

**עבודת 1:**

**שאלה 1 תכונות בסיסיות של חלוקה וה- gcd**  
 $b = qa$  ונתנו  $a, b, c \in \mathbb{Z}$  כדי לציין ש  $a$  מחלק את  $b$  **ללא** שארית, כלומר קיים שלם  $q$  כך ש:  $b = qa$ . הוכיחו את התענות הבאות.

- (א) אם  $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$  אז  $d = \gcd(a, b)$
- (ב) אם  $a | c$  וגם  $\gcd(a, b) = 1$  וגם  $b | c$  אז  $a | b$
- (ג) אם  $a | c$  אז  $\gcd(a, b) = 1$  ו-  $a | bc$
- (ד) יהי  $p$  ראשוני כלשהו כך ש-  $ab | p$  או  $a | p$  או  $b | p$
- (ה) יהי  $m \neq 0$  אז  $a | b$  אם ורק אם  $ma | mb$ .

**שאלה 2**

יהיו  $a, b$  מספרים שלמים זרים. הוכיחו כי כל מחלק ראשוני משותף של  $a^2 + b^2$  ו-  $a + b$  שוייך לקבוצה  $\{1, 2\}$ .

**שאלה 3**

יהיו  $n$ ,  $a, b$  שלמים חיוביים. הוכיחו כי  $\gcd(a^n, b^n) = \gcd(a, b)^n$ .

**שאלה 4**

(10 נקודות)

נתון את הטקסט מוצפן

ETCLPRLWCTGGVVCSIKASLAVFL

אשר מוצפן על ידי צופן ויז'נֶר עם המפתח SPY. מצאו את הטקסט גלי.

**שאלה 5**

(10 נקודות)

נתון הטקסט מוצפן

PEBUSSPZIIDUKOEKIPEONUSS

אשר מוצפן על ידי צופן אפייני עם המפתח 20.  $a = 23, b = 20$ . מצאו את הטקסט גלי.

**שאלה 6**

נתון צופן עם כלל מצפן  $e_k(x)$  וככל מפענה  $d_k(y)$ . אומרים כי הצופן נתן לפענו אם ורק אם  $x \in \mathbb{Z}_{26}$  לכל  $d_k(e_k(x)) = x \pmod{26}$ .

- (א) הוכיחו כי צופן האפייני נתן לפענו.
- (ב) הוכיחו כי צופן היל נתן לפענו.

**שאלה 7**

- א)** יהיו צופן האפיני מעלalfavit בת 30 אותיות. מצאו את הכלל מפענה.  
**ב)** חשבו כמה מפתחות האפשרות קיימות של צופן האפיני מעלalfavit בת  $m$  אותיות.

 **שאלה 8**

(10 נקודות)

נתנו הטקסט מוצפן

YZUSKKOPE

אשר מוצפן על ידי צופן היל עם המפתח

$$k = \begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} .$$

מצאו את הטקסט גלי.