

תרגילים 2: חוגים מתמטיים

שאלה 1 הוכיחו שאם p מספר ראשוני ו- n מספר שלם חיובי אז

$$\phi(pn) = \begin{cases} (p-1)\phi(n), & \text{אם } p \nmid n \\ p\phi(n), & \text{אם } p \mid n \end{cases}.$$

שאלה 2 יהיו a ו- b מספרים ראשוניים. הוכיחו:

(א) $\phi(a) = a - 1$

(ב) $\phi(ab) = (a-1)(b-1)$

שאלה 3 בחוגים הבאים מצאו את כמות האיברים עבורם קיים איבר הופכי:

(א) \mathbb{Z}_{200}

(ב) \mathbb{Z}_{400}

(ג) \mathbb{Z}_{1000}

(ד) \mathbb{Z}_{263}

(ה) \mathbb{Z}_{2521}

שאלה 4 מצאו את ההופכית של

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

שאלה 5 מצאו את ההופכית של

$$A = \begin{pmatrix} 1 & 0 & 3 \\ 3 & 1 & 5 \\ 0 & 0 & 7 \end{pmatrix} \in \mathbb{Z}_{26}^{3 \times 3}.$$

שאלה 6 חשבו את האיבר ההופכי של 19 ב- \mathbb{Z}_{26} .

שאלה 7 מצאו את מספר המפתחות של צופן האפיני מעל החוגים הבאים:

(א) \mathbb{Z}_{30}

(ב) \mathbb{Z}_{100}

(ג) \mathbb{Z}_{1225}

שאלה 8 חשבו את האיבר ההופכי של 7 ב- \mathbb{Z}_{20} .

פתרונות

שאלה 1

- אם $n \nmid p$ אז p לא מופיע לפירוק לראשוניים של n . ז"א אם הפירוק לראשוניים של n הוא

$$n = p_1^{e_1} p_2^{e_2} \cdot p_k^{e_k}$$

אז $p \neq p_i$ לכל $1 \leq i \leq k$. לכן הפירוק לראשוניים של pn הוא

$$pn = p^1 p_1^{e_1} p_2^{e_2} \cdot p_k^{e_k}.$$

מכאן הפונקציה אוילר עבור pn היא

$$\phi(pn) = (p^1 - p^0) (p_1^{e_1} - p_1^{e_1-1}) \cdots (p_k^{e_k} - p_k^{e_k-1}).$$

מצד שני הפונקציה אוילר של p היא $\phi(p) = p - 1$ והפונקציה אוילר של n היא

$$\phi(n) = (p_1^{e_1} - p_1^{e_1-1}) \cdots (p_k^{e_k} - p_k^{e_k-1})$$

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

- אם $n \mid p$ אז p מופיע בפירוק לראשוניים של n . ז"א אם הפירוק לראשוניים של n הוא

$$n = p_1^{e_1} \cdots p_{i-1}^{e_{i-1}} p_i^{e_i} p_{i+1}^{e_{i+1}} \cdots p_k^{e_k}$$

אז קיים $i, 1 \leq i \leq k$ עבורו $p_i = p$. לכן

$$np = p_1^{e_1} \cdots p_{i-1}^{e_{i-1}} p^{e_i+1} p_{i+1}^{e_{i+1}} \cdots p_k^{e_k}.$$

מכאן הפונקציית אוילר של np היא

$$\begin{aligned} \phi(np) &= (p_1^{e_1} - p_1^{e_1-1}) \cdots (p_{i-1}^{e_{i-1}} - p_{i-1}^{e_{i-1}-1}) (p^{e_i+1} - p^{e_i}) (p_{i+1}^{e_{i+1}} - p_{i+1}^{e_{i+1}-1}) \cdots (p_k^{e_k} - p_k^{e_k-1}) \\ &= (p_1^{e_1} - p_1^{e_1-1}) \cdots (p_{i-1}^{e_{i-1}} - p_{i-1}^{e_{i-1}-1}) p (p^{e_i} - p^{e_i-1}) (p_{i+1}^{e_{i+1}} - p_{i+1}^{e_{i+1}-1}) \cdots (p_k^{e_k} - p_k^{e_k-1}) \\ &= p (p_1^{e_1} - p_1^{e_1-1}) \cdots (p_{i-1}^{e_{i-1}} - p_{i-1}^{e_{i-1}-1}) (p^{e_i} - p^{e_i-1}) (p_{i+1}^{e_{i+1}} - p_{i+1}^{e_{i+1}-1}) \cdots (p_k^{e_k} - p_k^{e_k-1}) \\ &= p\phi(n). \end{aligned}$$

שאלה 2

- (א) a ראשוני לכן הפירוק לראשוניים שלו הוא $p_1^{e_1}$ כאשר $p_1 = a$ ו- $e_1 = 1$. לכן הפונקציה אוילר של a הינה

$$\phi(a) = (p_1^{e_1} - p_1^{e_1-1}) = a - 1.$$

(ב) a ראשוני ו- b ראשוני לכן הפירוק לראשוניים של ab הוא $ab = p_1^{e_1} p_2^{e_2}$ כאשר $p_1 = a, p_2 = b$ ו- $e_1 = 1, e_2 = 1$.
לכן הפונקציה אוילר של ab הינה

$$\phi(ab) = (p_1^{e_1} - p_1^{e_1-1}) (p_2^{e_2} - p_2^{e_2-1}) = (a - 1)(b - 1) .$$

שאלה 3 לכל a בחוג \mathbb{Z}_m קיים איבר הופכי a^{-1} אם ורק אם $\gcd(a, m) = 1$. נניח כי הפירוק לראשוניים של a הוא $a = \prod_{i=1}^n p_i^{e_i}$. אז מספר האיברים עבורם $\gcd(a, m) = 1$ ניתן ע"י הנסוחה

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

(א) \mathbb{Z}_{200}

$$200 = 2^3 5^2$$

לכן

$$\phi(200) = (2^3 - 2^2) (5^2 - 5^1) = 80 .$$

(ב) \mathbb{Z}_{400}

$$400 = 2^4 5^2$$

לכן

$$\phi(400) = (2^4 - 2^3) (5^2 - 5^1) = 160 .$$

(ג) \mathbb{Z}_{1000}

$$1000 = 2^3 5^3$$

לכן

$$\phi(1000) = (2^3 - 2^2) (5^3 - 5^2) = 400 .$$

(ד) \mathbb{Z}_{263}

שימו לב 263 הוא מספר ראשוני לכן הפירוק לראשוניים שלו הוא $263 = 263^1$ ו-

$$\phi(263) = 263^1 - 263^0 = 263 - 1 = 262 .$$

(בכללי, אם p מספר ראשוני אז $\phi(p) = p - 1$).

(ה) \mathbb{Z}_{2521}

שימו לב 2521 מספר ראשוני לכן הפירוק לראשוניים שלו הוא $2521 = 2521^1$ ו-

$$\phi(2521) = 2521^1 - 2521^0 = 2521 - 1 = 2520 .$$

(בכללי, אם p מספר ראשוני אז $\phi(p) = p - 1$).

שאלה 4

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

לפיכך

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

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

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

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

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

לפיכך

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

בדיקה:

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

שאלה 5 נחשב את הדטרמיננטה לפי השורה האחרונה:

$$|A| = 0 \cdot \begin{vmatrix} 0 & 3 \\ 1 & 5 \end{vmatrix} - 0 \begin{vmatrix} 1 & 3 \\ 3 & 5 \end{vmatrix} + 7 \begin{vmatrix} 1 & 0 \\ 3 & 1 \end{vmatrix} = 7 \cdot 1 = 7 .$$

$\gcd(7, 26) = 1$ לכן המטריצה הפיכה ב- \mathbb{Z}_{26} .

$$\begin{pmatrix} \cancel{1} & \cancel{0} & \cancel{3} \\ 3 & 1 & 5 \\ 0 & 0 & 7 \end{pmatrix} \Rightarrow C_{11} = (-1)^{1+1} \begin{vmatrix} 1 & 5 \\ 0 & 7 \end{vmatrix} = 7 .$$

$$\begin{pmatrix} \cancel{1} & \cancel{0} & \cancel{3} \\ 3 & \cancel{1} & 5 \\ 0 & 0 & 7 \end{pmatrix} \Rightarrow C_{12} = (-1)^{1+2} \begin{vmatrix} 3 & 5 \\ 0 & 7 \end{vmatrix} = -21 .$$

$$\begin{pmatrix} \cancel{1} & \cancel{0} & \cancel{3} \\ 3 & 1 & \cancel{5} \\ 0 & 0 & \cancel{7} \end{pmatrix} \Rightarrow C_{13} = (-1)^{1+3} \begin{vmatrix} 3 & 1 \\ 0 & 0 \end{vmatrix} = 0 .$$

$$\begin{pmatrix} 1 & 0 & 3 \\ 3 & 1 & 5 \\ 0 & 0 & 7 \end{pmatrix} \Rightarrow C_{21} = (-1)^{2+1} \begin{vmatrix} 0 & 3 \\ 0 & 7 \end{vmatrix} = 0 .$$

$$\begin{pmatrix} 1 & 0 & 3 \\ 3 & 1 & 5 \\ 0 & 0 & 7 \end{pmatrix} \Rightarrow C_{22} = (-1)^{2+2} \begin{vmatrix} 1 & 3 \\ 0 & 7 \end{vmatrix} = 7 .$$

$$\begin{pmatrix} 1 & 0 & 3 \\ 3 & 1 & 5 \\ 0 & 0 & 7 \end{pmatrix} \Rightarrow C_{23} = (-1)^{2+3} \begin{vmatrix} 1 & 0 \\ 0 & 0 \end{vmatrix} = 0 .$$

$$\begin{pmatrix} 1 & 0 & 3 \\ 3 & 1 & 5 \\ 0 & 0 & 7 \end{pmatrix} \Rightarrow C_{31} = (-1)^{3+1} \begin{vmatrix} 0 & 3 \\ 1 & 5 \end{vmatrix} = -3 .$$

$$\begin{pmatrix} 1 & 0 & 3 \\ 3 & 1 & 5 \\ 0 & 0 & 7 \end{pmatrix} \Rightarrow C_{32} = (-1)^{3+2} \begin{vmatrix} 1 & 3 \\ 3 & 5 \end{vmatrix} = 4 .$$

$$\begin{pmatrix} 1 & 0 & 3 \\ 3 & 1 & 5 \\ 0 & 0 & 7 \end{pmatrix} \Rightarrow C_{33} = (-1)^{3+3} \begin{vmatrix} 1 & 0 \\ 3 & 1 \end{vmatrix} = 1 .$$

$$C = \begin{pmatrix} C_{11} & C_{12} & C_{13} \\ C_{21} & C_{22} & C_{23} \\ C_{31} & C_{32} & C_{33} \end{pmatrix} = \begin{pmatrix} 7 & -21 & 0 \\ 0 & 7 & 0 \\ -3 & 4 & 1 \end{pmatrix}$$

$$\text{adj}(A) = C^t = \begin{pmatrix} 7 & 0 & -3 \\ -21 & 7 & 4 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 7 & 0 & 23 \\ 5 & 7 & 4 \\ 0 & 0 & 1 \end{pmatrix} \in \mathbb{Z}_{26}^{3 \times 3} .$$

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

$$|A|^{-1} = 7^{-1} = 15 \in \mathbb{Z}_{26}$$

לפיכך

$$A^{-1} = |A|^{-1} \text{adj}(A) = 15 \cdot \begin{pmatrix} 7 & 0 & 23 \\ 5 & 7 & 4 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 105 & 0 & 345 \\ 75 & 105 & 60 \\ 0 & 0 & 15 \end{pmatrix} .$$

$$105 \bmod 26 = 105 - 26 \cdot \left\lfloor \frac{105}{26} \right\rfloor = 1 .$$

$$345 \bmod 26 = 345 - 26 \cdot \left\lfloor \frac{345}{26} \right\rfloor = 7 .$$

$$75 \bmod 26 = 75 - 26 \cdot \left\lfloor \frac{75}{26} \right\rfloor = 23 .$$

$$60 \bmod 26 = 60 - 26 \cdot \left\lfloor \frac{60}{26} \right\rfloor = 8 .$$

לפיכך

$$A^{-1} = \begin{pmatrix} 1 & 0 & 7 \\ 23 & 1 & 8 \\ 0 & 0 & 15 \end{pmatrix} \in \mathbb{Z}_{26}^{3 \times 3} .$$

בדיקה:

$$A \cdot A^{-1} = \begin{pmatrix} 1 & 0 & 3 \\ 3 & 1 & 5 \\ 0 & 0 & 7 \end{pmatrix} \begin{pmatrix} 1 & 0 & 7 \\ 23 & 1 & 8 \\ 0 & 0 & 15 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 52 \\ 26 & 1 & 104 \\ 0 & 0 & 105 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \pmod{26} .$$

שאלה 6 נשתמש באלגוריתם של אוקלידס המוכלל כדי למצוא שלמים s, t, d עבורם $26s + 19t = d$.

$$\begin{aligned} r_0 &= a = 26 , & r_1 &= b = 19 , \\ s_0 &= 1 , & s_1 &= 0 , \\ t_0 &= 0 , & t_1 &= 1 . \end{aligned}$$

$q_1 = 1$	$r_2 = 26 - 1 \cdot 19 = 7$	$s_2 = 1 - 1 \cdot 0 = 1$	$t_2 = 0 - 1 \cdot 1 = -1$	שלב $k = 1$
$q_2 = 2$	$r_3 = 19 - 2 \cdot 7 = 5$	$s_3 = 0 - 2 \cdot 1 = -2$	$t_3 = 1 - 2 \cdot (-1) = 3$	שלב $k = 2$
$q_3 = 1$	$r_4 = 7 - 1 \cdot 5 = 2$	$s_4 = 1 - 1 \cdot (-2) = 3$	$t_4 = -1 - 1 \cdot (3) = -4$	שלב $k = 3$
$q_4 = 2$	$r_5 = 5 - 2 \cdot 2 = 1$	$s_5 = -2 - 2 \cdot 3 = -8$	$t_5 = 3 - 2 \cdot (-4) = 11$	שלב $k = 4$
$q_5 = 2$	$r_6 = 2 - 2 \cdot 1 = 0$			שלב $k = 5$

$$\gcd(a, b) = r_5 = 1 , \quad s = s_5 = -8 , \quad t = t_5 = 11 .$$

לכן:

$$sa + tb = -8(26) + 11(19) = 1 .$$

$$sa + tb = 1 \quad \text{אם ורק אם} \quad a^{-1} \equiv s \pmod{b}$$

$$\text{לכן } 19^{-1} \equiv 11 \pmod{26} .$$

שאלה 7 הכלל מצפין והכלל מעפנח של הצופן האפיני מעל אלפבית בת m אותיות הם:

$$e_k(x) = ax + b \bmod m ,$$

ו-

$$d_k(y) = a^{-1}(y - b) \bmod m .$$

הכלל מצפין $e_k(x)$ הפיך, כלומר קיים כלל מפענח $d_k(y) = a^{-1}(y - b) \bmod m$ רק אם קיים איבר הופכי $a^{-1} \in \mathbb{Z}_m$.

קיים איבר הופכי a^{-1} אם רק אם $\gcd(a, m) = 1$.
 אם הפירוק למספרים ראשוניים של m הוא $m = \prod_{i=1}^n p_i^{e_i}$ אז מספר האברים ב- \mathbb{Z}_m עבורם $\gcd(a, m) = 1$ נתון על ידי הפונקציה אוילר

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

לכן, קיימות $\phi(m)$ אפשרויות עבור a וקיימות m אפשרויות בשביל b . בסך הכל קיימות $m\phi(m)$ מפתחות של צופן אפיני מעל \mathbb{Z}_m .

(א) הפירוק לראשוניים של 30 הוא $30 = 2^1 \times 3^1 \times 5^1$ לכן

$$\phi(30) = (2^1 - 2^0) (3^1 - 3^0) (5^1 - 5^0) = (1)(2)(4) = 8 .$$

לכן עבור צופן האפיני מעל \mathbb{Z}_{30} קיימות $30 \times 8 = 240$ מפתחות.

(ב) הפירוק לראשוניים של 100 הוא $100 = 2^2 \times 5^2$. לכן

$$\phi(100) = (2^2 - 2^1) (5^2 - 5^1) = (2)(20) = 40 .$$

לכן עבור צופן האפיני מעל \mathbb{Z}_{100} קיימות $100 \times 40 = 4000$ מפתחות.

(ג) הפירוק לראשוניים של 1225 הוא $1225 = 5^2 \times 7^2$ לכן $1225 = 5 \times 245 = 5^2 \times 49 = 5^2 \times 7^2$

$$\phi(1225) = (5^2 - 5^1) (7^2 - 7^1) = (20)(42) = 840 .$$

לכן עבור הצופן האפיני מעל \mathbb{Z}_{1225} קיימות $1225 \times 840 = 1,029,000$ מפתחות.

שאלה 8

$$1 \cdot 7 = 7 \equiv 7 \pmod{20} ,$$

$$2 \cdot 7 = 14 \equiv 14 \pmod{20} ,$$

$$3 \cdot 7 = 21 \equiv 1 \pmod{20} .$$

לכן $7^{-1} \equiv 3 \pmod{20}$.