

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}^* .

ראשית, איבר היחידה של \mathbb{C}^* הוא 1, ואכן $1 \in G$.

כעת, יהיו שני איברים $z_1, z_2 \in G$ עלינו להוכיח כי $z_1 \cdot z_2^{-1} \in G$. אכן $|z_1 \cdot z_2^{-1}| = |z_1| \cdot \frac{1}{|z_2|} = 1$.

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

נביט בפונקציה $f: \mathbb{C}^* \rightarrow G$ המוגדרת ע"י $f(z) = \frac{z}{|z|}$.

נוכיח כי f הינה הומומורפיזם כי $\ker(f) = \mathbb{R}^+$ ו $\text{im}(f) = G$ ולכן התוצאה נובעת ממשפט האיזומורפיזם.

אכן $f(z \cdot w) = \frac{z \cdot w}{|z \cdot w|} = \frac{z}{|z|} \cdot \frac{w}{|w|} = f(z) \cdot f(w)$ (לכן הפונקציה הינה הומומורפיזם).

לכל $z \in G$ מתקיים כי $f(z) = \frac{z}{|z|} = z$ (לכן $\text{im}(f) = G$).

ולבסוף $\ker(f) = \{z \in \mathbb{C}^* : f(z) = 1\} = \left\{ z \in \mathbb{C}^* : \frac{z}{|z|} = 1 \right\} = \{x \in \mathbb{R} : x > 0\}$

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.

נב"ש כי הסדר של f הינו $2k+1$, לכן $f^{2k+1} = I$ כאשר I היא תמורת הזהות.

אבל $\text{sign}(f^{2k+1}) = (\text{sign}(f))^{2k+1} = -1$ בסתירה לכך שסימן הזהות הוא חיובי.

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

G הינה חבורה סופית, ולכן סדר כל איבר מחלק את כמות האיברים ב G .

כיוון שהסדר של כל תמורה אי זוגית הוא זוגי, נובע כי כמות האיברים 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 באותו מספר ראשוני בשתי

הזדמנויות שונות.

$$12 = x^{e'} \pmod{n'}$$

מהו המידע x שבוב שלח לאליס?

כיוון שאליס השתמשה באותו מספר ראשוני פעמיים, הוא שווה ל $\gcd(n, n')$.

$$\gcd(391, 493) = 17.$$

נחלק את 493 ב 17 ונקבל $493 = 17 \cdot 29$, ולכן $m' = 16 \cdot 28 = 448$

לכן אנחנו יכולים לחשב את ההופכי של $e' = 5$ מודולו 448.

$$448 - 89 \cdot 5 = 3$$

$$5 - 3 = 2$$

$$3 - 2 = 1$$

ולכן

$$1 = 3 - 2 = 3 - (5 - 3) = 2 \cdot 3 - 5 = 2 \cdot (448 - 89 \cdot 5) - 5 = 2 \cdot 448 - 179 \cdot 5$$

$$d' = 5^{-1} = -179 = 269 \pmod{448}$$

$$12^{269} \pmod{493} = 12^{2^8 + 2^3 + 2^2 + 1} \pmod{493} = 99$$

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.

נב"ש שקיים פולינום כזה, נבחר את n להיות הנמוך ביותר עבורו x^n מתחלק ב $g(x)$.

ברור ש $n \geq 4$.

אזי $x^n = q(x)g(x)$.

כעת, אם $q(x)$ מתחלק ב x נחלק את שני הצדדים ב x ונקבל כי x^{n-1} מתחלק ב $g(x)$, בסתירה.

לכן $q(x)$ מכיל את המונם הקבוע 1, כיוון שגם $g(x)$ מכיל את המונם הקבוע 1 נובע כי $q(x)q(x)$ מכיל את 1 בסתירה.

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

כידוע מילה היא חוקית אם"ם היא מתחלקת ב $g(x)$.

אם המרחק בין שתי מילים חוקיות $f(x), h(x)$ הוא 1, אזי $f(x) - h(x) = x^n$ עבור n כלשהו.

(שימו לב שבעצם הפולינום x^n מתאים לוקטור e_{n+1}).

לפי סעיף א', נובע שלא ייתכן שהמרחק בין שתי מילים חוקיות הוא 1, ולכן $d_{\min} > 1$.