

30/05/21 – מועד ג' – 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. תהי חבורה G ויהי $a \in G$.

א. הוכיחו או הפריכו: אם $o(a^3) = 2$ אזי $o(a) = 6$

ב. הוכיחו או הפריכו: אם $o(a^2) = 2$ אזי $o(a) = 4$

2. תהא G תת חבורה של S_n

א. תהי $f \in G$ כך ש f אי זוגית (בעלת סימן שלילי), הוכיחו כי הסדר של f הוא זוגי.

ב. הוכיחו שאם קיימת $f \in G$ אי זוגית, אזי כמות האיברים ב G היא זוגית.

3. נביט במספר $x = 247$ נבדוק את ראשוניותו באמצעות מבחן מילר-רבין

א. מצאו a עד המוכיח כי x אינו מספר ראשוני.

ב. האם $a = 12$ עד חזק לראשוניות של x ?

ג. האם $a = 30$ עד חזק לראשוניות של x ?

4. המטריצה $A \in \mathbb{Z}_2^{3 \times 5}$ מגדירה קוד לינארי עם $G = \begin{pmatrix} I \\ A \end{pmatrix}, H = (A \ I)$.

א. תנו דוגמא ל A כך שאם $Gx = v$ מילה חוקית אז $v + e_1 + e_2 + e_3$ בהכרח אינה חוקית (כלומר אם יש טעויות

בשלושת הביטים הראשונים, בהכרח נזהה שהתרחשה טעות). הוכיחו את תשובתכם.

ב. תנו דוגמא ל A כך שאם $Gx = v$ מילה חוקית אז $v + e_1 + e_2$ בהכרח חוקית (כלומר אם יש טעויות בשני הביטים

הראשונים, בהכרח לא נזהה שהתרחשה טעות). הוכיחו את תשובתכם.

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

5. (2 נק') מצאו את $30^{246} \bmod 247$

6. (2 נק') מצאו את $12^{246} \bmod 247$

7. (2 נק') מצאו את $2^{246} \bmod 247$