תרגילים 1: תורת המספרים

שאלה 1 מצאו את הפירוק מנה-שארית של השלמים הבאים:

א) $a = 7503, b = 81$.

ב) $a = -7503, b = 81$.

ג) $a = 81, b = 7503$.

ד) $a = -81, b = 7503$.

שאלה 2 יהיו $a, b, n > 0$ שלמים. הוכיחו כי $a \bmod n = b \bmod n$ אם ורק אם $a \equiv b \pmod n$.

שאלה 3 מצאו שלמים s, t, d עבורם $12327s + 409t = d$.

שאלה 4 הוכיחו כי 7563 ו- 526 מספרים זרים.

שאלה 5 הוכיחו שאם p מספר ראשוני ו- n מספר שלם חיובי אז

$$\phi(pn) = \begin{cases} (p-1)\phi(n) \ , & \text{אם } p \nmid n \\ p\phi(n) \ , & \text{אם } p \mid n \end{cases} .$$

שאלה 6 יהיו a ו- b מספרים ראשוניים. הוכיחו:

א) $\phi(a) = a - 1$.

ב) $\phi(ab) = (a-1)(b-1)$.

שאלה 7 יהיו a, b מספרים שלמים.

הוכיחו שאם קיימים שלמים s, t כך ש- $sa + tb = 1$ אז a ו- b זרים.

שאלה 8 יהיו a, b, n מספרים שלמים. הוכיחו את הטענה הבאה:

אם השלושה תנאים הבאים מתקיימים:

1) a ו- b זרים,

2) $a \mid n$,

3) $b \mid n$,

אז $ab \mid n$.

שאלה 9 הוכיחו את הטענות הבאות:

א) $\gcd(ma, mb) = m \gcd(a, b)$.

ב) אם $m > 0$ ואם $m \mid a$ ו- $m \mid b$ אז $\dfrac{\gcd(a,b)}{m} = \gcd\left(\dfrac{a}{m}, \dfrac{b}{m}\right)$.

ג) המספרים $\dfrac{a}{\gcd(a,b)}$ ו- $\dfrac{b}{\gcd(a,b)}$ מספרים זרים.

ד) אם $c \mid ab$ ו- c זר ביחס ל- b אז $c|a$.

ה) אם a, c מספרים זרים ואם b, c מספרים זרים אז c ו- ab מספרים זרים.

ו) $\gcd(a, b) = \gcd(a + cb, b)$.

שאלה 10 יהיו a, m מספרים זרים. הוכיחו כי $ab \equiv ac \mod m$ אם ורק אם $b \equiv c \mod m$.

שאלה 11 יהיו a, m מספרים (לא בהכרח זרים).
הוכיחו כי $ab \equiv ac \mod m$ אם ורק אם $b \equiv c \mod \dfrac{m}{\gcd(a,m)}$.

שאלה 12

א) חשבו את $\gcd(285, 89)$.

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

שאלה 13 **(10 נקודות)** הוכיחו: אם $a \mid bc$ ו- a, b זרים אז $a \mid c$.

שאלה 14 **(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 15 **(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 16 (10 נקודות)

נתון הטקסט מוצפן

IAFDXFUUWLFEIALLCRZ

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

שאלה 17 (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 18 (10 נקודות)

נתונה התמורה

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

פענחו את הטקסט מצפון

CEDOBAERKGNI

שאלה 19 (10 נקודות)

נתון את הטקסט מוצפן

ZFSXUHIYWU

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

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

שאלה 21 (10 נקודות)

א) חשבו את $\gcd(285, 89)$.

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

שאלה 22 (10 נקודות) הוכיחו: אם $a \mid bc$ ו- a, b זרים אז $a \mid c$.

שאלה 23 (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 24 (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 25 (10 נקודות)

נתון הטקסט מוצפן

IAFDXFUUWLFEIALLCRZ

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

שאלה 26 (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 27 (10 נקודות)

נתונה התמורה

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

פענחו את הטקסט מצפון

CEDOBAERKGNI

שאלה 28 (10 נקודות)

נתון את הטקסט מוצפן

ZFSXUHIYWU

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

שאלה 29 (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

מצב	סימן a	סימן b	מנה q	שארית r
1	$+$	$+$	$\left\lfloor \frac{a}{b} \right\rfloor$	$a \bmod b$
2	$+$	$-$	$-\left\lfloor \frac{a}{\lvert b\rvert} \right\rfloor$	$a \bmod \lvert b\rvert$
3	$-$	$+$	$-\left\lfloor \frac{\lvert a\rvert}{b} \right\rfloor - 1$	$b - \lvert a\rvert \bmod b$
4	$-$	$-$	$\left\lfloor \frac{\lvert a\rvert}{\lvert b\rvert} \right\rfloor + 1$	$\lvert b\rvert - \lvert a\rvert \bmod \lvert b\rvert$

א) נחשב שלמים q,r עבורם $a = qb + r$. השלם $a > 0$ ו- $b > 0$ לכן:

$$q = \left\lfloor \frac{a}{b} \right\rfloor = \left\lfloor \frac{7503}{81} \right\rfloor = 92$$

$$r = a \bmod b = a - b\left\lfloor \frac{a}{b} \right\rfloor = 7503 - (81)(92) = 75$$

לכן

$$7503 = (92)(81) + 51 \ .$$

ב) השלם $a < 0$ ו- $b > 0$ לכן:

$$q = -\left\lfloor \frac{|a|}{b} \right\rfloor - 1 = -\left\lfloor \frac{7503}{81} \right\rfloor - 1 = -93$$

$$r = b - |a| \bmod b = b - \left(|a| - b\left\lfloor \frac{|a|}{b} \right\rfloor \right) = 81 - (7503 - (81)(92)) = 30 \ .$$

לכן

$$-7503 = (-93)(81) + 30 \ .$$

ג) השלם $a > 0$ ו- $b > 0$ לכן:

$$q = \left\lfloor \frac{a}{b} \right\rfloor = \left\lfloor \frac{81}{7503} \right\rfloor = 0 \ .$$

$$r = a \bmod b = \left(a - b\left\lfloor \frac{a}{b} \right\rfloor \right) = 81 - (7503)\left\lfloor \frac{81}{7503} \right\rfloor = 81 \ .$$

לכן

$$81 = (0)(7503) + 81 \ .$$

ד) השלם $a<0$ ו- $b>0$ לכן:

$$q=-\left\lfloor\frac{|a|}{b}\right\rfloor-1=-\left\lfloor\frac{81}{7503}\right\rfloor-1=-1$$

$$r=b-|a| \bmod b=b-\left(|a|-b\left\lfloor\frac{|a|}{b}\right\rfloor\right)=7503-(81-(7503)(0))=7422\ .$$

לכן

$$-81=(-1)(7503)+7422\ .$$

שאלה 2

נניח כי $a \bmod n = b \bmod n$.

ממשפט החילוק של אוקלידס, מכיוון ש- $a>0$ ו- $b>0$:

- עבור a ו- n קיימים שלמים q_1 ו- r_1 כך ש:

$$a=q_1n+r_1=q_1n+a \bmod n \qquad\Rightarrow\qquad a \bmod n=a-q_1n\ .$$

- עבור b ו- n קיימים שלמים q_2 ו- r_2 כך ש:

$$b=q_2n+r_2=q_2n+b \bmod n \qquad\Rightarrow\qquad b \bmod n=b-q_2n\ .$$

נשווה ביניהם:

$$a \bmod n=b \bmod n \quad\Rightarrow\quad a-q_1n=b-q_2n \quad\Rightarrow\quad a=b+(q_1-q_2)n\ .$$

לכן $a\equiv b \pmod n$.

נניח כי $a\equiv b \pmod n$. אזי קיים שלם q עבורו

(*) $$a=qn+b\ .$$

לפי המשפט החילוק של אוקלידס, קיימים שלמים $\bar{q}$ ו- r עבורם

(**) $$b=\bar{q}n+r=\bar{q}n+b \bmod n\ .$$

נציב במשוואה (**) בבמשוואה (*):

$$a=qn+\bar{q}n+b \bmod n=(q+\bar{q})\,n+b \quad \bmod n\ .$$

הראנו שקיימים שלמים $Q=q+\bar{q}$ ו- $R=b \mod n$ עבורם

$$a=Qn+R\ ,$$

ומיוון ש- $a,n>0$ אזי $R=a \bmod n$. ז"א

$$a \bmod n=b \bmod n\ .$$

שאלה 3 קיימים שלמים s,t,d עבורם $12327s+2409t=d$ כאשר $d=\gcd(12327,2409)$.
נשתמש באלגוריתם המוכלל של אוקליד. נסמן $a=12327, b=2409$.

$$r_0=a=12327\ ,\quad r_1=2409\ ,\quad s_0=1\ ,\quad s_1=0\ ,\quad t_0=0\ ,\quad t_1=1\ .$$

$r_2=r_0-q_1r_1$ $=12327-(5)(2409)$ $=282$	$s_2=s_0-q_1s_1$ $=1-(5)(0)$ $=1$	$t_2=t_0-q_1t_1$ $=1-(5)(1)$ $=-5$
$r_3=r_1-q_2r_2$ $=2409-(8)(282)$ $=153$	$s_3=s_1-q_2s_2$ $=0-(8)(1)$ $=-8$	$t_3=t_1-q_2t_2$ $=1-(8)(-5)$ $=41$
$r_4=r_2-q_3r_3$ $=282-(1)(153)$ $=129$	$s_4=s_2-q_3s_3$ $=1-(1)(-8)$ $=9$	$t_4=t_2-q_3t_3$ $=-5-(1)(41)$ $=-46$
$r_5=r_3-q_4r_4$ $=153-(1)(129)$ $=24$	$s_5=s_3-q_4s_4$ $=-8-(1)(9)$ $=-17$	$t_5=t_3-q_4t_4$ $=41-(1)(-46)$ $=87$
$r_6=r_4-q_5r_5$ $=129-(5)(24)$ $=9$	$s_6=s_4-q_5s_5$ $=9-(5)(-17)$ $=94$	$t_6=t_4-q_5t_5$ $=-46-(5)(87)$ $=-481$
$r_7=r_5-q_6r_6$ $=24-(2)(9)$ $=6$	$s_7=s_5-q_6s_6$ $=-17-(2)(94)$ $=-205$	$t_7=t_5-q_6t_6$ $=87-(2)(-481)$ $=1049$
$r_8=r_6-q_7r_7$ $=9-(1)(6)$ $=3$	$s_8=s_6-q_7s_7$ $=94-(1)(-205)$ $=299$	$t_8=t_6-q_7t_7$ $=-481-(1)(1049)$ $=-1530$
$r_9=r_7-q_8r_8$ $=6-(2)(3)$ $=0$		

שאלה 5 אם $p\nmid n$ אז p לא מופיע לפירוק לראשוניים של n. ז"א אם הפירוק לראשוניים של n הוא

$$n=p_1^{e_1}p_2^{e_2}\cdot p_k^{e_k}$$

אז $p\neq p_i$ לכל $1\leq i\leq k$. לכן הפיקור לראשוניים של pn הוא

$$pn=p^1p_1^{e_1}p_2^{e_2}\cdot p_k^{e_k}\ .$$

מכאן הפונקציית אוילר עבור pn היא

$$\phi(pn)=\left(p^1-p^0\right)\left(p_1^{e_1}-p_1^{e_1-1}\right)\cdots\left(p_k^{e_k}-p_k^{e_k-1}\right)\ .$$

אבל הפונקציית אוילר של p היה $\phi(p)=p-1$ והפונקציית אוילר של n הוא $\phi(n)=\left(p_1^{e_1}-p_1^{e_1-1}\right)\cdots\left(p_k^{e_k}-p_k^{e_k-1}\right)$ לכן

$$\phi(pn)=(p-1)\phi(n)\ .$$

אם $p\mid n$ אז p מופיע בפירוק לראשוניים של n. ז"א אם הפירוק לראשוניים של n הוא

$$n=p_1^{e_1}\cdots p_{i-1}^{e_{i-1}}p_i^{e_i}p_{i+1}^{e_{i+1}}\cdots p_k^{e_k}$$

אז קיים i, $1\leq i\leq k$ עבורו $p_i=p$. לכן

$$np=p_1^{e_1}\cdots p_{i-1}^{e_{i-1}}p^{e_i+1}p_{i+1}^{e_{i+1}}\cdots p_k^{e_k}\ .$$

מכאן הפונקציית אוילר של np היא

$$\begin{aligned}\phi(np)&=\left(p_1^{e_1}-p_1^{e_1-1}\right)\cdots\left(p_{i-1}^{e_{i-1}}-p_i^{e_{i-1}-1}\right)\left(p^{e_i+1}-p^{e_i}\right)\left(p_{i+1}^{e_{i+1}}-p_{i+1}^{e_{i+1}-1}\right)\cdots\left(p_k^{e_k}-p_k^{e_k-1}\right)\\&=\left(p_1^{e_1}-p_1^{e_1-1}\right)\cdots\left(p_{i-1}^{e_{i-1}}-p_i^{e_{i-1}-1}\right)p\left(p^{e_i}-p^{e_i-1}\right)\left(p_{i+1}^{e_{i+1}}-p_{i+1}^{e_{i+1}-1}\right)\cdots\left(p_k^{e_k}-p_k^{e_k-1}\right)\\&=p\left(p_1^{e_1}-p_1^{e_1-1}\right)\cdots\left(p_{i-1}^{e_{i-1}}-p_i^{e_{i-1}-1}\right)\left(p^{e_i}-p^{e_i-1}\right)\left(p_{i+1}^{e_{i+1}}-p_{i+1}^{e_{i+1}-1}\right)\cdots\left(p_k^{e_k}-p_k^{e_k-1}\right)\\&=p\phi(n)\ .\end{aligned}$$

שאלה 6

א) a ראשוני לכן הפירוק לראשוניים שלו הוא $p_1^{e_1}$ כאשר $p_1=a$ ו- $e_1=1$.
לכן הפונקצית אוילר של a הינה

$$\phi(a)=\left(p_1^{e_1}-p_1^{e_1-1}\right)=a-1\ .$$

ב) a ראשוני ו- b ראשוני לכן הפירוק לראשוניים של ab הוא $ab=p_1^{e_1}p_2^{e_2}$ כאשר $p_1=a,p_2=b$, ו- $e_1=1,e_2=1$.
לכן הפונקצית אוילר של ab הינה

$$\phi(ab)=\left(p_1^{e_1}-p_1^{e_1-1}\right)\left(p_2^{e_2}-p_2^{e_2-1}\right)=(a-1)(b-1)\ .$$

שאלה 7 יהי d ה- gcd של a ו- b. אם $sa+tb=1$ אז בהכרח d מחלק 1. לכן $d=1$ לכן $\gcd(a,b)=1$.

שאלה 8

$$a\mid n\ ,\quad b\mid n$$

לכן קיימים שלמים k ו- l כך ש-

$$n=ak\ ,\qquad n=bl\ .$$

ז"א $n=ak=bl$.
מכאן $b\mid ak$.
נתון כי $\gcd(a,b)=1$, לכן $b\mid k$. לכן $k=bq$.
לכן $n=ak=abq$.

שאלה 9

א) יהי $d=\gcd(a,b)$. אז קיימים שלמים s,t עבורם

$$sa+tb=d\ .$$

מכאן

$$msa+mtb=md \quad\Rightarrow\quad s(ma)+t(mb)=md\ .$$

לכן $\gcd(ma,mb)=md=m\gcd(a,b)$.

ב) יהי $d=\gcd(a,b)$.
$\exists$ שלמים s,t כך ש-

(*)
$$sa+tb=d\ .$$

נחלק (*) ב- m ונקבל

(**)
$$s\frac{a}{m}+t\frac{b}{m}=\frac{d}{m}\ .$$

נשים לב $m\mid a$ ו- $m\mid b$. לכן $\frac{a}{m}$ שלמ ו- $\frac{b}{m}$ שלם.
לכן $\frac{d}{m}$ בהכרח שלם ולפי משפט בזו $\gcd\left(\frac{a}{m},\frac{b}{m}\right)=\frac{d}{m}$. לכן

$$\gcd\left(\frac{a}{m},\frac{b}{m}\right)=\frac{\gcd(a,b)}{m}\ .$$

ג) יהי $d=\gcd(a,b)$.
$\exists$ שלמים s,t עבורם

$$sa+tb=d\ .$$

נחלק ב- d ונקבל

$$s\frac{a}{d}+t\frac{b}{d}=1\ .$$

לפי משפט בזו, השלם בצד ימין הוא ה- gcd של $\frac{a}{d}$ ו- $\frac{b}{d}$. לכן

$$\gcd\left(\frac{a}{d},\frac{b}{d}\right)=1 \quad\Rightarrow\quad \gcd\left(\frac{a}{\gcd(a,b)},\frac{b}{\gcd(a,b)}\right)=1$$

לכן $\frac{a}{\gcd(a,b)}$ ו- $\frac{b}{\gcd(a,b)}$ זרים.

ד) a,b שלמים לכן קיימים שלמים s,t,d עבורם

$$sa+tb=d$$

כאשר $d=\gcd(a,b)$.

מכאן

$$s\left(\frac{a}{d}\right)+t\left(\frac{b}{d}\right)=1\ .$$

נשים לב ש- $d=\gcd(a,b)$ לכן בהכרח $\frac{a}{d}$ ו- $\frac{b}{d}$ שלמים. לכן קיבלנו שלמים s,t עבורם

$$s\left(\frac{a}{\gcd(a,b)}\right)+t\left(\frac{b}{\gcd(a,b)}\right)=1\ .$$

לכן השלמים $\frac{a}{\gcd(a,b)}$ ו- $\frac{b}{\gcd(a,b)}$ זרים.

ה) אם a,c מספרים זרים ואם b,c מספרים זרים אז c ו- ab מספרים זרים.

a ו- c זרים אז קיימים s ו- t שלמים עבורם

$$sa+tc=1\ .$$

b ו- c זרים אז קיימים $\bar{s}$ ו- $\bar{t}$ שלמים עבורם

$$\bar{s}b+\bar{t}c=1\ .$$

לכן

$$\begin{aligned}(sa+tc)\left(\bar{s}b+\bar{t}c\right)&=1\\ \Rightarrow\quad s\bar{s}(ab)+\left(t\bar{s}b+t\bar{t}c+s\bar{t}a\right)c&=1\end{aligned}$$

ז"א קיימים שלמים x,y עבורם $x(ab)+yc=1$ לכן ab ו- c זרים.

ו) אם a,b שלמים אז קיימים שלמים s ו- t עבורם $sa+tb=d$ כאשר $d=\gcd(a,b)$. מכאן

$$\begin{aligned}sa+tb&=d\\ s\left(a+cb\right)+tb&=d+scb\\ s\left(a+cb\right)+tb-scb&=d\\ s\left(a+cb\right)+\left(t-sc\right)b&=d\end{aligned}$$

לכן קיימים שלמים $x=s$ ו- $y=t-cb$ עבורם

$$x(a+cb)+yb=d$$

ולכן $\gcd(a+cb,b)=d=\gcd(a,b)$.

שאלה 10

נניח כי $ab\equiv ac \mod m$.

$$ab\equiv ac\mod m\quad\Rightarrow\quad ab=ac+qm\quad\Rightarrow\quad ab-ac=qm\quad\Rightarrow\quad a(b-c)=qm\ .$$

מכאן $a\mid qm$.
a,m זרים לכן $a\nmid m$ לכן $a\mid q$. ז"א $\exists\ k$ שלם עבורו $q=ak$.

לפיכך

$$a(b-c)=qm \quad\Rightarrow\quad a(b-c)=akm \quad\Rightarrow\quad b-c=km \quad\Rightarrow\quad b=c+km \quad\Rightarrow\quad b\equiv c \mod m \ .$$

נניח כי $b\equiv c \mod m$. אז

$$b=qm+c \quad\Rightarrow\quad ab=aqm+ac \quad\Rightarrow\quad ab\equiv ac \mod m \ .$$

<u>שאלה 11</u> נניח כי $ab\equiv ac \mod m$. אז

$$ab=ac+qm \quad\Rightarrow\quad ab-ac=qm \quad\Rightarrow\quad m\mid a(b-c) \quad\Rightarrow\quad \frac{m}{\gcd(a,m)} \mid \frac{a}{\gcd(a,m)}(b-c) \ .$$

מכיוון ש- $\frac{m}{\gcd(a,m)}$ ו- $\frac{a}{\gcd(a,m)}$ זרים, אז

$$\frac{m}{\gcd(a,m)} \mid (b-c) \ .$$

לכן

$$b\equiv c \mod \left(\frac{m}{\gcd(a,m)}\right) \ .$$

<u>שאלה 12</u>

$a=285, b=89$.

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

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 $k=4$:	$r_5=17-17\cdot 1=0$	$s_5=-4-17\cdot 5=-89$	$t_5=13-17\cdot(-16)=285$	$q_4=17$

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

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

■

<u>שאלה 13</u> $a \mid bc$ לכן $\exists$ שלם q עבורו

(#1)
$$bc = qa$$

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

מכאן

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

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 $a \mid c$.

<u>שאלה 14</u>

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

$$sa+tb=1 \ .$$

נקח את $\mod b$ 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 $1 \neq d$ כך ש- $d \mid a$ ו- $d \mid b$.

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

סתירה!

<u>שאלה 15</u>

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.

שאלה 16

הכלל מפענח הוא

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

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

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

$357\%26 = 357 - 26\left\lfloor \frac{357}{26} \right\rfloor = 357 - 26(13) = 19$ 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

שאלה 17

$y \in C$	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- $\mathbb{Z}_{26}$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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 18

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 19

$$d_k\left(y_1 y_2 y_3 y_4 y_5\right) = (x_1 - 6, x_2 - 17, x_3 - 4, x_4 - 4, x_5 - 13) \mod 26 \ .$$

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

שאלה 20

$$1 \cdot 7 = 7 \quad \equiv 7 \mod 20 \ ,$$
$$2 \cdot 7 = 14 \quad \equiv 14 \mod 20 \ ,$$
$$3 \cdot 7 = 21 \quad \equiv 1 \mod 20 \ .$$

לכן $7^{-1} \equiv 3 \mod 20$.

שאלה 21

$a = 285, b = 89$.

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

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 22

$a \mid bc$ לכן $\exists$ שלם q עבורו

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

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

מכאן

$$b = \frac{1 - xa}{y} \ . \tag{\#2}$$

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 23

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

$$sa + tb = 1 \ .$$

נקח את $\mod b$ 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 24__

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 25</u> הכלל מפענח הוא

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

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

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

$357\%26 = 357 - 26\left\lfloor \frac{357}{26} \right\rfloor = 357 - 26(13) = 19$ 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 26</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- $\mathbb{Z}_{26}$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$\mathtt{y} \in C$	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
$\mathtt{x} \in C$	i	s	r	a	e	l

שאלה 27

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 28

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

$y \in C$	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