

פתרון תרגיל בית 2 מבוא לתורת החבורות 88-211 סמסטר א' תשע"ח

שאלות חימום

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

פתרון. כן, כן, לא. למה לא? הוכיחו ש- $n|m$ וגם $m|n$, אם ורק אם $n = \pm m$.

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

פתרון. המספרים $1, p, -1, -p$.

שאלה 3. 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).

פתרון. היחס רפלקסיבי כי לכל $a \in \mathbb{Z}$ מתקיים כי $n|0$. לכן $n|a - a$, כלומר $a \equiv a \pmod{n}$. היחס סימטרי כי אם $n|x$, אז גם $n|-x$. בפרט

$$a \equiv b \pmod{n} \Leftrightarrow n|(a - b) \Leftrightarrow n|(b - a) \Leftrightarrow b \equiv a \pmod{n}$$

היחס טרנזיטיבי כי אם $n|x$ וגם $n|y$, אז $n|x + y$. בפרט אם $a \equiv b \pmod{n}$ וגם $b \equiv c \pmod{n}$, אז

$$n|(a - b) \wedge n|(b - c) \Rightarrow n|(a - b + b - c) \Rightarrow n|(a - c)$$

כלומר $a \equiv c \pmod{n}$.

שאלות רגילות

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.

פתרון. א. מצד אחד, אם $a\mathbb{Z} \subseteq b\mathbb{Z}$, אזי בפרט $a \in b\mathbb{Z}$. לכן קיים $n \in \mathbb{Z}$ כך שמתקיים $a = bn$, כלומר $b|a$. מצד שני, אם $b|a$, אז קיים $n \in \mathbb{Z}$ כך שמתקיים $a = bn$. לכן אם $x \in a\mathbb{Z}$, קיים $m \in \mathbb{Z}$ כך ש- $x = am$ ולכן $x = bnm$, כלומר $x \in b\mathbb{Z}$.

ב. נוכיח בהכלה דו-כיוונית. נתחיל עם \subseteq : ידוע כי ניתן להציג את (a, b) כצירוף לינארי של a, b . כלומר קיימים $u, v \in \mathbb{Z}$ כך שמתקיים $(a, b) = au + bv$. יהי $x \in a\mathbb{Z} + b\mathbb{Z}$, ולכן קיימים $n_a, n_b \in \mathbb{Z}$ כך ש- $x = an_a + bn_b$. אנו צריכים למצוא $m \in \mathbb{Z}$ כך שיתקיים $(a, b)m = an_a + bn_b$. אפשר לבחור את $m = \frac{a}{(a,b)}n_a + \frac{b}{(a,b)}n_b$.

הכיוון השני \supseteq הוא יותר קל כי ידוע לנו שניתן להציג את (a, b) כצירוף לינארי של a, b , ולכן גם כל כפולה שלו.

ג. בעזרת הסעיפים הקודמים אנו למעשה נדרשים להוכיח $(a, bc) | (a, b)(a, c)$. קיימים s, t, u, v כך שמתקיים

$$\begin{aligned}(a, b) &= sa + tb \\ (a, c) &= ua + vc\end{aligned}$$

נכפול את שתי המשוואות האלו ונקבל

$$(a, b)(a, c) = (sa + tb)(ua + vc) = n_1a + n_2bc$$

עבור $n_1, n_2 \in \mathbb{Z}$. לפי הגדרה $(a, bc) | a, bc$ ולכן (a, bc) מחלק כל צירוף לינארי של a ושל bc , בפרט את $n_1a + n_2bc$.

שאלה 5. הוכיחו כי לכל $a, n, m \in \mathbb{Z}$ מתקיים $(an, am) = |a|(n, m)$.

פתרון. נסמן $d = (n, m)$. בשורה אחת, שאינה הוכחה מלאה,

$$(an, am) = |a|d \Leftrightarrow \left(\frac{an}{d}, \frac{am}{d}\right) = |a| \Leftrightarrow |a| \left(\frac{n}{d}, \frac{m}{d}\right) = |a| \Leftrightarrow \left(\frac{n}{d}, \frac{m}{d}\right) = 1 \Leftrightarrow (n, m) = d$$

דרך אחרת, היא דו-כיוונית (ומפורטת יותר). מצד אחד, ישנם מספרים u, v כך שמתקיים $(an, am) = uan + v am$. ידוע כי d מחלק כל צירוף לינארי של n ו- m , ובפרט את $uan + v am$. לכן $|a|d$ מחלק את $uan + v am$, ולכן $(|a|d) | (an, am)$. מצד שני, ישנם מספרים s, t כך שמתקיים $d = sn + tm$. נכפיל ב- $|a|$ ונקבל $|a|d = asn + atm$. ידוע כי (an, am) מחלק כל צירוף לינארי של an ו- am , ובפרט את $as'n + at'm$. לכן $(an, am) | |a|d$. לסיכום קיבלנו $(an, am) = |a|d$. כדורש.

ניתן להוכיח את הטענה גם בעזרת שימוש בהצגה של m כמכפלת חזקות ראשוניים. במקרה זה מוכיחים כי $\min(n + a, m + a) = \min(n, m) + a$, שהיא אנלוגית להוכחה $(an, am) = |a|(n, m)$.

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

א. $(88, 211)$

ב. $(-26400, 63300)$, רמז: העזרו בשאלה הקודמת.

פתרון. א. נשתמש באלגוריתם אוקלידס:

$$\begin{aligned} (88, 211) &= (211, 88) = [211 = 2 \cdot 88 + 35] \\ (88, 35) &= [88 = 2 \cdot 35 + 18] \\ (35, 18) &= [35 = 1 \cdot 18 + 17] \\ (18, 17) &= [18 = 1 \cdot 17 + 1] \\ (17, 1) &= 1 \end{aligned}$$

ולכן $(88, 211) = 1$.

ב. נשים לב כי $-26400 = -300 \cdot 88$ וכן $63300 = 300 \cdot 211$. לכן לפי השאלה הקודמת

$$(-26400, 63300) = (26400, 63300) = |300| \cdot (88, 211) = 300$$

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

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

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

א. אם $m|a$ וגם $n|a$ אז $[n, m]|a$.

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

הוכחה. א. יהיו q, r כך ש- $a = q[n, m] + r$ כאשר $0 \leq r < [n, m]$. מהנתון כי $n, m|a$ ולפי הגדרה $[n, m]$ נובע כי $n, m|r$. אם $r \neq 0$ אז סתירה למינימליות של $[n, m]$. לכן $a = q[n, m]$, כלומר $[n, m]|a$.

ב. נראה דרך קלה לחישוב הממ"מ והכמ"מ בעזרת הפירוק של מספר למכפלת גורמים ראשוניים. נניח כי הפירוק הוא

$$|n| = \prod_{i=1}^{\infty} p_i^{\beta_i} = p_1^{\beta_1} p_2^{\beta_2} p_3^{\beta_3} \dots \quad |m| = \prod_{i=1}^{\infty} p_i^{\alpha_i} = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots$$

כאשר $\alpha_i, \beta_i \geq 0$ (והם כמעט תמיד אפס כי המכפלה סופית). כעת צריך להשתכנע כי

$$(n, m) = \prod_{i=1}^{\infty} p_i^{\min(\alpha_i, \beta_i)} \quad [n, m] = \prod_{i=1}^{\infty} p_i^{\max(\alpha_i, \beta_i)}$$

ומפני שלכל שני מספרים α, β מתקיים $\alpha + \beta = \min(\alpha, \beta) + \max(\alpha, \beta)$ אז $n, m = |nm|$.

□

שאלה 8. הוכיחו:

א. לכל n שלם מתקיים $(4n + 3, 7n + 5) = 1$.

ב. מצאו $s, t \in \mathbb{Z}$ (התלויים ב- n) כך ש- $(4n + 3)s + (7n + 5)t = 1$.

פתרון. א. נשתמש כמה פעמים שאם $n = qm + r$ אז $(n, m) = (m, r)$.

$$(7n + 5, 4n + 3) = [7n + 5 = 2 \cdot (4n + 3) + (-n - 1)]$$

$$(4n + 3, -n - 1) = [4n + 3 = -4 \cdot (-n - 1) - 1]$$

$$(-n - 1, -1) = 1$$

אפשר לעשות את החישוב בכמה דרכים, למשל כאשר נמנעים ממקדמים שליליים ל- n :

$$(7n + 5, 4n + 3) = [7n + 5 = 1 \cdot (4n + 3) + (3n + 2)]$$

$$(4n + 3, 3n + 2) = [4n + 3 = 1 \cdot (3n + 2) + (n + 1)]$$

$$(3n + 2, n + 1) = [3n + 2 = 3 \cdot (n + 1) - 1]$$

$$(n + 1, -1) = 1$$

ב. משתמשים בשלבים של אלגוריתם אוקלידס המורחב, לפי הסעיף הקודם:

$$\begin{aligned} -n - 1 &= 1 \cdot (7n + 5) - 2 \cdot (4n + 3) \Rightarrow \\ -1 &= 1 \cdot (4n + 3) + 4 \cdot (-n - 1) \\ &= 4 \cdot (7n + 5) - 7 \cdot (4n + 3) \end{aligned}$$

ולכן נקבל $s = 7, t = -4$, שאינם תלויים ב- n !

שאלה 9. מצאו את כל המספרים השלמים n כך ש- $(n^2 + 11) | (n + 1)$.
פתרון. נשים לב כי $n + 1$ מחלק את עצמו, ואם הוא מחלק את $n^2 + 11$, הוא גם יחלק את הממ"מ שלהם (ולכן גם יחלק כל צירוף לינארי של $n + 1$ ושל $n^2 + 11$). בעזרת החישוב

$$n^2 + 11 = (n - 1) \cdot (n + 1) + 12$$

ושימוש בטענה שאם $n = qm + r$, אז $(n, m) = (m, r)$, נקבל

$$(n^2 + 11, n + 1) = (n + 1, 12)$$

כלומר מספיק למצוא את המספרים n כך ש- $12 | (n + 1)$. המחלקים של 12 הם ידועים, ולכן המספרים המבוקשים הם $11, 5, 3, 2, 0, -2, -3, -4, -5, -7, -13$. החישוב שעשינו היה למעשה

$$\frac{n^2 + 11}{n + 1} = \frac{n^2 - 1 + 12}{n + 1} = \frac{(n + 1)(n - 1)}{n + 1} + \frac{12}{n + 1} = (n - 1) + \frac{12}{n + 1}$$

ומפני ש- $n - 1$ הוא שלם, נותר לבדוק מתי $\frac{12}{n + 1}$ שלם.

בהצלחה!