

## פתרון - 89-214 מבנים אלגבריים – מועד א' – 12/02/21

משך המבחן – שעתיים. השימוש במחשבון מותר. מרצה – דר' ארז שיינר

כל שאלה שווה 28 נקודות, לאחריהן – שאלות מיטיבות. כל ציון מעל 100 יעוגל ל100.

1. תהינה  $G, H$  חבורות, ויהי  $f: G \rightarrow H$  הומומורפיזם כך ש  $|G| = 15, |H| = 21$

א. האם ייתכן ש  $\ker(f) = \text{Im}(f)$ ? אם כן תנו דוגמא ל  $G, H, f$  כאלה, אחרת הוכיחו שאינם קיימים.

לא ייתכן. לפי משפט האיזומורפיזם הראשון מתקיים כי

$$G/\ker(f) \cong \text{im}(f)$$

כעת לפי משפט לאגרנז' גודל חבורת המנה שווה לגודל החבורה חלק גודל תת החבורה

$$|G/\ker(f)| = \frac{|G|}{|\ker(f)|}$$

וכן לחבורות איזומורפיות אותו הגודל (סדר)

לכן סה"כ

$$\frac{|G|}{|\ker(f)|} = |\text{im}(f)|$$

אם  $\ker(f) = \text{im}(f)$  נקבל כי  $|\ker(f)|^2 = |\ker(f)| \cdot |\text{im}(f)| = |G|$

אבל  $|G| = 15$  ולא ייתכן שזה שווה למספר שלם בריבוע.

ב. האם  $\text{Im}(f)$  אבלית בהכרח? אם כן, הוכיחו, אם לא תנו דוגמא ל  $G, H, f$  כאלה.

ידוע כי התמונה כי תת חבורה של הטווח, ולכן סדר התמונה מחלק את סדר הטווח.

כיוון ש  $|H| = 21$  גודל התמונה יכול להיות  $\{1, 3, 7, 21\}$ .

כעת, כפי שראינו בסעיף א' (ובאופן כללי) גודל התמונה קטן או שווה לגודל התחום, וכיוון ש  $|G| = 15$  בהכרח  $|\text{im}(f)| \neq 21$

אם  $|\text{im}(f)| = 1$  אז התמונה היא החבורה הטריטיואלית בעלת איבר היחידה בלבד, והיא בוודאי אבלית (איבר היחידה מתחלף עם עצמו).

אחרת,  $|\text{im}(f)| = 3, 7$  הם מספרים ראשוניים, וחבורה מגודל ראשוני היא ציקלית, ולכן אבלית.

2. תהי  $S_n$  חבורת התמורות, ותהי  $H = \{f \in S_n | \text{sign}(f) = 1\}$  קבוצת כל התמורות הזוגיות.

א. הוכיחו כי  $H$  תת חבורה של  $S_n$ .

נוכיח באמצעות הקריטריון המקוצר, והרי נתון כי  $H \subseteq S_n$ .

ראשית, למדנו שסימן תמורה הזהות הוא זוגי, כלומר  $\text{sign}(Id) = 1$  ולכן  $Id \in H$  והרי תמורת הזהות היא איבר היחידה של החבורה  $S_n$ .

כעת, תהיינה  $f, g \in H$  כלומר נתון כי  $\text{sign}(f) = \text{sign}(g) = 1$ .

כמו כן

$$1 = \text{sign}(Id) = \text{sign}(gg^{-1}) = \{\text{כפליות הסימן}\} = \text{sign}(g) \cdot \text{sign}(g^{-1})$$

ולכן

$$\text{sign}(g^{-1}) = \frac{1}{\text{sign}(g)} = \text{sign}(g)$$

(המעבר האחרון הוא מכיוון ש  $\frac{1}{\pm 1} = \pm 1$ )

לכן

$$\text{sign}(fg^{-1}) = \{\text{כפליות הסימן}\} = \text{sign}(f) \cdot \text{sign}(g^{-1}) = \text{sign}(f) \cdot \text{sign}(g) = 1 \cdot 1 = 1$$

ולכן  $fg^{-1} \in H$  כפי שרצינו.

ב. הוכיחו כי  $H$  תת חבורה נורמלית של  $S_n$ .

תהי  $f \in S_n$  תמורה זוגית, נוכיח כי  $fH = H$  באמצעות הכלה דו כיוונית.

תהי  $g = fh \in fH$  אזי

$$\text{sign}(g) = \text{sign}(fh) = \{\text{כפליות הסימן}\} = \text{sign}(f) \cdot \text{sign}(h) = 1 \cdot 1 = 1$$

ולכן אכן  $fh \in H$

מצד שני, תהי  $h \in H$  אזי  $hf^{-1} = h$

כעת ראינו כי  $\text{sign}(f^{-1}) = \text{sign}(f)$  ויחד עם כפליות הסימן נקבל כי

$$\text{sign}(f^{-1}h) = \text{sign}(f^{-1}) \cdot \text{sign}(h) = \text{sign}(f) \cdot \text{sign}(h) = 1 \cdot 1 = 1$$

ולכן  $f^{-1}h \in H$  ולכן

$$h = f(f^{-1}h) \in fH$$

לפי הוכחה דומה גם  $H = Hf$  וסה"כ  $fH = Hf$

כעת תהי  $f \in S_n$  אי זוגית, כלומר  $f \notin H$

באופן דומה ניתן להוכיח כי  $fH = Hf = S_n \setminus H$  הוא אוסף התמורות האי זוגיות.

לכן סה"כ  $H$  תת חבורה נורמלית.

3. בוב רוצה לשלוח לאליס מסר מוצפן בשיטת RSA.

אליס בחרה מספרים ראשוניים  $p, q$  הקרובים זה לזה, וחישבה את  $n = 62473207$ .

א. מצאו את  $m = \phi(n)$ , מדוע יכולתם לעשות זאת?

נתון כי  $p, q$  קרובים זה לזה, כלומר קיים  $a$  קטן כך ש  $q = p + a$  (בחרנו לסמן את הראשוני הגדול ב  $q$ )

כעת

$$p = \sqrt{p^2} \leq \sqrt{pq} = \sqrt{n} \leq \sqrt{q^2} = q = p + a$$

כלומר  $\sqrt{n}$  שייך לטווח המספרים הטבעיים בין  $p$  ל  $p + a$

ולכן אם נתחיל מ  $\sqrt{n}$  ונלך לאחד הכיוונים (למעלה או למטה) על מספרים טבעיים, ונבדוק האם המספר מחלק את  $n$  לכל היותר

לאחר  $a$  צעדים (נתון שזה מספר קטן) נגיע למספר שמחלק את  $n$ , המספר השני הוא תוצאת החלוקה.

שימו לב – אין שום צורך או הגיון בנסות לעבור על ראשוניים בלבד, הרי בדיקה אם המספר מחלק את  $n$  יעילה בהרבה מבדיקת

הראשוניות.

נקבל כי  $p = 7901, q = 7907$  ולכן

$$m = \phi(n) = (p - 1)(q - 1) = 7900 \cdot 7906 = 62645700$$

ב. האם ייתכן שאליס בחרה  $e = 78545$ ? הצדיקו תשובתכם.

לא, הרי  $e, m$  צריכים להיות זרים ושניהם מתחלקים ב-5.

הערה לגבי הבדיקה:  $\gcd(e, m) \neq 0$  למרות שרבים רשמו זאת בבחינה. זו טעות חמורה שהרי לעולם  $\gcd$  בין שני שלמים חיוביים הוא לפחות 1, וכמו כן לפי האלגוריתם בו השתמשו התלמידים כל  $\gcd$  היה נגמר באפס ולכן לא מתבצעת הבדיקה הנכונה.

4. נביט בפולינום  $g(x) = x^3 + x + 1$ , המגדיר קוד פולינומי.

מצאו את כל ערכי הפרמטרים  $a, b, c \in \mathbb{Z}_2$  כך ש  $(1, 0, a, b, c, 1, 0, 1)$  היא מילה מקודדת חוקית בקוד.

מילה מקודדת היא חוקית אם ורק אם הפולינום המתאים לה מתחלק ב- $g$  ללא שארית.

הערה ראשונה לגבי הבדיקה: אין שום תהליך בו כופלים את המילה שהתקבלה ב- $x^3$  ואז בודקים אם התוצאה מתחלקת ב- $g$ . הזזת הביטים עשויה לשנות את חוקיות המילה, ובוודאי לא מדובר בהליך קידוד.

הערה שנייה לגבי הבדיקה: אין הגיון לדרוש שבשלב כלשהו לפני שנגיע לשארית נקבל אפס או את  $g$ . ייתכן שהמילה חוקית ונקבל אפס בהמשך. (חלק מהתלמידים דרשו שהמקדמים הגבוהים יתאפסו בשלב מוקדם).

כעת לחילוק:

$$x^4 + (a + 1)x^2 + (b + 1)x + (a + c + 1)$$

$$x^7 + ax^5 + bx^4 + cx^3 + x^2 + 1 \mid x^3 + x + 1$$

$$x^7 + x^5 + x^4$$

$$(a + 1)x^5 + (b + 1)x^4 + cx^3 + x^2 + 1$$

$$(a + 1)x^5 + (a + 1)x^3 + (a + 1)x^2$$

$$(b + 1)x^4 + (a + c + 1)x^3 + ax^2 + 1$$

$$(b + 1)x^4 + (b + 1)x^2 + (b + 1)x$$

$$(a + c + 1)x^3 + (a + b + 1)x^2 + (b + 1)x + 1$$

$$(a + c + 1)x^3 + (a + c + 1)x + (a + c + 1)$$

$$(a + b + 1)x^2 + (a + b + c)x + (a + c)$$

המילה חוקית אם ורק אם השארית היא אפס, כלומר אם ורק אם

$$a + b + 1 = a + b + c = a + c = 0$$

כיוון ש  $a + c = 0$  נובע כי  $a = c$  ויחד עם זה ש  $a + b + c = 0$  נובע כי  $b = 0$

לבסוף, יחד עם זה ש  $a + b + 1 = 0$  נקבל כי  $a = 1$

וסה"כ  $a = c = 1, b = 0$  אם ורק אם המילה חוקית.

שאלות מיטיבות: (ניקוד יתקבל בלבד עבור דרך מלאה+תשובה ללא טעויות חישוב)

5. (2 נק') מצאו  $a, b \in \mathbb{Z}$  כך ש  $a \cdot 12345 + b \cdot 67890 = 15$

6. (2 נק') מצאו את  $13^{-1} \bmod 1111$

7. (2 נק') מצאו את  $2^{1055} \bmod 63$