

19/03/21 – מועד ב' – 89-214 מבנים אלגבריים

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 ותהי H תת חבורה של G .

א. הוכיחו או הפריכו: תת חבורה נורמלית אם ורק אם לכל $g \in G$ ולכל $h \in H$ מתקיים $ghg^{-1} \in H$.

ב. הוכיחו או הפריכו: אם H אבלית אזי H תת חבורה נורמלית.

2. תהי S_n חבורת התמורות, ותהי H תת חבורה של S_n .

א. הוכיחו או הפריכו: אם $|H| = 7$ אזי כל התמורות ב- H זוגיות.

ב. הוכיחו או הפריכו: אם $|H| = 8$ אזי חצי מהתמורות ב- H אי זוגיות.

3. בוב רוצה לשלוח לאליס מסר מוצפן בשיטת RSA.

אליס בחרה מספרים ראשוניים p, q וחישבה את $n = pq = 39618757$.

א. נספר לכם כי $m = \phi(n) = 39605836$, מצאו את p, q . כיצד נעזרתם ב- m ?

ב. חשבו את $\gcd(m, n)$.

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

א. תנו דוגמא ל- A כך שאם $v = Gx$ 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 $v = Gx$ 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 $\gcd(32555009, 39618757)$

6. (2 נק') מצאו $a, b \in \mathbb{Z}$ כך ש $a \cdot 32555009 + b \cdot 39618757 = \gcd(32555009, 39618757)$

7. (2 נק') מצאו את $2^{127} \bmod 117$