

# תרגול מס' 2 במבנים אלגבריים 1

## מבוא לתורת המספרים

**הגדרה:** בהינתן שני מספרים טבעיים, הממג"ב הוא המחלק המשותף הגדול ביותר של שני המספרים.

כלומר:  $(a, b) = n \Leftrightarrow n = \max\{m : m|a \wedge m|b\}$ . למשל:  $\gcd(6, 10) = 2$ .

**הגדרה:** בהינתן שני מספרים טבעיים, הכמק"ב הוא הכפולה המשותפת הקטנה ביותר של שני

המספרים. כלומר:  $[a, b] = n \Leftrightarrow n = \min\{m : a|m \wedge b|m\}$ . למשל:  $[6, 10] = 30$ .

דרך קלה לחשב את הממג"ב ואת הכמק"ב של שני מספרים הוא להיעזר בפירוק שלהם למס' ראשוניים.

כלומר אם:  $a = \prod_{i=1}^{\infty} p_i^{\alpha_i} = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots$  ו-  $b = \prod_{i=1}^{\infty} p_i^{\beta_i} = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \dots$

אזי הממג"ב הוא:  $(a, b) = \prod_{i=1}^{\infty} p_i^{\min(\alpha_i, \beta_i)}$  והכמק"ב הוא:  $[a, b] = \prod_{i=1}^{\infty} p_i^{\max(\alpha_i, \beta_i)}$

**הערה:** עפ"י הדרך הנ"ל קל לראות כי מתקיים:  $\forall a, b \in \mathbb{Z} : [a, b] \cdot (a, b) = |a \cdot b|$ .

## אלגוריתם אוקלידס למציאת ממג"ב:

$$\begin{aligned}
 a &= bq_1 + r_1 \\
 b &= r_1q_2 + r_2 \\
 r_1 &= r_2q_3 + r_3 \\
 &\dots \\
 r_{k-2} &= r_{k-1}q_k + r_k \\
 r_{k-1} &= r_kq_{k+1}
 \end{aligned}$$

יהיו  $a, b \in \mathbb{Z}$ . נחשב:

ואז:  $(a, b) = r_k$ .

הוכחה: השאריות הולכות וקטנות. כיוון שהן אי-שליליות, התהליך חייב להסתיים בשלב מסוים.

מתוך המשוואה האחרונה נסיק כי:  $r_k | r_{k-1}$ . לכן בתוספת המשוואה הלפני האחרונה נקבל כי:  $r_k | r_{k-2}$ .

כך נמשיך ונקבל ש:  $r_2 | r_1, r_k | r_1$  ולכן גם:  $r_k | b$  ולכן עפ"י המשוואה הראשונה גם:  $r_k | a$ .

נותר להראות מקסימליות של  $r_k$ . נניח באופן כללי כי  $t|a$  וגם  $t|b$ . נרצה להראות כי:  $t \leq r_k$ .

$$\begin{aligned} t|(a - bq_1) &= r_1 \\ t|(b - r_1q_2) &= r_2 \\ \text{אכן: } t|(r_1 - r_2q_3) &= r_3 \\ &\dots \\ t|r_k &\Rightarrow t \leq r_k \end{aligned}$$

אם כן נוכל לייצג כל שארית ע"י שאריות קדומות יותר וכך להגיע בסופו של דבר לקומבינציה לינארית של  $a, b$  באמצעות מספרים שלמים שתהיה שווה ל- $(a, b)$ .

$$\begin{aligned} 133 &= 1 \cdot 95 + 38 \\ 95 &= 2 \cdot 38 + 19 & \text{ :דוגמה: נחשב את: } (133, 95) \\ 38 &= 2 \cdot 19 \end{aligned}$$

ולכן:  $(133, 95) = 19$ .

**תרגיל:** חשבו את  $(1488, 1368)$  ומצאו שלמים  $s$  ו- $t$  כך ש-  $(1488, 1368) = 1488s + 1368t$ .

**פתרון:** באמצעות אלגוריתם אוקלידס מקבלים כי:  $(1488, 1368) = 24 = 23 \cdot 1488 - 25 \cdot 1368$ .

**משפט:**  $(m, n) = d \Rightarrow \exists k_1, k_2 \in \mathbb{Z} \mid k_1m + k_2n = d$  (נובע ישירות מאלגוריתם אוקלידס).

**הערה:**  $(m, n) = 1 \Leftrightarrow \exists k_1, k_2 \in \mathbb{Z} \mid k_1m + k_2n = 1$ .

**הוכחה:** עבור הכיוון  $(\Rightarrow)$  - נובע מהמשפט.

עבור  $(\Leftarrow)$ : נתון  $\exists k_1, k_2 \in \mathbb{Z} \mid k_1m + k_2n = 1$ . נניח:  $(m, n) = d$ . אזי:

$$(m, n) = d \Rightarrow d|m \wedge d|n \Rightarrow d|k_1m + k_2n = 1 \Rightarrow d|1 \Rightarrow d = 1$$

**תרגיל:** הוכח כי כל שני מספרים עוקבים זרים זה לזה.

**פתרון:** צ"ל:  $(n, n-1) = 1$ .  $\forall n > 1$ . הוכחה:  $n - (n-1) = 1$  כלומר  $k_1 = 1, k_2 = -1$ .

**הגדרה:** החבורה:  $U_n = (\{1 \leq m \leq n \mid \gcd(m, n) = 1\}, \cdot, (\text{mod } n))$  נקראת "חבורת אוילר".

**הערה:** ראינו בתרגול הקודם כי לכל שתי חבורות מסדר 2 או 3 יש את אותו לוח הכפל, כלומר כל החבורות מסדר 2 הן איזומורפיות, וכן כל החבורות מסדר 3 הן איזומורפיות. התכונה הזו כבר לא מתקיימת עבור חבורות מסדר 4, לדוגמא:  $U_8 \not\cong U_{10}$  למרות ששתי החבורות הן בנות 4 איברים.

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

$$\begin{aligned} a \equiv b \pmod{n} &\Rightarrow \exists k_1 \in \mathbb{Z} \mid a = k_1n + b \\ c \equiv d \pmod{n} &\Rightarrow \exists k_2 \in \mathbb{Z} \mid c = k_2n + d \end{aligned} \quad \text{פתרון: נשים לב כי:}$$

$$. ac = (k_1n + b) \cdot (k_2n + d) = k_1k_2n^2 + dk_1n + bk_2n + bd \equiv bd \pmod{n} \quad \text{ולכן:}$$

$$. a + c = k_1n + b + k_2n + d \equiv b + d \pmod{n} \quad \text{כמו כן:}$$

$$. a \equiv b \pmod{n} \Rightarrow \forall m \in \mathbb{N}: a^m \equiv b^m \pmod{n}, ma \equiv mb \pmod{n} \quad \text{מסקנה:}$$

**תרגיל:** חשב את  $177^{-1}$  ב-  $\mathbb{Z}_{661}$  (אם קיים).

**פתרון:** נוודא תחילה כי 177 ו-661 אכן זרים עפ"י אלגוריתם אוקלידס, ואז נשחזר את המקדמים כך ש-

$$. b \equiv 177^{-1} \pmod{661} \quad \text{ומכאן ש: } a * 661 + b * 177 = 1$$

**תרגיל:** פתור את המשוואות:

$$. \text{א. } 7x = 12 \text{ ב- } \mathbb{Z}_{34}$$

$$. \text{ב. } 3x = 55 \text{ ב- } \mathbb{Z}_{2000}$$

**פתרון:** א. נשים לב כי:  $(7, 34) = 1$  לכן 7 הפיך ב- $\mathbb{Z}_{34}$ . עפ"י אלגוריתם אוקלידס נמצא כי:  $7^{-1} = 5$ .

$$\begin{aligned} 5 \cdot 7 &\equiv 1 \pmod{34} \Rightarrow 5 \cdot 7 \cdot 12 \equiv 12 \pmod{34} \\ \Rightarrow 60 \cdot 7 &\equiv 12 \pmod{34} \Rightarrow 26 \cdot 7 \equiv 12 \pmod{34} \end{aligned}$$

מכאן נקבל:

$$\begin{aligned} 3 \cdot 667 &= 2001 \equiv 1 \pmod{2000} \Rightarrow 3 \cdot 667 \cdot 55 \equiv 55 \pmod{2000} \\ \Rightarrow 3 \cdot 667 \cdot 55 &\equiv 55 \pmod{2000} \Rightarrow 3 \cdot 685 \equiv 55 \pmod{2000} \end{aligned}$$

ב.

**תרגיל:** חשב את שארית החלוקה של  $2^{1000}$  ב-7.

$$2^{1000} = 2^{3 \cdot 333 + 1} = (2^3)^{333} \cdot 2 \equiv 1 \cdot 2 \pmod{7} \equiv 2 \pmod{7}$$

**פתרון:**

**תרגיל:** חשב את הספרה האחרונה של המספר  $333^{333}$ .

$$333^{333} = (3 \cdot 111)^{333} = 3^{333} \cdot 111^{333} \equiv 3^{333} = (3^4)^{83} \cdot 3 = (81)^{83} \cdot 3 \equiv 3 \pmod{10}$$

**פתרון:**