

אלגברה יישומית (88374) \ פרופ' רון עדין בחינת סיום (מועד ב')

משך הבחינה: שעתיים וחצי (150 דקות).
אין להשתמש בכל חומר עזר, פרט למחשבון.
יש לענות על 5 מתוך 6 השאלות. כל השאלות שוות-משקל.
נא להסביר ולנמק בבירור את הפתרון, ולכלול במחברת את כל החישובים הנחוצים.

קהל צלחה!

1. יהי n מספר טבעי גדול, ותהיינה A, B שתי קבוצות של מספרים שלמים בתחום $[10n, 20n]$. הראה כיצד למצוא בזמן $O(n \log n)$ את כל אברי הקבוצה $C := \{2a + 3b \mid a \in A, b \in B\}$.

2. בתחילתו של משחק "מחשבת" תלת-ממדי פזורים חיילים בחלק מנקודות השריג בחצי המרחב התחתון $\{(x, y, z) \in \mathbb{Z}^3 \mid z \leq 0\}$. בכל צעד של המשחק "קופץ" חייל מעל חייל סמוך לו (במקביל לאחד מכיווני הצירים) ומוריד אותו מהלוח. הוכח שבתנאים אלו לא ניתן להגיע עם חייל לנקודת שריג (x, y, z) עם $z = 8$.

3. נסח והוכח את חסם סינגלטון לקוד כללי (לאו דוקא ליניארי).

4. תאר את שיטת ההצפנה של ElGamal. על איזו בעיה קשה היא מסתמכת?

5. יהי C קוד בינארי ליניארי עם מטריצה יוצרת

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

(א) רשום מטריצת בדיקת זוגיות H עבור C .
(ב) מצא את מרחק הקוד $d(C)$. נמק.

6.

(א) הראה שקיים קוד טרנארי (מעל שדה בעל 3 אברים) ציקלי באורך 11 עם פולינום יוצר $g(x) = x^5 + x^4 - x^3 + x^2 - 1$.
(ב) מהו מימד הקוד הנ"ל? הראה שמרחק הקוד $d \leq 5$.
(ג) נתון שמרחק הקוד הנ"ל הוא בדיוק $d = 5$. הוכח שזהו קוד מושלם.