עבודת 1: תורת המספרים וצפנים בסיסיים

שאלה 1 **(10 נקודות)** חשבו את האיבר ההופכי של 7 ב- $\mathbb{Z}_{20}$.

שאלה 2 **(10 נקודות)**

א) חשבו את $\gcd(285, 89)$.

ב) מצאו שלמים s, t, d עבורם $285s + 89t = d$.

שאלה 3 **(10 נקודות)** הוכיחו: אם $a \mid bc$ ו- a, b זרים אז $a \mid c$.

שאלה 4 **(10 נקודות)**

א) הוכיחו: אם a, b זרים אז קיים c עבורו $ac \equiv 1 \mod b$.

ב) הוכיחו: אם a, b לא זרים אז לא קיים c עבורו $ac \equiv 1 \mod b$.

שאלה 5 **(10 נקודות)**

א) הוכיחו: אם $a \equiv b \mod m$ אז $a + c \equiv b + c \mod m$.

ב) הוכיחו: אם $a \equiv b \mod m$ ו- $c \equiv d \mod m$ אז $ac \equiv bd \mod m$.

ג) הוכיחו: אם $a \equiv b \mod m$ אז $a^n \equiv b^n \mod m$.

שאלה 6 **(10 נקודות)**

נתון הטקסט מוצפן

```
IAFDXFUUWLFEIALLCRZ
```

אשר מוצפן על ידי צופן אפיני עם המפתח $a = 5, b = 17$. מצאו את הטקסט גלוי.

שאלה 7 **(10 נקודות)**

נתון הטקסט מוצפן

```
HVFDDP
```

אשר מוצפן על ידי צופן היל עם המפתח

$$k = \begin{pmatrix} 13 & 5 & 6 \\ 2 & 1 & 7 \\ 9 & 7 & 13 \end{pmatrix} .$$

מצאו את הטקסט גלוי.

שאלה 8 (10 נקודות)

נתונה התמורה

$$\pi = \begin{pmatrix} 1 & 4 & 3 & 2 \end{pmatrix}$$

פענחו את הטקסט מצפון

```
CEDOBAERKGNI
```

שאלה 9 (10 נקודות)

נתון את הטקסט מוצפן

```
ZFSXUHIYWU
```

אשר מוצפן על ידי צופן ויז'נר עם המפתח `GREEN`. מצאו את הטקסט גלוי.

שאלה 10 (10 נקודות) נניח כי $k = (13, 8)$ הוא מפתח של צופן האפיני מעל החוג $\mathbb{Z}_{31}$.

א) מצאו את האיברים a', b' בכלל מפענח

$$d_k(y) = a'y + b'$$

כאשר $a', b' \in \mathbb{Z}_{31}$.

ב) הוכיחו כי $d_k\left(e_k(x)\right) = x$ לכל $x \in \mathbb{Z}_{31}$.

פתרונות

שאלה 1

$$\begin{aligned} 1 \cdot 7 = 7 &\equiv 7 \mod 20 \ , \\ 2 \cdot 7 = 14 &\equiv 14 \mod 20 \ , \\ 3 \cdot 7 = 21 &\equiv 1 \mod 20 \ . \end{aligned}$$

לכן $7^{-1} \equiv 3 \mod 20$.

שאלה 2

$a = 285, b = 89$.

$$\begin{aligned} r_0 &= a = 285 \ , & r_1 &= b = 89 \ , \\ s_0 &= 1 \ , & s_1 &= 0 \ , \\ t_0 &= 0 \ , & t_1 &= 1 \ . \end{aligned}$$

שלב $k = 1$:	$r_2 = 285 - 3 \cdot 89 = 18$	$s_2 = 1 - 3 \cdot 0 = 1$	$t_2 = 0 - 3 \cdot 1 = -3$	$q_1 = 3$
שלב $k = 2$:	$r_3 = 89 - 4 \cdot 18 = 17$	$s_3 = 0 - 4 \cdot 1 = -4$	$t_3 = 1 - 4 \cdot (-3) = 13$	$q_2 = 4$
שלב $k = 3$:	$r_4 = 18 - 1 \cdot 17 = 1$	$s_4 = 1 - 1 \cdot (-4) = 5$	$t_4 = -3 - 1 \cdot (13) = -16$	$q_3 = 1$
שלב $k = 4$:	$r_5 = 17 - 17 \cdot 1 = 0$	$s_5 = -4 - 17 \cdot 5 = -89$	$t_5 = 13 - 17 \cdot (-16) = 285$	$q_4 = 17$

$$\gcd(a, b) = r_4 = 1 \ , \qquad s = s_4 = 5 \ , \qquad t = t_4 = -16 \ .$$

$$ta + sb = 5(289) - 16(85) = 1 \ .$$

■

שאלה 3

$a \mid bc$ לכן $\exists$ שלם q עבורו

$$bc = qa \tag{\#1}$$

$\gcd(a, b) = 1$ לכן $\exists\ x, y$ שלמים עבורם $xa + yb = 1$.

מכאן

$$b = \frac{1 - xa}{y} \ . \qquad \text{(\#2)}$$

על די הצבה של (#2) ב- (#1) נקבל

$$\begin{aligned}\left(\frac{1-xa}{y}\right)c &= qa \\ (1-xa)c &= qay \\ c - xac &= qay \\ c &= qay + xac \\ c &= a\left(xc + qy\right) \ .\end{aligned}$$

לכן $a \mid c$.

שאלה 4

א) לפי משפט בזו, מכיוון ש- a, b זרים אז קיימים שלמים s, t עבורם

$$sa + tb = 1 \ .$$

נקח את $\bmod b$ של הצד שמאל והצד ימין ונקבל

$$(sa + tb) \mod b = 1 \mod b \quad \Rightarrow \quad sa \mod b = 1 \mod b \quad \Rightarrow \quad sa \equiv 1 \mod b \ .$$

ב) נוכיח את הטענה דרך השלילה. נניח $\exists\, c$ שלם עבורו $ac \equiv 1 \mod b$.

ז"א $\exists\, q$ שלם עבורו $ac = qb + 1$.

מכאן

$$ac - qb = 1 \quad \Rightarrow \quad ac + (-q)b - 1$$

עכשיו a, b אינם זרים אז קיים מחלק משותף $d \neq 1$ כך ש- $d \mid a$ ו- $d \mid b$.

ז"א $d \mid (ac + (-q)b)$ לכן $d \mid 1$.

סתירה!

שאלה 5

א) $a \equiv b \mod m$ אז $\exists\, q$ שלם עבורו $a = qm + b$.

מכאו

$$a + c = qm + b + c \quad \Rightarrow \quad a + c \equiv b + c \mod m \ .$$

ב) $a \equiv b \mod m$ אז $\exists\, q$ שלם עבורו $a = qm + b$.

$c \equiv d \mod m$ אז $\exists\, q'$ שלם עבורו $c = q'm + d$.

מכאו

$$ac = (mq + b)\,(q'm + d) = qq'm^2 + bq'm + dqm + bd = (qq'm + bq' + dq)\,m + bd \ .$$

לכן $\exists \bar{q} = qq'm + bq' + dq$ כך ש-

$$ac = \bar{q}m + bd$$

לפיכך $ac \equiv bd \mod m$.

ג) אינדוקציה על n.

<u>שאלה 6</u> הכלל מפענח הוא

$$d_k(y) = a^{-1}\,(y - b) \mod 26$$

לכן $a^{-1} \mod 26 = 5^{-1} \mod 26 = 21$.

$$d_k(y) = 21(y - 17) \mod 26 = 21y - 357 \mod 26 \ .$$

$357\%26 = 357 - 26\left\lfloor \frac{357}{26} \right\rfloor = 357 - 26(13) = 19$ לכן $(-357)\%26 = 26 - (357\%26) = 26 - 19 = 7$ לכן
$-289 \mod 26 = 7$. מכאן

$$d_k(y) = 21y + 7 \ .$$

y $\in C$	I	A	F	D	X	F	U	U	W	L	F	E	I	A	L	L	C	R	Z
$y \in \mathbb{Z}_{26}$	8	0	5	3	23	5	20	20	22	11	5	4	8	0	11	11	2	17	25
$x \in \mathbb{Z}_{26}$	19	7	8	18	22	8	11	11	1	4	8	13	19	7	4	4	23	0	12
x $\in P$	t	h	i	s	w	i	l	l	b	e	i	n	t	h	e	e	x	a	m

<u>שאלה 7</u>

y $\in C$	H	V	F	D	D	P
$y \in \mathbb{Z}_{26}$	7	21	5	3	3	15

דטרמיננטה של k היא $|k| = 7 \mod 26 = 7$.
$\gcd(7, 26) = 1$ לכן המטריצה הפיכה ב- $\mathbb{Z}_{26}$.

$$\begin{pmatrix} \cancel{13} & \cancel{5} & \cancel{6} \\ 2 & 1 & 7 \\ 9 & 7 & 13 \end{pmatrix} \Rightarrow C_{11} = (-1)^{1+1} \begin{vmatrix} 1 & 7 \\ 7 & 13 \end{vmatrix} \mod 26 = -36 \mod 26 = 16 .$$

$$\begin{pmatrix} \cancel{13} & \cancel{5} & \cancel{6} \\ 2 & 1 & 7 \\ 9 & 7 & 13 \end{pmatrix} \Rightarrow C_{12} = (-1)^{1+2} \begin{vmatrix} 2 & 7 \\ 9 & 13 \end{vmatrix} \mod 26 = 37 \mod 26 = 11 .$$

$$\begin{pmatrix} \cancel{13} & \cancel{5} & \cancel{6} \\ 2 & 1 & 7 \\ 9 & 7 & 13 \end{pmatrix} \Rightarrow C_{13} = (-1)^{1+3} \begin{vmatrix} 2 & 1 \\ 9 & 7 \end{vmatrix} \mod 26 = 5 \mod 26 = 5 .$$

$$\begin{pmatrix} 13 & 5 & 6 \\ \cancel{2} & \cancel{1} & \cancel{7} \\ 9 & 7 & 13 \end{pmatrix} \Rightarrow C_{21} = (-1)^{2+1} \begin{vmatrix} 5 & 6 \\ 7 & 13 \end{vmatrix} \mod 26 = -23 \mod 26 = 3 .$$

$$\begin{pmatrix} 13 & \cancel{5} & 6 \\ \cancel{2} & \cancel{1} & \cancel{7} \\ 9 & 7 & 13 \end{pmatrix} \Rightarrow C_{22} = (-1)^{2+2} \begin{vmatrix} 13 & 6 \\ 9 & 13 \end{vmatrix} \mod 26 = 115 \mod 26 = 11 .$$

$$\begin{pmatrix} 13 & 5 & 6 \\ \cancel{2} & \cancel{1} & \cancel{7} \\ 9 & 7 & 13 \end{pmatrix} \Rightarrow C_{23} = (-1)^{2+3} \begin{vmatrix} 13 & 5 \\ 9 & 7 \end{vmatrix} \mod 26 = -46 \mod 26 = 6 .$$

$$\begin{pmatrix} 13 & 5 & 6 \\ 2 & 1 & 7 \\ \cancel{9} & \cancel{7} & \cancel{13} \end{pmatrix} \Rightarrow C_{31} = (-1)^{3+1} \begin{vmatrix} 5 & 6 \\ 1 & 7 \end{vmatrix} \mod 26 = 29 \mod 26 = 3 .$$

$$\begin{pmatrix} 13 & \cancel{5} & 6 \\ 2 & \cancel{1} & 7 \\ \cancel{9} & \cancel{7} & \cancel{13} \end{pmatrix} \Rightarrow C_{32} = (-1)^{3+2} \begin{vmatrix} 13 & 6 \\ 2 & 7 \end{vmatrix} \mod 26 = -79 \mod 26 = 25 .$$

$$\begin{pmatrix} 13 & 5 & \cancel{6} \\ 2 & 1 & \cancel{7} \\ \cancel{9} & \cancel{7} & \cancel{13} \end{pmatrix} \Rightarrow C_{33} = (-1)^{3+3} \begin{vmatrix} 13 & 5 \\ 2 & 1 \end{vmatrix} \mod 26 = 3 \mod 26 = 3 .$$

$$C = \begin{pmatrix} C_{11} & C_{12} & C_{13} \\ C_{21} & C_{22} & C_{23} \\ C_{31} & C_{32} & C_{33} \end{pmatrix} = \begin{pmatrix} 16 & 11 & 5 \\ 3 & 11 & 6 \\ 3 & 25 & 3 \end{pmatrix} .$$

$$\text{adj}(A) = C^t = \begin{pmatrix} 16 & 3 & 3 \\ 11 & 11 & 25 \\ 5 & 6 & 3 \end{pmatrix} .$$

$$k^{-1} \mod 26 = |k|^{-1}\text{adj}(k) .$$

$$|k|^{-1} \mod 26 = 7^{-1} \mod 26 = 15 .$$

$$k^{-1} = 15 \begin{pmatrix} 16 & 3 & 3 \\ 11 & 11 & 25 \\ 5 & 6 & 3 \end{pmatrix} = \begin{pmatrix} 240 & 45 & 45 \\ 165 & 165 & 375 \\ 75 & 90 & 45 \end{pmatrix} \mod 26 = \begin{pmatrix} 6 & 19 & 19 \\ 9 & 9 & 11 \\ 23 & 12 & 19 \end{pmatrix}$$

$$(7, 21, 5) \cdot k^{-1} = (346, 382, 459) \mod 26 = (8, 18, 17)$$

$$(3, 3, 15) \cdot k^{-1} = (390, 264, 375) \mod 26 = (0, 4, 11)$$

y $\in C$	H	V	F	D	D	P
$y \in \mathbb{Z}_{26}$	7	21	5	3	3	15
$x \in \mathbb{Z}_{26}$	8	18	17	0	4	11
x $\in C$	i	s	r	a	e	l

שאלה 8

x	1	2	3	4
$\pi^{-1}(x)$	1	4	3	2

y $\in C$	C	E	D	O	B	A	E	R	K	G	N	I
$y \in \mathbb{Z}_{26}$	2	4	3	14	1	0	4	17	10	6	13	8
$x \in \mathbb{Z}_{26}$	2	14	3	4	1	17	4	0	10	8	13	6
x $\in P$	c	o	d	e	b	r	e	a	k	i	n	g

שאלה 9

$$d_k\left(y_1y_2y_3y_4y_5\right) = (x_1 - 6, x_2 - 17, x_3 - 4, x_4 - 4, x_5 - 13) \mod 26 .$$

y $\in C$	Z	F	S	X	U	H	I	Y	W	U
$y \in \mathbb{Z}_{26}$	25	5	18	23	20	7	8	24	22	20
$d_k(y)$	19	14	14	19	7	1	17	20	18	7
x $\in P$	t	o	o	t	h	b	r	u	s	h