

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

כל שאלה שווה 28 נקודות, כל ציון מעל 100 יעוגל ל-100.

1. תהי  $G = \mathbb{C}^* = \{z \in \mathbb{C} \mid z \neq 0\}$  חבורת המרוכבים ללא אפס עם פעולת הכפל.

נגדיר את הפונקציה  $f: G \rightarrow G$  ע"י  $f(z) = z^2$ .

א. הוכיחו כי  $f$  הינה הומומורפיזם.

ב. האם  $f$  איזומורפיזם? הוכיחו.

ג. תהי  $H = \{-1, 1\}$  תת חבורה של  $G$ , הוכיחו כי  $G/H \cong G$ .

2. תהי  $S_n$  חבורת התמורות, ותהי  $G \subseteq S_n$  תת חבורה.

א. נניח כי  $G$  היא אבלית (חילופית), הוכיחו/הפריכו:  $G$  תת חבורה ציקלית של  $S_n$ .

ב. נניח כי  $|G| = 7$ , הוכיחו/הפריכו:  $n \geq 7$ .

3. בוב רוצה לשלוח לאליס מסר מוצפן בשיטת RSA.

אליס הגרילה שני ראשוניים  $p, q$ , ופרסמה את  $n = pq = 17113$ .

על מנת לחסוך בחישובים אליס בחרה  $e$  כך  $d$  יהיה מספר נמוך, ופרסמה אותו  $e = 581$ .

בוב שלח לאליס את המידע המוצפן  $13056 = x^{581} \pmod{17113}$ .

א. בהנחה ש  $d = 29$ , מהו המידע שבוב שלח לאליס?

ב. הוכיחו כי תשובתכם לסעיף א' היא אכן המידע  $x$  שבוב שלח לאליס.

4. נביט בפולינום  $g(x) = x^2 + ax + b$ , המגדיר קוד פולינומי, כאשר  $a, b \in \mathbb{Z}_2$ .

א. האם ייתכן כי המילה 1101 חוקית בקוד הפולינומי הנתון?

ב. קודדו את המידע 11 באמצעות הקוד הפולינומי. הביעו תשובתכם באמצעות  $a, b$ .

ג. נתון בנוסף כי  $g(x) \cdot (x+1) = x^3 + x^2 + x + c$ , מצאו את  $a, b, c$ .

## נוסחאות עזר:

שימו לב – ייתכן וחלק מהנוסחאות מיותרות.

$$170459136 \bmod 17113 = 13656$$

$$186486336 \bmod 17113 = 5975$$

$$35700625 \bmod 17113 = 2907$$

$$8450649 \bmod 17113 = 13940$$

$$194323600 \bmod 17113 = 5485$$

$$3161228266368000 \bmod 17113 = 42$$

$$3111696 \bmod 17113 = 14243$$

$$14243^{145} \bmod 17113 = 7645$$

$$321090 \bmod 17113 = 13056$$