מופשטת 1 תשע"ו - פתרון תרגיל בית 2

לאורך התרגיל נסמן את המחלק המשותף המקסימלי של שני מספרים $a,b \in \mathbb{Z}$ ע"י (a,b).

1. עבור שני מספרים $a,b \in \mathbb{Z}$ הראו שמתקיים $a|b \iff b\mathbb{Z} \subseteq a\mathbb{Z}$.

פתרון:
$a|b \Leftrightarrow \exists k \in \mathbb{Z}\, b = ak \Leftrightarrow b \in a\mathbb{Z} \Leftrightarrow b\mathbb{Z} \subseteq a\mathbb{Z}$.

2. יהיו $a,b \in \mathbb{Z}$ ונסמן $d = (a,b)$. הוכיחו כי $(\frac{a}{d}, \frac{b}{d}) = 1$.

פתרון:
נניח $k \in \mathbb{N}$ הוא מחלק משותף, כלומר $k|\frac{a}{d}$ וגם $k|\frac{b}{d}$. אזי קל לראות ש $kd|a$ וגם $kd|b$ כלומר ש kd הוא מחלק משותף של aוb. אבל d הוא המחלק המשותף המקסימלי ולכן בהכרח $k = 1$.

3. נגדיר: **הכפולה המשותפת המינימלית** (lcm) של שני מספרים a,b היא המספר

$$[a,b] = \min_{k \in \mathbb{N}} \{k \,|\, a|k \,\wedge\, b|k\}$$

למשל $[15,6] = 30$.

(א) הוכיחו כי אם $a|m$ וגם $b|m$ אז $[a,b]|m$

פתרון:
נסמן $t = [a,b]$, ונרשום $m = qt + r$ כך ש $r < t$ או $r = 0$ (אנחנו בעצם מנסים להראות ש $r = 0$).
ע"י העברת אגפים נקבל ש $r = m - qt$.
מכיוון ש $a|t$ וגם $a|m$ אז $a|r$ (כי r הוא צירוף ליניארי שלהם), ובאותו אופן $b|r$.

כלומר קיבלנו ש r הוא כפולה משותפת של a ו־ b.
מהמינימליות של t נקבל ש $t \leq r$, אבל לפי הבחירה של r בהכרח $r = 0$.

(ב) הוכיחו כי $a\mathbb{Z} \cap b\mathbb{Z} = [a,b]\mathbb{Z}$.

פתרון:
לפי השאלה הראשונה אפשר לראות ש $a\mathbb{Z} \cap b\mathbb{Z} \supseteq [a,b]\mathbb{Z}$.
ומצד שני, אם $m \in a\mathbb{Z} \cap b\mathbb{Z}$ אז $a|m$ וגם $b|m$, ולפי הסעיף הקודם זה אומר ש $[a,b]|m$ כלומר ש $m \in [a,b]\mathbb{Z}$.

4. חשבו את המחלק המשותף המקסימלי של זוגות המספרים הבאים:

(א) ‎-11, 24

$$\begin{aligned} 24 &= (-2)\cdot(-11)+2 \\ -11 &= (-5)\cdot 2 - 1 \\ 2 &= (-2)\cdot(-1)+0 \end{aligned}$$

ולכן הממ"מ הוא $|-1| = 1$.

(ב) 22, 117

$$\begin{aligned} 117 &= 5\cdot 22+7 \\ 22 &= 3\cdot 7+1 \\ 7 &= 7\cdot 1+0 \end{aligned}$$

ולכן הממ"מ הוא 1.

(ג) 785 , 2780

5. עבור המונואידים הכפליים והאיברים הבאים, האם האיבר הפיך? אם כן, מי ההופכי שלו? (טיפ: העזרו בשאלה הקודמת)

(א) ‎-11 ב $\mathbb{Z}_{24}$

לפי סעיף א' $(-11, 24) = 1$ ולכן ‎-11 הפיך. נציב לאחור:

$$1 = -(-11) - 5\cdot 2 = -(-11) - 5(24 - 2\cdot 11) = -11\cdot(-11) + (-5)\cdot 24$$

ולכן ההופכי שלו הוא ‎-11.

(ב) 22 ב $\mathbb{Z}_{117}$

לפי סעיף ב' $(22, 117) = 1$ ולכן 22 הפיך. נציב לאחור ונקבל:

$$1 = 22 - 3\cdot 7 = 22 - 3(117 - 5\cdot 22) = 16\cdot 22 + (-3)117$$

ולכן ההופכי שלו הוא 61.

6. פתרו את המשוואות הבאות: (טיפ: היעזרו בשאלה הקודמת)

(א) $-11x + 2 = 19$ ב $\mathbb{Z}_{24}$

נסדר את המשוואה $-11x = 17$ כעת נכפול ב־11- (שהוא הופכי של ‎-11 לפי השאלה הקודמת) את שני האגפים ונקבל $x = -11\cdot 17 = -19$.

(ב) $20x + 1 = 3 - 2x$ ב $\mathbb{Z}_{117}$

נסדר את המשוואה: $22x = 2$ ונכפול ב 61 (שהוא ההופכי של 22 לפי שאלה 3) את שני האגפים ונקבל $x = 16\cdot 2 = 32$.

7. יהי p מספר ראשוני. כמה איברים הפיכים יש במונואיד הכפלי $\mathbb{Z}_p$? כמה איברים הפיכים יש במונואיד הכפלי $\mathbb{Z}_{p^2}$?

עבור $\mathbb{Z}_p$: מתוך האיברים $0,1,\ldots,p-1$ כולם חוץ מ0 זרים ל p כי הוא ראשוני. ולכן יש $p-1$ איברים הפיכים.

עבור $\mathbb{Z}_{p^2}$: מכיוון ש p הוא ראשוני , מספר יהיה זר לp^2 אם"ם אין לו גורם ראשוני p, כלומר אם"ם הוא זר לp.

מתוך המספרים $0,1,\ldots,p^2$ נחשוב כמה מהם לא זרים לp: אלו כל המספרים שיש להם גורם p דהיינו $p\{0,1,2,\ldots p-1\}=\{0,p,2p,\ldots,(p-1)p\}$ - כלומר שיש p מספרים כאלו.

ולכן מספר האיברים ההפיכים (שכן זרים) הוא p^2-p.

8. רשמו את לוחות הכפל של החבורות U_5, U_6. כאשר $U_n = U\left(\mathbb{Z}_n, \cdot\right)$ היא חבורת אוילר.

U_5	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

U_6	1	5
1	1	5
5	5	1

9. תהי $G=\{a_1,a_2,\ldots,a_n\}$ חבורה אבלית. נסמן $b=a_1a_2\cdots a_n$. הוכיחו כי $b^2=e$.

פתרון:

כיוון ש G אבלית, לא משנה סדר המכפלה של האיברים בb^2. נשים לב שבb^2 כל איבר בחבורה מופיע פעמיים. נסדר את המכפלות כך של איבר יהיה ליד ההופכי שלו $b^2=a_1a_1^{-1}a_2a_2^{-1}\cdots a_na_n^{-1}$. ואז קל לראות ש $b^2=e$.