

פתרון תרגיל בית 9 במבנים אלגבריים 89-214 סמסטר א' תשפ"ג

שאלה 1 (חזרה). מצאו את כל המחלקות השמאליות ב- $\mathbb{Z}_{30}/\langle 3 \rangle$. פתרו. האיבר $3 \in \mathbb{Z}_{30}$ הוא מסדר 10, ולכן $|\langle 3 \rangle| = 10$. לפי משפט לגראנז' נקבל

$$|\mathbb{Z}_{30}/\langle 3 \rangle| = \frac{|\mathbb{Z}_{30}|}{|\langle 3 \rangle|} = \frac{30}{10} = 3$$

והמחלקות, עד כדי בחירת נציגים, הן $\{\langle 3 \rangle, 1 + \langle 3 \rangle, 2 + \langle 3 \rangle\}$.

שאלה 2. תזכורת: מספר פריק n נקרא מספר קרמייקל אם ורק אם לכל $b \leq n$ הזר ל- n מתקיים $b^{n-1} \equiv 1 \pmod{n}$ (או באופן שקול $b^n \equiv b \pmod{n}$ לכל b). הריצו את אלגוריתם מילר-רבין עבור המספר 29341 והעדים (הפוטנציאליים) $a, b+2$, כאשר a הוא 3 הספרות הראשונות בת"ז שלכם ו- b הוא 2 הספרות האחרונות. כתבו את מסקנתכם מההרצה.

שאלה 3. הוכיחו או הפריכו האם $H \triangleleft G$ עבור החבורות ותת־הקבוצות הבאות:

א. $H = \langle (89)(214) \rangle, G = S_9$.

ב. $H = \{\sigma \in S_n \mid \sigma(1) = 1\}, G = S_n$.

ג. $H = \{\alpha I \mid \alpha \in F^*\}, G = GL_n(F)$ (כאן H היא קבוצת המטריצות הסקלריות ההפיכות מעל השדה F).

פתרון.

א. הפרכה: ניקח לדוגמה את $(89)(214) \in H$ ואת $(13) \in G$, ונראה ש- H אינה סגורה להצמדה:

$$(13)(89)(214)(13)^{-1} = (13)(89)(214)(13) = (89)(234) \notin H$$

התמורה הזו לא ב- H כי 3 היא נקודת שבת של כל התמורות ב- H .

ב. הפרכה, $H \not\triangleleft G$ עבור $n \geq 3$. אכן, בעוד ש- $(23) \in H$ כי $\sigma(1) = 1$, אחרי הצמדה $(12)(23)(12) = (13) \notin H$. עבור $n < 3$ החבורה S_n היא אבלית, ולכן כל תת־חבורה שלה היא נורמלית.

ג. הוכחה: לכל $A \in G, B \in H$ מתקיים ש- $B = \alpha I$ עבור $\alpha \in F^*$ כלשהו ולכן

$$AB = A\alpha I = \alpha AI = \alpha A = \alpha IA = BA$$

בפרט $AH = HA$ לכל $A \in G$.

שאלה 4. הפריכו את הטענות השגויות הבאות:

- כל תת-חבורה אבלית היא נורמלית.
 - כל תת-חבורה נורמלית היא אבלית.
 - התמונה של כל הומומורפיזם $f: G \rightarrow H$ היא תת-חבורה נורמלית של H .
- פתרון.

א. למשל $\langle (1\ 2) \rangle$ היא תת-חבורה אבלית של S_3 שאינה נורמלית.

ב. למשל $SL_2(\mathbb{R})$ אינה אבלית, אבל היא נורמלית ב- $GL_2(\mathbb{R})$.

ג. למשל בכל שיכון $f: \langle (1\ 2) \rangle \rightarrow S_3$ התמונה היא לא תת-חבורה נורמלית.

שאלה 5. תהי G חבורה מסדר 46, ותהי H תת-חבורה לא נורמלית שלה. מצאו את הסדר של H .

פתרון. לפי משפט לגראנז' הסדר של H מחלק את $|G|$. לכן $|H| \in \{1, 2, 23, 46\}$. אם $|H| = 1$, זו בהכרח תת-החבורה הטריוויאלית שתמיד נורמלית. אם $|H| = 46$, זו בהכרח G כולה ולכן נורמלית. אם $|H| = 23$, אז זו תת-חבורה מאינדקס 2, ולכן לפי טענה שהוכחנו בכיתה, שוב נורמלית. לכן בהכרח $|H| = 2$.

שאלה 6. תהי $H \leq G$ תת-חבורה. הוכיחו כי $H \triangleleft G$ אם ורק אם לכל $x, y \in G$ מתקיים

$$yx \in H \iff xy \in H$$

פתרון. בכיוון אחד, נניח כי H תת-חבורה נורמלית של G , לכן $H = \ker(f)$ עבור הומומורפיזם f שתחמו G .

יהיו $x, y \in G$ כך ש- $xy \in H$ (ההוכחה דומה עבור המקרה שבו $yx \in H$). מתקיים: $f(x)f(y) = f(xy) = e$ כיוון ש- $H = \ker(f)$. זאת אומרת ש- $f(x), f(y)$ הופכיים זה לזה, לכן גם $f(y)f(x) = e$, ומכאן $yx \in \ker(f) = H$.

בכיוון השני, יהיו $h \in H, g \in G$, ונרצה להוכיח כי $g^{-1}hg \in H$ (זה יראה סגירות להצמדה, כלומר $g^{-1}Hg \subseteq H$ לכל $g \in G$, וזה תנאי שהוכחנו ששקול לנורמליות). נשים לב כי $g^{-1}gh = h \in H$, ולכן לפי ההנחה, גם $g^{-1}hg \in H$ (כדורש) (חשבו על זה כך: $x = g^{-1}, y = gh$).

ניתן להוכיח גם את הכיוון הראשון ע"י סגירות להצמדה, אך קצת גיוון לא יזיק.

שאלה 7. חבורה G נקראת פשוטה אם אין לה תת-חבורות נורמליות לא טריוויאליות (כלומר שונות מ- $\{e\}$, G).

א. תהי G חבורה פשוטה ו- H חבורה כלשהי. הוכיחו שאם $f: G \rightarrow H$ הוא הומומורפיזם לא טריוויאלי, אז f מונומורפיזם.

ב. הוכיחו שלא קיימת חבורה אבלית פשוטה אינסופית.

ג. תהי A חבורה אבלית פשוטה. הוכיחו כי A טריוויאלית או שקיים p ראשוני כך ש- $A \cong \mathbb{Z}_p$.

פתרון.

א. גרעין של הומומורפיזם הוא תת-חבורה נורמלית. אזי $\ker(f) \triangleleft G$. נתון כי תת-החבורות הנורמליות של G (כמו $\ker(f)$) הן $\{e\}$ או G . בנוסף $\ker(f) \neq G$ כי f הוא הומומורפיזם לא טריוויאלי, ולכן $\ker(f) = \{e\}$. ראינו בהרצאה שאם הגרעין טריוויאלי, אז f הוא ח"ע. כלומר f הוא מונומורפיזם.

ב. נניח בשלילה כי G היא חבורה אבלית פשוטה ואינסופית. לכן קיים איבר $e \neq g \in G$ שהרי יש בה אינסוף איברים. אם $o(g) < \infty$, אז $\langle g \rangle \triangleleft G$ היא תת-חבורה נורמלית כי G אבלית. נשים לב כי $\langle g \rangle$ אינה $\{e\}$ שהרי $g \notin \{e\}$ ולכן $g \in \langle g \rangle \neq \{e\}$, ואינה G כי ב- G יש אינסוף איברים ואילו ב- $\langle g \rangle$ רק מספר סופי. זו סתירה לכך שיש ל- G איבר מסדר סופי שאינו איבר היחידה.
 אחרת, אם $o(g) = \infty$, אז נתבונן בתת-החבורה $\langle g^2 \rangle$. גם $\langle g^2 \rangle$ תת-חבורה נורמלית של G כי G אבלית. הפעם $g \notin \langle g^2 \rangle$ ולכן $\langle g^2 \rangle \neq G$ וגם $\langle g^2 \rangle \neq \{e\}$ כי $g^2 \neq e$ מפני שהסדר של g אינסופי. זו סתירה לכך שיש ל- G איברים מסדר אינסופי. לכן אין חבורה אבלית פשוטה אינסופית (כי אין לה איברים מסדר סופי או אינסופי).

ג. לפי הסעיף הקודם, אפשר להניח כי A היא סופית. אם A טריוויאלית, סיימנו. אחרת, החבורה A לא טריוויאלית וקיים איבר $e \neq g \in A$ שאינו טריוויאלי. נסמן $n = o(g)$. ברור כי $\langle g \rangle \triangleleft A$ מפני ש- A אבלית. בנוסף $\langle g \rangle$ אינה $\{e\}$ ולכן $\langle g \rangle = A$ ובפרט $|A| = n$. אם n הוא פריק, למשל $n = pm$ כאשר p ראשוני ו- $m > 1$, אז נתבונן בתת-החבורה $H = \langle g^m \rangle$. לפי טענה שראינו בהרצאה הסדר של g^m הוא

$$o(g^m) = \frac{o(g)}{(o(g), m)} = \frac{n}{(n, m)} = \frac{pm}{(pm, m)} = \frac{pm}{m} = p$$

כלומר $\langle g^m \rangle$ היא תת-חבורה של A מסדר $1 < p < n$, והיא תת-חבורה נורמלית כי A אבלית. זו סתירה להנחה ש- A פשוטה. לכן n לא פריק, למשל $n = p$ ראשוני. ראינו שכל חבורה מסדר ראשוני היא ציקלית, ושכל חבורה ציקלית מסדר סופי n נתון איזומורפית ל- \mathbb{Z}_n . אצלנו $A \cong \mathbb{Z}_p$.

שאלה 8. בשאלה הזו תראו שאלגוריתם מילר-רבין הוא דטרמיניסטי למספרים לא כל כך קטנים עבור קבוצת עדים נתונה.

א. חשבו ש-97 הוא עד חזק לראשוניות של 469 ואילו 133 לא. לעומת זאת, חשבו כי 133 הוא עד חזק לראשוניות של 305 ואילו 79 לא. ודאו חישובים אלו בסעיף הבא.

ב. בחרו שפת תכנות כרצונכם וכתבו פונקציה בשם `millerabin(N, W)` המממשת את אלגוריתם מילר-רבין למספר טבעי N ולקבוצת עדים נתונה W (בכיתה במקום W בחרנו באקראי כמה מספרים).
 הראו שהעדים החזקים לראשוניות של 505 בקטע [2, 503] הם רק 192, 212, 293, 313.

ג. כתבו פונקציה נוספת `first_mistake(W)` שמחזירה את המספר $N \geq 3$ האי זוגי הקטן ביותר שעבורו הפונקציה `millerabin(N, W)` טועה. כלומר התשובה של `millerabin(N, W)` שונה מהתשובה של `is_prime(N)`, המחזירה בודאות האם N ראשוני. רק עבור המימוש של `is_prime(N)` אפשר להשתמש בספריות חיצוניות!¹

דוגמה להרצה היא `first_mistake({2}) = 2047`. כלומר לכל מספר אי זוגי $3 \leq N < 2047$ הקריאה `millerabin(N, {2})` מחזירה ש-2047 כנראה ראשוני, אבל הוא למעשה פריק: $2047 = 23 \cdot 89$. כתבו את התוצאות של הרצת:

- `first_mistake({3})` •
- `first_mistake({3, 5})` •
- `first_mistake({4, 9})` •
- `first_mistake({7, 11})` •

¹כמובן שאפשר לממש בעצמכם. אפשרות טובה לשאלה הנוכחית היא [הנפה של ארטוסנס](#) עם מטמון (Cache). לחלק הזה אפשר להשתמש במערכת תוכנה מתמטית.

first_mistake({7, 11, 13}) •

פתרון.

א. בפתרון מלא יש לפרט את חישובי החזקות המודולריות.
נסמן $N = 469$ ולפי הסימונים $N - 1 = 2^s M$ מהכיתה נקבל $468 = 2^2 \cdot 117$. יהי
 $a = 97 \in [2, 467]$. לפי אלגוריתם מילר-רבין נסמן $x = a^M$ ונחשב בלולאה את x^{2^i}
עבור $0 \leq i < s$. נתחיל עם החישוב

$$x = a^{2^0 M} = 97^{117} \equiv 468 \pmod{469}$$

והרי $468 \equiv -1 \pmod{469}$. לכן 97 הוא עד חזק לראשוניות של 469. עבור
 $a = 133$ נחשב

$$x = a^{2^0 M} = 133^{117} \equiv 133 \pmod{469}$$

$$x^2 = a^{2^1 M} = (133^{117})^2 \equiv 336 \pmod{469}$$

אף אחד מאלו אינו שקול ל-1 מודולו 469. לכן מעיד כי 469 הוא פריק. אגב,
הפירוק שלו לגורמים ראשוניים הוא $469 = 7 \cdot 67$.
נסמן $N = 305$ ולכן במקרה זה בסימונים $N - 1 = 2^s M$ נקבל $304 = 2^4 \cdot 19$. יהי
 $a = 133 \in [2, 303]$. כמו מקודם, לפי אלגוריתם מילר-רבין נסמן $x = a^M$ ונחשב
בלולאה את x^{2^i} עבור $0 \leq i < s$:

$$x = a^{2^0 M} = 133^{19} \equiv 172 \pmod{305}$$

והרי 172 אינו ± 1 מודולו 305. לכן נמשיך

$$x^2 = a^{2^1 M} = (133^{19})^2 \equiv 304 \equiv -1 \pmod{305}$$

ולכן 133 הוא עד חזק לראשוניות של 305. עבור $a = 79$ נחשב

$$x = a^{2^0 M} = 79^{19} \equiv 189 \pmod{305}$$

$$x^2 = a^{2^1 M} = (79^{19})^2 \equiv 36 \pmod{305}$$

$$x^4 = a^{2^2 M} = ((79^{19})^2)^2 \equiv 76 \pmod{305}$$

$$x^8 = a^{2^3 M} = (((79^{19})^2)^2)^2 \equiv 286 \pmod{305}$$

אף אחד מאלו אינו שקול ל-1 מודולו 305. לכן מעיד כי 305 הוא פריק. אגב,
הפירוק שלו לגורמים ראשוניים הוא $305 = 5 \cdot 61$.

ב. נשמח לשמוע על מימושים מקוריים.

ג. שימו לב שהשגיאה היחידה שיכולה להיות באלגוריתם מילר-רבין היא שהוא יחזיר
מספר פריק בתור "כנראה ראשוני". לכן התוצאות להרצות תמיד יהיו מספרים פריקים:

first_mistake({3}) = 121 •

first_mistake({3, 5}) = 112141 •

first_mistake({4, 9}) = 8911 •

first_mistake({7, 11}) = 88831 •

first_mistake({7, 11, 13}) = 1152271 •

בהצלחה!