מבנים אלגבריים

תרגיל בית 2*

1 תורת המספרים השלמים

טענות שימושיות:

- אלגוריתם אוקלידס.
- $\gcd(m,n) = (m,n) = \max\{d \in \mathbb{Z}\colon d \mid m \wedge d \mid n\}$.
- $\gcd(m,n)$ ניתן להצגה כצירוף לינארי של m ו־n עם מקדמים שלמים. יתר על כן, מבין הצירופים הלינאריים האלה שערכם חיובי, הממג"ב הוא מינימלי. בנוסחא:

$$\gcd(m,n) = \min\{sm+tn\colon s,t \in \mathbb{Z}, am+tn>0\}$$

1. יהי d מספר טבעי. הוכיחו: $d=\gcd(m,n)$ א.ס.ם. d מחלק משותף של m ו־n וגם צירוף לינארי שלהם. ובנוסחא:

$$d=\gcd(m,n) \Longleftrightarrow (d \mid m) \wedge (d \mid n) \wedge (\exists s,t \in \mathbb{Z}, sm+tn=d)$$

2. פתרו את התרגילים הבאים (אין להשתמש במחשבון):

(א) $6+5\cdot 7 \pmod{11}$.

(ב) $-5-6\cdot 18 \pmod{11}$.

(ג) $7^{14} \pmod{5}$.

(ד) $7^{14} \pmod{6}$.

3. מצאו מספרים שלמים m,n שיקיימו

(א) $\gcd(81,42) = 81n+42m$.

(ב) $\gcd(81,43) = 81n+43m$.

* להגשה עד ט"ו בכסלו (7 דצמ').

(ג) $\gcd(30,455) = 30n + 455m$.

4. נניח כי d הוא מחלק משותף של a ו־b.[1] הוכיחו: $d = \gcd(a,b)$ א.ם.ם. $\gcd\left(\frac{a}{d},\frac{b}{d}\right) = 1$.

רמז: היעזרו בשאלה 1.

5. נביט ב־$\mathbb{Z}_n$ עם פעולת הכפל. מצאו מי מבין האיברים הבאים הוא הפיך במונואיד זה, וחשבו את ההופכי.

   (א) $15 \in \mathbb{Z}_{42}$.
   (ב) $17 \in \mathbb{Z}_{59}$.
   (ג) $35 \in \mathbb{Z}_{52}$.

6. יהיו a,b,c מספרים שלמים המקיימים $a \mid c$, $b \mid c$ וכן $(a,b) = 4$. הוכיחו כי $ab \mid 4c$.

2 סדר של איבר, סדר של חבורה

7. תהי G חבורה, ויהי $g \in G$. הוכיחו כי $o(g) = o\left(g^{-1}\right)$.

8. חשבו מהו סדרו של כל איבר בחבורות הבאות:

   (א) $\mathbb{Z}_{10}$ עם פעולת החיבור.
   (ב) U_9 עם פעולת הכפל.

בהצלחה!

[1] לא אמרנו מקסימלי. נתון בסה"כ כי $d \mid a \wedge d \mid b$.