

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

כל שאלה שווה 28 נקודות, כל ציון מעל 100 יעוגל ל-100.

1. תהינה G, H חבורות סופיות כך ש $|G| = |H|$.

א. יהיו $a, b \in G$ איברים מסדר n . הוכיחו/הפריכו: גם ab הוא איבר מסדר n .

לכל איבר a מסדר n מתקיים כי a^{-1} גם הוא מסדר n (הוכיחו זאת בעצמכם), אך המכפלה $aa^{-1} = e$ היא מסדר 1.

לכן כל שעלינו לעשות הוא לבחור איבר מסדר שאינו איבר היחידה (כלומר מסדר שונה מ-1), ואת ההופכי שלו. למשל האיבר $a = 2 \in \mathbb{Z}_3$, ו $a^{-1} = 1$. הסדר של a, a^{-1} , אך הסדר של $2+1=0$ הוא אחד.

ב. יהי $\varphi: G \rightarrow H$ הומומורפיזם, הוכיחו כי φ איזומורפיזם אם ורק אם $\ker(\varphi) = \{e_G\}$.

ראשית, כיוון שהקבוצות סופיות ובגודל זהה, נובע שאם φ חח"ע אזי היא גם על ולכן הפיכה. כמובן שטיעון זה אינו נכון לקבוצות אינסופיות, או לקבוצות סופיות בגדלים שונים.

נותר להוכיח כי φ חח"ע אם ורק אם $\ker(\varphi) = \{e_G\}$.

בכיוון ראשון, נניח כי φ חח"ע, ונוכיח כי $\ker(\varphi) = \{e_G\}$.

ברור כי $e_G \in \ker(\varphi)$. נניח כי $a \in \ker(\varphi)$ ונוכיח כי $a = e_G$.

כיוון ש a שייך לגרעין אזי $\varphi(a) = e_H$. מצד שני $\varphi(e_G) = e_H$ ולכן $\varphi(a) = \varphi(e_G)$.

לפי החח"ע, נובע כי $a = e_G$.

בכיוון השני, נניח כי $\ker(\varphi) = \{e_G\}$ ונוכיח כי φ חח"ע.

יהיו $a, b \in G$ כך ש $\varphi(a) = \varphi(b)$, צ"ל כי $a = b$.

$$ab^{-1} \in \ker(\varphi) \text{ ולכן } e_H = \varphi(a)(\varphi(a))^{-1} = \varphi(ab^{-1})$$

$$\text{לכן } ab^{-1} = e_G \text{ ולכן } a = b$$

2. תהא G תת חבורה של S_n , ותהא $H \subseteq G$ קבוצת כל התמורות בעלות סימן חיובי (זוגיות) ב G .

א. נניח שקיימת $f \in G$ תמורה בעלת סימן שלילי (אי זוגית). הוכיחו ש fH היא קבוצת כל

התמורות בעלות סימן שלילי ב G .

נוכיח הכלה דו-כיוונית. תהי $fh \in fH$. כיוון ש f אי זוגית ו h זוגית, נובע כי fh אכן אי זוגית.

מצד שני, תהי g אי זוגית כלשהי אזי ברור כי $g = ff^{-1}g$, נותר להוכיח כי $f^{-1}g$ זוגית.

כיוון ש f אי זוגית, גם f^{-1} אי זוגית (הרי מכפלתן $ff^{-1} = I$ היא זוגית).

לכן מכפלת האי זוגיות $f^{-1}g$ היא אכן זוגית.

ב. הוכיחו שאם קיימת תמורה בעלת סימן שלילי ב G , אז כמות התמורות הזוגיות ב G שווה

לכמות התמורות האי זוגיות.

לפי סעיף א', אם אוסף התמורות הזוגיות הוא H ו f אי זוגית אזי fH הוא אוסף התמורות האי זוגיות.

כל שנותר להוכיח הוא ש $|fH| = |H|$. נבנה פונקציה חח"ע ועל בין שתי הקבוצות הללו.

$$\text{נגדיר } \varphi: H \rightarrow fH \text{ ע"י } \varphi(h) = fh.$$

אם $\varphi(g) = \varphi(h)$ אזי $fg = fh$ ולכן $g = h$ לפי תכונת הצמצום. לכן φ חח"ע.

תהי $g \in fH$ אזי $g = ff^{-1}g$, וכמו בסעיף א' $f^{-1}g \in H$, לכן φ על.

(דרך נוספת: ניתן להוכיח כי H תת חבורה, ולמדנו בכיתה שכל קוסט fH שווה בגודלו לגודל של H).

3. בוב רוצה לשלוח לאליס מסר מוצפן בשיטת RSA.

אליס פרסמה את המפתח הציבורי $n = 265$, $e = 3$.

א. חשבו את הפרמטרים הסודיים $m = \phi(n)$, $d = e^{-1} \bmod m$. מדוע יכולתם לעשות זאת?

כיוון שהמספר $n = 265$ מסתיים בספרה 5, ברור שזה אחד הראשוניים המחלק אותו. לכן $n = 53 \cdot 5$.

לכן $m = \phi(265) = 52 \cdot 4 = 208$. כעת נחשב את d :

$$208 - 69 \cdot 3 = 1$$

ולכן $d = -69 = 139$.

ב. בוב שלח לאליס את המידע המוצפן $155 = x^3 \bmod n$.

מהו המידע x שבוב שלח לאליס?

המידע הוא $x = 155^{139} \bmod 265$.

ראשית, $139 = 128 + 8 + 2 + 1$, לכן

$$155^{139} = \left(\left(\left(\left(\left((155^2)^2 \right)^2 \right)^2 \right)^2 \right)^2 \right)^2 \cdot \left((155^2)^2 \right)^2 \cdot 155^2 \cdot 155.$$

(זה מזכיר לי פרפר).

סה"כ נקבל כי $100 = 155^{139} \bmod 265$.

4. נביט במטריצה $A = \begin{pmatrix} 0 & 1 & 1 \\ a & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$ נתון כי הקוד הלינארי המתאים ל A מקיים כי המרחק המינימלי בין

שתי מילים חוקיות הוא $d_{\min} = 2$.

א. מצאו את a .

כיוון ש $d_{\min} = 2$ אסור שבמטריצה H תהיה עמודת אפסים (אחרת המרחק המינימלי הוא 1) אבל חייבות להיות שתי עמודות זהות (אחרת המרחק המינימלי הוא לפחות 3).

כעת $H = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ a & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$, רק העמודה הראשונה והאחרונה יכולות להיות שוות, ולכן $a = 0$.

ב. נתון כי v הינה מילה חוקית, והמילה v' מתקבלת משגיאה אחת ב v .

נתון כי $v' = (1,1,1,1,1,1)$ מצאו את v .

ידוע כי $v' = v + e_i$ ולכן $Hv' = Hv + He_i = 0 + C_i(H)$

$$Hv' = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = C_4(H)$$

נחשב $C_4(H)$

לכן השגיאה היא במקום הרביעי, כלומר $v = (1,1,1,0,1,1)$.