

פתרון תרגיל בית 3 בתורת החבורות 88-218 סמסטר א' תש"ף

שאלה 1 (חימום). הוכיחו או הפריכו כל אחת מהטענות הבאות:

א. כל חבורה ציקלית היא אבלית.

ב. כל חבורה אבלית היא ציקלית.

ג. אם $o(a) = n$, אז $a^{-1} = a^{n-1}$.

פתרון. וודאו שאתם יודעים לתת דוגמאות לכל אחד מן הסעיפים.

א. נכון.

ב. לא נכון.

ג. נכון.

שאלה 2 (חימום). כתבו את לוחות הכפל של U_5, U_8 ובדקו האם הן ציקליות.

פתרון.

·	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_5 לוח הכפל של

·	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

U_8 לוח הכפל של

בנוסף, החבורה U_5 היא ציקלית (נוצרת על ידי כל איבר שאינו איבר היחידה) ואילו U_8 לא ציקלית (כי הסדר של כל איבר קטן מ-4), ולכן אלו חבורות שונות, אפילו אם נשנה את שמות האיברים.

שאלה 3. תהי G חבורה, ותהי $\emptyset \neq H \subseteq G$ תת-קבוצה לא ריקה.

א. הוכיחו שאם G חבורה סופית, אז כדי להוכיח ש- H היא תת-חבורה של G מספיק לבדוק סגירות לפעולה.

ב. הפריכו את הסעיף הקודם כאשר G אינסופית.

פתרון.

א. צריך להראות שבמקרה זה סגירות לפעולה מבטיחה קיום יחידה וסגירות להופכי. לשם כך נראה שבחבורה סופית ההופכי של כל איבר הוא חזקה שלו. נניח $|G| = n$, אז כפי שידוע לנו $o(g) \leq n$ לכל $g \in G$. נסמן $o(g) = m$, אזי

$$\underbrace{(g * \dots * g)}_{m \text{ פעמים}} = \underbrace{(g * \dots * g)}_{m-1 \text{ פעמים}} * g = e$$

ולכן g^{m-1} הוא ההופכי של g . כעת, אם $g \in H$, אז גם $g^k \in H$ לכל $k \in \mathbb{Z}$ בגלל הסגירות לפעולה. בפרט, $g^m = e \in H$ ולכן H מכילה את היחידה של G , וכן $g^{-1} = g^{m-1} \in H$ ולכן יש סגירות להופכי. בסך הכל קיבלנו כי H תת-חבורה של G .

הדרישה $H \neq \emptyset$ הכרחית, שכן אחרת H אינה חבורה (אפילו שמתקיימת סגירות לפעולה).

ב. יש הרבה אפשרויות כאן. החבורה האינסופית "הראשונה" שפגשנו תתאים. נבחר $G = \mathbb{Z}$ ואת $H = \mathbb{N} \cup \{0\}$ שבודאי אינה ריקה. אז סגורה לפעולה (אם $a, b \geq 0$, אז גם $a + b \geq 0$) ומכילה אפילו את איבר היחידה 0, אבל אינה סגורה להופכי. לכן H אינה תת-חבורה.

שאלה 4. תהי G חבורה ויהיו $a, b \in G$ איברים. הוכיחו כי $o(ab) = o(ba)$.
זהירות: לא הנחנו שהחבורה אבלית או שהסדרים סופיים.

פתרון. נפריד למקרים בהם הסדר סופי ובהם הסדר אינסופי.
תחילה נניח $o(ab) = n < \infty$. נשים לב שמכך נובע $(ab)^{n-1} = (ab)^{-1}$. כעת

$$\begin{aligned} (ba)^n &= \underbrace{baba \dots ba}_n = b(ab)(ab) \dots (ab)a = b(ab)^{n-1}a = \\ &= b(ab)^{-1}a = bb^{-1}a^{-1}a = e \end{aligned}$$

ולכן $o(ba) | n$. באופן דומה אפשר להראות ש $n | o(ba)$, ולכן $o(ab) = o(ba)$.
אם $o(ab) = \infty$, ונניח בשלילה כי $o(ba) = m \neq \infty$, אז לפי המקרה שבו הסדר סופי, נקבל בסתירה שגם $o(ab) = m$ מסדר סופי. לכן $o(ba) = \infty = o(ab)$.

שאלה 5. מצאו את כל המספרים השלמים $x \in \mathbb{Z}$ המהווים פתרון לכל אחת מהמשוואות הבאות:

א. $33x \equiv 1 \pmod{218}$

ב. $-7x + 3 \equiv 9 \pmod{30}$

פתרון.

א. אנו בעצם נדרשים לחשב את ההופכי של 33 בחבורה U_{218} . בעזרת אלגוריתם אוקלידס המורחב נחשב

$$\begin{aligned}(218, 33) &= [218 = 6 \cdot 33 + 20] \\ (33, 20) &= [33 = 1 \cdot 20 + 13] \\ (20, 13) &= [20 = 1 \cdot 13 + 7] \\ (13, 7) &= [13 = 1 \cdot 7 + 6] \\ (7, 6) &= [7 = 1 \cdot 6 + 1] \\ (6, 1) &= 1\end{aligned}$$

ולכן $(218, 33) = 1$. קיבלנו שאכן $33 \in U_{218}$. בעזרת הצבה לאחור נקבל

$$\begin{aligned}1 &= 7 - 1 \cdot 6 = 7 - 1 \cdot (13 - 1 \cdot 7) = -1 \cdot 13 + 2 \cdot 7 = -1 \cdot 13 + 2 \cdot (20 - 1 \cdot 13) = \\ &= 2 \cdot 20 - 3 \cdot 13 = 2 \cdot 20 - 3 \cdot (33 - 1 \cdot 20) = -3 \cdot 33 + 5 \cdot 20 = \\ &= -3 \cdot 33 + 5 \cdot (218 - 6 \cdot 33) = 5 \cdot 218 - 33 \cdot 33\end{aligned}$$

ולכן ההופכי של 33 הוא -33 , ונקבל $x \equiv -33 \equiv 185 \pmod{218}$

ב. נסדר את המשוואה כך שנקבל $-7x \equiv 6 \pmod{30}$ ולצורך נוחות $23x \equiv 6 \pmod{30}$. בעזרת אלגוריתם אוקלידס המורחב נחשב

$$\begin{aligned}(30, 23) &= [30 = 1 \cdot 23 + 7] \\ (23, 7) &= [23 = 3 \cdot 7 + 2] \\ (7, 2) &= [7 = 3 \cdot 2 + 1] \\ (2, 1) &= 1\end{aligned}$$

ולכן $(30, 23) = 1$ ומכאן שאכן $23 \in U_{30}$. בעזרת הצבה לאחור נקבל

$$\begin{aligned}1 &= 7 - 3 \cdot 2 = 7 - 3 \cdot (23 - 3 \cdot 7) = -3 \cdot 23 + 10 \cdot 7 \\ &= -3 \cdot 23 + 10 \cdot (30 - 1 \cdot 23) = 10 \cdot 30 - 13 \cdot 23\end{aligned}$$

ולכן ההופכי של 23 ב- U_{30} הוא $-13 \equiv 17 \pmod{30}$. נכפיל את המשוואה ב-17 ונקבל

$$17 \cdot 23x \equiv 17 \cdot 6 \equiv 12 \pmod{30}$$

והפתרון המבוקש הוא $x \equiv 12 \pmod{30}$.

שאלה 6. זה בסדר לדחות את השאלה הזאת לשבוע הבא.

א. יהיו $a, b, c \in \mathbb{Z}$. הוכיחו כי $(a, b) = (a, c) = 1$ אם ורק אם $(a, bc) = 1$. רמז: אפשר להעזר בשאלה 4 מתרגיל הבית הראשון.

ב. פונקציית אוילר $\varphi(n)$ מתאימה לכל $n \in \mathbb{N}$ כמה מספרים טבעיים קטנים וזרים ל- n יש. כלומר

$$\varphi(n) = |\{a \mid 0 < a < n, (a, n) = 1\}|$$

הוכיחו כי $(n, m) = 1$ אם ורק אם $\varphi(nm) = \varphi(n)\varphi(m)$.

ג. הוכיחו שכשסוכמים את פונקציית אוילר על פני כל המחלקים (הטבעיים) של n מקבלים

$$n = \sum_{d|n} \varphi(d)$$

רמז: יש כל מיני דרכים לפתור את זה. אחת הדרכים היא עם תכונות ציקליות. הזכרו כמה יוצרים יש לחבורה ציקלית וכי כל תת-חבורה שלה היא ציקלית.

פתרון.

א. לפי הרמז, ראינו בתרגיל הבית הראשון כי $(a, bc) | (a, b)(a, c)$. לכן אם $(a, b) = 1$, אז בוודאי נקבל $(a, bc) = 1$, כי אין מחלקים טבעיים אחרים ל-1. בכיוון השני, נניח $(a, bc) = 1$. בפרט קיימים s, t כך ש- $1 = sa + tbc$. לפי איפיון הממ"מ כצירוף לינארי מזערי, נשים לב כי 1 הוא צירוף לינארי של a ו- c (עם מקדמים s עבור a ו- tb עבור c) ולכן $(a, c) = 1$, ובאופן דומה $(a, b) = 1$ (עם מקדמים s עבור a ו- tc עבור b).

ב. תחילה נניח $(n, m) = 1$ ונוכיח $\varphi(nm) = \varphi(n)\varphi(m)$. הערך $\varphi(nm)$ סופר את כמות המספרים הטבעיים $0 \leq x < nm$ שזרים ל- nm . אם x זר ל- n וגם ל- m , אז לפי הסעיף הקודם נקבל

$$(x, nm) = (x, n)(x, m) = 1 \cdot 1 = 1$$

כלומר x זר ל- nm . אם x זר ל- nm , אז בוודאי שהוא זר ל- n וגם ל- m . לכל $0 \leq b < m$ שזר ל- m נשים לב כי $(km + b, m) = (b, m) = 1$ לכל k . כאשר $0 \leq k < n$ נקבל כי $0 \leq km + b < nm$. מודולו n מתקיים

$$km + b \equiv k'm + b \pmod{n}$$

אם ורק אם $km \equiv k'm \pmod{n}$. מפני ש- $(n, m) = 1$, אז $m \in U_n$ הוא הפיך ולכן $k \equiv k' \pmod{n}$. מכאן שהקבוצה $\{km + b \pmod{n} | 0 \leq k < n\}$ מכילה בדיוק n מספרים, והם כל השאריות האפשריות מודולו n , כלומר $\{0, \dots, n-1\}$. בקבוצה הזאת יש בדיוק $\varphi(n)$ מספרים שזרים ל- n . נשים לב כי האיחוד (הזר) של הקבוצות מהצורה הזאת הוא

$$\{0, 1, \dots, nm-1\} = \{km + b | 0 \leq b < m, 0 \leq k < n\}$$

קצת נספור בשני האגפים את המספרים שזרים ל- nm . באגף שמאל נקבל $\varphi(nm)$. באגף ימין נספור מספרים שזרים ל- n וגם ל- m . לכל b יש $\varphi(n)$ מספרים $km + b$ שזרים ל- n באגף ימין, ויש בדיוק $\varphi(m)$ אפשרויות ל- b . כלומר $\varphi(nm) = \varphi(n)\varphi(m)$. מהוכחת כיוון זה נסיק את הנוסחה שראינו בכיתה: $\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$. המכפלה רצה על כל הראשוניים שמחלקים את n . לכיוון ההפוך, נניח $\varphi(nm) = \varphi(n)\varphi(m)$. נסמן $d = (n, m)$. אם p ראשוני שמחלק את nm , אז p מחלק את n או m . אם p מחלק גם את n וגם m , אז p מחלק d . לכן

$$\begin{aligned} \varphi(nm) &= nm \prod_{p|nm} \left(1 - \frac{1}{p}\right) = nm \frac{\prod_{p|n} \left(1 - \frac{1}{p}\right) \prod_{p|m} \left(1 - \frac{1}{p}\right)}{\prod_{p|d} \left(1 - \frac{1}{p}\right)} \\ &= n \prod_{p|n} \left(1 - \frac{1}{p}\right) m \prod_{p|m} \left(1 - \frac{1}{p}\right) \frac{d}{d \prod_{p|d} \left(1 - \frac{1}{p}\right)} = \varphi(n)\varphi(m) \frac{d}{\varphi(d)} \end{aligned}$$

ולפי ההנחה קיבלנו $\varphi(d) = d$. אבל $\varphi(d) = d$ אם ורק אם $d = 1$, כי לפי הנוסחה קל לראות שעבור $d > 1$ מתקיים $\varphi(d) < d$. כלומר $(n, m) = 1$.

ג. לכל $d|n$ יש $\varphi(d)$ יוצרים של Ω_d . כל איבר של Ω_n יוצר תת-חבורה ציקלית מן הסדר שלו (למשל d), וכל תת-חבורה של Ω_n היא מן הצורה Ω_d ונוצרת על ידי איבר של Ω_n (מסדר d). כלומר כל איבר מסדר d יוצר את Ω_d . באגף שמאל סופרים שישנם $n = |\Omega_n|$ איברים בחבורה, ובאגף ימין סוכמים לכל תת-חבורה של Ω_n את מספר היוצרים של תת-החבורה, שכאמור הם בהתאמה לאיברי Ω_n .

שיטה יותר ישירה: אנחנו יודעים שלחזקת ראשוני p^k מתקיים $\varphi(p^k) = p^k - p^{k-1}$ ו-
 $\varphi(1) = 1$. המחלקים של p^k הם רק p^i עבור $0 \leq i \leq k$. נסמן $F(n) = \sum_{d|n} \varphi(d)$ ונחשב

$$F(p^k) = \sum_{d|p^k} \varphi(d) = \sum_{i=0}^k \varphi(p^i) = 1 + (p-1) + (p^2-p) + \dots + (p^k - p^{k-1}) = p^k$$

כלומר הוכחנו את הטענה לחזקות של ראשוניים. כעת צריך להוכיח ש- $F(n)$ כפליית אריתמטית (כלומר $F(nm) = F(n)F(m)$ עבור $(n, m) = 1$) ומסיימים לפי פירוק של $n = p_1^{k_1} \dots p_r^{k_r}$ לראשוניים:

$$n = p_1^{k_1} \dots p_r^{k_r} = F(p_1^{k_1}) \dots F(p_r^{k_r}) = F(p_1^{k_1} \dots p_r^{k_r})$$

שאלות רשות

שאלה 7. תהי G חבורה סופית. הוכיחו כי מספר האיברים מסדר 3 הוא זוגי (אולי אפס).
 מה לגבי מספר האיברים מסדר p כאשר p מספר ראשוני אי זוגי?

שאלה 8. מצאו חבורה אינסופית שלכל $n \in \mathbb{N}$ קיים בה איבר מסדר n . האם אתם יכולים גם להבטיח שהסדר של כל האיברים הוא סופי?
 כמו כן, לכל $m > 1$ מצאו חבורה אינסופית G_m שהסדר של כל איבר בה הוא לכל היותר m .

האם אתם יכולים למצוא דוגמאות לשאלות האלו כך שהחבורות הן מעוצמה \aleph_0 ?

בהצלחה!