

## תרגילים 2: חוגים מתמטיים

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

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

**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 קיימים 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)  $\mathbb{Z}_{30}$

$\mathbb{Z}_{100}$  ב)

$\mathbb{Z}_{1225}$  ג)

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

**פתרונות** **שאלה 1**

- אם  $n \nmid p$  אז  $p$  לא מופיע בפירוק הראשוניים של  $n$ . אז אם הפירוק הראשוניים של  $n$  הוא

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

אז  $p \neq p_i$  לכל  $i \leq k$ . לכן הפיקור הראשוניים של  $pn$  הוא

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

מכאן הפונקציית 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 הפונקציית אוילר של  $p$  היא  $\phi(p) = p - 1$  והפונקציית 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 הראשוניים של  $n$ . אז אם הפירוק הראשוניים 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 קיימים  $i$ ,  $1 \leq i \leq k$ ,  $p_i \mid n$ . לכן

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

מכאן הפונקציית אוילר של  $np$  היא

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

 **שאלה 2**

- a) ראשוני לכן הפירוק הראשוניים שלו הוא  $p_1^{e_1}$  כאשר  $e_1 = 1$  ו-  $p_1 = a$  שכן הפונקציית אוילר של  $a$  הינה

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

**(ב)**  $a$  ראשוני ו-  $b$  ראשוני لكن הפרק לראשוניים של  $ab$  הוא  $p_1^{e_1}p_2^{e_2}$  כאשר  $b = ab = p_1^{e_1}p_2^{e_2}$  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 הפרק לראשוניים של  $a$  הוא  $\prod_{i=1}^n p_i^{e_i}$ . אז מספר האיברים עבורם  $\gcd(a, m) = 1$  ניתן ע"י הנוסחה

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

$$\mathbb{Z}_{200} \quad (\text{א})$$

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

לכן

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

$$\mathbb{Z}_{400} \quad (\text{ב})$$

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

לכן

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

$$\mathbb{Z}_{1000} \quad (\text{ג})$$

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

לכן

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

$$\mathbb{Z}_{263} \quad (\text{ד})$$

シימו לב 263 הוא מספר ראשוני ולכן הפרק לראשוניים שלו הוא  $263^1$  ו-

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

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

$$\mathbb{Z}_{2521} \quad (\text{ה})$$

シימו לב 2521 הוא מספר ראשוני ולכן הפרק לראשוניים שלו הוא  $2521^1$  ו-

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

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

**שאלה 4**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

לפי

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

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

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

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

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

לפי

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

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 האחורונה:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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 אוקליד המוכפל כדי למצוא שלמים  $s, t, d$  עבורם  $.26s + 19t = d$

### השיטה של האלגוריתם אוקליד המוכפל

$$.a = 26, b = 19$$

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

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

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

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

$$.19^{-1} \in \mathbb{Z}_{26} \text{ ולכון קיימים } d = \gcd(26, 19) = 1 \text{ נ"מ}$$

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

■

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

### פתרונות עם השיטה השנייה של האלגוריתם אוקליד המוכפל

לשיטתה הזאת יש 2 שלבים. בשלב הראשון מבצעים האלגוריתם של אוקלייד במשפט ??.

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

$$\text{לכן } d = \gcd(26, 19) = 1$$

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

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

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

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

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

■

## שאלה 7 הצופן האפיני מעל $\mathbb{Z}_m$ מכיל כלל מצפין

$$e_k(x) = ax + b \pmod{m}$$

והכלל המפענה

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

הכלל מצפין  $e_k(x)$  הפיך, כלומר קיים כלל מפענה  $d_k(y) = a^{-1}(y - b) \pmod{m}$  אם ורק אם קיים איבר הופכי  $a^{-1}$  כך ש  $\gcd(a, m) = 1$ .

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 הfonkציות אוילר

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

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

$$\text{לכן } 30 = 2^1 \times 3^1 \times 5^1 \quad (\text{א})$$

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

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

$$5^2 \times 100 = 2^2 \text{ לכן} \quad (\text{ב})$$

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

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

$$1225 = 5 \times 245 = 5^2 \times 49 = 5^2 \times 7^2 \quad (\text{ג})$$

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

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

### שאלה 8

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

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

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

$$\text{לכן } 7^{-1} \equiv 3 \pmod{20}$$