

# הרצאה 3

## חבורת אוילר (Euler)

הגדרה

שני מספרים שלמים  $a, b$  יקראו זרים  $\Leftrightarrow (a, b) = 1$ .

משפט

$$(m, n) = 1 \Leftrightarrow \exists k_1, k_2 \in \mathbb{Z} : k_1 m + k_2 n = 1$$

הוכחה

הכיוון  $\Rightarrow$  נובע ממשפט כללי יותר שהוכחנו

בכיוון  $\Leftarrow$  נניח

$$\exists k_1, k_2 \in \mathbb{Z} : k_1 m + k_2 n = 1$$

ונניח  $(m, n) = d$

אזי

$$d|m \wedge d|n \Rightarrow d|(k_1 m + k_2 n) \Rightarrow d|1 \Rightarrow d = 1$$

טענה

כל שתי מספרים טבעיים עוקבים זרים זה לזה

הוכחה

$$1(n+1) - 1n = 1 \Rightarrow (n+1, n) = 1$$

מסקנה

יש אינסוף מספרים ראשוניים

נניח בשלילה כי קבוצת המספרים הראשוניים סופית.

נסמן את מכפלת כל הראשוניים האלו ב- $n$ . לפי הטענה הנ"ל,  $n+1$  זר ל- $n$  כלומר אין להם מחלקים משותפים גדולים מ-1 לפיכך בפירוק של  $n+1$  לגורמים ראשוניים בהכרח יופיעו מספרים ראשוניים אחרים מהרשימה הנ"ל, סתירה.

טענה

איבר  $m \in \mathbb{Z}_n$  הוא הפיך לגבי כפל מודולו  $\Leftrightarrow (m, n) = 1$

הוכחה

$$(m, n) = 1 \Leftrightarrow \exists k_1, k_2 \in \mathbb{Z} : k_1 m + k_2 n = 1 \Leftrightarrow \exists k_1 \in \mathbb{Z} k_1 m = 1 \pmod n$$

הגדרה

חבורת אוילר היא קבוצת ההפיכים ב- $\mathbb{Z}_n$  לגבי כפל מודולו  $n$

$$U_n := Gr(\mathbb{Z}, * \pmod n)$$

דוגמא

$$\langle 3 \rangle = \{1, 3, 9, 7\} \text{ - צקלית כי } U_{10} = (\{1, 3, 7, 9\}, * \pmod{10})$$

$$U_8 = \{1, 3, 5, 7\} \text{ לא צקלית}$$

תרגיל

חשב את  $90^{-1} \pmod{143}$

פתרון

ע"פ אלגוריתם אוקלידס כאשר תחילה נראה כי  $(143, 90) = 1$ , נשחזר את המקדמים כך ש:

$$143 * 17 - 90 * 24 = 1$$

$$\text{ולכן } 90^{-1} = -27 \pmod{143} = 116 \pmod{143}$$

טענה

$$\begin{cases} a \equiv b \pmod{n} \\ c \equiv d \pmod{n} \end{cases} \Rightarrow \begin{cases} ac \equiv bd \pmod{n} \\ a + c \equiv (b + d) \pmod{n} \end{cases}$$

הוכחה

$$\exists k_1 \in \mathbb{Z} : a = k_1 n + b$$

$$\exists k_2 \in \mathbb{Z} : c = k_2 n + d$$

כאשר מכפילים מודולו או מחברים מודולו את a, b כל מכפלה של n מצטמצמת.

תרגיל

פתור את המשוואה  $3x = 55 \pmod{2000}$

פתרון

$$3 * 667 = 2001 = 1 \pmod{2000}$$

$$\Rightarrow 3 * \underbrace{667 * 55}_x = 55 \pmod{2000}$$

משפט השאריות הסיני CRT

תהא  $\{m_1, \dots, m_k\}$  קבוצת מספרים טבעיים הזרים זה לזה.

נסמן את מכפלתם ב-m. בהינתן קבוצה כלשהי של שאריות  $\{a_i \pmod{m_i}\}$  קיימת שארית יחידה  $x \pmod{m}$

$$\begin{cases} x = a_1 \pmod{m_1} \\ x = a_2 \pmod{m_2} \\ \dots \\ x = a_k \pmod{m_k} \end{cases}$$
 המהווה פתרון למערכת המשוואות

דוגמא

$$\begin{cases} x = 1 \pmod{4} \\ x = 2 \pmod{7} \\ x = 3 \pmod{15} \end{cases}$$
 מצא פתרון למערכת למערכת

הוכחת המשפט

נבנה בסיס של שאריות  $\{e_1, \dots, e_k\}$  כך ש

$$\forall i, j : e_i = \delta_{ij} \pmod{m_j} = \begin{cases} 0 & i \neq j \\ 1 & i = j \end{cases}$$

ואז

$$x = a_1 e_1 + \dots + a_k e_k$$

הבנייה של  $\{e_k\}$  תעשה בצורה הבאה:

לכל  $1 \leq i \leq k$  נגזיר  $n_i = \frac{m}{m_i}$ . כיוון שכל  $m_i$  זרים אחד לשני, נקבל  $(n_i, m_i) = 1$ , מכאן ש:

$$\exists s_i, r_i \in \mathbb{Z} : s_i n_i + r_i m_i = 1$$

נגדיר  $e_i := s_i n_i$  ונקבל  $e_i = 1 \pmod{m_i}$

כמו כן לכל  $i \neq j$   $m_j | n_i$  ולכן  $e_i = 0 \pmod{m_j}$ , כדרוש, נניח כי קיים פתרון אחר  $y$

אז מתוך מערכת המשוואות נקבל  $\forall i : m_i | (x - y)$

אבל כל  $\{m_i\}$  זרים אחד לשני ולכן  $m | (x - y)$  ומכאן  $x = y \pmod{m}$

### הגדרה

תהינה  $H, K$  חבורות עם איברים נטרליים  $e_H, e_K$

המכפלה הישרה  $H$ -ו- $K$  היא הקבוצה של הזוגות הסדורים

$$H \times K = \{(h, k) : h \in H, k \in K\}$$

$$(h_1, k_1) * (h_2, k_2) = (h_1 h_2, k_1 k_2)$$

$H \times K$  היא חבורה.

### דוגמא

$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \langle (1, 1) \rangle = \{(0, 0), (1, 1), (0, 2), (1, 0), (0, 1), (1, 2)\}$$

### הגדרה

העתקה בין מונואידים  $\varphi: (G, *) \rightarrow (H, *)$  היא הומומורפיזם אם היא משמרת פעולה

$$\forall a, b \in G : \varphi(ab) = \varphi(a)\varphi(b)$$

- אם  $\varphi$  היא חח"ע אז היא נקראת מונומורפיזם.
- אם  $\varphi$  היא על אז היא נקראת אפימורפיזם.
- אם  $\varphi$  היא חח"ע ועל אז היא נקראת אזומורפיזם.

### דוגמאות

1.  $\varphi: \mathbb{Z} \rightarrow \mathbb{Z} \quad x \mapsto 2x$  – מונומורפיזם

2.  $\varphi: U_{10} \rightarrow \langle 9 \rangle \quad x \mapsto x^2$  – אפימורפיזם

$$\text{Im}(\varphi) = \{1, 9\} = \langle 9 \rangle$$

3.

$$\varphi: (\mathbb{R}, +) \rightarrow ((0, \infty), *) \quad x \mapsto 2^x$$

$$\varphi(x + y) = 2^{x+y} = \varphi(x)\varphi(y)$$

$$G \cong H$$

### טענה

אם  $f: G \rightarrow H$  ההומומורפיזם של חבורות אזי

$$f(1_G) = 1_H \quad (1)$$

$$f(x^{-1}) = f(x)^{-1} \quad \text{אם } x \text{ הפיך ב-} G \quad (2)$$

### הוכחה

$$f(1_G) = f(1_G 1_G) = f(1_G) f(1_G) \Rightarrow f(1_G) = 1_H \quad (1)$$

$$1_H = f(1_G) = f(xx^{-1}) = f(x) f(x^{-1}) \Rightarrow f(x^{-1}) = f(x)^{-1} \quad (2)$$

### מסקנה

בהינתן איזומורפיזם של מונואידים  $G \cong H$  נקבל איזומורפיזם של חבורות  $Gr(G) \cong Gr(H)$

### טענה

אם  $(n, m) = 1$  אזי  $\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m$  וזהו איזומורפיזם של חוגים (לגבי שתי הפעולות).

### דוגמא

$$\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$$

### הוכחה

נסמן  $\varphi: \mathbb{Z}_{nm} \rightarrow \mathbb{Z}_n \times \mathbb{Z}_m$  ע"י:

$$\varphi(x) = (x \bmod n, x \bmod m)$$

$$\varphi(x + y) = ((x + y) \bmod n, (x + y) \bmod m) = (x \bmod n, x \bmod m) + (y \bmod n, y \bmod m)$$

וכנ"ל לגבי כפל.

תכונות החזקה ועל של  $\varphi$  נובעות כעת מהזרות של  $n, m$  יחס עם משפט השאריות הסיני, שאומר שלכל 2 שאריות  $a_1 \bmod n, a_2 \bmod m$  קיים פתרון  $x$  יחיד בתוך  $\mathbb{Z}_{nm}$ .

### הגדרה

לכל מספר טבעי  $n$  נגדיר את פונקציית אוילר.

$$\varphi(n) = |U_n|$$

### לדוגמא

אם  $p$  מספר ראשוני אזי  $\varphi(p) = p - 1$

$\varphi(p^k) = ?$  מיהם המספרים  $1 \leq m \leq p^k$  שאינם זרים ל- $p$ ?

$$|\{p, 2p, \dots, p^2, 2p^2, \dots, p^k\}| = p^{k-1}$$

$$\varphi(p^k) = p^k - p^{k-1}$$

### טענה

אם  $(n, m) = 1$  אז  $\varphi(nm) = \varphi(n)\varphi(m)$

הוכחה

$$\varphi(nm) = |U_{nm}| = |Gr(\mathbb{Z}_{nm})| = |Gr(\mathbb{Z}_n \times \mathbb{Z}_m)| = |Gr(\mathbb{Z}_n)||Gr(\mathbb{Z}_m)| = \varphi(n)\varphi(m)$$

מסקנה – נוסחה לחישוב פונקציית אוילר

בהינתן פירוק של  $n = \prod_{i=1}^k p_i^{\alpha_i}$

$$\varphi(n) = \varphi\left(\prod_{i=1}^k p_i^{\alpha_i}\right) = \prod_{i=1}^k \varphi(p_i^{\alpha_i}) = \prod_{i=1}^k (p_i^{\alpha_i} - p_i^{\alpha_i-1}) = \prod_{i=1}^k \left(p_i^{\alpha_i} \left(1 - \frac{1}{p_i}\right)\right) = n \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right)$$

לדוגמא

$$\varphi(160) = \varphi(2^5 * 5) = 160 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 64$$