תרגילים 2: חוגים וצפנים בסיסיים

שאלה 1 בחוגים הבאים מצאו את איברים יש 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 2 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 3 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 4 חשבו את האיבר ההופכי של 19 ב- $\mathbb{Z}_{26}$.

שאלה 5 הטקסט מוצפן הבא מוצפן על ידי צופן הזזה (צופן קיסר).

```
VWDUZDUV
```

מצאו את המפתח של הצופן ומצאו את הטקסט גלוי (רמז: חיפוש ממצה).

שאלה 6 מצאו את מספר המפתחות של צופן האפיני מעל החוגים הבאים:

א) $\mathbb{Z}_{30}$

ב) $\mathbb{Z}_{100}$

ג) $\mathbb{Z}_{1225}$

שאלה 7

שאלה 8 נתונה התמורה הבאה:

$$\pi = \begin{pmatrix} 4 & 1 & 6 & 2 & 7 & 3 & 8 & 5 \end{pmatrix}$$

א) מצאו את התמורה ההופכית.

ב) פענחו את הטקסט מוצפן הבא

```
TGEEMNELNNTDROEOAAHDOETCSHAEIRLM
```

שאלה 9 נתון המפתח

$$k = \begin{pmatrix} 1 & 3 & 0 \\ 0 & 0 & 1 \\ 3 & 0 & 1 \end{pmatrix}$$

של הצופן היל. לכל טקסט מוצפן למטה מתון את הטקסט גלוי

א) `VAZMJR`

ב) `NDIMZZEMV`

שאלה 10

נתון הטקסט מוצפן

```
FPHOEMJSUPSZZYJ
```

אשר מוצפן על ידי צופן היל עם המפתח

$$k = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix} .$$

מצאו את הטקסט גלוי.

שאלה 11

נתון את הטקסט מוצפן

```
YGSOYNGSUUTOYZNKHKYZIURRKMKOTOYXGKR
```

אשר מוצפן על ידי צופן קיסר. מצאו את המפתח ואת הטקסט גלוי.

שאלה 12 נניח כי $K = (5, 21)$ הוא מפתח של צופן האפיני מעל החוג $\mathbb{Z}_{29}$.

א) מצאו את האיברים a', b' בכלל מפענח

$$d_K(y) = a'y + b'$$

כאשר $a', b' \in \mathbb{Z}_{29}$.

ב) הוכיחו כי $d_K\left(e_K(x)\right) = x$ לכל $x \in \mathbb{Z}_{29}$.

פתרונות

<u>שאלה 1</u> 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 $\prod_{i=1}^{n} p_i^{e_i}$. אז מספר האיברים עבורם $\gcd(a,m)=1$ ניתן ע"י הנסוחה

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

א) $\mathbb{Z}_{200}$

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

לכן

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

ב) $\mathbb{Z}_{400}$

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

לכן

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

ג) $\mathbb{Z}_{1000}$

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

לכן

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

ד) $\mathbb{Z}_{263}$.

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

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

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

ה) $\mathbb{Z}_{2521}$.

$\mathbb{Z}_{2521}$. 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 מסספר ראשוני אז $\phi(p)=p-1$.

שאלה 2

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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:

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

<u>שאלה 3</u> 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- $\mathbb{Z}_{26}$.

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

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

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

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

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

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

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

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

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

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

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

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

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

לפיכך

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

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

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

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

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

לפיכך

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

בדיקה:

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

<u>שאלה 4</u> נשתמש באלגוריתם של אוקליד המוכלל כדי למצוא שלמים s, t, d עבורם $26s + 19t = d$.

<u>השיטה של האלגוריתם איוקליד המוכלל</u>

$a = 26, b = 19$.

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

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

$$\gcd(a, b) = r_5 = 1 \ , \qquad s = s_5 = -3 \ , \qquad t = t_5 = 11 \ .$$

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

ז"א $d = \gcd(26, 19) = 1$ ולכן קיים $19^{-1} \in \mathbb{Z}_{26}$.

$$-8(26)+11(19) = 1 \quad \Rightarrow \quad 11(19) = 1+8(26) \quad \Rightarrow \quad 11(19) = 1 \mod 26 \quad \Rightarrow \quad 19^{-1} = 11 \mod 26 \ .$$

■

יש שיטה נוספת למציאת המקדמים s, t במשסט בזו. נתאר אותה על ידי הדוגמה הקודמת.

<u>פתרון עם השיטה השניה של האלגוריתם איוקליד המוכלל</u>

לשיטה הזאת יש 2 שלבים. בשלב הראשון מבצעים האלגוריתם של אוקליד במשפט **??**.

$$\begin{aligned}
\boxed{26} &= 1 \cdot \boxed{19} + \boxed{7} \\
\boxed{19} &= 2 \cdot \boxed{7} + \boxed{5} \\
\boxed{7} &= 1 \cdot \boxed{5} + \boxed{2} \\
\boxed{5} &= 2 \cdot \boxed{2} + \boxed{1} \\
\boxed{2} &= 2 \cdot \boxed{1}
\end{aligned}$$

לכן $d = \gcd(26, 19) = 1$.

בשלב השני רושמים 1 כצירוף לינארי של 26 ו- 19 באמצעות המשוואות למעלה:

$$\begin{aligned}
\boxed{1} &= \boxed{5} - 2 \cdot \boxed{2} \\
&= \boxed{5} - 2 \cdot \Big(\boxed{7} - 1 \cdot \boxed{5} \Big) \\
&= 3 \cdot \boxed{5} - 2 \cdot \boxed{7} \\
&= 3 \cdot \Big(\boxed{19} - 2 \cdot \boxed{7} \Big) - 2 \cdot \boxed{7} \\
&= 3 \cdot \boxed{19} - 8 \cdot \boxed{7} \\
&= 3 \cdot \boxed{19} - 8 \cdot \Big(\boxed{26} - 1 \cdot \boxed{19} \Big) \\
&= 11 \cdot \boxed{19} - 8 \cdot \boxed{26} \ .
\end{aligned}$$

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

ז"א $d = \gcd(26, 19) = 1$ ולכן קיים $19^{-1} \in \mathbb{Z}_{26}$.

$$-8(26)+11(19) = 1 \quad \Rightarrow \quad 11(19) = 1+8(26) \quad \Rightarrow \quad 11(19) = 1 \mod 26 \quad \Rightarrow \quad 19^{-1} = 11 \mod 26 \ .$$

■

שאלה 5

$\mathtt{y} \in C$	V	W	D	U	Z	D	U	V
$y \in C$	21	22	3	20	25	3	20	21
$x = y - 0 \in P$	21	22	3	20	25	3	20	21
$\mathtt{x} \in P$	v	w	d	u	z	d	u	v
$x = y - 1 \in P$	20	21	2	19	24	2	19	20
$\mathtt{x} \in P$	u	v	c	t	y	c	t	u
$x = y - 2 \in P$	19	20	1	18	23	1	18	19
$\mathtt{x} \in P$	t	u	b	s	x	b	s	t
$x = y - 3 \in P$	18	19	0	17	22	0	17	18
$\mathtt{x} \in P$	s	t	a	r	w	a	r	s

המפתח הוא 3 והטקסט גלוי הוא

starwars

שאלה 6 הצופן האפיני מעל $\mathbb{Z}_m$ מכיל כלל מצפין

$$e_k(x) = ax + b \mod m$$

וכלל המפענח

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

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

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

לכן, יש $\phi(m)$ אפשריות ל- a ו- m אפשריות ל- b. בסך הכל קיימים $m\ \phi(m)$ מפתחות של צופן אפיני מעל $\mathbb{Z}_m$.

א) $30 = 2^1 \times 3^1 \times 5^1$ לכן

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

לכן לצופן האפיני מעל $\mathbb{Z}_{30}$ יש $30 \times 8 = 240$ מפתחות.

ב) $100 = 2^2 \times 5^2$ לכן

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

לכן לצופן האפיני מעל $\mathbb{Z}_{100}$ יש $100 \times 40 = 4000$ מפתחות.

ג) $1225 = 5 \times 245 = 5^2 \times 49 = 5^2 \times 7^2$ לכן

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

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

שאלה 7

שאלה 8

y $\in C$	T	G	E	E	M	N	E	L	N	N	T	D	R	O	E	O
$y \in \mathbb{Z}_{26}$	19	6	4	4	12	13	4	11	13	13	19	3	17	14	4	14

y $\in C$	A	A	H	D	O	E	T	C	S	H	A	E	I	R	L	M
$y \in \mathbb{Z}_{26}$	0	0	7	3	14	4	19	2	18	7	0	4	8	17	11	12

נפרק את האותיות לתת-קבוצות מאורך $m = 8$ (לפי האורך של התמורה).
נפעיל את התמורה ההופכית:

$\mathtt{y} \in C$	T	G	E	E	M	N	E	L	N	N	T	D	R	O	E	O
$y \in \mathbb{Z}_{26}$	19	6	4	4	12	13	4	11	13	13	19	3	17	14	4	14

$\mathtt{y} \in C$	A	A	H	D	O	E	T	C	S	H	A	E	I	R	L	M
$y \in \mathbb{Z}_{26}$	0	0	7	3	14	4	19	2	18	7	0	4	8	17	11	12

i	1	2	3	4	5	6	7	8
$\pi^{-1}(i)$	2	4	6	1	8	3	5	7

$\mathtt{y} \in C$	T	G	E	E	M	N	E	L	N	N	T	D	R	O	E	O
$y \in \mathbb{Z}_{26}$	19	6	4	4	12	13	4	11	13	13	19	3	17	14	4	14
$x = \pi^{-1}(y)$	6	4	13	19	11	4	12	4	13	3	14	13	14	19	17	4

$\mathtt{y} \in C$	A	A	H	D	O	E	T	C	S	H	A	E	I	R	L	M
$y \in \mathbb{Z}_{26}$	0	0	7	3	14	4	19	2	18	7	0	4	8	17	11	12
$x = \pi^{-1}(y)$	0	3	4	0	2	7	14	19	7	4	17	18	12	0	8	11

$\mathtt{y} \in C$	T	G	E	E	M	N	E	L	N	N	T	D	R	O	E	O
$y \in \mathbb{Z}_{26}$	19	6	4	4	12	13	4	11	13	13	19	3	17	14	4	14
$x = \pi^{-1}(y)$	6	4	13	19	11	4	12	4	13	3	14	13	14	19	17	4
$\mathtt{x} \in P$	g	e	n	t	l	e	m	e	n	d	o	n	o	t	r	e

$\mathtt{y} \in C$	A	A	H	D	O	E	T	C	S	H	A	E	I	R	L	M
$y \in \mathbb{Z}_{26}$	0	0	7	3	14	4	19	2	18	7	0	4	8	17	11	12
$x = \pi^{-1}(y)$	0	3	4	0	2	7	14	19	7	4	17	18	12	0	8	11
$\mathtt{x} \in P$	a	d	e	a	c	h	o	t	h	e	r	s	m	a	i	l

gentlemandonotreadeachothersmail

שאלה 9

$$|k| = 1 \cdot \begin{vmatrix} 0 & 1 \\ 0 & 1 \end{vmatrix} - 3 \begin{vmatrix} 0 & 1 \\ 3 & 1 \end{vmatrix} + 0 \begin{vmatrix} 0 & 0 \\ 3 & 0 \end{vmatrix} = 9 \ .$$

$\gcd(9, 26) = 1$ לכן המטריצה הפיכה ב- $\mathbb{Z}_{26}$.

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

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

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

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

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

$$\begin{pmatrix} 1 & 3 & 0 \\ 0 & 0 & 1 \\ 3 & 0 & 1 \end{pmatrix} \quad \Rightarrow \quad C_{23} = (-1)^{2+3} \begin{vmatrix} 1 & 3 \\ 3 & 0 \end{vmatrix} = 9 \ .$$

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

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

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

$$C = \begin{pmatrix} C_{11} & C_{12} & C_{13} \\ C_{21} & C_{22} & C_{23} \\ C_{31} & C_{32} & C_{33} \end{pmatrix} = \begin{pmatrix} 0 & 3 & 0 \\ -3 & 1 & 9 \\ 3 & -1 & 0 \end{pmatrix}$$

$$\text{adj}(A) = C^t = \begin{pmatrix} 0 & -3 & 3 \\ 3 & 1 & -1 \\ 0 & 9 & 0 \end{pmatrix} \mod 26 = \begin{pmatrix} 0 & 23 & 3 \\ 3 & 1 & 25 \\ 0 & 9 & 0 \end{pmatrix} \in \mathbb{Z}_{26}^{3\times 3} \ .$$

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

$$|A|^{-1} = 9^{-1} = 3 \in \mathbb{Z}_{26}$$

לפיכך

$$\begin{aligned}A^{-1} =& |A|^{-1}\text{adj}(A)\\ =& 3\cdot\begin{pmatrix}0 & 23 & 3\\ 3 & 1 & 25\\ 0 & 9 & 0\end{pmatrix} \mod 26\\ =& \begin{pmatrix}0 & 69 & 9\\ 9 & 3 & 75\\ 0 & 27 & 0\end{pmatrix} \mod 26\\ =& \begin{pmatrix}0 & 17 & 9\\ 9 & 3 & 23\\ 0 & 1 & 0\end{pmatrix}\end{aligned}$$

א) שלב 1:

נעביר את האותיות של הטקסט גלוי לערכים של $\mathbb{Z}_{26}$:

$y \in C$	V	A	Z	M	J	R
$y \in \mathbb{Z}_{26}$	21	0	25	12	9	17

שלב 2:

נפרק את הטבלה של התווים של הטקסט מוצפן יחד עם הערכים המתאימים של $\mathbb{Z}_{26}$ לתת-קבוצות של $m = 3$ תווים:

$y \in C$	V	A	Z	M	J	R
$y \in \mathbb{Z}_{26}$	21	0	25	12	9	17

שלב 3:

עבור כל תת-קבוצה המתקבל נחשב

$$\begin{aligned}\begin{pmatrix}x_1 & x_2 & x_3\end{pmatrix} &= \begin{pmatrix}y_1 & y_2 & y_3\end{pmatrix} k^{-1} \mod 26\\ &= \begin{pmatrix}y_1 & y_2 & y_3\end{pmatrix}\begin{pmatrix}0 & 17 & 9\\ 9 & 3 & 23\\ 0 & 1 & 0\end{pmatrix} \mod 26\end{aligned}$$

עבור התת-קבוצה הראשונה נקבל

$$\begin{aligned}\begin{pmatrix}x_1 & x_2 & x_3\end{pmatrix} &= \begin{pmatrix}21 & 0 & 25\end{pmatrix}\begin{pmatrix}0 & 17 & 9\\ 9 & 3 & 23\\ 0 & 1 & 0\end{pmatrix} \mod 26\\ &= \begin{pmatrix}0 & 382 & 189\end{pmatrix} \mod 26\\ &= \begin{pmatrix}0 & 18 & 7\end{pmatrix}\end{aligned}$$

עבור התת-קבוצה השנייה נקבל

$$\begin{aligned}\begin{pmatrix}x_1 & x_2 & x_3\end{pmatrix} &= \begin{pmatrix}12 & 9 & 17\end{pmatrix}\begin{pmatrix}0 & 17 & 9\\ 9 & 3 & 23\\ 0 & 1 & 0\end{pmatrix} \mod 26\\ &= \begin{pmatrix}81 & 248 & 315\end{pmatrix} \mod 26\\ &= \begin{pmatrix}3 & 14 & 3\end{pmatrix}\end{aligned}$$

y $\in C$	V	A	Z	M	J	R
$y \in \mathbb{Z}_{26}$	21	0	25	12	9	17
$x \in \mathbb{Z}_{26}$	0	18	7	3	14	3

שלב 5:

נעבור את הערכים $y \in \mathbb{Z}_{26}$ לאותיות של הטקסט מוצפן:

y $\in C$	V	A	Z	M	J	R
$y \in \mathbb{Z}_{26}$	21	0	25	12	9	17
$x \in \mathbb{Z}_{26}$	0	18	7	3	14	3
x $\in \mathbb{Z}_{26}$	a	s	h	d	o	d

הטקסט גלוי המתקבל הוא

ashdod

ב) שלב 1:

נעביר את האותיות של הטקסט גלוי לערכים של $\mathbb{Z}_{26}$:

y $\in C$	N	D	I	M	Z	Z	E	M	V
$y \in \mathbb{Z}_{26}$	13	3	8	12	25	25	4	12	21

שלב 2:

נפרק את הטבלה של התווים של הטקסט מוצפן יחד עם הערכים המתאימים של $\mathbb{Z}_{26}$ לתת-קבוצות של $m = 3$ תווים:

y $\in C$	N	D	I	M	Z	Z	E	M	V
$y \in \mathbb{Z}_{26}$	13	3	8	12	25	25	4	12	21

שלב 3:

עבור כל תת-קבוצה המתקבל נחשב

$$\begin{aligned}(x_1 \quad x_2 \quad x_3) &= (y_1 \quad y_2 \quad y_3)\, k^{-1} \mod 26 \\ &= (y_1 \quad y_2 \quad y_3) \begin{pmatrix} 0 & 17 & 9 \\ 9 & 3 & 23 \\ 0 & 1 & 0 \end{pmatrix} \mod 26\end{aligned}$$

עבור התת-קבוצה הראשונה נקבל

$$\begin{aligned}(x_1 \quad x_2 \quad x_3) &= (13 \quad 3 \quad 8) \begin{pmatrix} 0 & 17 & 9 \\ 9 & 3 & 23 \\ 0 & 1 & 0 \end{pmatrix} \mod 26 \\ &= (27 \quad 238 \quad 186) \mod 26 \\ &= (1 \quad 4 \quad 4)\end{aligned}$$

עבור התת-קבוצה השנייה נקבל

$$\begin{aligned}(x_1 \quad x_2 \quad x_3) &= (12 \quad 25 \quad 25)\begin{pmatrix}0 & 17 & 9\\ 9 & 3 & 23\\ 0 & 1 & 0\end{pmatrix} \mod 26\\ &= (225 \quad 304 \quad 683) \mod 26\\ &= (17 \quad 18 \quad 7)\end{aligned}$$

עבור התת-קבוצה השלישית נקבל

$$\begin{aligned}(x_1 \quad x_2 \quad x_3) &= (4 \quad 12 \quad 21)\begin{pmatrix}0 & 17 & 9\\ 9 & 3 & 23\\ 0 & 1 & 0\end{pmatrix} \mod 26\\ &= (108 \quad 125 \quad 312) \mod 26\\ &= (4 \quad 21 \quad 0)\end{aligned}$$

y $\in C$	N	D	I	M	Z	Z	E	M	V
$y \in \mathbb{Z}_{26}$	13	3	8	12	25	25	4	12	21
$x \in \mathbb{Z}_{26}$	1	4	4	17	18	7	4	21	0

<u>שלב 5:</u>

נעבור את הערכים $y \in \mathbb{Z}_{26}$ לאותיות של הטקסט מוצפן:

y $\in C$	N	D	I	M	Z	Z	E	M	V
$y \in \mathbb{Z}_{26}$	13	3	8	12	25	25	4	12	21
$x \in \mathbb{Z}_{26}$	1	4	4	17	18	7	4	21	0
x $\in P$	b	e	e	r	s	h	e	v	a

הטקסט גלוי המתקבל הוא

beersheva

שאלה 10

y $\in C$	F	P	H	O	E	M	J	S	U	P	S	Z	Z	Y	J
$y \in \mathbb{Z}_{26}$	5	15	7	14	4	12	9	18	20	15	18	25	25	24	9

דטרמיננטה של k היא $|k| = -3 \mod 26 = 23$.
$\gcd(23, 26) = 1$ לכן המטריצה הפיכה ב- $\mathbb{Z}_{26}$.

$$\begin{pmatrix}1 & 2 & 3\\ 4 & 5 & 6\\ 11 & 9 & 8\end{pmatrix} \Rightarrow C_{11} = (-1)^{1+1}\begin{vmatrix}5 & 6\\ 9 & 8\end{vmatrix} \mod 26 = -14 \mod 26 = 12\ .$$

$$\begin{pmatrix}1 & 2 & 3\\ 4 & 5 & 6\\ 11 & 9 & 8\end{pmatrix} \Rightarrow C_{12} = (-1)^{1+2}\begin{vmatrix}4 & 6\\ 11 & 8\end{vmatrix} \mod 26 = 24 \mod 26 = 8\ .$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix} \quad \Rightarrow \quad C_{13} = (-1)^{1+3} \begin{vmatrix} 4 & 5 \\ 11 & 9 \end{vmatrix} \mod 26 = -19 \mod 26 = 7 \ .$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix} \quad \Rightarrow \quad C_{21} = (-1)^{2+1} \begin{vmatrix} 2 & 3 \\ 9 & 8 \end{vmatrix} = 11 \ .$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix} \quad \Rightarrow \quad C_{22} = (-1)^{2+2} \begin{vmatrix} 1 & 3 \\ 11 & 8 \end{vmatrix} \mod 26 = -25 \mod 26 = 1 \ .$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix} \quad \Rightarrow \quad C_{23} = (-1)^{2+3} \begin{vmatrix} 1 & 2 \\ 11 & 9 \end{vmatrix} = 13 \ .$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix} \quad \Rightarrow \quad C_{31} = (-1)^{3+1} \begin{vmatrix} 2 & 3 \\ 5 & 6 \end{vmatrix} \mod 26 = -3 \mod 26 = 23 \ .$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix} \quad \Rightarrow \quad C_{32} = (-1)^{3+2} \begin{vmatrix} 1 & 3 \\ 4 & 6 \end{vmatrix} = 6 \ .$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix} \quad \Rightarrow \quad C_{33} = (-1)^{3+3} \begin{vmatrix} 1 & 2 \\ 4 & 5 \end{vmatrix} \mod 26 = -3 \mod 26 = 23 \ .$$

$$C = \begin{pmatrix} C_{11} & C_{12} & C_{13} \\ C_{21} & C_{22} & C_{23} \\ C_{31} & C_{32} & C_{33} \end{pmatrix} = \begin{pmatrix} -14 & 34 & -19 \\ 11 & -25 & 13 \\ -3 & 6 & -3 \end{pmatrix} \mod 26 = \begin{pmatrix} 12 & 8 & 7 \\ 11 & 1 & 13 \\ 23 & 6 & 23 \end{pmatrix} \ .$$

$$\text{adj}(A) = C^t = \begin{pmatrix} 16 & 3 & 18 \\ 9 & 9 & 1 \\ 21 & 5 & 20 \end{pmatrix} \in \mathbb{Z}_{26}^{3\times 3} \ .$$

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

$$|k|^{-1} = 23^{-1} = 17 \in \mathbb{Z}_{26}$$

$$k^{-1} = 17 \begin{pmatrix} 16 & 3 & 18 \\ 9 & 9 & 1 \\ 21 & 5 & 20 \end{pmatrix} = \begin{pmatrix} 204 & 187 & 391 \\ 136 & 17 & 102 \\ 119 & 221 & 391 \end{pmatrix} = \begin{pmatrix} 22 & 5 & 1 \\ 6 & 17 & 24 \\ 15 & 13 & 1 \end{pmatrix}$$

$$(5, 15, 7) \cdot k^{-1} = (19, 7, 8) \ , \qquad (14, 4, 12) \cdot k^{-1} = (18, 8, 18) \ , \qquad (9, 18, 20) \cdot k^{-1} = (8, 13, 19) \ ,$$

$$(15, 18, 25) \cdot k^{-1} = (7, 4, 4) \ , \qquad (25, 24, 9) \cdot k^{-1} = (23, 0, 12) \ .$$

$y \in C$	F	P	H	O	E	M	J	S	U	P	S	Z	Z	Y	J
$y \in \mathbb{Z}_{26}$	5	15	7	14	4	12	9	18	20	15	18	25	25	24	9
$x \in \mathbb{Z}_{26}$	19	7	8	18	8	18	8	13	19	7	4	4	23	0	12
$x \in P$	t	h	i	s	i	s	i	n	t	h	e	e	x	a	m

שאלה 11

$y \in C$	Y	G	S	O	Y	N	G	S	U	U	T	O	Y	Z	N	K	H	K	Y	Z
$y \in \mathbb{Z}_{26}$	24	6	18	14	24	13	6	18	20	20	19	14	24	25	13	10	7	10	24	25
$d_6(y)$	18	0	12	8	18	7	0	12	14	14	13	8	18	19	7	4	1	4	18	19
$x \in P$	s	a	m	i	s	h	a	m	o	o	n	i	s	t	h	e	b	e	s	t

$y \in C$	I	U	R	R	K	M	K	O	T	O	Y	X	G	K	R
$y \in \mathbb{Z}_{26}$	8	20	17	17	10	12	10	14	19	14	24	23	6	10	17
$d_6(y)$	2	14	11	11	4	6	4	8	13	8	18	17	0	4	11
$x \in P$	c	o	l	l	e	g	e	i	n	i	s	r	a	e	l

שאלה 12

א) נתון המפתח $a = 5, b = 21$ בכלל מצפין $e_k(x) = ax + b$. אז הכלל מפענח הינו

$$d_k(y) = a^{-1}(y - b) = 5^{-1}(y - 21) \ .$$

ב- $\mathbb{Z}_{29}$, $5^{-1} = 6$ מכיוון ש- $5 \cdot 6 \mod 29 = 30 \mod 29 = 1$. לפיכך

$$d_k(y) = 6(y-21) = 6y-126 \mod 29 = 6y-4\cdot 29-10 \mod 29 = 6y-10 \mod 29 = 6y+19 \ .$$

לפיכך $a' = 6, b' = 19$.

ב)

$$d_k\left(e_k(x)\right) = 6\left(5x + 21\right)+19 \mod 29 = 30x+126+19 \mod 29 = 1\cdot x+145 \mod 29 = x+5\cdot 29 \mod 29 = x \ .$$