ באמצעות האלגוריתם של אוקליד המוכלל.
יהיו $a = 26, b = 11$.

$$\begin{aligned} r_0 &= a = 26 \ , & r_1 &= b = 11 \ , \\ s_0 &= 1 \ , & s_1 &= 0 \ , \\ t_0 &= 0 \ , & t_1 &= 1 \ . \end{aligned}$$

שלב $i = 1$:	$r_2 = 26 - 2 \cdot 11 = 4$	$s_2 = 1 - 2 \cdot 0 = 1$	$t_2 = 0 - 2 \cdot 1 = -2$	$q_1 = 2$
שלב $i = 2$:	$r_3 = 11 - 2 \cdot 4 = 3$	$s_3 = 0 - 2 \cdot 1 = -2$	$t_3 = 1 - 2 \cdot (-2) = 5$	$q_2 = 2$
שלב $i = 3$:	$r_4 = 4 - 1 \cdot 3 = 1$	$s_4 = 1 - 1 \cdot (-2) = 3$	$t_4 = -2 - 1 \cdot (5) = -7$	$q_3 = 1$
שלב $i = 4$:	$r_5 = 3 - 3 \cdot 1 = 0$	$s_5 = -2 - 3 \cdot (3) = -11$	$t_5 = 5 - 3 \cdot (-7) = 28$	$q_4 = 3$

$$\gcd(a, b) = r_4 = 1 \ , \qquad x = s_4 = 3 \ , \qquad y = t_4 = -7 \ .$$

$$ax + by = 3(26) - 7(11) = 1 \ .$$

מכאן

$$-7(11) = 1 - 9(26) \quad \Rightarrow \quad -7(11) = 1 \mod 26 \quad \Rightarrow \quad 19(11) = 1 \mod 26 \quad \Rightarrow \quad 11^{-1} = 19 \mod 26 \ .$$

■

הגדרה 2.3 פונקצית אוילר $\phi(m)$

נתון החוג $\mathbb{Z}_m$ כאשר $m \geq 2$ מספר טבעי. נגדיר $\phi(m)$ להיות הפונקציה הנותנת את מספר איברים ב-$\mathbb{Z}_m$ אשר זרים ל-m.

(ראו הגדרה 1.7.)

2.2 הפיכת מטריצות בחוג $\mathbb{Z}_m$

הגדרה 2.4 המטריצה של קופקטורים

תהי $A \in \mathbb{R}^{n \times n}$.

הקופקטור ה-(i, j) של A מוגדר להיות הדטרמיננטה של המטריצה המתקבלת מ-A ע"י מחיקת שורה i ועמודה j, כפול $(-1)^{i+j}$.

המטריצה של קופקטורים של המטריצה A מוגדרת

$$C = \begin{pmatrix} C_{11} & \cdots & C_{1n} \\ \vdots & \ddots & \vdots \\ C_{n1} & \cdots & C_{nn} \end{pmatrix}$$

כאשר C_{ij} הקופקטור ה-(i, j) של A.

הגדרה 2.5 המטריצה המצורפת

תהי $A \in \mathbb{R}^{n\times n}$. המטריצה המצורפת של A היא מטריצה מסדר $n \times n$ שמסומנת $\text{adj}(A)$ ומוגדרת

$$\text{adj}(A) = C^t$$

כאשר C המטריצה של קופקטורים של A.

משפט 2.3 נוסחת קיילי המילטון

נניח כי $A \in \mathbb{R}^{n\times n}$ מטריצה ריבועית. אם A הפיכה, כלומר אם $|A| \neq 0$ אז המטריצה ההופכית נתונה ע"י נוסחת קיילי המילטון:

$$A^{-1} = \frac{1}{|A|}\text{adj}(A) \ ,$$

כאשר $\text{adj}(A)$ המטריצה המצורפת של A.

דוגמה 2.3

מצאו את ההופכית של

$$A = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} \in \mathbb{Z}_{26}^{2\times 2} \ .$$

פתרון:

$$|A| = 11 \cdot 7 - 8 \cdot 3 = 53 = 1 \mod 26 \ .$$

$\gcd(1, 26) = 1$ לכן המטריצה הפיכה ב- $\mathbb{Z}_{26}$.

$$\begin{pmatrix} \cancel{11} & \cancel{8} \\ \cancel{3} & 7 \end{pmatrix} \quad \Rightarrow \quad C_{11} = (-1)^{1+1}7 = 7$$

$$\begin{pmatrix} \cancel{11} & \cancel{8} \\ 3 & \cancel{7} \end{pmatrix} \quad \Rightarrow \quad C_{12} = (-1)^{1+2}7 = -3$$

$$\begin{pmatrix} \cancel{11} & 8 \\ \cancel{3} & \cancel{7} \end{pmatrix} \quad \Rightarrow \quad C_{21} = (-1)^{2+1}8 = -8$$

$$\begin{pmatrix} 11 & \cancel{8} \\ 3 & \cancel{7} \end{pmatrix} \quad \Rightarrow \quad C_{22} = (-1)^{2+2}11 = 11$$

$$C = \begin{pmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{pmatrix} = \begin{pmatrix} 7 & -3 \\ -8 & 11 \end{pmatrix}$$

$$\text{adj}(A) = C^t = \begin{pmatrix} 7 & -8 \\ -3 & 11 \end{pmatrix}$$

$$A^{-1} = |A|^{-1}\text{adj}(A) \ .$$

$$|A|^{-1} = 1^{-1} = 1 \in \mathbb{Z}_{26}$$

לפיכך

$$A^{-1} = |A|^{-1}\text{adj}(A) = 1 \cdot \begin{pmatrix} 7 & -8 \\ -3 & 11 \end{pmatrix} = \begin{pmatrix} 7 & 22 \\ 23 & 11 \end{pmatrix} \in \mathbb{Z}_{26}^{2\times 2} \ .$$

■

דוגמה 2.4

מצאו את ההופכית של

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 5 & 0 \\ 2 & 0 & 3 \end{pmatrix} \in \mathbb{Z}_{26}^{3\times 3} \ .$$

פתרון:

$$|A| = 1 \cdot \begin{vmatrix} 5 & 0 \\ 0 & 3 \end{vmatrix} + 0 \begin{vmatrix} 0 & 0 \\ 2 & 3 \end{vmatrix} + 1 \begin{vmatrix} 0 & 5 \\ 2 & 0 \end{vmatrix} = 1 \cdot 15 + 1 \cdot (-10) = 5 \ .$$

$\gcd(15, 26) = 1$ לכן המטריצה הפיכה ב- $\mathbb{Z}_{26}$.

$$\begin{pmatrix} \cancel{1} & \cancel{0} & \cancel{1} \\ \cancel{0} & 5 & 0 \\ \cancel{2} & 0 & 3 \end{pmatrix} \quad \Rightarrow \quad C_{11} = (-1)^{1+1} \begin{vmatrix} 5 & 0 \\ 0 & 3 \end{vmatrix} = 15 \ .$$

$$\begin{pmatrix} \cancel{1} & \cancel{0} & \cancel{1} \\ 0 & \cancel{5} & 0 \\ 2 & \cancel{0} & 3 \end{pmatrix} \quad \Rightarrow \quad C_{12} = (-1)^{1+2} \begin{vmatrix} 0 & 0 \\ 2 & 3 \end{vmatrix} = 0 \ .$$

$$\begin{pmatrix} \cancel{1} & \cancel{0} & \cancel{1} \\ 0 & 5 & \cancel{0} \\ 2 & 0 & \cancel{3} \end{pmatrix} \quad \Rightarrow \quad C_{13} = (-1)^{1+3} \begin{vmatrix} 0 & 5 \\ 2 & 0 \end{vmatrix} = -10 \ .$$

$$\begin{pmatrix} 1 & 0 & 1 \\ \cancel{0} & \cancel{5} & \cancel{0} \\ 2 & 0 & 3 \end{pmatrix} \quad \Rightarrow \quad C_{21} = (-1)^{2+1} \begin{vmatrix} 0 & 1 \\ 0 & 3 \end{vmatrix} = 0 \ .$$

$$\begin{pmatrix} 1 & 0 & 1 \\ \cancel{0} & \cancel{5} & \cancel{0} \\ 2 & \cancel{0} & 3 \end{pmatrix} \quad \Rightarrow \quad C_{22} = (-1)^{2+2} \begin{vmatrix} 1 & 1 \\ 2 & 3 \end{vmatrix} = 1 \ .$$

$$\begin{pmatrix} 1 & 0 & \cancel{1} \\ \cancel{0} & \cancel{5} & \cancel{0} \\ 2 & 0 & \cancel{3} \end{pmatrix} \quad \Rightarrow \quad C_{23} = (-1)^{2+3} \begin{vmatrix} 1 & 0 \\ 2 & 0 \end{vmatrix} = 0 \ .$$

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 5 & 0 \\ \cancel{2} & \cancel{0} & \cancel{3} \end{pmatrix} \quad \Rightarrow \quad C_{31} = (-1)^{3+1} \begin{vmatrix} 0 & 1 \\ 5 & 0 \end{vmatrix} = -5 \ .$$

$$\begin{pmatrix} 1 & \cancel{0} & 1 \\ 0 & \cancel{5} & 0 \\ \cancel{2} & \cancel{0} & \cancel{3} \end{pmatrix} \quad \Rightarrow \quad C_{32} = (-1)^{3+2} \begin{vmatrix} 1 & 1 \\ 0 & 0 \end{vmatrix} = 0 \ .$$

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 5 & 0 \\ 2 & 0 & 3 \end{pmatrix} \qquad \Rightarrow \qquad C_{33} = (-1)^{3+3} \begin{vmatrix} 1 & 0 \\ 0 & 5 \end{vmatrix} = 5 \ .$$

$$C = \begin{pmatrix} C_{11} & C_{12} & C_{13} \\ C_{21} & C_{22} & C_{23} \\ C_{31} & C_{32} & C_{33} \end{pmatrix} = \begin{pmatrix} 15 & 0 & -10 \\ 0 & 1 & 0 \\ -5 & 0 & 5 \end{pmatrix}$$

$$\text{adj}(A) = C^t = \begin{pmatrix} 15 & 0 & -5 \\ 0 & 1 & 0 \\ -10 & 0 & 5 \end{pmatrix} = \begin{pmatrix} 15 & 0 & 21 \\ 0 & 1 & 0 \\ 16 & 0 & 5 \end{pmatrix} \in \mathbb{Z}_{26}^{3\times 3} \ .$$

$$A^{-1} = |A|^{-1}\text{adj}(A) \ .$$

$$|A|^{-1} = 5^{-1} = 21 \in \mathbb{Z}_{26}$$

לפיכך

$$A^{-1} = |A|^{-1}\text{adj}(A) = 21 \cdot \begin{pmatrix} 15 & 0 & 21 \\ 0 & 1 & 0 \\ 16 & 0 & 5 \end{pmatrix} = \begin{pmatrix} 315 & 0 & 441 \\ 0 & 21 & 0 \\ 336 & 0 & 105 \end{pmatrix} \in \mathbb{Z}_{26}^{3\times 3} \ .$$

$$315 \ \texttt{\%} \ 26 = 315 - 26 \cdot \left\lfloor \frac{315}{26} \right\rfloor = -23 \equiv 3 \mod 26 \quad \Rightarrow \quad 315 \equiv 3 \mod 26 \ .$$

$$441 \ \texttt{\%} \ 26 = 441 - 26 \cdot \left\lfloor \frac{441}{26} \right\rfloor = 25 \quad \Rightarrow \quad 441 \equiv 25 \mod 26 \ .$$

$$336 \ \texttt{\%} \ 26 = 336 - 26 \cdot \left\lfloor \frac{336}{26} \right\rfloor = 24 \quad \Rightarrow \quad 336 \equiv 24 \mod 26 \ .$$

$$105 \ \texttt{\%} \ 26 = 105 - 26 \cdot \left\lfloor \frac{105}{26} \right\rfloor = 1 \quad \Rightarrow \quad 105 \equiv 1 \mod 26 \ .$$

לפיכך

$$A^{-1} = \begin{pmatrix} 3 & 0 & 25 \\ 0 & 21 & 0 \\ 24 & 0 & 1 \end{pmatrix} \in \mathbb{Z}_{26}^{3\times 3} \ .$$

בדיקה:

$$A \cdot A^{-1} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 5 & 0 \\ 2 & 0 & 3 \end{pmatrix} \begin{pmatrix} 3 & 0 & 25 \\ 0 & 21 & 0 \\ 24 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 27 & 0 & 26 \\ 0 & 105 & 0 \\ 78 & 0 & 53 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mod 26 \ .$$

■