תורת החבורות – תרגיל בית 1 – פתרון

שאלה 2

יהיו a,b זרים שונים מאפס, הוכח מבלי להשתמש בפירוק לראשוניים:

א. אם c זר ל-b, אז ac, b זרים.

ב. $4a+3b,\ 3a+2b$ גם הם זרים.

פתרון:

א) $(a,b)=1 \Leftarrow$ קיימים $\alpha,\beta\in\mathbb{Z}$ כך ש-$\alpha a+\beta b=1$.

$(b,c)=1 \Leftarrow$ קיימים $\alpha',\beta'\in\mathbb{Z}$ כך ש-$\alpha' b+\beta' c=1$.

אם נכפיל את שתי המשוואות נקבל כי $(\alpha\beta')ac+(\alpha\alpha' a+\beta\alpha' b+\beta\beta' c)b=1$.

מכאן $(ac,b)\mid 1 \Leftarrow (ac,b)=1$.

ב)

$$(b,a)=1 \Leftarrow (a+b,a)=1 \Leftarrow (a+b,3a+2b)=1 \overset{(*)}{\Leftarrow} (4a+3b,3a+2b)=1$$

הסבר $(*)$: נניח כי $(a+b,3a+2b)=d$, אז $d\mid 3a+2b$ וגם $d\mid a+b$, לכן d מחלק את כל צירוף שלם של $a+b,3a+2b$, בפרט $4a+3b$. מכאן $d\mid 3a+2b$ וגם $d\mid 4a+3b$, לכן d מחלק את $(4a+3b,\ 3a+2b)=1 \Leftarrow d=1$.

באותו אופן מראים את שאר המעברים.

שאלה 3

הוכח כי לכל a,b,n שלמים מתקיים $n\cdot(a,b)=(n\cdot a,n\cdot b)$.

פתרון:

נניח כי $(a,b)=d,(n\cdot a,n\cdot b)=c$. עלינו להראות כי $n\cdot d=c$.

d מחלק את a,b, לכן $n\cdot d$ מחלק את $n\cdot a,n\cdot b \Leftarrow n\cdot d\mid(n\cdot a,n\cdot b) \Leftarrow n\cdot d$ מחלק את c.

להפך, c מחלק את $n\cdot a,n\cdot b \Leftarrow$ מחלק את כל צירוף שלם שלהם.

$(a,b)=d$, לכן קיימים $\alpha,\beta\in\mathbb{Z}$ כך ש-$\alpha a+\beta b=d \Leftarrow \alpha(an)+\beta(bn)=nd$.

c מחלק את $\alpha(an)+\beta(bn)$, ולכן מחלק את nd.

בכך $n\cdot d,c$ מחלקים זה את זה, לכן שווים כי שניהם מספרים שלמים חיוביים.

שאלה 4

יהי n מספר טבעי, הוכח:

א. אם $a \equiv b \pmod n$, אז לכל $k \in \mathbb{N}$ $a^k \equiv b^k \pmod n$.

ב. אם $a_i \equiv b_i \pmod n$ לכל $1 \le i \le m$, אז לכל $k_1, \cdots, k_m$ שלמים

$$\sum_{i=1}^{m} k_i a_i \equiv \sum_{i=1}^{m} k_i b_i \pmod n.$$

ג. אם $(a,n)=1$, אז כל שני פתרונות של המשוואה $ax = 1 \pmod n$ שווים מודולו n

פתרון של ג':

$(a,n)=1 \Leftarrow$ קיימים $\alpha, \beta \in \mathbb{Z}$ כך ש- $\alpha a + \beta n = 1$ (1).

יהיו $x, y \in \mathbb{Z}$ שני פתרונות המשוואה. אז מ- (1) מקבלים $\alpha a x + \beta n x = x$ (2), ו-

$\alpha a y + \beta n y = y$ (3).

כעת מ- (2) ו- (3) יוצא כי $x = \alpha a x + \beta n x \equiv_n \alpha a x \equiv_n \alpha \equiv_n \alpha a y \equiv_n \alpha a y + \beta n y = y$

שאלה 5

א. מצא את הספרה האחרונה של המספר 777^{777}.

ב. מצא את שארית החלוקה של $2222^{5555} + 5555^{2222}$ ב- 7.

פתרון:

א) $777^{777} \equiv_{10} 7^{777} \Leftarrow 777 \equiv_{10} 7$.

נחשב חזקות של 7: $7^2 = 9, 7^3 = 3, 7^4 = 1$ (כל החישובים הם מודולו 10).

כעת $777^{777} = 7^{777} = 7^{776+1} = 7^{776} \cdot 7^1 = 1 \cdot 7 = 7$ (כל החישובים הם מודולו 10).

ב) $2222^{5555} \equiv_{10} 3^{5555} \Leftarrow 2222 \equiv_{10} 3$.

נחשב חזקות של 3: $3^2 = 2, 3^3 = 6 = -1 \Leftarrow 3^6 = 1$ (כל החישובים הם מודולו 7).

כעת $2222^{5555} = 3^{5555} = 3^5 = 6 \cdot 2 = 5$.

כמו כן $5555^{2222} = (-2222)^{2222} = (-3)^{2222} = 3^{2222} = 3^2 = 2$.

לכן $2222^{5555} + 5555^{2222} = 5 + 2 = 0$ (כל החישובים הם מודולו 7).

<u>שאלה 6</u>

<u>הוכח</u> כי לכל a,b,n שלמים מתקיים $a^2+b^2 \neq 4\cdot n+3$.

<u>פתרון</u>:

לכל $a\in\mathbb{Z}$ זוגי $a^2 \equiv_4 0$, ולכל $a\in\mathbb{Z}$ אי-זוגי $a^2 \equiv_4 1$. לכן לכל a,b שלמים מתקיים כי

$a^2+b^2 \equiv_4 0,1,2 \quad \Leftarrow \quad a^2+b^2 \not\equiv_4 3$.