

תרגיל 6 במבנים אלגבריים

89-214 סמסטר א' תשע"ח

הוראות בהגשת הפתרון יש לרשום בכל דף שם מלא, מספר ת"ז ומספר קבוצת תרגול.

שאלה 1. חשבו בעזרת משפט אוילר:

א. את הספרה האחרונה של המספר 63^{63} .

ב. שתי הספרות האחרונות של 543^{3838} .

ג. $89^{214} \pmod{91}$.

שאלה 2. יהיה p ראשוני. כמה איברים הפיכים יש במונואיד הכפלי \mathbb{Z}_p ? כמה איברים הפיכים יש במונואיד הכפלי \mathbb{Z}_{p^2} ?

שאלה 3. חשבו בשיטה של חישוב חזקה את הביטויים הבאים. מותר להשתמש במחשבון (כולל בפונקציית המודולו) לחישובי הביניים, שאותם תפרטו:

א. $2790^{2753} \in \mathbb{Z}_{3233}$ בתרגול ראייתם שהתוצאה הסופית היא ההודעה שבוב רצה לשלוח לאליס.

ב. $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}^{12} \in GL_2(\mathbb{Z}_{10000})$.

שאלה 4. בוב מעוניין לשלוח לאליס הודעה באופן מוצפן. ולכן, אליס בוחרת שני מספרים ראשוניים. $p=13$,

$q=23$. בנוסף, אליס בוחרת את המספר $e=35$.

א. הראה ש- e הנ"ל אכן בחירה תקינה.

ב. חשב את d (המקיים $de \equiv 1 \pmod{\phi(n)}$ כאשר $n = p * q$)

ג. אליס שולחת לבוב את n ואת e וכעת הוא יכול להצפין. בוב מעוניין להצפין את ההודעה $m=15$. נשים

לב כי ההודעה m אכן עומדת בקרטיונים. חשבו את ההודעה אותה בוב יעביר לאליס.

ד. הראו כי אליס אכן יכולה לפענח את ההודעה.