89-214 מבנים אלגבריים – מועד ב' – 15/03/20

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, ויהי $f:G\to G$ הומומורפיזם.
   א. האם ייתכן ש $\ker(f)=Im(f)$? אם כן תנו דוגמא לG,f כאלה, אחרת הוכיחו שאינם קיימים.
   ב. נתון בנוסף כי $|G|>1$. האם ייתכן ש $\ker(f)=Im(f)$? אם כן תנו דוגמא לG,f כאלה, אחרת הוכיחו שאינם קיימים.
   ג. נתון בנוסף כי $|G|=35$, הוכיחו כי לא ייתכן ש $\ker(f)=Im(f)$.
2. תהי S_n חבורת התמורות.
   א. מצאו תת חבורה ציקלית $G\subseteq S_4$ כך ש $|G|=4$.
   ב. מצאו תת חבורה שאינה ציקלית $G\subseteq S_4$ כך ש $|G|=4$.
   ג. מצאו תת חבורה $G\subseteq S_8$ כך ש $|G|=4$, וכל התמורות בG חיוביות (זוגיות).
3. בוב רוצה לשלוח לאליס מסר מוצפן בשיטת RSA.
   ידוע כי לכל מספר ראשוני מהצורה $p=2^q-1$ מתקיים כי בהכרח q ראשוני.
   אליס מצאה ראשוני כזה ובנתה את המפתח הציבורי $n=pq$ בעזרת הזוג.
   א. תארו אלגוריתם לפירוק המפתח n לגורמיו הראשוניים הדורש לכל היותר $2\log_2(n)$ פעולות חשבון.
   ב. נתון כי המפתח הציבורי של אליס הוא $n=9961453$ וכן $e=8912863$. מצאו את הפרמטר הסודי d.
4. נביט בפולינום $g(x)=x^4+x+1$, המגדיר קוד פולינומי.
   א. קודדו את המידע $(1,1,0,1,0)$ באמצעות הקוד הפולינומי הנתון.
   ב. האם g מגדיר קידוד ציקלי עבור מידע באורך 11 ביטים?