קונגרואנציה

3-2-25

תרגיל 1 יהיו a,b,m שלמים, הוכיחו:
אם $a\%m=b\%m$ אז $a\equiv b \bmod m$.

פתרון

נסמן $r=a\%m=b\%m$.
צ״א, לפי משפט החילוק של אוקלידס,

$$a=q_1m+r\ ,\qquad b=q_2m+r$$

q_1,q_2 שלמים. נבודד את r:

$$r=a-q_1m\ ,\qquad r=b-q_2m$$

נשווה ביניהם:

$$a-q_1m=b-q_2m$$

$$\Longrightarrow\quad a=b-q_2m+q_1m$$

$$a=b+(q_1-q_2)m.$$

כלומר, $\exists\, Q=q_1-q_2$ שלם כך ש $a=Qm+b$

$\Longleftarrow$ $a\equiv b \bmod m$.

תרגיל 2:
יהיו a,b ראשוניים, הוכיחו:

$$\phi(a)=a-1$$

פתרון

- לכל שלם a קיים פירוק לראשוניים

$$a=p_1^{e_1}\cdots p_k^{e_k} \qquad \text{\_\_\_\_\_\_\_\_} \quad (1)$$

$p_1,\dots,p_k$ ראשוניים ו- $e_1,\dots,e_k$ שלמים

הפונקצית אוילר $\phi(a)$, הינה:

$$② \text{———} \quad \phi(a) = (p_1^{e_1} - p_1^{e_1 - 1}) \cdots (p_k^{e_k} - p_k^{e_k - 1})$$

<u>הוכחה:</u> הפירוק לראשוניים של-a, מכיוון ש-a עצמו מספר ראשוני, הינו:

$$a = a^1.$$

לכן לפי ②

$$\phi(a) = a^1 - a^{1-1} = a - 1.$$

<u>תרגיל:</u> יהיו a, b שלמים וראשוניים. הוכיחו:

$$\phi(ab) = (a-1)(b-1).$$

<u>פתרון</u> a, b ראשוניים שונים לכן הפירוק לראשוניים של המספר ab הינו:

$$ab = a^1 b^1.$$

לכן לפי הנוסחה לפונקצית אוילר:

$$\phi(ab) = (a^1 - a^{1-1})(b^1 - b^{1-1})$$

$$= (a^1 - a^0)(b^1 - b^0).$$

$$= (a-1)(b-1)$$

<u>תרגיל:</u>

יהיו a, b מספרים ראשוניים <u>שונים</u>.

הוכיחו:

$$\phi(a^k b^n) = (a^k - a^{k-1})(b^n - b^{n-1})$$

<u>פתרון</u>

a, b ראשוניים שונים לכן הפירוק לראשוניים של $a^k b^n$ הוא

$$a^k b^n = a^k b^n.$$

לכן, לפי נוסחת פונקציית אוילר

$$\phi\left(a^k b^n\right)=\left(a^k-a^{k-1}\right)\left(b^n-b^{n-1}\right)$$

<u>תרגיל:</u> יהיו a, b, n טבעיים. הוכיחו:

אם שלושת התנאים הבאים מתקיימים:

① a ו-b זרים

② $a \mid n$

③ $b \mid n$

אזי $ab \mid n$.

<u>פתרון</u> <u>כיוון:</u> $a \mid n$ לכן $\exists$ s שלם $n=as$.

$b \mid n$ לכן $\exists$ t שלם $n=bt$.

a, b זרים $\Longleftarrow$ $\gcd(a,b)=1$.

<u>3 כיוון להוכחה:</u> $ab \mid n$, כלומר ש- $n=abq$.

כאשר q שלם.

<u>ולכן:</u> נתון ש- $n=as$ ו- $n=bt$.

נשווה ביניהם:

$(*)$ — $n=bt=as$

לכן $b \mid as$.

נתון: $\gcd(a,b)=1$, לכן, $b \nmid a$ לכן $b \mid s$

לפי $(*)$.

לכן, $s=\underbrace{bk}$ כאשר k שלם.

לכן, $n=as=abk$. לכן $ab \mid n$.

תרגיל 6: הוכיחו את הטענות הבאות.
בכל הסעיפים, a,b,m שלמים.

א) $$\gcd(ma,mb) = m\gcd(a,b)$$

ב) אם $m>0$, ו- $m|a$ ו- $m|b$ אזי:
$$\gcd\left(\frac{a}{m}, \frac{b}{m}\right) = \frac{\gcd(a,b)}{m}$$

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

ד) אם $c|ab$ ו- c זר ביחס ל- b אזי $c|a$.

פתרון:

א) נוכיח $\gcd(ma,mb) = m\gcd(a,b)$.

נסמן $\gcd(a,b)=d$. לפי משפט אוקלידס,
$\exists$ שלמים s,t כך ש:
$$sa + tb = d$$
$$\Rightarrow m(sa+tb) = md$$
$$\Rightarrow sma + tmb = md$$
$$\Rightarrow s(ma) + t(mb) = (md)$$
לכן, לפי משפט אוקלידס, הושלם בצק הימין
הוא ה- $\gcd$ של השלמים ma ו- mb,
ז"א
$$\gcd(ma,mb) = md = m\gcd(a,b)$$
מש"ל.

ב) <u>טענה:</u> אם $m|a$, ו- $m|b$ ו- $m>0$ אז

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

<u>הוכחה:</u>

לפי משפט אוקלידס, $\exists$ שלמים s,t עבורם

$d=\gcd(a,b)$ $\qquad sa+tb=d$ ———— $(*)$

$$\boxed{\text{בגלל ש } d=\gcd(a,b) \text{, כלומר זה ה } \gcd \text{ של שני שלמים, אז } d\neq 0.}$$

נתון: $m|a$ ו $m|b$ לכן אפשר לחלק
את הצד השמאל ואת הצד ימין
ב- m:

$(\#)$ ———— $\frac{sa}{m}+\frac{tb}{m}=\frac{d}{m}$

$m|a \Leftarrow$ $\frac{a}{m}$ שלם.

(m|a אומר ש $\exists$ שלם q $a=qm$ $\Leftarrow$ $\frac{a}{m}=q$ שלם)

$m|b \Leftarrow$ $\frac{b}{m}$ שלם.

לכן, הצד ימין, $\frac{d}{m}$ שלם.

ונובע מ- $(\#)$:

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

לכן, לפי משפט אוקלידס:

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