89-214 מבנים אלגבריים – מועד א' – 31/01/19

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. יהיו $h,g\in G$ איברים מסדר $o(g)=o(h)=2$, הוכיחו/הפריכו: $o(gh)\le 2$.

ב. יהי $g\in G$ איבר מסדר $o(g)=113$. נסמן $h=g^3$ מצאו את $o(h)$.

2. תהי S_n חבורת התמורות מקבוצה בגודל n לעצמה, ותהי $G\subseteq S_n$ תת חבורה.

א. האם ייתכן ש $(1\ \ 2),(1\ \ 3)\in G$ אך $(1\ \ 3\ \ 2)\notin G$? הוכיחו קביעתכם.

ב. נניח כי G מכילה את כל התמורות האי זוגיות (מסימן שלילי) של S_n, הוכיחו כי $G=S_n$.

3. בוב רוצה לשלוח לאליס מסר מוצפן בשיטת RSA.

אליס מצאה ראשוני בטוח, כלומר ראשוני מהצורה $p=2q+1$ כאשר q ראשוני.

אליס נעזרה (בטעות) בראשוניים p,q ובנתה את המפתח הציבורי $n=pq=34453$ ו $e=7569$.

בוב שלח לאליס את המידע המוצפן $24847=x^{7569}\bmod 34453$

א. חשבו את הפרמטר הסודי $m=\phi(n)$. מדוע יכולתם לעשות זאת?

ב. מהו המידע x שבוב שלח לאליס?

4. נביט בפולינום $g(x)=x^5+x+1$, המגדיר קוד פולינומי.

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

א. קודדו את המידע 1011 באמצעות הקוד הפולינומי.

ב. קבעו לגבי כל אחת מהמילים המקודדות הבאות האם היא חוקית:

1100101, 1000111.

ג. הוכיחו כי $d_{\min}\le 3$.

נוסחאות עזר:

שימו לב – ייתכן וחלק מהנוסחאות מיותרות.

$$617373409 \bmod 34453 = 10102$$
$$102050404 \bmod 34453 = 618$$
$$381924 \bmod 34453 = 2941$$
$$8649481 \bmod 34453 = 1778$$
$$73075027 \bmod 34453 = 214$$
$$214913654407 \bmod 34453 = 9220$$
$$2535646388188 \bmod 34453 = 23861$$