

עבודת 1:**שאלה 1**

יהיו $a, b, c \in \mathbb{Z}$ ונכתב כי $b | a$ 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 $c | a$ וגם $\gcd(a, b) = 1$ אז $b | c$ וגם $a | c$

(ג) אם $a | c$ אז $\gcd(a, b) = 1$ ו- $a | bc$

(ד) יהיו p ראשוני כלשהו כך ש- $ab | p$ או $a | p$ או $b | p$

(ה) יהיו m, a, b שלמים זרים. הוכיחו כי $\gcd(ma, mb) = m \gcd(a, b)$

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 המקורי.

שאלה 5

(10 נקודות)

נתון הטקסט מוצפן

PEBUSSPZIIDUKOEKIPEONUSS

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

שאלה 6

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

(א) הוכיחו כי צופן האפייני ניתן לפענוח.

(ב) הוכיחו כי צופן היל ניתן לפענוח.

שאלה 7

- א)** יהיו צופן האפיני מעל אלפבית בת 30 אותיות. מצאו את הכלל מפענה.
- ב)** חשבו כמה מפתחות האפשרות קיימות של צופן האפיני מעל אלפיבית 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.