23/03/15

Ασκήσεις Φυλλαδίου 3 – Ασκήσεις στον ΜΚΔ

Ασκ 1: $(130, 2275) = ;$ $(1998, 2004, 2016) = ;$

Λύση:
$$\left.\begin{aligned} 130 &= 2\cdot 5\cdot 13 = 2^1\cdot 5^1\cdot 7^0\cdot 13^1 \\ 2275 &= 5^2\cdot 7\cdot 13 = 2^0\cdot 5^2\cdot 7^1\cdot 13^1 \end{aligned}\right\} \Rightarrow$$

$$\Rightarrow (130, 2275) = \underbrace{2^0\cdot 5^1\cdot 7^0\cdot 13^1}_{} = 5\cdot 13 = 65$$

παίρνουμε όλους τους ~~κοινούς~~ πρώτους στο ελάχιστο των εκθετών!

$$\left.\begin{aligned} 1998 &= 2\cdot 3^3\cdot 37 = 2^1\cdot 3^3\cdot 37^1\cdot 167^0 \\ 2004 &= 2^2\cdot 3\cdot 167 = 2^2\cdot 3^1\cdot 37^0\cdot 167^1 \\ 2016 &= 2^5\cdot 3^2\cdot 37 = 2^5\cdot 3^2\cdot 37^1\cdot 167^0 \end{aligned}\right\} \Rightarrow (1998, 2004, 2016) = 2^1\cdot 3^1\cdot 37^0\cdot 167^0 = 2\cdot 3 = 6.$$

Ασκ 2 $(8k+3, 5k+2) = ;$ $k\in\mathbb{Z}$.

$d = (\alpha, b) \Leftrightarrow$
$\Leftrightarrow \exists\, x, y\in\mathbb{Z} : d = \alpha x + by$
κ' $d|\alpha$ κ' $d|b$

Λύση:
$$\left.\begin{aligned} d|8k+3 &\Rightarrow d|5(8k+3) \Rightarrow d|40k+15 \\ d|5k+2 &\Rightarrow d|8(5k+2) \Rightarrow d|40k+16 \end{aligned}\right\}\Rightarrow$$

$$\left.\begin{aligned} &\Rightarrow d|40k+15-40k-16 \Rightarrow d|-1 \Rightarrow d\,|\,|-1| \Rightarrow d|1 \\ &d\in\mathbb{N} \end{aligned}\right\}\Rightarrow \boxed{d=1}$$

Ασκ 4: $\alpha_1, \dots, \alpha_n, b\in\mathbb{Z}$ και: ~~$(\alpha_1, \dots, b) = 1$~~, $(\alpha_1, b) = 1, \dots, (\alpha_n, b) = 1$

Τότε $(\alpha_1 \cdot \ldots \cdot \alpha_n, b) = 1$.

Λύση: Έστω ότι $(\alpha_1\cdot\alpha_2\cdot\ldots\cdot\alpha_n, b) = d\neq 1$ (δηλ. $d>1$). Τότε ο d έχει έναν πρώτο διαιρέτη, έστω P.
Τότε P/d. Όμως $d|\alpha_1\cdot\ldots\cdot\alpha_n$
Τότε $P|\alpha_1\cdot\ldots\cdot\alpha_n \Rightarrow P$: πρώτος τότε $\rightarrow$

$\exists\, i=1,\dots,n : p|\alpha_i$
Επίσης : $p|d$, $d|b$ $\Rightarrow p|b$ $\Rightarrow p|(\alpha_i,b)=1 \Rightarrow p|1$ άτοπο διότι p: πρώτος κ' άρα $p\geq 2$

άρα $\boxed{(\alpha_1\cdots\alpha_n,b)=1}$

Άσκ 5 (i) $(\alpha,b)=1$ κ' $c|(\alpha+b) \Rightarrow (\alpha,c)=1=(b,c)$

(ii) Αν $(b,c)=1 \Rightarrow (\alpha,bc)=(\alpha,b)\cdot(\alpha,c)$.

Λύση: (i) Έστω $d=(\alpha,c)$. Τότε $d|c$ κ' $c|\alpha+b \Rightarrow d|\alpha+b$, $d|\alpha$ $\Rightarrow d|b$

$d|\alpha$, $d|b$ $\Rightarrow d|(\alpha,b)=1$, $d\in\mathbb{N}$ $\Rightarrow \boxed{d=1}$

Παρόμοια δείχνουμε ότι $(b,c)=1$

(ii) Θέτουμε $d=(\alpha,bc)$, $d_1=(\alpha,b)$, $d_2=(\alpha,c)$ | Θ.δ.ο. $\boxed{d=d_1\cdot d_2}$

Πρώτα θ.δ.ο. $(d_1,d_2)=1$

Έστω ότι $\delta=(d_1,d_2) \Rightarrow \begin{cases}\delta|d_1=(\alpha,b)\Rightarrow \delta|b \\ \text{κ'} \\ \delta|d_2=(\alpha,c)\Rightarrow \delta|c\end{cases} \Rightarrow$

$\Rightarrow \delta|(b,c)=1$, $\delta\in\mathbb{N}$ $\Rightarrow \boxed{\delta=1}$

$d_1=(\alpha,b) \Rightarrow \exists\, x_1,y_1\in\mathbb{Z} : d_1=\alpha x_1+by_1$
$d_2=(\alpha,c) \Rightarrow \exists\, x_2,y_2\in\mathbb{Z} : d_2=\alpha x_2+cy_2$ $\Rightarrow$

$\Rightarrow \boxed{d_1\cdot d_2=\alpha(\alpha x_1x_2+c\cdot y_1y_2+by_1x_2)+bcy_1y_2}$ (1)

Για να ισχύει ότι $d_1d_2=(\alpha,bc)$ πρέπει νδο $d_1d_2|\alpha$ κ' $d_1d_2|b\cdot c$

Επειδή $\left.\begin{matrix} d_1 | b \\ d_2 | c \end{matrix}\right\} \Rightarrow \boxed{d_1 d_2 | b \cdot c}$

Επειδή $d_1 | \alpha$
$d_2 | \alpha$

Έστω $\alpha = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ πρωτογενής ανάλυση του α.

Τότε $\left.\begin{matrix} d_1 = p_1^{b_1} \cdot \ldots \cdot p_k^{b_k} \text{ με } 0 \le b_i \le \alpha_i, \ \forall i = 1, \ldots, k \\ d_2 = p_1^{\gamma_1} \cdot \ldots \cdot p_k^{\gamma_k} \text{ με } 0 \le \gamma_i \le \alpha_i, \ \forall i = 1, \ldots, k. \end{matrix}\right\} \Rightarrow$

$\Rightarrow (d_1, d_2) = p_1^{\min(b_1, \gamma_1)} \cdot \ldots \cdot p_k^{\min\{b_k, \gamma_k\}} = 1$

Τότε $\min\{b_i, \gamma_i\} = 0$, $\forall i = 1, \ldots, k$.

Όμως $b_i + \gamma_i \le \alpha_i$ $\forall i = 1, \ldots, k$

(διότι $\min\{b_i, \gamma_i\} = 0$ οπότε $b_i + \gamma_i = b_i$ ή γ_i ανάλογα ποιο από τα 2 είναι 0 οπότε το άλλο θα είναι $\le \alpha_i$)

Άρα $\boxed{d_1 \cdot d_2 | \alpha \text{ κ' } d_1 \cdot d_2 | b \cdot c}$ ②

①, ②, $\Rightarrow d_1 \cdot d_2 = (\alpha, bc) = d$.

Άσκ. 17: Αν $\alpha, b > 1$ κ' $\alpha | b^2$, $b^2 | \alpha^3$, $\alpha^3 | b^4$, $b | \alpha^5$, ...
Τότε νδο $\alpha = b$.

Λύση: $\alpha > 1 \Rightarrow \alpha = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$: πρωτογενής ανάλυση του α.
$b > 1 \Rightarrow b = q_1^{b_1} \cdot \ldots \cdot q_\lambda^{b_\lambda}$: —//— b.

Τότε $\forall n \ge 1$: η πρωτογενής ανάλυση του $n \ge 1$:
$\alpha^n = p_1^{n \cdot \alpha_1} \cdot \ldots \cdot p_k^{n \cdot \alpha_k}$

Όμοια: $b^n = q_1^{n \cdot b_1} \cdot \ldots \cdot q_\lambda^{n \cdot b_\lambda}$

$\alpha | b^2 \Rightarrow \forall p_1, \ldots, p_k$: $p_i | b^2 = q_1^{2b_1} \cdot \ldots \cdot q_\lambda^{2b_\lambda} \Rightarrow p_i = q_j$, για κάποιο $j = 1, \ldots, \lambda$

Άρα $\{p_1, \ldots, p_k\} \subseteq \{q_1, \ldots, q_\lambda\}$ ①

$b^2 | \alpha^3 \Rightarrow \forall q_1, \ldots, q_\lambda$: $q_i | \alpha^3 = p_1^{3\alpha_1} \cdot \ldots \cdot p_k^{3\alpha_k} \Rightarrow q_i = p_j$ για κάποιο $j = 1, \ldots, k$.
άρα $\{q_1, \ldots, q_\lambda\} \subseteq \{p_1, \ldots, p_k\}$ ②

Από ①, ② $\Rightarrow \{p_1, \dots, p_k\} = \{q_1, \dots, q_\lambda\}$.

Επειδή οι p_i είναι ανά 2 διαφορετικοί μεταξύ τους $\Rightarrow$

$\Rightarrow k = \lambda$

Και χωρίς βλάβη της γενικότητας $\Rightarrow p_1 = q_1, \dots, p_k = q_k$.

Άρα $\alpha = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$

$b = p_1^{b_1} \cdots p_k^{b_k}$

Οπότε πλέον αρκεί νδο $\alpha_i = b_i$, $\forall i = 1, \dots, k$.

- $\alpha | b^2 \Rightarrow \forall i = 1, \dots, k : \alpha_i \leq 2b_i$
- $b^2 | \alpha^3 \Rightarrow \forall i = 1, \dots, k : 2b_i \leq 3\alpha_i$
- $\alpha^3 | b^4 \Rightarrow \forall i = 1, \dots, k : 3\alpha_i \leq 4b_i$
- $b^4 | \alpha^5 \Rightarrow \forall i = 1, \dots, k : 4b_i \leq 5\alpha_i$

Οπότε $\forall i = 1, \dots, k : \alpha_i \leq 2b_i \leq 3\alpha_i \leq 4b_i \leq 5\alpha_i$

δηλ) $\alpha_i \leq 2b_i \leq 3\alpha_i$ ①

$3\alpha_i \leq 4b_i \leq 5\alpha_i$ ②

Τότε ② − ① $\Rightarrow 2\alpha_i \leq 2b_i \leq 2\alpha_i \Rightarrow 2\alpha_i = 2b_i \Rightarrow$

$\Rightarrow \boxed{\alpha_i = b_i}$ $\forall i = 1, \dots, k$

Τότε όμως $\boxed{\alpha = b}$.

Ασκ. 15 : $(\alpha, b) = 1$. Τότε:

① $(\alpha+b, \alpha-b) = ;$ ② $(2\alpha+b, \alpha+2b) = ;$ ③ $(\alpha+b, \alpha-b, \alpha b) = ;$

Λύση: Έστω $d = (\alpha+b, \alpha-b)$. $\Rightarrow \begin{cases} d | \alpha+b \\ d | \alpha-b \end{cases} \Rightarrow \begin{cases} d | (\alpha+b)+(\alpha-b) = 2\alpha \\ d | (\alpha+b)-(\alpha-b) = 2b \end{cases}$

$\Rightarrow \begin{cases} d | 2\alpha \\ d | 2b \end{cases} \Rightarrow d | (2\alpha, 2b) \Rightarrow d | 2(\alpha, b) \Rightarrow d | 2 \cdot 1 = 2 \Rightarrow$

$\Rightarrow d = 1$ ή $d = 2$

Επειδή $(\alpha, b)=1 \Rightarrow$ οι α, b δεν είναι και οι 2 άρτιοι.

- α, b περιττοί: $\Rightarrow \begin{cases} \alpha+b \\ \alpha-b \end{cases}$ άρτιοι δηλ. $\begin{array}{l} 2 \mid \alpha+b \\ 2 \mid \alpha-b \end{array} \Rightarrow$

$$\Rightarrow 2 \mid (\alpha+b, \alpha-b)=1 \, ? \Rightarrow \boxed{d=2}.$$

- $\left.\begin{array}{l}\alpha: \text{άρτιος} \\ b: \text{περιττός}\end{array}\right\} \Rightarrow \begin{array}{l}\alpha+b \\ \alpha-b\end{array}$: περιττοί $\Rightarrow 2 \nmid \alpha+b, \alpha-b \Rightarrow$

$$\Rightarrow \boxed{d=(\alpha+b, \alpha-b)=1}$$

Όμοια αν α = περιττός κ' b = άρτιος $\Rightarrow \boxed{d=1}$.

(0, 2, 3 θα βρίσκονται λυμένες στη σελίδα κ' λύνονται όμοια.)

Ασκ 9: Έστω $\alpha, n, m \in \mathbb{N}$, n: περιττός. Τότε:

Νδο $(\alpha^n-1, \alpha^m+1)=1$ ή 2.

Λύση: Έστω $d=(\alpha^n-1, \alpha^m+1) \Rightarrow \begin{cases} d \mid \alpha^n-1 \\ d \mid \alpha^m+1 \end{cases} \Rightarrow$

$$\Rightarrow \begin{cases} \exists r \in \mathbb{Z}: \alpha^n-1=d \cdot r \\ \exists s \in \mathbb{Z}: \alpha^m+1=d \cdot s \end{cases} \Rightarrow \boxed{\begin{cases} \alpha^n=1+d \cdot r \\ \alpha^m=-1+d \cdot s \end{cases}}$$

$$(\alpha^n)^m=\alpha^{n \cdot m}=(1+d \cdot r)^m=\sum_{k=0}^{m}\binom{m}{k}(d \cdot r)^k=$$

$$=1+\sum_{k=1}^{m}\binom{m}{k}(d \cdot r)^k=1+d \cdot A$$

$$(\alpha^m)^n=\alpha^{m \cdot n}=(-1+d s)^n=[(-1)(1-d s)]^n= \Rightarrow$$

$$\overset{n \text{ περιττός}}{=}(-1) \cdot (1-d s)^n=-(1+B \cdot d)$$

$\Rightarrow 1 + d \cdot A = \cancel{dB} 1 - dB \Rightarrow 2 = d(-B-A) \Rightarrow$

$\Rightarrow d \mid 2 \Rightarrow \boxed{d=1}$ ή $\boxed{d=2}$

– Αν α : άρτιος $\Rightarrow \alpha^m, \alpha^n$: άρτιοι $\Rightarrow \alpha^n - 1, \alpha^m + 1$: περιττοί, δηλ. $2 \nmid \alpha^n - 1, \alpha^m + 1 \Rightarrow \boxed{d=1}$

– Αν α : περιττός $\Rightarrow \alpha^n, \alpha^m$: περιττοί $\Rightarrow \alpha^n - 1, \alpha^m + 1$: άρτιοι $\Rightarrow$

$\Rightarrow 2 \mid \alpha^n - 1, \alpha^m + 1 \Rightarrow \boxed{(\alpha^n - 1, \alpha^m + 1) = 2}$