

מבנים אלגבריים

תרגיל בית 2*

1 תורת המספרים השלמים

טענות שימושיות:

• אלגוריתם אוקלידס.

$$\bullet \gcd(m, n) = (m, n) = \max \{d \in \mathbb{Z} : d \mid m \wedge d \mid n\}$$

• $\gcd(m, n)$ ניתן להצגה כצירוף לינארי של m ו- n עם מקדמים שלמים. יתר על כן, מבין הצירופים הלינאריים האלה שערכם חיובי, הממג"ב הוא מינימלי. בנוסחא:

$$\gcd(m, n) = \min \{sm + tn : s, t \in \mathbb{Z}, sm + tn > 0\}$$

1. יהי d מספר טבעי. הוכיחו: $d = \gcd(m, n)$ א.ס.ס. d מחלק משותף של m ו- n וגם צירוף לינארי שלהם. ובנוסחא:

$$d = \gcd(m, n) \iff (d \mid m) \wedge (d \mid n) \wedge (\exists s, t \in \mathbb{Z}, sm + tn = d)$$

פתרון (\Leftarrow). הממג"ב הוא מחלק משותף לפי הגדרתו, וטענו קודם כבר שהוא ניתן להצגה כצירוף לינארי.

(\Rightarrow). נניח $d = sm + tn$ וגם d מחלק משותף שלהם. מכיוון שהממג"ב הוא הצ"ל החיובי המינימלי והמ"מ המקסימלי, יש רק מספר אחד שיכול לקיים את שניהם, וזהו הממג"ב. d מקיים את שניהם, ולכן הוא הממג"ב בעצמו. ■

2. פתרו את התרגילים הבאים (אין להשתמש במחשבון):

(א) $6 + 5 \cdot 7 \pmod{11}$

(ב) $-5 - 6 \cdot 18 \pmod{11}$

(ג) $7^{14} \pmod{5}$

(ד) $7^{14} \pmod{6}$

* להגשה עד ט"ו בכסלו (7 דצמ').

פתרון

(א) נחשב:

$$6 + 5 \cdot 7 \equiv 6 + 35 \equiv 6 + 2 \equiv 8 \pmod{11}$$

(ב) מתקיים $(\text{mod } 11)$ $18 \equiv 7$, $-6 \equiv 5$, $-5 \equiv 6$, ולכן זה בדיוק כמו סעיף (א).
(ג) $7^{14} \equiv 2^{14} \pmod{5}$. כעת נחפש מה הסדר של 2 ב- U_5 . $2^1 = 2, 2^2 = 4, 2^3 = 8 = 3, 2^4 = 16 = 1$
כך:

$$7^{14} \equiv 2^{14} = 2^{3 \cdot 4 + 2} = (2^4)^3 2^2 \equiv 1^3 \cdot 2^2 = 1 \cdot 4 = 4 \pmod{5}$$

(ד)

$$7^{14} \equiv 1^{14} = 1 \pmod{6}$$



3. מצאו מספרים שלמים m, n שיקיימו

(א) $\text{gcd}(81, 42) = 81n + 42m$

(ב) $\text{gcd}(81, 43) = 81n + 43m$

(ג) $\text{gcd}(30, 455) = 30n + 455m$

פתרון נחשב כל סעיף בעזרת אוקלידס.

(א)

$$81 = 1 \cdot 42 + 39$$

$$42 = 1 \cdot 39 + 3$$

$$39 = 13 \cdot 3$$

ולכן $\text{gcd}(81, 42) = 3$ כעת,

$$3 = 42 - 39 = 42 - (81 - 42) = (-1) \cdot 81 + 2 \cdot 42$$

(ב)

$$81 = 1 \cdot 43 + 38$$

$$43 = 1 \cdot 38 + 5$$

$$38 = 7 \cdot 5 + 3$$

$$5 = 1 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

ולכן הם זרים.

$$\begin{aligned} 1 &= 3 - 2 = 3 - (5 - 3) = 2 \cdot 3 - 5 = 2(38 - 7 \cdot 5) - 5 = 2 \cdot 38 - 15 \cdot 5 \\ &= 2 \cdot 38 - 15(43 - 38) = 17 \cdot 38 - 15 \cdot 43 = 17(81 - 43) - 15 \cdot 43 \\ &= 17 \cdot 81 + (-32) \cdot 43 \end{aligned}$$

(ג)

$$\begin{aligned} 455 &= 15 \cdot 30 + 5 \\ 30 &= 6 \cdot 5 \end{aligned}$$

אם כן, הממג"ב הוא 5, ומתקיים $5 = 1 \cdot 455 + (-15) \cdot 30$ ■

4. נניח כי d הוא מחלק משותף של a ו- b . הוכיחו: $d = \gcd(a, b)$ א.ס.מ. $1 = \gcd\left(\frac{a}{d}, \frac{b}{d}\right)$.

רמז: היעזרו בשאלה 1.

פתרון (\Leftarrow). נניח כי $d = \gcd(a, b)$. לכן קיימים s, t שלמים שיקיימו $sa + tb = d$. נחלק משוואה זו ב- d , ונקבל $s\frac{a}{d} + t\frac{b}{d} = 1$. אם כן, 1 הוא צירוף לינארי של $\frac{a}{d}$ ו- $\frac{b}{d}$, ולכן הם זרים, כנדרש.

(\Rightarrow). נניח $1 = \gcd\left(\frac{a}{d}, \frac{b}{d}\right)$. נזכיר כי נתון ש- d הוא מחלק משותף של a ו- b , ולכן כל שנותר הוא להראות שאין גדול ממנו. לפי הנתון, קיימים s, t שלמים שיקיימו $s\frac{a}{d} + t\frac{b}{d} = 1$. נכפיל משוואה זו ב- d ונקבל $sa + tb = d$. מצאנו אפוא כי d הוא צירוף לינארי של a, b וגם מחלק משותף שלהם, ולכן הוא ממג"ב (שאלה 1). ■

5. נביט ב- \mathbb{Z}_n עם פעולת הכפל. מצאו מי מבין האיברים הבאים הוא הפיך במונואיד זה, וחשבו את ההופכי.

(א) $15 \in \mathbb{Z}_{42}$

(ב) $17 \in \mathbb{Z}_{59}$

(ג) $35 \in \mathbb{Z}_{52}$

פתרון נבדוק בכל פעם אם האיבר זר ל- n . אם לא – האיבר איננו הפיך. אם כן – נחשב את ההפיך בעזרת אלגוריתם אוקלידס.

(א) $(15, 42) = 3 \neq 1$, ולכן 15 איננו הפיך.

(ב) 59 הוא ראשוני, וכל האיברים שאינם מתחלקים בו זרים אליו. לכן 17 הפיך. נפנה לאלגוריתם אוקלידס המתאים:

$$59 = 3 \cdot 17 + 8$$

$$17 = 2 \cdot 8 + 1$$

¹ לא אמרנו מקסימלי, נתון בשה"כ כי $d \mid a \wedge d \mid b$.

הגענו ל-1, כעת נחשב אחורנית:

$$1 = 17 - 2 \cdot 8 = 17 - 2(59 - 3 \cdot 17) = 7 \cdot 17 - 2 \cdot 59$$

קיבלנו $7 \cdot 17 = 1 \pmod{59}$, ולכן 7 הוא ההפיד.

(ג) ניתן להראות שהגורמים של 35 אינם הגורמים של 52. מכיוון שבסוף נצטרך לחשב אוקלידס, נחשב כך את הממג"ב.

$$52 = 1 \cdot 35 + 17$$

$$35 = 2 \cdot 17 + 1$$

הגענו ל-1, ולכן הם זרים וקיים הופכי. נחשבו:

$$1 = 35 - 2 \cdot 17 = 35 - 2(52 - 35) = 3 \cdot 35 - 2 \cdot 52$$

ולכן 3 הוא ההופכי ל-35 ב- \mathbb{Z}_{52} . ■

6. יהיו a, b, c מספרים שלמים המקיימים $a \mid c, b \mid c, a \mid b$ וכן $(a, b) = 4$. הוכיחו כי $4c \mid ab$.

פתרון נמיר את הנתונים למשוואות: קיימים s, t, m, n שלמים כך ש-

$$sa + tb = (a, b) = 4 \quad (1)$$

$$am = c \quad (2)$$

$$bn = c \quad (3)$$

כעת,

$$4c \stackrel{(1)}{=} (sa + tb)c = sac + tbc \stackrel{(2),(3)}{=} sabn + tbam = ab(sn + tm)$$

אם כן, מצאנו $4c = ab(sn + tm)$, ולכן $4c \mid ab$. ■

2 סדר של איבר, סדר של חבורה

7. תהי G חבורה, ויהי $g \in G$. הוכיחו כי $o(g) = o(g^{-1})$.

פתרון נראה ראשית כי $g^n = e$ א.ס.ס. $(g^{-1})^n = e$. ואכן,

$$g^n = e \iff (g^n)^{-1} = e^{-1} = e \iff (g^{-1})^n = e$$

מצאנו כי הקבוצות $\{n \in \mathbb{N} : g^n = e\}$ ו- $\{n \in \mathbb{N} : (g^{-1})^n = e\}$ שוות זו לזו. בפרט, המינימום שלהן שווה (אם הוא מוגדר; כאשר המינימום אינו מוגדר שתי הקבוצות ריקות, והסדר הוא ∞). ■

8. חשבו מהו סדרו של כל איבר בחבורות הבאות:

(א) \mathbb{Z}_{10} עם פעולת החיבור.

(ב) U_9 עם פעולת הכפל.

פתרון

(א) $\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ מחפשים, לכל איבר בחבורה, k מינימלי (טבעי) כך ש- $nk = 0$. עבור $n = 0$ ברור ש- $k = 1$, ולכן $o(0) = 1$. בהמשך החישוב נגלה ש-

$$o(2) = o(4) = o(6) = o(8) = 5, o(1) = o(3) = o(7) = o(9) = 10, o(5) = 2$$

שימו לב לכך שהסדר המקסימלי מתקבל באיברי U_{10} .

(ב)

$$U_9 = \{1, 2, 4, 5, 7, 8\}$$

לפי שאלה 7, הסדר של איבר שווה לסדר של ההופכי לו. לכן כאשר נמצא תוך כדי החישוב איבר הופכי, לא נחשב בעבורו את הסדר בשנית.

$1^1 = 1$					
$2^1 = 2$	$2^2 = 4$	$2^3 = 8$	$2^4 = 16 = 7$	$2^5 = 32 = 5$	$2^6 = 64 = 1$
$4^1 = 4$	$4^2 = 16 = 7$	$4^3 = 64 = 1$			
5 הוא ההפיך של 2, כי הוא האיבר לפני האחרון בשורה של 2. לכן הוא מאותו סדר.					
7 הוא ההפיך של 4, כי הוא האיבר לפני האחרון בשורה של 4. לכן הוא מאותו סדר.					
$8^1 = 8$	$8^2 = 64 = 1$				

לסיכום התוצאות, $o(1) = 1$, $o(2) = o(5) = 6$, $o(4) = o(7) = 3$, $o(8) = 2$ ■

בהצלחה!

² קיצור דרך למי שהקשיב בשיעורים הבאים: לפי משפט לגרנז', סדר אפשרי לאיבר בחבורה U_9 מחלק את סדר החבורה, 6. הסדרים האפשריים הם, אפוא, 1, 2, 3, 6, ואין צורך להעלות את 2 בחזקת 4 או בחזקת 5.