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 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. $(890,214)$

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

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-$(4n+3)s+(7n+5)t=1$.

שאלה 6. מצאו את כל המספרים השלמים n כך ש-$(n+1)|(n^2+11)$.

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

$$\mathrm{xgcd}(5779,2018)\qquad \mathrm{xgcd}(437437,142142)\qquad \mathrm{xgcd}(289214,-1414213)$$

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

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

בהצלחה!