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 ב-n אם $n|a-b$, וסימנו יחס זה כ-$a \equiv b \pmod{n}$. הוכיחו כי שקילות מודולו n היא אכן יחס שקילות (כלומר יחס רפלקסיבי, סימטרי וטרנזיטיבי).

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.

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

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

א. $(222, 123)$

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

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 $s_1 n_1 + \cdots + s_k n_k = d$. רמז: אינדוקציה על k.

שאלה 6. בחרו שפת תכנות (לא איזוטרית) כרצונכם וכתבו פונקציה בשם $\texttt{xgcd}$ 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

$$\texttt{xgcd}(5776, 2015) \qquad \texttt{xgcd}(123456, 888888) \qquad \texttt{xgcd}(89214, -3141596)$$

הערה: בעוד ש-d הוא יחודי, המקדמים s, t הם לא בהכרח יחודיים. לדוגמה $\texttt{xgcd}(24, 44)$ 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

$$\texttt{xgcd}(-5, 0) \longrightarrow (5, -1, 0) \qquad \texttt{xgcd}(100, 11) \longrightarrow (1, 1, -9)$$

בהצלחה!