89-214 מבנים אלגבריים – מועד א' – 19/02/18

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 חבורה סופית.

א. הוכיחו שאם הסדר של $a \in G$ הוא n אזי גם הסדר של a^{-1} הוא n.

ב. נניח כי $|G| \geq 3$ האם ייתכן כי לכל שני איברים שונים ב G יש סדר שונה?

האם עבור $|G| = 2$ זה אפשרי?

2.

א. מצאו תת חבורה של S_4 האיזומורפית לתת החבורה הכפלית $\{1,-1,i,-i\} \subseteq \mathbb{C}^*$.

ב. הוכיחו כי $H \subseteq S_n$ אוסף התמורות הזוגיות (בעלות סימן חיובי) הינו תת חבורה של S_n.

3. בוב רוצה לשלוח לאליס מסר מוצפן בשיטת RSA.

אליס פרסמה את המפתח הציבורי $n = 899$ ו $e = 593$.

אליס בחרה בטעות זוג מספרים ראשוניים מאד קרובים אחד לשני.

בוב שלח לאליס את המידע המוצפן $734 = x^{593} \bmod 899$

א. חשבו את הפרמטרים הסודיים $m = \phi(n)$, $d = e^{-1} \bmod m$. מדוע יכולתם לעשות זאת?

ב. מהו המידע x שבוב שלח לאליס?

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

נסמן את המרחק המינימלי בין שתי מילים חוקיות ב $d_{\min}$.

א. האם ייתכן כי שתי המילים $v = (1,0,0,0,1,0)$ ו $v' = (1,1,1,0,1,0)$ הינן חוקיות?

ב. נתון בנוסף כי $d_{\min} \geq 3$ מצאו את a,b,c.

נוסחאות עזר:

שימו לב – ייתכן וחלק מהנוסחאות מיותרות.

$$88209 \bmod 899 = 107$$
$$538756 \bmod 899 = 255$$
$$485174 \bmod 899 = 613$$
$$65025 \bmod 899 = 297$$
$$11449 \bmod 899 = 661$$
$$436921 \bmod 899 = 7$$
$$217998 \bmod 899 = 440$$
$$5138 \bmod 899 = 643$$