תרגילים 1: תורת המספרים

שאלה 1 מצאו את

א) $7503 \,\%\, 81$

ב) $(-7503) \,\%\, 81$

ג) $81 \,\%\, 7503$

ד) $(-81) \,\%\, 7503$

שאלה 2 הוכיחו כי $a \,\%\, m = b \,\%\, m$ אם ורק אם $a \equiv b \mod m$.

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

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

ד) אם $ab \mid c$ 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 $b \equiv c \mod \frac{m}{\gcd(a,m)}$.

פתרונות

שאלה 1

א) לכל $a>0$ השארית בחלוקה ב- m נתונה ע"י $m \left\lfloor \frac{a}{m} \right\rfloor$ $a \,\%\, m = a -$.

$$7503 \,\%\, 81 = 7503 - \left\lfloor \frac{7503}{81} \right\rfloor \cdot 81 = 7503 - 92 \cdot 81 = 7503 - 7452 = 51 \ .$$

ב) לכל $a>0$ השארית של $-a$ בחלוקה ב- m נתונה ע"י $(-a) \,\%\, m = m - (a \,\%\, m)$

$$(-7503) \,\%\, 81 = 81 - 51 = 30 \ .$$

ג) $a \,\%\, m = a - \left\lfloor \frac{a}{m} \right\rfloor m$.

$$a \,\%\, m = 81 - \left\lfloor \frac{81}{7503} \right\rfloor \cdot 7503 = 81 - 0 \cdot 81 = 81 \ .$$

ד) $(-a) \,\%\, m = m - a \,\%\, m$.

$$(-81) \,\%\, 7503 = 7503 - (81 \,\%\, 7503) = 7503 - 81 = 7422 \ .$$

שאלה 2

נניח כי $a \,\%\, m = b \,\%\, m$.

נסמן $r = a \,\%\, m = b \,\%\, m$. אז

$$a = mq_1 + r \ , \qquad b = mq_2 + r$$

כאשר q_1, q_2 מספרים שלמים. ז"א

$$a - b = mq_1 - mq_2 = m(q_1 - q_2) \ .$$

$q_1 - q_2$ מספר שלם לכן $m \mid a-b$ לכן $a \equiv b \mod m$ כנדרש.

כעת נניח כי $a \equiv b \mod m$.

ז"א $m \mid a-b \Leftarrow$ קיים q שלם כך ש-

$$a - b = mq$$

נסמן $r = a \,\%\, m$. קיים מספר שלם q_1 כך ש-

$$a = q_1 m + r \ .$$

מכאן

$$b = a - qm = q_1 m + r - qm = (q_1 - q)m + r \ .$$

ז"א $b \,\%\, m = r$.

כנדרש.

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, $1\le i\le k$ 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-

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

נחלק $(*)$ ב- m ונקבל

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

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)

ה)

ו)

<u>שאלה 10</u> 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

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