

# תרגיל בית 1 במבנים אלגבריים

## 89-214 סמסטר א' תשע"ז

**הוראות** בהגשת הפתרון יש לרשום בכל דף שם מלא, מספר ת"ז ומספר קבוצת תרגול. תאריך הגשת התרגיל הוא בתרגול בשבוע המתחיל בתאריך י"ט חשוון ה'תשע"ז, 20.11.2016.

### שאלות חימום

שאלות החימום הן שאלות שאינן להגשה, והן בדרך כלל קלות יותר. אבל כדאי מאוד לוודא שיודעים איך לפתור אותן, אפילו בעל פה.

**שאלה 1.** יהיו  $n, m$  מספרים שלמים, ונניח  $n|m$ . האם בהכרח  $n|m - n$ ? האם בהכרח  $n|2m - n$ ? (כלומר  $m \nmid n$  לא מחלק את  $n$ )

**שאלה 2.** יהי  $p$  מספר ראשוני. מצאו את כל המספרים  $x \in \mathbb{Z}$  כך ש- $x|p$ .

**שאלה 3.** יהי  $n$  מספר טבעי. הגדרנו יחס על  $\mathbb{Z}$  לפיו נאמר כי  $a, b \in \mathbb{Z}$  שקולים בשארית חלוקה  $n$ -אם  $a - b$  נחלק על ידי  $n$ , וסימנו יחס זה כ- $a \equiv b \pmod{n}$ . הוכיחו כי שקילות מודולו  $n$  היא אכן יחס שקילות (כלומר יחס רפלקסיבי, סימטרי וטרנזיטיבי).

### שאלות להגשה

**שאלה 4.** 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.

**שאלה 5.** הוכיחו כי לכל  $a, n, m \in \mathbb{Z}$  מתקיים  $(an, am) = |a|(n, m)$ .

**שאלה 6.** מצאו בעזרת אלגוריתם אוקלידס את הממ"מ הבאים:

א.  $(890, 214)$

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

**שאלה 7.** הוכיחו:

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

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

**שאלה 8.** מצאו את כל המספרים השלמים  $n$  כך ש- $(n + 1)|(n^2 + 11)$ .

## שאלות רשות

את שאלות הרשות אין חובה לפתור, אבל אם פתרתם אותן, בבקשה צרפו את הפתרון שלהן.

**שאלה 9.** בחרו שפת תכנות (לא איזוטרית) כרצונכם וכתבו פונקציה בשם  $\text{xgcd}$  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

$$\text{xgcd}(5777, 2016) \quad \text{xgcd}(437437, 142142) \quad \text{xgcd}(289214, -1414213)$$

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

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

**שאלה 10.** 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  $s_1 n_1 + \dots + s_k n_k = d$ . רמז: אינדוקציה על  $k$ .

**שאלה 11.** יהיו  $P(x), Q(x) \in \mathbb{R}[x]$  פולינומים עם מקדמים ממשיים. נאמר כי  $P(x)$  מחלק את  $Q(x)$  אם קיים פולינום  $f(x) \in \mathbb{R}[x]$  כך ש- $Q(x) = f(x) \cdot P(x)$ , ונסמן  $P(x) | Q(x)$ . נסחו והוכיחו גרסאות של משפט החילוק ואלגוריתם אוקלידס עבור פולינומים עם מקדמים ממשיים. ממשו פונקציית  $\text{xgcd}$  לפיהם. מה יקרה אם נחליף את  $\mathbb{R}[x]$  ב- $\mathbb{Z}[x]$ ?

בהצלחה!