89-214 מבנים אלגבריים – מועד א' – 09/02/22

משך המבחן – שלוש שעות. חומר עזר אסור - השימוש במחשבון מותר. מרצה – דר' ארז שיינר

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

1. יהיו $p \neq q \in \mathbb{N}$ שני מספרים ראשוניים שונים, ויהי $n \in \mathbb{N}$ כך ש $1 \leq n < pq$.

   א. הוכיחו שקיימים $a, b \in \mathbb{Z}$ כך ש $\frac{n}{pq} = \frac{a}{p} + \frac{b}{q}$.

   ב. הוכיחו שקיימים $a, b \in \mathbb{Z}$ כך ש $\frac{n}{pq} = \frac{a}{p} + \frac{b}{q}$ המקיימים $|a| < p, |b| < q$.

2. תהי S_n חבורת התמורות, ונביט בתת הקבוצה $U \subseteq S_n$ המכילה את כל התמורות מסדר אי זוגי:

   $U = \{f \in S_n |\ o(f) \equiv_2 1\}$.

   א. תהי $f \in S_n$ תמורה זוגית (עם סימן חיובי). הוכיחו או הפריכו: הסדר של f הוא אי זוגי בהכרח, כלומר $f \in U$.

   ב. הוכיחו או הפריכו: U תת חבורה של S_n.

   ג. הוכיחו או הפריכו: $|U| \leq \frac{|S_n|}{2}$ כאשר $n \geq 2$.

3. בוב רוצה לשלוח לאליס מסר מוצפן בשיטת RSA.

   אליס מצאה אלגוריתם מעניין לבדיקת ראשוניות של מספרים מהצורה $2^k - 1$, ולכן בחרה שני ראשוניים

   $$p = 2^{k_1} - 1, \quad q = 2^{k_2} - 1$$

   כך ש k_1, k_2 אינם רחוקים זה מזה. אליס חישבה את $n = 68718821377$ ובחרה $e = 37$.

   א. מצאו את המספר הסודי $m = \Phi(n)$, הסבירו מדוע יכולתם לעשות את זה.

   ב. בוב מעוניין לשלוח לאליס את המידע $x = 2$, מה המסר המוצפן אותו ישלח לאליס?

4. המטריצה $A \in \mathbb{Z}_2^{3\times 4}$ (3 שורות ו4 עמודות) מגדירה קידוד לינארי יחד עם המטריצה המקודדת $G = \begin{pmatrix} I \\ A \end{pmatrix}$.

   א. מצאו A כך שאם $v = Gx$ מילה חוקית, אז גם $v + e_1$ וגם $v + e_1 + e_2 + e_4$ מילה חוקית, או הוכיחו שאין כזו.

   ב. מצאו A כך שאם $v = Gx$ מילה חוקית, אז גם $v + e_1$ וגם $v + e_1 + e_5$ מילה חוקית, או הוכיחו שאין כזו.

   ג. מצאו A כך שאם $v = Gx$ מילה חוקית, אז $v + e_1 + e_6$ <u>אינה</u> מילה חוקית, או הוכיחו שאין כזו.