

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

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

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

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.

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

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

א. הוכיחו כי H תת חבורה של S_n .

ב. הוכיחו כי H תת חבורה נורמלית של S_n .

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?

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

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.

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 $13^{-1} \pmod{1111}$

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