מבנים דיסקרטיים – תרגיל 3

שאלה 1

בשיעור הגדרנו לכל $n \in \mathbb{N}$ את $U_n = \{0 < k < n \mid \gcd(k, n) = 1\}$ ואמרנו (בלי להוכיח) שהיא חבורה ביחס לפעולה $a \cdot b = (ab) \bmod n$ (החבורה $(U_n, \cdot)$ נקראת <u>חבורת אוילר של n</u>).

א. מצאו את האיברים של U_{10}, U_{12}.
ב. הראו כי U_{10} ציקלית ו- U_{12} לא ציקלית.
ג. מצאו איבר מסדר 3 ב-U_7. הראו כי הוא אכן מסדר 3.

שאלה 2

תהי $(G,\cdot)$ חבורה ויהי $g \in G$. הוכיחו:

א. $o(g) = o(g^{-1})$.
ב. אם G סופית אז $o(g) < \infty$.

שאלה 3

תהי $(G,\cdot)$ חבורה <u>סופית</u> ו<u>אבלית</u>. נגדיר $b = \prod_{g \in G} g$.

א. הראו כי $b^2 = e$.
ב. נניח שב-G אין איברים מסדר 2. הראו כי $b = e$.
ג. **<u>רשות:</u>** יהי p ראשוני. השתמשו בסעיף א עם $G = U_p$ כדי להראות ש-$\left((p-1)!\right)^2 - 1$ מתחלק ב-p.

שאלה 4

תהי $(G,\cdot)$ חבורה ו-$g \in G$. נניח ש-$o(g) = 6$. מה הסדר של g^2? של g^3? של g^4? מדוע?

שאלה 5

תהי $(G,\cdot)$ חבורה <u>ציקלית</u> עם k איברים.

א. הוכיחו כי G חילופית.
ב. הוכיחו כי לכל $g \in G$ מתקיים $g^k = e$.
ג. נניח כי k ראשוני. הראו כי לכל $e \neq g \in G$ מתקיים $o(g) = k$.

[בפתרון השאלה אתם יכולים להשתמש בטענה הבאה שהוכחנו בכיתה: עבור $n \in \mathbb{N}$ מתקיים $g^n = e$ אם"ם $o(g) \mid n$.]