

## פתרון תרגיל בית 1 במבנים אלגבריים 89-214 סמסטר א' תשע"ו

**הוראות** בהגשת הפתרון יש לרשום בכל דף שם מלא, מספר ת"ז ומספר קבוצת תרגול. תאריך הגשת התרגיל הוא לתרגול בשבוע המתחיל בתאריך י"ט חשוון ה'תשע"ו, 1.11.2015.

**שאלה 1.** יהי  $n$  מספר טבעי. הגדרנו יחס על  $\mathbb{Z}$  לפיו נאמר כי  $a, b \in \mathbb{Z}$  שקולים בשארית חלוקה  $n$ -אם  $a \equiv b \pmod{n}$ , וסימנו 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  $a \equiv a \pmod{n}$ . 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

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

כלומר  $a \equiv c \pmod{n}$ .

**שאלה 2.** יהי  $n$  מספר טבעי. נסמן את הכפולות שלו ב- $n\mathbb{Z} = \{0, \pm n, \pm 2n, \dots\}$ . למשל  $4\mathbb{Z} = \{\dots, -12, -8, -4, 0, 4, 8, 12, \dots\}$ . נזכיר כי סימנו  $\gcd(a, b) = (a, b)$ .

א. הוכיחו כי  $b$  מחלק את  $a$  אם ורק אם  $a\mathbb{Z} \subseteq b\mathbb{Z}$ .

ב. נגדיר סכום על קבוצות כאלו לפי  $\{a\mathbb{Z} + b\mathbb{Z} = \{\alpha + \beta : \alpha \in a\mathbb{Z}, \beta \in b\mathbb{Z}\}$ . הוכיחו כי מתקיים  $a\mathbb{Z} + b\mathbb{Z} = (a, b)\mathbb{Z}$ .

ג. הוכיחו כי  $(a, b) \cdot (a, c)\mathbb{Z} \subseteq a\mathbb{Z} + bc\mathbb{Z}$ . רמז: העזרו בסעיפים הקודמים.

פתרון. א. מצד אחד, אם  $a\mathbb{Z} \subseteq b\mathbb{Z}$ , אזי בפרט  $a \in b\mathbb{Z}$ . לכן קיים  $n \in \mathbb{Z}$  כך שמתקיים  $a = bn$ . מצד שני, אם  $b|a$ , אז קיים  $n \in \mathbb{Z}$  כך שמתקיים  $a = bn$ . לכן אם  $x \in a\mathbb{Z}$ , קיים  $m \in \mathbb{Z}$  כך ש- $x = am$  ולכן  $x = bnm$ , כלומר  $x \in b\mathbb{Z}$ .

ב. נוכיח בהכלה דו-כיוונית. נתחיל עם  $\subseteq$ : ידוע כי ניתן להציג את  $(a, b)$  כצירוף לינארי של  $a, b$ . כלומר קיימים  $u, v \in \mathbb{Z}$  כך שמתקיים  $(a, b) = au + bv$ . יהי  $x \in a\mathbb{Z} + b\mathbb{Z}$ , ולכן קיימים  $n_a, n_b \in \mathbb{Z}$  כך ש- $x = an_a + bn_b$ . אנו צריכים למצוא  $m \in \mathbb{Z}$  כך שיתקיים  $(a, b)m = an_a + bn_b$ . אפשר לבחור את  $m = \frac{a}{(a,b)}n_a + \frac{b}{(a,b)}n_b$ . הכיוון השני  $\supseteq$  הוא יותר קל כי ידוע לנו שניתן להציג את  $(a, b)$  כצירוף לינארי של  $a, b$ , ולכן גם כל כפולה שלו.

ג. בעזרת הסעיפים הקודמים אנו למעשה נדרשים להוכיח  $(a, bc) | (a, b)(a, c)$ . קיימים  $s, t, u, v$  כך שמתקיים

$$(a, b) = sa + tb$$

$$(a, c) = ua + vc$$

נכפול את שתי המשוואות האלו ונקבל

$$(a, b)(a, c) = (sa + tb)(ua + vc) = n_1a + n_2bc$$

עבור  $n_1, n_2 \in \mathbb{Z}$ . לפי הגדרה  $(a, bc) | a, bc$  ולכן  $(a, bc)$  מחלק כל צירוף לינארי של  $a$  ושל  $bc$ , בפרט את  $n_1a + n_2bc$ .

**שאלה 3.** הוכיחו כי לכל  $a, n, m \in \mathbb{Z}$  מתקיים  $(an, am) = |a|(n, m)$ . פתרו. נסמן  $d = (n, m)$ . בשורה אחת אפשר להוכיח זאת כך

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

דרך אחרת, היא דו-כיוונית (ומפורטת יותר). מצד אחד, ישנם מספרים  $u, v$  כך שמתקיים  $(an, am) = uan + v am$ . ידוע כי  $d$  מחלק כל צירוף לינארי של  $n$  ו- $m$ , ובפרט את  $uan + v am$ . לכן  $|a|d | (an, am)$  ולכן  $uan + v am$  נכפיל ב- $|a|$  ונקבל  $|a|d = sn + tm$  כך שמתקיים  $s, t$  מתאימים. ידוע כי  $(an, am)$  מחלק כל צירוף לינארי של  $an$  ו- $am$ , ובפרט את  $s'an + t'am$ . לכן  $|a|d | (an, am)$ . 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.  $(222, 123)$

ב.  $(4440, 2460)$ , רמז: העזרו בשאלה הקודמת.

פתרו. א. נשתמש באלגוריתם אוקלידס:

$$\begin{aligned} (222, 123) &= [222 = 1 \cdot 123 + 99] \\ (123, 99) &= [123 = 1 \cdot 99 + 24] \\ (99, 24) &= [99 = 4 \cdot 24 + 3] \\ (24, 3) &= [24 = 8 \cdot 3 + 0] \\ (3, 0) &= 3 \end{aligned}$$

ולכן  $(222, 123) = 3$ .

ב. נשים לב כי  $4440 = 20 \cdot 222$  וכן  $2460 = 20 \cdot 123$ . לכן לפי השאלה הקודמת

$$(4440, 2460) = |20| \cdot (222, 123) = 20 \cdot 3 = 60$$

**שאלה 5.** אפשר להגדיר ממ"מ ליותר מזוג מספרים. יהי  $d$  הממ"מ של המספרים  $n_1, \dots, n_k$  (כלומר  $d$  הוא המספר הטבעי הגדול ביותר המחלק את כולם).

הראו שקיימים מספרים שלמים  $s_1, \dots, s_k$  המקיימים  $s_1n_1 + \dots + s_kn_k = d$ . רמז: אינדוקציה על  $k$ .

פתרו. תחילה נוכיח טענת עזר, שלכל  $a, b, c$  מתקיים  $\gcd(a, b, c) = \gcd(\gcd(a, b), c)$ . נסמן  $g = \gcd(a, b, c)$  ו- $f = \gcd(\gcd(a, b), c)$ . לפי הגדרה  $g | a, b$  ולכן  $g | \gcd(a, b)$ . בנוסף  $g | c$  ולכן  $g \leq f$ . לפי הגדרה  $f | \gcd(a, b)$ , ולכן  $f | a, b$  (טרנזיטיביות של "מחלק את"). בנוסף  $f | c$ , ולכן  $f | a, b, c$ . בפרט  $f \leq g$ , וקיבלנו כי  $f = g$ . כעת נמשיך להוכחת הדרוש בשאלה בעזרת אינדוקציה. אם  $k = 1$  אז הטענה ברורה. פשוט נבחר  $s_1 = \pm 1$  בהתאם לסימן של  $n_1$ .

אם  $k = 2$ , אפשר למצוא את  $s_1, s_2$  בעזרת אלגוריתם אוקלידס המורחב. נניח את נכונות הטענה לכל  $k' < k$ , ונוכיח אותה בעבור  $k$ . נחשב את הממ"מ בעזרת טענת העזר כ-

$$\begin{aligned} \gcd(n_1, n_2, \dots, n_{k-1}, n_k) &= \gcd(\gcd(\gcd(n_1, n_2), n_3), \dots, n_{k-1}), n_k) \\ &= \gcd(\gcd(n_1, n_2, \dots, n_{k-1}), n_k) \end{aligned}$$

ואנו יודעים כי לפי הנחת האינדוקציה קיימים  $t_1, \dots, t_{k-1}$  כך שמתקיים

$$\gcd(n_1, n_2, \dots, n_{k-1}) = t_1 n_1 + \dots + t_{k-1} n_{k-1}$$

וגם  $u_1, u_2$  כך שמתקיים

$$\gcd(\gcd(n_1, n_2, \dots, n_{k-1}), n_k) = u_1 \gcd(n_1, n_2, \dots, n_{k-1}) + u_2 n_k$$

מאיחוד שתי המשוואות האחרונות נקבל

$$\gcd(n_1, n_2, \dots, n_{k-1}, n_k) = u_1 t_1 n_1 + \dots + u_1 t_{k-1} n_{k-1} + u_2 n_k$$

אם לכל  $1 \leq i < k$  נסמן  $s_i = u_1 t_i$  וכן  $s_k = u_2$ , אז נקבל את הדרוש.

**שאלה 6.** בחרו שפת תכנות (לא איזוטרי) 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

$$\text{xgcd}(5776, 2015) \quad \text{xgcd}(123456, 888888) \quad \text{xgcd}(89214, -3141596)$$

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  $(b, r)$ . 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

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

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

$$r_0 = a = s_0 a + t_0 b \quad r_1 = b = s_1 a + t_1 b$$

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

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 2–8 נועדו לתיעוד הפונקציה. בשורה 9, וגם בהמשך הקוד, מופיע שימוש בהשמה מקבילית (בפיית'ון המינוח הוא tuple packing and sequence unpacking) ובו בויזמנית מציבים ערכים בשני משתנים. הערכים באגף ימין בהשמה מקבילית מחושים 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  $0 \leq |r|$ , ולא בהכרח  $0 \leq r$ . 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

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

התוצאות שנתבקשו בשאלה הן

$$\text{xgcd}(5776, 2015) = (1, -809, 2319)$$

$$\text{xgcd}(123456, 888888) = (24, -36, 5)$$

$$\text{xgcd}(89214, -3141596) = (2, -775451, -22021)$$

בהצלחה!