

עבודת 1:

שאלה 1

תכונות בסיסיות של חלוקה וה- gcd

יהיו $a, b, c \in \mathbb{Z}$ ונכתוב כי $a \mid b$ כדי לציין ש a מחלק את b **ללא** שארית, כלומר קיים שלם q כך ש: $b = qa$. הוכיחו את הטענות הבאות.

(א) אם $d = \gcd(a, b)$ אז $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

(ב) אם $a \mid c$ וגם $b \mid c$ וגם $\gcd(a, b) = 1$ אז $ab \mid c$

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

(ד) יהי p ראשוני כלשהו כך ש- $p \mid ab$ אזי $p \mid a$ או $p \mid b$.

(ה) יהי $m \neq 0$ אז $a \mid b$ אם ורק אם $ma \mid mb$.

שאלה 2

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

שאלה 3

יהיו a, b, n 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'נר עם המפתח SPY. מצאו את הטקסט גלוי.

שאלה 5

(10 נקודות)

נתון הטקסט מוצפן

PEBUSSPZIIDUKOEKIPEONUSS

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

שאלה 6

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

(א) הוכיחו כי צופן האפיני ניתן לפענוח.

(ב) הוכיחו כי צופן היל ניתן לפענוח.

שאלה 7

(א) יהי $e_k(x) = 23x + 28 \bmod 30$ צופן האפיני מעל אלפבית בת 30 אותיות. מצאו את הכלל מפענח.

(ב) חשבו כמה מפתחות האפשריות קיימות של צופן האפיני מעל אלפבית בת m אותיות.

שאלה 8

(10 נקודות)

נתון 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 גלוי.