

## פתרון תרגיל בית 5 במבנים אלגבריים 89-214 סמסטר א' תשע"ט

**שאלה 1** (חימום). יהי  $n$  מספר טבעי. נגדיר יחס על  $\mathbb{Z}$  לפיו  $a, b \in \mathbb{Z}$  שקולים בשארית חלוקה  $n$ -ב אם  $n|a-b$ , ונסמן יחס זה כ- $a \equiv b \pmod{n}$ . הוכיחו כי שקילות מודולו  $n$  היא אכן יחס שקילות (כלומר יחס רפלקסיבי, סימטרי וטרנזיטיבי).

פתרון. היחס רפלקסיבי כי לכל  $a \in \mathbb{Z}$  מתקיים כי  $n|0$ . לכן  $n|a-a$ , כלומר  $a \equiv a \pmod{n}$ . היחס סימטרי כי אם  $n|x$ , אז גם  $n|-x$ . בפרט

$$a \equiv b \pmod{n} \Leftrightarrow n|(a-b) \Leftrightarrow n|(b-a) \Leftrightarrow b \equiv a \pmod{n}$$

היחס טרנזיטיבי כי אם  $n|x$  וגם  $n|y$ , אז  $n|x+y$ . בפרט אם  $a \equiv b \pmod{n}$  וגם  $b \equiv c \pmod{n}$ , אז

$$n|(a-b) \wedge n|(b-c) \Rightarrow n|(a-b+b-c) \Rightarrow n|(a-c)$$

כלומר  $a \equiv c \pmod{n}$ .

**שאלה 2.** תהינה  $G, H$  חבורות, ויהיו  $g \in G, h \in H$  איברים מסדר סופי. נסתכל על האיבר  $(g, h) \in G \times H$ . הוכיחו  $[o(g), o(h)] = o((g, h))$ . כלומר הוכיחו שהסדר של  $(g, h)$  הוא הכפולה המשותפת המינימלית של  $o(g)$  ו- $o(h)$ . נסו להוכיח זאת פעם אחת כמסקנה ישירה מטענה בכיתה, ופעם שנייה לבד.

פתרון. נסמן  $m = o(g), n = o(h), k = [m, n]$ . צריך להראות שני דברים: היתכנות, כלומר  $(g, h)^k = (e_G, e_H)$  ומינימליות, כלומר אם  $(g, h)^t = (e_G, e_H)$ , אז  $k \leq t$  (אנחנו נראה  $k|t$  שזה יותר קל להוכיח).

לפי הגדרת כמ"מ מתקיים  $k | m$  ו- $k | n$ . כלומר  $\frac{k}{m}, \frac{k}{n} \in \mathbb{Z}$ . לכן

$$(g, h)^k = (g^k, h^k) = \left( (g^m)^{\frac{k}{m}}, (h^n)^{\frac{k}{n}} \right) = (e_G, e_H)$$

עבור המינימליות, נניח כי  $(g, h)^t = (e_G, e_H)$ . לכן, בפרט  $g^t = e_G$ ,  $h^t = e_H$ . לפי טענה שראינו בכיתה, נובע כי  $t | m = o(g)$  וגם  $t | n = o(h)$ . הוכחנו ש- $m | t$  וגם  $n | t$ , ולכן  $k = [m, n] | t$ , לפי תכונות הכמ"מ.

להוכחה כמסקנה מהטענה הכללית יותר שראינו בכיתה נשים לב כי  $o(g) = o((g, e_H))$  וגם  $o(h) = o((e_G, h))$ . מפני ש- $(g, e_H)$  ו- $(e_G, h)$  מתחלפים וקל לראות כי

$$\langle (g, e_H) \rangle \cap \langle (e_G, h) \rangle = \{(e_G, e_H)\}$$

אז  $o((g, h)) = [o((g, e_H)), o((e_G, h))] = [o(g), o(h)]$ .

**שאלה 3.** הוכיחו כי לכל  $a, n, m \in \mathbb{Z}$  מתקיים  $(an, am) = |a|(n, m)$ .

פתרון. נסמן  $d = (n, m)$ . בשורה אחת, שאינה הוכחה מלאה,

$$(an, am) = |a| \cdot d \Leftrightarrow \left(\frac{an}{d}, \frac{am}{d}\right) = |a| \Leftrightarrow |a| \left(\frac{n}{d}, \frac{m}{d}\right) = |a| \Leftrightarrow \left(\frac{n}{d}, \frac{m}{d}\right) = 1 \Leftrightarrow (n, m) = d$$

דרך אחרת, דו-כיוונית (ומפורטת יותר): מצד אחד, ישנם מספרים  $u, v$  כך שמתקיים  $(an, am) = uan + vam$ . ידוע כי  $d$  מחלק כל צירוף לינארי של  $n$  ו- $m$ , ובפרט את  $uan + vam$ . לכן  $|a| \cdot d$  מחלק את  $uan + vam$ , ולכן  $(|a| \cdot d) | (an, am)$ . מצד שני, ישנם מספרים  $s, t$  כך שמתקיים  $d = sn + tm$ . נכפיל ב- $|a|$  ונקבל  $|a|d = s'an + t'am$ . ידוע כי  $(an, am)$  מחלק כל צירוף לינארי של  $an$  ו- $am$ , ובפרט את  $s'an + t'am$ . לכן  $(an, am) | |a|d$ . לסיכום קיבלנו  $(an, am) = |a|d$ , כדרוש. ניתן להוכיח את הטענה גם בעזרת שימוש בהצגה של ממ"מ כמכפלת חזקות ראשוניים. במקרה זה מוכיחים כי  $\min(n + a, m + a) = \min(n, m) + a$ , שהיא אנלוגית להוכחת  $(an, am) = |a|(n, m)$ .

**שאלה 4.** מצאו בעזרת אלגוריתם אוקלידס את הממ"מ הבאים:

א.  $(890, 214)$

ב.  $(4450, 1070)$ , רמז: העזרו בשאלה הקודמת.

פתרון.

א. נשתמש באלגוריתם אוקלידס:

$$(890, 214) = [890 = 4 \cdot 214 + 34]$$

$$(214, 34) = [214 = 6 \cdot 34 + 10]$$

$$(34, 10) = [34 = 3 \cdot 10 + 4]$$

$$(10, 4) = [10 = 2 \cdot 4 + 2]$$

$$(4, 2) = [4 = 2 \cdot 2 + 0]$$

$$(2, 0) = 2$$

ולכן  $(890, 214) = 2$ .

ב. נשים לב כי  $1070 = 5 \cdot 214$  וכן  $4450 = 5 \cdot 890$ . לכן לפי השאלה הקודמת

$$(4450, 1070) = |5| \cdot (890, 214) = 5 \cdot 2 = 10$$

**שאלה 5.** אלגוריתם אוקלידס עובד גם עם פרמטרים:

א. הוכיחו שלכל  $n$  שלם מתקיים  $(4n + 3, 7n + 5) = 1$ .

ב. מצאו  $s, t \in \mathbb{Z}$  (התלויים ב- $n$ ) כך ש- $(4n + 3)s + (7n + 5)t = 1$ .

פתרון.

א. נשתמש כמה פעמים בכך שאם  $n = qm + r$  אז  $(n, m) = (m, r)$

$$(7n + 5, 4n + 3) = [7n + 5 = 2 \cdot (4n + 3) + (-n - 1)]$$

$$(4n + 3, -n - 1) = [4n + 3 = -4 \cdot (-n - 1) - 1]$$

$$(-n - 1, -1) = 1$$

אפשר לעשות את החישוב בכמה דרכים, למשל כאשר נמנעים ממקדמים שליליים ל- $n$ :

$$\begin{aligned}(7n + 5, 4n + 3) &= [7n + 5 = 1 \cdot (4n + 3) + (3n + 2)] \\(4n + 3, 3n + 2) &= [4n + 3 = 1 \cdot (3n + 2) + (n + 1)] \\(3n + 2, n + 1) &= [3n + 2 = 3 \cdot (n + 1) - 1] \\(n + 1, -1) &= 1\end{aligned}$$

ב. משתמשים בשלבים של אלגוריתם אוקלידס המורחב, לפי הסעיף הקודם:

$$\begin{aligned}-n - 1 &= 1 \cdot (7n + 5) - 2 \cdot (4n + 3) \Rightarrow \\-1 &= 1 \cdot (4n + 3) + 4 \cdot (-n - 1) \\&= 4 \cdot (7n + 5) - 7 \cdot (4n + 3)\end{aligned}$$

ולכן נקבל  $s = 7, t = -4$ , שאינם תלויים ב- $n$ !

**שאלה 6.** מצאו את כל המספרים השלמים  $n$  כך ש- $(n^2 + 11) | (n + 1)$ . פתרו. נשים לב כי  $n + 1$  מחלק את עצמו, ואם הוא מחלק את  $n^2 + 11$ , הוא גם יחלק את הממ"מ שלהם (ולכן גם יחלק כל צירוף לינארי של  $n + 1$  ושל  $n^2 + 11$ ). בעזרת החישוב

$$n^2 + 11 = (n - 1) \cdot (n + 1) + 12$$

ושימוש בטענה שאם  $n = qm + r$ , אז  $(n, m) = (m, r)$ , נקבל

$$(n^2 + 11, n + 1) = (n + 1, 12)$$

כלומר מספיק למצוא את המספרים  $n$  כך ש- $12 | (n + 1)$ . המחלקים של 12 הם ידועים, ולכן המספרים המבוקשים הם  $11, 5, 3, 2, 1, 0, -2, -3, -4, -5, -7, -13$ . החישוב שעשינו היה למעשה

$$\frac{n^2 + 11}{n + 1} = \frac{n^2 - 1 + 12}{n + 1} = \frac{(n + 1)(n - 1)}{n + 1} + \frac{12}{n + 1} = (n - 1) + \frac{12}{n + 1}$$

ומפני ש- $n - 1$  הוא שלם, נותר לבדוק מתי  $\frac{12}{n + 1}$  שלם.

**שאלה 7** (רשות). תהינה תמורות  $\sigma, \tau \in S_n$ . הוכיחו שאם  $|\text{supp}(\sigma) \cap \text{supp}(\tau)| = 1$ , אז  $\sigma\tau\sigma^{-1}\tau^{-1}$  הוא מחזור מאורך 3.

רמז: הראו כי  $\text{supp}(\sigma^{-1}) = \text{supp}(\sigma)$  לכל תמורה ובדקו לאן נשלח המספר ששייך לחיתוך התומכים.

**שאלה 8** (רשות). בחרו שפת תכנות כרצונכם וכתבו פונקציה בשם `xgcd` המממשת את אלגוריתם אוקלידס המורחב. כלומר כתבו פונקציה המקבלת כקלט שני מספרים שלמים  $a, b$  ומחזירה שלשה של מספרים  $(d, s, t)$  כך שמתקיים  $d = (a, b) = sa + tb$ . הוסיפו את התוצאות של הרצת

$$\text{xgcd}(5779, 2018) \quad \text{xgcd}(437437, 142142) \quad \text{xgcd}(289214, -1414213)$$

הערה: בעוד ש- $d$  הוא יחודי, המקדמים  $s, t$  הם לא בהכרח יחודיים. לדוגמה  $\text{xgcd}(24, 44)$  תוכל להחזיר את השלשה  $(4, 2, -1)$  כי  $4 = 2 \cdot 24 - 1 \cdot 44$  אבל גם  $(4, 13, -7)$  זו תוצאה מותרת, ולכן יתכנו מימושים נכונים שונים. דוגמאות נוספות

$$\text{xgcd}(-5, 0) \rightarrow (5, -1, 0) \quad \text{xgcd}(100, 11) \rightarrow (1, 1, -9)$$

פתרון. נזכר כי באלגוריתם אוקלידס הרגיל מתחילים עם זוג מספרים  $(a, b)$  כשמניחים כי  $0 \leq b < a$ . אם  $b = 0$ , אזי  $(a, b) = a$ . אחרת נכתוב  $a = qb + r$  כאשר  $0 \leq r < |b|$  ונמשיך בשלב הבא עם חישוב  $(a, b) = (b, r)$ . בכל שלב באלגוריתם קיבלנו כי ניתן להציג את השארית  $r$  כצירוף לינארי  $r = a - qb$ .

באלגוריתם אוקלידס המורחב אנו שומרים בשלב מספר  $i$  את המקדמים  $s_i, t_i$  והשארית  $r_i$  כך שמתקיים  $r_i = s_i a + t_i b$ , שבעזרתם נביע לבסוף את  $d$  כצירוף לינארי. נניח ובשלב קודם באלגוריתם קיבלנו כי

$$r_{\text{prev}} = s_{\text{prev}}a + t_{\text{prev}}b$$

ובשלב הנוכחי  $r = sa + tb$ . נרצה לדעת מי יהיו המקדמים  $s_{\text{new}}, t_{\text{new}}$  לשלב הבא. נבצע חלוקה אוקלידית של השאריות מהשלב הקודם והשלב הנוכחי  $r_{\text{prev}} = qr + r_{\text{new}}$ . כעת נשתמש במשוואות לעיל ונקבל

$$r_{\text{new}} = r_{\text{prev}} - qr = (s_{\text{prev}}a + t_{\text{prev}}b) - q(sa + tb) = (s_{\text{prev}} - qs)a + (t_{\text{prev}} - qt)b$$

לכן

$$s_{\text{new}} = s_{\text{prev}} - qs \qquad t_{\text{new}} = t_{\text{prev}} - qt$$

האלגוריתם מתחיל בשלב שבו  $r_0 = a, r_1 = b$  כלומר

$$r_0 = a = s_0a + t_0b \qquad r_1 = b = s_1a + t_1b$$

$$.s_0 = 1, t_0 = 0, s_1 = 0, t_1 = 1$$

נציג פתרון איטרטיבי בפית'ון, ולאחריו נוסיף הערות על המימוש.

```

1 def xgcd(a, b):
2     """
3     Extended Euclidean algorithm
4
5     Returns (d, s, t) where 'd' is the greatest common
6     divisor of the integers 'a' and 'b' where the
7     numbers 's' and 't' are such that 'd = sa+tb'.
8     """
9     prev_r, r = a, b
10    prev_s, s = 1, 0
11    prev_t, t = 0, 1
12    while r:
13        q = prev_r // r
14        prev_s, s = s, prev_s - q*s
15        prev_t, t = t, prev_t - q*t
16        prev_r, r = r, prev_r - q*r
17
18    if prev_r < 0:
19        return (-prev_r, -prev_s, -prev_t)
20    else:
21        return (prev_r, prev_s, prev_t)

```

שורות 8–2 נועדו לתיעוד הפונקציה. בשורה 9, וגם בהמשך הקוד, מופיע שימוש בהשמה מקבילית (בפית'ון המינוח הוא tuple packing and sequence unpacking) ובו ב־זמנית מציבים ערכים בשני משתנים. הערכים באגף ימין בהשמה מקבילית מחושבים לפני ההשמה באגף שמאל.

בשורה 13 מופיע שימוש ב"חלוקת רצפה", המחזירה את המנה השלמה של שני מספרים. בשפות תכנות רבות זו החלוקה הרגילה. הלולאה שמתחילה בשורה 12 מבטיחה רק כי  $|r| \leq 0$ , ולא בהכרח  $r \leq 0$ . האלגוריתם עדין יעצר שכן  $|r_i|$  קטן. במקרה וקיבלנו  $a < b$ , האיטרציה הראשונה בלולאה תהפוך את הסדר שלהם (עד כדי שינוי בסימן, שאינו משפיע על הממ"מ). הבדיקה בשורה 18 מוודאת כי הממ"מ המתקבל הוא לא שלילי. פתרון רקורסיבי לבעיה בפיית'ון:

```

1 def rxgcd(a,b):
2     "Recursive version of xgcd."
3     if b == 0:
4         if a < 0:
5             return (-a, -1, 0)
6         else:
7             return (a, 1, 0)
8     else:
9         q, r = divmod(a, b)
10        d, s, t = rxgcd(b, r)
11        return (d, t, s - q*t)

```

הפונקציה `divmod` בשורה 9 היא פונקציה סטנדרטית המחזירה שני מספרים  $q, r$  שהם המנה והשארית בחלוקה  $a/b$  כך שמתקיים  $a = qb + r$ . בשורה 10 נקבל  $d = sb + tr$ , ולכן בשורה 11 מחזירים לאחר הצבה

$$d = sb + tr = sb + t(a - qb) = ta + (s - qt)b$$

תוצאות אפשריות לחישובים שנתבקשו בשאלה הן

$$\text{xgcd}(5779, 2018) = (1, -499, 1429)$$

$$\text{xgcd}(437437, 142142) = (1001, 13, -40)$$

$$\text{xgcd}(289214, -1414213) = (41, 10743, 2197)$$

בהצלחה!