89-214 מבנים אלגבריים – מועד ג' – 03/10/18

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

כל שאלה שווה 28 נקודות, כל ציון מעל 100 יעוגל ל100.

1. תהי $G \subseteq \mathbb{R}^{3\times3}$ חבורת המטריצות ההפיכות בגודל 3×3 עם פעולת כפל מטריצות.

נגדיר בנוסף את הפונקציה $f : G \to G$ על ידי $f(A) = \frac{A}{\sqrt[3]{|A|}}$.

א. הוכיחו/הפריכו: f הינה הומומורפיזם בין חבורות.

ב. הוכיחו/הפריכו: f הינה איזומורפיזם בין חבורות.

ג. נסמן ב $H_1 = \{aI \in \mathbb{R}^{3\times3} \mid a \neq 0\}, H_2 = \{A \in \mathbb{R}^{3\times3} \mid |A| = 1\}$ תתי חברות של G.

הוכיחו כי $G/H_1 \cong H_2$.

2. נביט בקבוצת התמורות

$$B = \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 6 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 6 & 4 & 5 \end{pmatrix} \right\}.$$

א. הוכיחו כי B תת חבורה של S_6.

ב. מצאו תת חבורה של S_4 שאיזומורפית ל B.

.3

א. אליס תוהה האם 2465 הוא מספר ראשוני, והיא רוצה לבדוק זאת באמצעות מבחן מילר-רבין.

הוכיחו כי 302 הוא 'עד חזק' (או שקרן חזק) לראשוניות של 2465.

אליס שוכנעה בטעות כי 2465 הוא מספר ראשוני. היא בחרה לפרסם כמפתח ציבורי בשיטת ההצפנה RSA את $n = 2465 \cdot 17 = 41905$ ואת $e = 7885$.

אליס חישבה את $m = 39424$.

ב. חשבו את המפתח הסודי $d = e^{-1} \bmod m$.

ג. בוב הצפין את המידע 640 עבור אליס ושלח לה את $27020 = 640^{7885} \bmod 41905$.

מה המידע שאליס חשבה שבוב שלח? למה זה קרה?

4. נביט במטריצה $A = \begin{pmatrix} 1 & 1 & 1 \\ a & 1 & 0 \\ b & 0 & c \end{pmatrix}$, המגדירה קוד לינארי.

א. האם ייתכן כי שתי המילים $v_1 = (1,1,1,1,0,0), v_2 = (1,1,1,1,0,1)$ הן חוקיות?

ב. נתון כי שתי המילים $v_1 = (1,1,1,1,0,0), v_2 = (1,1,0,0,0,1)$ הן חוקיות, מצאו את a, b, c.

נוסחאות עזר:

שימו לב – ייתכן וחלק מהנוסחאות מיותרות.

$$302^{77} \bmod 2465 = 302$$
$$730080400 \bmod 41905 = 11490$$
$$132020100 \bmod 41905 = 19350$$
$$374422500 \bmod 41905 = 1325$$
$$522837000 \bmod 41905 = 30220$$
$$1551125 \bmod 41905 = 640$$