

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

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

1. נביט בחבורות  $\mathbb{C}^* = \{z \in \mathbb{C} \mid z \neq 0\}$ ,  $\mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$  עם פעולת הכפל.

כמו כן נגדיר את תת הקבוצה  $G = \{z \in \mathbb{C} \mid |z| = 1\} \subseteq \mathbb{C}^*$ .

א. הוכיחו כי  $G$  תת חבורה של  $\mathbb{C}^*$ .

ב. הוכיחו כי  $\mathbb{C}^*/\mathbb{R}^+ \cong G$ .

2. תהא  $G$  תת חבורה של  $S_n$ .

א. תהי  $f \in G$  תמורה בעלת סימן שלילי (אי-זוגית). הוכיחו כי הסדר של  $f$  הינו זוגי.

ב. הוכיחו שאם קיימת תמורה בעלת סימן שלילי ב- $G$ , אזי כמות התמורות ב- $G$  היא זוגית.

3. בוב רוצה לשלוח לאליס מסר מוצפן בשיטת RSA.

אליס פרסמה פעם אחת את המפתח הציבורי  $n = 391$ ,  $e = 5$ , ובהזדמנות אחרת את המפתח

$$e' = 5, n' = 493$$

אליס רצתה לחסוך בתהליך יצירת הראשוניים, ולכן בחרה להשתמש במספר ראשוני בשתי הזדמנויות שונות.

בפעם השנייה בוב שלח לאליס את המידע המוצפן  $12 = x^{e'} \pmod{n'}$ .

מהו המידע  $x$  שבו שלח לאליס?

4. נתון הפולינום  $g(x) = x^4 + x + 1$  בעזרתו ניצור קידוד פולינומי.

א. הוכיחו כי לכל  $n$  הפולינום  $x^n$  אינו מתחלק ב- $g(x)$  ללא שארית.

ב. הוכיחו כי המרחק המינימלי בין שתי מילים חוקיות מקיים  $d_{\min} > 1$ .