

שיעור 2

חוגים מתמטיים

2.1 הפונקציה אוילר

הגדרה 2.1 פונקציית אוילר

יהי m מספר שלם. הפונקציית אוילר מסומנת $(m) \phi$ ומוגדרת להיות כמות השלמים שקטנים ממש מ- m וזרים ביחס ל- m .

$$\phi(m) := |\{a \in \mathbb{N} \mid \gcd(a, m) = 1, a < m\}| .$$

דוגמה 2.1

מכיוון ש- $26 = 2 \times 13$, הערכים של a עבורם $\gcd(a, 26) = 1$ הם

$$\{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\} .$$

זהו יש בדיק 12 ערכים של a עבורם $\gcd(a, 26) = 1$

$$\phi(26) = 12 .$$

משפט 2.1 הפרק לראשוניים של פונקציית אוילר

יהי $2 \leq m$ מספר שלם ונניח כי הפרק למספרים ראשוניים שלו הוא

$$m = \prod_{i=1}^n p_i^{e_i} .$$

אז

$$\phi(m) = \prod_{i=1}^n (p_i^{e_i} - p_i^{e_i-1}) .$$

דוגמה 2.2

מצאו את $\phi(60)$.

פתרון:

$$60 = 2^2 \times 3^1 \times 5^1$$

$$\phi(60) = (2^2 - 2^1)(3^1 - 3^0)(5^1 - 5^0) = (2)(2)(4) = 16 .$$



דוגמה 2.3

חשבו את $\phi(24)$

פתרונות:

$$24 = 2^3 3^1 .$$

לכן

$$\phi(24) = (2^3 - 2^2)(3^1 - 3^0) = (8 - 4)(3 - 1) = 8 .$$

משפט 2.2אם p מספר ראשוני אז

$$\phi(p) = p - 1 .$$

הוכחה: תרגיל בית.**משפט 2.3**אם p מספר ראשוני אז

$$\phi(p^n) = p^n - p^{n-1} .$$

הוכחה: תרגיל בית.**משפט 2.4**אם a, b שלמים זרים (כלומר $(\gcd(a, b) = 1)$ אז

$$\phi(a \cdot b) = \phi(a) \cdot \phi(b) .$$

הוכחה:

- נניח ש- a, b זרים.
- נניח שהפירוקים הראשוניים של a ו- b הם:

$$a = p_1^{e_1} \cdots p_n^{e_n}, \quad b = q_1^{f_1} \cdots q_m^{f_m} .$$
- a ו- b זרים שכן הראשוניים בין השני הפירוקים יכולים להיות שונים, כלומר $p_i \neq q_j$ לכל $i, j \leq \min(n, m)$.
- לכן אם הפירוק הראשוני של ab הוא

$$ab = p_1^{e_1} \cdots p_n^{e_n} q_1^{f_1} \cdots q_m^{f_m} .$$

- מכאן

$$\phi(ab) = (p_1^{e_1} - p_1^{e_1-1}) \cdots (p_n^{e_n} - p_n^{e_n-1}) (q_1^{f_1} - q_1^{f_1-1}) \cdots (q_m^{f_m} - q_m^{f_m-1}) = \phi(a)\phi(b) .$$

משפט 2.5

אם p ו- q מספרים ראשוניים שונים אז

$$\phi(p \cdot q) = (p - 1)(q - 1) .$$

הוכחה: תרגיל בית.

2.2 החוג \mathbb{Z}_m **הגדרה 2.2 החוג \mathbb{Z}_m**

החוג \mathbb{Z}_m מוגדר להיות הקבוצה של מספרים שלמים

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

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

לכל

$$a, b \in \mathbb{Z}_m \quad a \oplus b = (a + b) \bmod m \quad a \odot b = ab \bmod m .$$

במילים אחרות, \mathbb{Z}_m היא קבוצת השארית בחלוקת ב- m .

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

דוגמה 2.4

חשבו את 11×13 ב- \mathbb{Z}_{16} .

פתרון:

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

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

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

משפט 2.6 תכונות של החוג \mathbb{Z}_m

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

1. סגירה תחת חיבור:

$$a + b \in \mathbb{Z}_m .$$

2. חוק החלוף 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 $m - a$, א"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 החלוף 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 אומירות כי \mathbb{Z}_m הינו "חבורה מתמטית".
יחד עם תכונה 2, \mathbb{Z}_m הינו חבורה אбелית.
כל התכונות 1-10 אומירות כי \mathbb{Z}_m הוא חוג מתמטי.

הגדלה 2.3 איבר ההופכי ב-

יהי $a \in \mathbb{Z}_m$. האיבר ההופכי של a מסומן ב- a^{-1} ומקיים את התנאי

$$a^{-1}a \equiv 1 \pmod{m} \quad \text{וגם} \quad aa^{-1} \equiv 1 \pmod{m} .$$

משפט 2.7

נתון היחס שקולות

$$ax \equiv y \pmod{m} .$$

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

הוכחה:

כיוון

נניח בשילילה כי למשוואה m יש פתרון יחיד $x = x_1$ אבל $1 < x < m$.

אזי $ax_1 \equiv y \pmod{m}$ ולכן קיימים q, r שלם עבורו $ax_1 \equiv qm + y \pmod{m}$
לכן $ax_1 + \frac{am}{d} = qm + y + \frac{am}{d}$ הוא שלם ולכן $\frac{am}{d}$ קיימים שלם $Q = q + \frac{a}{d}$, א"א $a \left(x_1 + \frac{m}{d} \right) = \left(q + \frac{a}{d} \right) m + y$ כך ש-

$$a \left(x_1 + \frac{m}{d} \right) = Qm + y \Rightarrow a \left(x_1 + \frac{m}{d} \right) \equiv y \pmod{m}$$

ולכן $x_2 = x_1 + \frac{m}{d}$ כאשר $ax_2 \equiv y \pmod{m}$

לכן x_2 הוא גם פתרון, בסתירה לכך שיש רק פתרון יחיד.

כיוון ⇒

נניח ש: $\gcd(a, m) = 1$ ונניח בשלילה כי יש שני פתרונות $(x_1 \pmod{26}, x_2 \pmod{26})$. כלומר:

$$ax_1 \equiv y \pmod{m} \quad \text{և} \quad ax_2 \equiv y \pmod{m} .$$

לפי טרנסיטיביות m ולבן $ax_1 \equiv ax_2 \pmod{m}$.

■ $x_1 \not\equiv x_2 \pmod{26}$ לכן $a \nmid m$ שכן $m \mid x_1 - x_2$, בסתירה לכך ש- $\gcd(a, m) = 1$

מסקנה 2.1

יהי $a \in \mathbb{Z}_m$. קיים איבר הופכי $a^{-1} \in \mathbb{Z}_m$ כך ש- 2.3 מקיים את התנאי

$$aa^{-1} \equiv 1 \pmod{m} ,$$

אם ורק אם $\gcd(a, m) = 1$

הוכחה:

כיוון ⇔

נניח ש- $\gcd(a, m) = 1$. לכן לפי משפט באז קיימים שלמים x, y כך ש- $xa + ym = 1$. נעביר אגפים ונקבל: $xa \equiv 1 \pmod{m}$ וכך $xa = 1 - ym$.

כיוון ⇒

נניח ש- $ax + (-q)m = 1$. אז קיימים שלם q עבורו $ax = qm + 1$. נעביר אגפים ונקבל: $ax \equiv 1 \pmod{m}$. לכן $\gcd(a, m) = 1$.

■

דוגמה 2.5

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

פתרונות:

קיימים איבר הופכי של a ב- \mathbb{Z}_m אם ורק אם $\gcd(a, m) = 1$ (באמצעות האלגוריתם של אוקליד המוכלל).
יהיו $a = 26, b = 11$.

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

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

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

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

מכאן אנחנו רואים כי $1 = \gcd(26, 11)$ ולכן לפי משפט 2.7 ההופכי של 11 קיים ב- \mathbb{Z}_{26} מחשבים את האיבר ההופכי לפי השיטה הבאה:

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

■

כלל 2.1

האיברים של \mathbb{Z}_{26} שעבורם קיימים איברים הופכיים הינם

1^{-1}	3^{-1}	5^{-1}	7^{-1}	9^{-1}	11^{-1}	15^{-1}	17^{-1}	19^{-1}	21^{-1}	23^{-1}	25^{-1}
1	9	21	15	3	19	7	23	11	5	17	25

הגדרה 2.4 פונקציה אוילר ($\phi(m)$)

נתון החוג \mathbb{Z}_m כאשר $2 \leq m$ מספר טבעי. $\phi(m)$ תוגדר להיות הפונקציה הנונתת את מספר האיברים ב- \mathbb{Z}_m אשר זרים ל- m .

(שםו לב ההגדרה הזאת זהה להגדרה 2.1)

מסקנה 2.2 מספר איברים הפיכיים ב-

מספר האיברים של החוג \mathbb{Z}_m שעבורם קיימים איברים הופכיים שווה ל- $\phi(m)$.

■

הוכחה: $a \in \mathbb{Z}_m$ שווה למספר איברים $\phi(m)$ עבורם $\gcd(a, m) = 1$, ולפי משפט 2.1 אוטם האיברים הם האיברים הפיכיים של \mathbb{Z}_m .

2.3 הפיכת מטריצות בחוג \mathbb{Z}_m

הגדרה 2.5 המטריצה של קופקטוריים

תהי $A \in \mathbb{R}^{n \times n}$.

הkopקטור 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 .

הגדה 2.6 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 2.8 נוסחת למטריצה ההפכית

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

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

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

2.6 דוגמה

מצאו את הההפכית של

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

פתרון:

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

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

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

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

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

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

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

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

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

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

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 2.7

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:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

לפי כן

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

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

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

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

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

לפי כן

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

בדיקה:

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

