

## פתרון תרגיל בית 3 בתורת החבורות 88-218 סמסטר א' תשע"ח

**הוראות** בהגשת הפתרון יש לרשום שם מלא, מספר ת"ז ומספר קבוצת תרגול. הגישו את התרגיל בתרגול שלכם בשבוע המתחיל בתאריך 26.11.2017.

### שאלות חימום

שאלות החימום הן שאלות שאינן להגשה, והן בדרך כלל קלות יותר. אבל כדאי מאוד לוודא שיודעים איך לפתור אותן, אפילו בעל פה.

**שאלה 1.** עבור כל אחת מהטענות הבאות, קבע האם היא נכונה ואם לא מצא דוגמה נגדית:

א. כל חבורה צקלית היא אבלית.

ב. כל חבורה אבלית היא צקלית.

ג. אם  $\phi(a) = n$  אז  $a^{-1} = a^{n-1}$ .

פתרון. א. נכון.

ב. לא נכון.

ג. נכון.

**שאלה 2.** כתבו את לוחות הכפל של  $U_5, U_8$ . האם מדובר באותה חבורה (עד כדי שינוי שמות)?

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

$U_5$  של הכפל

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

$U_8$  של הכפל

בנוסף, החבורה  $U_5$  היא ציקלית ואילו  $U_8$  לא ציקלית, ולכן אלו חבורות שונות.

**שאלה 3.** מצאו איבר מסדר 6 בחבורה  $S_5$ . רמז: מצאו איבר מסדר 2 ב- $S_2$  ואיבר מסדר 3 ב- $S_3$ .

פתרון. האיברים מסדר 6 בחבורה  $S_5$  הם בדיוק התמורות שניתן לרשום כמכפלה של מחזורים זרים מאורך 2 ומאורך 3. למשל התמורה (12)(345).

## שאלות להגשה

**שאלה 4.** הזכרו בהגדרת פונקציית אוילר

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

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

הערה. שאלה זו עברה להיות שאלת רשות, מפני שההדרכה הייתה מבלבלת. הטענה בשאלה למעשה שקולה למשפט השאריות הסיני עבור מספרים.

טענה (משפט השאריות הסיני). אם  $n, m$  זרים, אזי לכל  $a, b \in \mathbb{Z}$  קיים  $x$  יחיד עד כדי שקילות מודולו  $nm$  כך ש- $x \equiv a \pmod{n}$  וגם  $x \equiv b \pmod{m}$ .

הוכחת הטענה. מפני ש- $(n, m) = 1$ , אזי קיימים  $s, t \in \mathbb{Z}$  כך ש- $sn + tm = 1$ . כדי להוכיח קיום של  $x$  נתבונן ב- $bsn + atm$ . מתקיים

$$bsn + atm \equiv atm \equiv a \cdot 1 \equiv a \pmod{n}$$

$$bsn + atm \equiv bsn \equiv b \cdot 1 \equiv b \pmod{m}$$

ולכן  $x = bsn + atm$  הוא פתרון אפשרי. ברור כי גם  $x' = x + kmn$  לכל  $k \in \mathbb{Z}$  הוא פתרון תקף.

כדי להראות יחידות של  $x$  מודולו  $nm$  נשתמש בטיעון קומבינטורי. לכל זוג  $(a, b)$  יש  $(nm)$  (לפחות אחד) המתאים לו מודולו  $nm$ . ישנם בסה"כ  $nm$  זוגות שונים  $(a, b)$  (מודולו  $nm$ ), וכן רק  $nm$  ערכים אפשריים ל- $x$  (מודולו  $nm$ ). ההתאמה הזו היא פונקציה חח"ע בין קבוצות סופיות שוות עוצמה, ולכן ההתאמה היא גם על. דרך אחרת: אם קיים מספר  $y$  המקיים את הטענה, אז  $n|x - y$  וגם  $m|x - y$ . מהנתון  $(n, m) = 1$  נקבל כי  $nm|x - y$  ולכן  $x \equiv y \pmod{nm}$ .  $\square$

פתרון. תחילה נניח  $(n, m) = 1$  ונוכיח  $\varphi(nm) = \varphi(n)\varphi(m)$ .

לכל  $a \in \{1, 2, \dots, n\}$  ו- $b \in \{1, 2, \dots, m\}$  נתאים  $x \in \{1, 2, \dots, nm\}$  כך ש- $x \equiv a \pmod{n}$ ,  $x \equiv b \pmod{m}$  לפי משפט השאריות הסיני. נניח  $n = p_1^{n_1} \dots p_k^{n_k}$  ו- $m = q_1^{m_1} \dots q_r^{m_r}$  הוא פירוק לראשוניים של  $n$  ו- $m$ , בהתאמה. אז  $p_i \neq q_j$  לכל  $i, j$  מפני ש- $(n, m) = 1$ . אנו יודעים כי

$$(x, nm) = (x, n)(x, m) = (a, n)(b, m)$$

שהרי אם  $p$  ראשוני ו- $(x, nm) = p$ , אז  $p|x$  והוא מחלק בדיוק אחד מ- $n$  או  $m$ . ולהפך, אם  $(a, n) = p$  (בלי הגבלת הכלליות), אז  $p$  מחלק את  $x = bsn + atm$ , אבל לא מחלק את  $m$ . לכן  $(x, nm) = 1$  אם ורק אם  $(a, n) = 1$  וגם  $(b, m) = 1$ . מספר הטבעיים שזרים ל- $nm$  וקטנים ממנו זה בדיוק  $\varphi(nm)$ , ונסיק שמספר זה שווה למספר הזוגות  $(a, b)$  כאשר  $a$  זר ל- $n$  וקטן מ- $n$  (יש  $\varphi(n)$  כאלו), ו- $b$  זר ל- $m$  וקטן מ- $m$  (יש  $\varphi(m)$  כאלו). כלומר  $\varphi(nm) = \varphi(n)\varphi(m)$ .

מהוכחת כיוון זה נסיק את הנוסחה שראינו בכיתה:  $\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$  כאשר המכפלה רצה על כל הראשוניים שמחלקים את  $n$ .

לכיוון ההפוך, נניח  $\varphi(nm) = \varphi(n)\varphi(m)$ . נסמן  $d = (n, m)$ . אז

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

ונקבל  $\varphi(d) = d$  שכן אם  $d = 1$ .

**שאלה 5.** 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  $o(g) = m$ , אז

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

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,  $e = g^m \in H$  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  $H$  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 6.** 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 7.** פתרו את המשוואות הבאות. כלומר מצאו כל  $x \in \mathbb{Z}$  המקיים אותן, ולא רק אחד.

$$\begin{aligned} \text{א. } 33x &\equiv 1 \pmod{218} \\ \text{ב. } -7x + 3 &\equiv 9 \pmod{30} \end{aligned}$$

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 8.** לכל תמורה  $\sigma$  מהתמורות הבאות, כתבו את  $\sigma$  כמכפלת מחזורים זרים וחשבו את  $\sigma^2$ , את  $\sigma^{20}$  ואת  $o(\sigma)$ .

$$\text{א. } \left( \begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 2 & 9 & 7 & 1 & 6 & 4 & 3 & 8 \end{array} \right) \in S_9$$

$$\text{ב. } (1 \ 2) (2 \ 5 \ 4) (3 \ 1 \ 4) (1 \ 5) \in S_5$$

פתרון.

א. נסמן את התמורה הנתונה  $\sigma$ . מפרקים לפי הדרך שראינו בתרגול. מקבלים כי יש את המעגלים הבאים:

$$1 \mapsto 5 \mapsto 1, 3 \mapsto 9 \mapsto 8 \mapsto 3, 4 \mapsto 7 \mapsto 4$$

לכן  $\sigma = (1\ 5)(3\ 9\ 8)(4\ 7)$  (2 ו-6 נשלחים כל אחד לעצמו).  
נחשב את  $\sigma^2$  בעזרת העובדה שמחזורים זרים מתחלפים זה עם זה, ונקבל:

$$\sigma^2 = (1\ 5)^2 (3\ 9\ 8)^2 (4\ 7)^2 = (3\ 8\ 9)$$

הסדר של תמורה בהצגה כמכפלת מחזורים זרים היא הכמ"מ של אורכי המחזורים. אצלנו  $o(\sigma) = [2, 3, 2] = 6$ . לכן  $\sigma^6 = \text{id}$ . מכאן קל לחשב

$$\sigma^{20} = (\sigma^6)^3 \sigma^2 = \text{id}^3 \cdot \sigma^2 = (3\ 8\ 9)$$

ב. נסמן את התמורה הנתונה  $\sigma$ . פה התמורה בכלל לא נתונה בצורה נוחה, ולכן נכתוב אותה כמטריצה:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 3 & 1 \end{pmatrix}$$

לכן קל לראות שיש פה מעגל אחד, כלומר  $\sigma = (1\ 4\ 3\ 2\ 5)$ . נחשב את  $\sigma^2$ :

$$\sigma^2 = (1\ 4\ 3\ 2\ 5)^2 = (1\ 3\ 5\ 4\ 2)$$

סדר של מחזור הוא אורכו, ולכן  $o(\sigma) = 5$ . לכן  $\sigma^5 = \text{id}$  ונקבל  $\sigma^{20} = (\sigma^5)^4 = \text{id}$ .

**שאלה 9.** תהי  $\sigma \in S_n$  תמורה, ויהי מחזור  $a = (a_1, a_2, \dots, a_k) \in S_n$ . הוכיחו כי

$$\sigma a \sigma^{-1} = \sigma(a_1, a_2, \dots, a_k) \sigma^{-1} = (\sigma(a_1), \sigma(a_2), \dots, \sigma(a_k))$$

למשל, עבור  $\sigma = (1\ 2)(4\ 5)$  ו- $a = (2\ 3\ 5\ 6)$  נקבל

$$\sigma(2\ 3\ 5\ 6)\sigma^{-1} = (1\ 3\ 4\ 6)$$

כרשות, האם אתם יכולים למצוא נוסחה עבור  $\sigma a \sigma^{-1}$  כאשר  $a$  היא תמורה כלשהי?

פתרון. שיוויון בין שתי פונקציות, כמו למשל התמורות בשאלה, אפשר להוכיח על ידי זה שנראה שכל קלט נשלח לאותו פלט בשתי הפונקציות. כלומר נבדוק לאן האיברים  $\{1, 2, \dots, n\}$  מועתקים בשתי התמורות.

ראשית, נניח כי  $m = \sigma(a_i)$  עבור איזשהו  $1 \leq i \leq k$ . התמורה באגף ימין תשלח את  $m$  ל- $\sigma(a_{i+1})$  כאשר האינדקס  $i+1$  מחושב מודולו  $k$ . נסתכל מה קורה באגף שמאל:

$$\begin{aligned} (\sigma(a_1, a_2, \dots, a_k) \sigma^{-1})(m) &= \sigma((a_1, a_2, \dots, a_k) (\sigma^{-1}(\sigma(a_i)))) \\ &= \sigma((a_1, a_2, \dots, a_k)(a_i)) = \sigma(a_{i+1}) \end{aligned}$$

ולכן התמורות פועלות אותו דבר על  $\sigma(a_1), \dots, \sigma(a_k)$ . כעת נניח כי  $m$  אינו מהצורה  $\sigma(a_i)$  לאף  $1 \leq i \leq k$ ; לכן התמורה באגף ימין תשלח אותו לעצמו. לגבי אגף שמאל: נשים לב כי  $\sigma^{-1}(m) \neq a_i$  לכל  $i$ , ולכן

$$(\sigma(a_1, a_2, \dots, a_k) \sigma^{-1})(m) = \sigma((a_1, a_2, \dots, a_k) (\sigma^{-1}(m))) = \sigma(\sigma^{-1}(m)) = m$$

מכאן ששתי התמורות האלו שוות.

**שאלה 10.** נתבונן ב- $S_n$  עבור  $n > 2$ .

א. הוכיחו שלכל מחזור  $\tau \in S_n$   $\text{id} \neq \tau$  קיימת תמורה  $\sigma \in S_n$  כך ש- $\tau\sigma \neq \sigma\tau$ . רמז: העזרו בשאלה הקודמת.

ב. הוכיחו כי  $Z(S_n) = \{\text{id}\}$ .

פתרון.

א. נניח כי  $\tau = (a_1, \dots, a_k)$ . נשים לב ש- $\tau\sigma = \sigma\tau$  אם ורק אם  $\tau\sigma\tau^{-1} \neq \tau$ . בעזרת השאלה הקודמת, נוכל למצוא  $\sigma$  כדרוש. אם האורך של המחזור  $k \geq 3$ , אז נבחר  $\sigma = (a_1, a_2)$  ונקבל

$$(a_1, a_2)(a_1, a_2, a_3, \dots, a_k)(a_1, a_2)^{-1} = (\sigma(a_1), \sigma(a_2), \sigma(a_3), \dots, \sigma(a_k)) \\ = (a_2, a_1, a_3, \dots, a_k)$$

מפני ש- $\tau$  שולח את  $a_1$  ל- $a_2$  ואילו  $\sigma\tau\sigma^{-1}$  שולח את  $a_1$  ל- $a_3$ , אז בודאי  $\tau\sigma\tau^{-1} \neq \tau$ . נותרנו עם המקרה שבו  $k = 2$ . כלומר  $\tau = (a_1, a_2)$ . מן הנתון  $n > 2$ , נסיק שקיים  $b \in \{1, \dots, n\} \setminus \{a_1, a_2\}$ . נבחר  $\sigma = (a_1, b)$  ונחשב

$$(a_1, b)(a_1, a_2)(a_1, b)^{-1} = (\sigma(a_1), \sigma(a_2)) = (b, a_2)$$

מפני ש- $\tau$  שולח את  $a_2$  ל- $a_1$  ואילו  $\sigma\tau\sigma^{-1}$  שולח את  $a_2$  ל- $b$ , אז בודאי  $\tau\sigma\tau^{-1} \neq \tau$ .

ב. המרכז הוא תת-חבורה, ולכן תמיד כולל את איבר היחידה. כלומר  $\text{id} \in Z(S_n)$ . נניח בשלילה שקיימת תמורה  $\sigma \in Z(S_n)$ ,  $\text{id} \neq \sigma$ , ויהי  $\sigma = \sigma_1 \dots \sigma_r$  פירוק שלה למכפלת מחזורים זרים.

אם  $r = 1$ , אז  $\sigma$  היא מחזור, וסיימנו לפי הסעיף הקודם שבו מצאנו תמורה שלא מתחלפת עם  $\sigma$ .

נניח  $r > 1$  ושקיים בפירוק למחזורים זרים מחזור מאורך לפחות 3. בלי הגבלת הכלליות נניח  $\sigma_1$  הוא מחזור מאורך  $k \geq 3$  (כי מחזורים זרים מתחלפים, כלומר  $\sigma_i\sigma_j = \sigma_j\sigma_i$ ). נסמן  $\sigma_1 = (a_1, \dots, a_k)$ . כמו בסעיף הקודם נבחר  $\mu = (a_1, a_2)$ , נשים לב כי  $\mu$  מתחלף עם  $\sigma_2, \dots, \sigma_r$  ונחשב

$$\mu\sigma\mu^{-1} = \mu\sigma_1\sigma_2 \dots \sigma_r\mu^{-1} = \mu\sigma_1\mu^{-1}\sigma_2 \dots \sigma_r$$

נניח בשלילה כי  $\sigma = \mu\sigma\mu^{-1}$ , ונכפיל ב- $(\sigma_2 \dots \sigma_r)^{-1}$  מימין ונקבל  $\sigma_1 = \mu\sigma_1\mu^{-1}$ . בסתירה לסעיף הקודם.

נותרנו רק עם המקרה שבו בפירוק של  $\sigma$  למחזורים זרים מופיעים רק חילופים (מחזורים מאורך 2). נניח  $\sigma_1 = (a_1, a_2)$  ו- $\sigma_2$  עבור  $a_1, a_2, b_1, b_2$  שונים (הבינו למה מקרה זה לא יקרה עבור  $n = 3$ ). נבחר  $\mu = (a_1, b_1)$  ונקבל

$$\mu\sigma\mu^{-1} = \mu\sigma_1\sigma_2\sigma_3 \dots \sigma_r\mu^{-1} = \mu\sigma_1\sigma_2\mu^{-1}\sigma_3 \dots \sigma_r$$

כי  $\mu$  מתחלף עם  $\sigma_3, \dots, \sigma_r$ . נניח בשלילה כי  $\sigma = \mu\sigma\mu^{-1}$ , ונכפיל ב- $(\sigma_3 \dots \sigma_r)^{-1}$  מימין ונקבל  $\sigma_1\sigma_2 = \mu\sigma_1\sigma_2\mu^{-1}$ , אבל

$$\mu\sigma_1\sigma_2\mu^{-1} = (a_1, b_1)(a_1, a_2)(b_1, b_2)(a_1, b_1) = (a_1, b_2)(a_2, b_1) \neq (a_1, a_2)(b_1, b_2)$$

וזו סתירה. בסך הכל קיבלנו כי  $\sigma \notin Z(S_n)$  לכן  $Z(S_n) = \{\text{id}\}$ .

## שאלות רשות

את שאלות הרשות אין חובה לפתור, אבל אם פתרתם אותן, בבקשה צרפו את הפתרון שלהן.

**שאלה 11.** 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 12.** 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  $\aleph_0$ ?

**שאלה 13.** כתבו תוכנה שמקבלת כקלט רשימת מספרים המייצגת תמורה, כלומר מקבלת את השורה השנייה בהצגת תמורה כמטריצה בגודל  $2 \times n$ . התוכנה תחזיר בפלט את התמורה כמכפלת מחזורים זרים. הרחיבו את התוכנה כך שתקבל כמה תמורות, ותחזיר את מכפלתן כמכפלת מחזורים זרים.

בהצלחה!