

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.

יהיו שני מרוכבים z_1, z_2 צריך להוכיח כי $f(z_1 \cdot z_2) = f(z_1) \cdot f(z_2)$.

$$(z_1 \cdot z_2)^2 = z_1^2 \cdot z_2^2$$

ב. האם f איזומומורפיזם? הוכיחו.

הפונקציה אינה חח"ע ולכן אינה איזומומורפיזם.

$$f(-1) = f(1) \text{ , לדוגמא}$$

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

ראשית נחשב את הגרעין של ההומומורפיזם.

$$\ker f = \{z \mid f(z) = 1\} = \{z \mid z^2 = 1\} = \{-1, 1\}$$

כמו כן התמונה היא $\text{Im } f = G$ כיוון שההומומורפיזם הינו על. אכן, לכל מרוכב $z = rcis\theta$ יש מקור

$$z = \sqrt{r} cis\left(\frac{\theta}{2}\right)$$

לכן לפי משפט האיזומומורפיזם הראשון, $G/\ker f \cong \text{Im } f$ ולכן $G/H \cong G$.

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 .

הפרכה:

נביט ב $\mathbb{Z}_2 \times \mathbb{Z}_2$ עם חיבור מודולו 2. זו חבורה חילופית שאינה ציקלית כיוון ש $\langle (a,b) \rangle \neq \mathbb{Z}_2 \times \mathbb{Z}_2$ לכל $(a,b) \in \mathbb{Z}_2 \times \mathbb{Z}_2$.

לפי משפט קיילי, $\mathbb{Z}_2 \times \mathbb{Z}_2$ איזומורפית לתת חבורה של S_4 , ולכן תת חבורה זו אינה ציקלית.

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

הוכחה:

ידוע $|S_n| = n!$ וידוע כי הסדר של תת חבורה חייב לחלק את סדר החבורה.

לכן $n!$ מתחלק ב-7. כיוון ש-7 הוא מספר ראשוני $n \geq 7$, הרי העצרת של מספרים נמוכים מ-7 לא מכילה את 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 $13056 = x^{581} \bmod 17113$.

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

$$13056^{29} \bmod 17113 = 42$$

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

נחשב את $42^{581} \bmod 17113$ ונקבל אכן 13056.

כיוון שההצפנה היא חח"ע, זה חייב להיות המידע שבוב שלח.

הערה לגבי התרגיל:

ראינו שאנחנו יכולים להיות בטוחים שגילינו את המידע של בוב, גם אם ניחשנו את d .

לכן אם יש דרך לנחש את d בזמן סביר אפשר לשבור את ההצפנה, אפילו שאנחנו לא יודעים את m ולא יודעים

לבדוק האם $e \cdot d \bmod m = 1$.

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?

תשובה: לא.

הוכחה:

השאלה היא אם הפולינום $x^3 + x^2 + 1$ יכול להתחלק ב g ללא שארית.

נבצע חילוק ונקבל כי השארית היא $(b+a(a+1))x+(a+1)b+1$.

כיוון שאנו בשדה \mathbb{Z}_2 נובע כי $a(a+1) = 0$ ולכן השארית היא בעצם $bx+(a+1)b+1$.

לכן השארית לא יכולה להתאפס, כי אם $b = 0$ (המקדם של x) יוצא שהשארית היא 1.

כלומר לא ייתכן כי המילה הנ"ל חוקית בקוד הפולינומי הנתון.

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

ראשית נתרגם את המידע לפולינום $f(x) = x+1$.

שנית, נחלק את $x^2 f(x)$ ב $g(x)$ ונקבל את השארית $bx+(a+1)b$ (שוב השתמשנו בעובדה כי $a(a+1) = 0$)

לכן סה"כ המידע המקודד הוא $x^2 f(x) + bx + (a+1)b = x^3 + x^2 + bx + (a+1)b$

כלומר $(1, 1, b, ab+b)$

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

פתרון:

פשוט נבצע את הכפל, נפתח סוגריים ונשווה מקדמים.

$$g(x) \cdot (x+1) = (x^2 + ax + b)(x+1) = x^3 + (a+1)x^2 + (a+b)x + b$$

לפי המקדם של x^2 נקבל כי $a = 0$.

לפי המקדם של x נובע כי $b = 1$.

לפי הקבוע $b = c$.

נוסחאות עזר:

שימו לב – ייתכן וחלק מהנוסחאות מיותרות.

$$170459136 \bmod 17113 = 13656$$

$$186486336 \bmod 17113 = 5975$$

$$35700625 \bmod 17113 = 2907$$

$$8450649 \bmod 17113 = 13940$$

$$194323600 \bmod 17113 = 5485$$

$$3161228266368000 \bmod 17113 = 42$$

$$3111696 \bmod 17113 = 14243$$

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

$$321090 \bmod 17113 = 13056$$