

תרגיל בית 1 בתורת החבורות 88-218 סמסטר א' תשפ"ב

שאלה 1 (חימום). יהיו n, m מספרים שלמים, ונניח $n|m$. האם בהכרח $n|m - m$? האם בהכרח $n|2m$? האם בהכרח $m \nmid n$ (כלומר m לא מחלק את n)?

שאלה 2 (חימום). יהי p מספר ראשוני. מצאו את כל המספרים $x \in \mathbb{Z}$ כך ש- $x|p$.

שאלה 3 (חימום). יהי n מספר טבעי. הגדרנו יחס על \mathbb{Z} לפיו נאמר כי $a, b \in \mathbb{Z}$ שקולים מודולו 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 4. 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 5. הוכיחו כי לכל $a, n, m \in \mathbb{Z}$ מתקיים $(an, am) = |a|(n, m)$.

שאלה 6. מצאו בעזרת אלגוריתם אוקלידס את הממ"מ הבאים:

א. $(88, 218)$

ב. $(-26400, 65400)$, רמז: העזרו בשאלה הקודמת.

שאלה 7. יהיו n, m מספרים שלמים. הכפולה המשותפת המזערית (כמ"מ, least common multiple) שלהם מוגדרת להיות

$$\text{lcm}(n, m) = [n, m] = \min \{d \in \mathbb{N} : n|d \wedge m|d\}$$

למשל $[2, 5] = 10$ ו- $[6, 10] = 30$. הוכיחו:

א. אם $m|a$ וגם $n|a$, אז $[n, m]|a$.

ב. $n, m = |nm|$. למשל $6, 4 = 12 \cdot 2 = 24 = 6 \cdot 4$.

שאלה 8. אלגוריתם אוקלידס עובד גם עם פרמטרים. הוכיחו:

א. לכל 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 9. מצאו את כל המספרים השלמים n כך ש- $(n + 1)|(n^2 + 11)$.

שאלות רשות

את שאלות הרשות אין חובה לפתור, אבל אם פתרתם אותן, בבקשה שלחנו לנו פתרון שלהן.

שאלה 10. בחרו שפת תכנות (לא איזטרית) 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

$$\text{xgcd}(5782, 2022) \quad \text{xgcd}(112233, 445566) \quad \text{xgcd}(81288218, -5134756)$$

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

$$\text{xgcd}(-5, 0) \rightarrow (5, -1, 0) \quad \text{xgcd}(100, 11) \rightarrow (1, 1, -9)$$

שאלה 11. יהיו $P(x), Q(x) \in \mathbb{R}[x]$ פולינומים עם מקדמים ממשיים. נאמר כי $P(x)$ מחלק את $Q(x)$ אם קיים פולינום $f(x) \in \mathbb{R}[x]$ כך ש- $Q(x) = f(x) \cdot P(x)$, ונסמן $P(x)|Q(x)$. נסחו והוכיחו גרסאות של משפט החילוק ואלגוריתם אוקלידס עבור פולינומים עם מקדמים ממשיים. ממשו פונקציית xgcd לפיהם. מה יקרה אם נחליף את $\mathbb{R}[x]$ ב- $\mathbb{Z}[x]$?

בהצלחה!