תרגיל בית 4 באלגברה מתקדמת
83-804 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 ב-n 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).

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

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

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

א. $(838, 104)$

ב. $(3352, -416)$, רמז: העזרו בשאלה הקודמת.

שאלה 5. מצאו את כל המספרים השלמים n כך ש-$(n+1)|(n^2+11)$.

שאלה 6. תהינה G, H חבורות. האם כל תת־חבורה K של $G \times H$ היא בהכרח מהצורה $K_1 \times K_2$, כאשר K_1 תת־חבורה של G ו-K_2 תת־חבורה של H? הוכיחו או תנו דוגמה נגדית.

שאלה 7 (רשות)**.** בחרו שפת תכנות כרצונכם וכתבו פונקציה בשם $\mathtt{xgcd}$ הממממשת 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

$$\mathtt{xgcd}(5779, 2018) \qquad \mathtt{xgcd}(437437, 142142) \qquad \mathtt{xgcd}(83804, -1414213)$$

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

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

בהצלחה!