89-214 מבנים אלגבריים – מועד א' – 09/02/20

משך המבחן – שלוש שעות. השימוש במחשבון מותר. מרצה – דר' ארז שיינר

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

1. תהיינה G,H חבורות, ויהי $f:G\to H$ הומומורפיזם.

א. הוכיחו כי f חח"ע אם ורק אם $\ker f=\{e_G\}$.

ב. נתון בנוסף כי $|G|=11$, ו $|H|=8$, חשבו את $\ker f$ ואת $\operatorname{Im} f$.

2. תהי S_n חבורת התמורות.

א. <u>הוכיחו או הפריכו</u>: לכל תמורה $f\in S_n$ קיימת תמורה $g\in S_n$ כך ש $f=g\circ g$.

ב. <u>הוכיחו או הפריכו</u>: לכל תמורה $f\in S_3$ קיימת תמורה $g\in S_3$ כך ש $f=g\circ g\circ g$.

3. בוב רוצה לשלוח לאליס מסר מוצפן בשיטת RSA.

אליס רוצה להצפין באמצעות שני ראשוניים p,q המיוצגים על ידי 7 ביטים כל אחד.

אליס מפחדת שאם הראשוניים יהיו קטנים מידי ההצפנה שלה תהא חלשה, ולכן מחליטה ששלושת הביטים השמאליים יהיו שווים 1 בשני הראשוניים.

אליס מצאה שני ראשוניים כאלה ובנתה את המפתח הציבורי $n=pq=14,351$ ו $e=1,283$.

בוב שלח לאליס את המידע המוצפן $450=x^{1283}\bmod 14351$

א. פרקו את n למכפלה של ראשוניים. בכמה מספרים היה צריך לנסות לחלק את n לכל היותר?

ב. מהו המידע x שבוב שלח לאליס?

4. נביט בפולינום $g(x)=x^4+x+1$, המגדיר קוד פולינומי.

א. קודדו את המידע $(1,1,0,1)$ באמצעות הקוד הפולינומי הנתון.

ב. נתון מידע $(b_1,b_2,...,b_5)$ שלאחר קידוד נותן $(b_1,b_2,...,b_5,0,0,0,0)$, כלומר היתירות מכילה רק אפסים.

מצאו דוגמא אחת למידע כזה. האם יש דוגמא נוספת? הוכיחו.

ג. האם g מגדיר קידוד ציקלי עבור מידע באורך 5 ביטים?

נוסחאות עזר:

שימו לב – ייתכן וחלק מהנוסחאות מיותרות.

$$202500 \bmod 14351 = 1586$$
$$2515396 \bmod 14351 = 3971$$
$$15768841 \bmod 14351 = 11443$$
$$130942249 \bmod 14351 = 3725$$
$$8166869100 \bmod 14351 = 2020$$
$$72068082658 \bmod 14351 = 1242$$