9/11/2015

Πρόταση:

Έστω $a_1, a_2, \dots, a_k \in \mathbb{Z}$ όχι όλοι ίσοι με 0. Τότε:

1. $(a_1, a_2, \dots, a_k) = (|a_1|, |a_2|, \dots, |a_k|)$
2. $\lambda \neq 0 \Rightarrow (\lambda a_1, \lambda a_2, \dots, \lambda a_k) = |\lambda| (a_1, a_2, \dots, a_k)$
3. $y = a_1 x_1 + \dots + a_k x_k \not\Rightarrow (a_1, a_2, \dots, a_k) = (a_1, a_2, \dots, a_k, y)$
   $x_i \in \mathbb{Z}$, $1 \leq i \leq k$
4. $(a_1, a_2, \dots, a_k) = d \Rightarrow \left(\frac{a_1}{d}, \frac{a_2}{d}, \dots, \frac{a_k}{d}\right) = 1$

Απόδειξη:

1. Έχει αποδειχθεί

2. $d = (a_1, a_2, \dots a_k)$ δδο $|\lambda| d = (\lambda a_1, \dots \lambda a_k)$

Τότε θα έχουμε:

$d | a_1, \dots, d | a_k \Rightarrow |\lambda| d \,|\, |\lambda| a_i$, $i = 1, \dots, k$

Τότε $|\lambda| d \,|\, (|\lambda| a_1, \dots, |\lambda| a_k)$ $(*)$

$d = (a_1, a_2, \dots, a_k) \Rightarrow$

$\Rightarrow d = a_1 x_1 + \dots + a_k x_k$

όπου $x_i \in \mathbb{Z}$, $1 \leq i \leq k$

Τότε: $|\lambda| \cdot d = |\lambda| x_1 a_1 + \dots + |\lambda| x_k a_k$

Αν $\delta | a_1, \dots, a_k$

κ' $\delta = a_1 x_1 + \dots + a_k x_k$

$\Rightarrow \delta = (a_1, \dots, a_k)$ $\not\Rightarrow$

Αν $\lambda > 0$

$|\lambda| d = \lambda x_1 a_1 + \dots + \lambda x_k a_k$

Αν $\lambda < 0$

$|\lambda| d = \lambda(-x_1) a_1 + \dots + \lambda(-x_k) a_k$

$(**)$

Από $(*)$, $(**)$ $\Rightarrow |\lambda| d = (\lambda a_1, \dots, \lambda a_k)$

3. Θέτουμε $d=(a_1,\dots,a_k)$ και $\delta=(a_1,\dots,a_k,\gamma)$

Θδο: $\delta=d$

$d|a_1,\dots,d|a_k \overset{①}{\Rightarrow} d|a_1x_1,\dots,d|a_kx_k \Rightarrow$

$d|a_1x_1+\dots+a_kx_k \Rightarrow d|\gamma$ ②

Από ①, ② $\Rightarrow d|\delta$

Παρόμοια $\delta|a_1,\dots,\delta|a_k \Rightarrow \delta|(a_1,\dots,a_k)=d \Rightarrow \delta|d$

Επειδή $\delta|d$ κ' $d|\delta \Rightarrow d=\delta$

4. Έστω $d=(a_1,a_2,\dots,a_k)$ Τότε $d|a_1,\dots,d|a_k \Rightarrow$

$\Rightarrow \frac{a_1}{d},\dots,\frac{a_k}{d}\in\mathbb{Z}$ Τότε:

$$d=(a_1,a_2,\dots,a_k)=\left(d\frac{a_1}{d},d\frac{a_2}{d},\dots,d\frac{a_k}{d}\right)\overset{②}{=}$$

$$=d\left(\frac{a_1}{d},\frac{a_2}{d},\dots,\frac{a_k}{d}\right)\Rightarrow\left(\frac{a_1}{d},\dots,\frac{a_k}{d}\right)=1$$

Πρόταση

Έστω $a_1,a_2,a_3,\dots,a_n\in\mathbb{Z}$, όχι όλοι ίσοι με 0. Τότε για κάθε $k: 1\le k\le n-2$:

$$(a_1,a_2,\dots,a_n)=(a_1,a_2,\dots,a_k,(a_{k+1},a_{k+2},\dots,a_n))$$

Απόδειξη

Θέτουμε: $d=(a_1,\dots,a_n)$, $\delta=(a_{k+1},\dots,a_n)$

και $d'=(a_1,\dots,a_k,\delta)$, Θδο: $d=d'$

$d=(a_1,\dots,a_n)\Rightarrow d|a_1,\dots,d|a_k$

$d|a_{k+1},\dots,d|a_n \Rightarrow d|\delta$ $\Big\}\Rightarrow$

$\Rightarrow d|a_1,\dots,a_k,\delta \Rightarrow d|(a_1,\dots,a_k,\delta)=d'$

Άρα $d|d'$ ①

$d'=(a_1,\dots,a_k,(a_{k+1},\dots,a_n))\Rightarrow d'|a_1,\dots,d'|a_k$

$d'|(a_{k+1},\dots,a_n) \Rightarrow$

$$\left.\begin{array}{l} \\ d' | a_{k+1}, \dots, d' | a_n \end{array}\right\} \Rightarrow d' | a_1, \dots, a_k, a_{k+1}, \dots, a_n \Rightarrow$$

$\Rightarrow d' | d$ (2)

Από (1), (2) $\Rightarrow d = d'$

Παραδείγματα:

① $(7, -21, -35) = (7, 21, 35) = (7 \cdot 1, 3 \cdot 7, 5 \cdot 7) =$
$= 7(1, 3, 5) = 7 \cdot 1 = 7$

② $(20, 35, 60) = (5 \cdot 4, 5 \cdot 7, 5 \cdot 12) = 5(4, 7, 12) = 5 \cdot 1 = 5$

③ $(20, 35, 90) = (20, 35, 90 + 2 \cdot 35) = (20, 35) = (4 \cdot 5, 5 \cdot 7) =$
$= 5(4, 7) = 5 \cdot 1 = 5$

④ $(6, 10) = 2 \Rightarrow \left(\frac{6}{2}, \frac{10}{2}\right) = 1$ ($(3,5) = 1$ πράγματι ισχύει)

ΘΕΩΡΗΜΑ:

Έστω $a = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k}$, $a_i, \beta_i \geq 0$, $1 \leq i \leq k$

p_i : πρώτοι, $1 \leq i \leq k$

$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ $\quad i \neq j \Rightarrow p_i \neq p_j$

Τότε: $(a, b) = p_1^{\min\{a_1, \beta_1\}} p_2^{\min\{a_2, \beta_2\}} \cdots p_k^{\min\{a_k, \beta_k\}}$

Απόδειξη.

Θέτουμε $d = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}$, όπου $\gamma_i = \min\{a_i, \beta_i\}$
$1 \leq i \leq k$, δδο $(a, b) = d$

$\gamma_i = \min\{a_i, \beta_i\} \Rightarrow \gamma_i \leq a_i$, $\forall i = 1, \dots, k \Rightarrow \boxed{d | a}$ $\Rightarrow$
$\gamma_i \leq \beta_i$ $\quad d | b$

$\Rightarrow \boxed{d | (a, b)}$ (*)

$a = p_1^{a_1} \cdots p_k^{a_k}$ Τότε
$d | a \Leftrightarrow d = p_1^{\gamma_1} \cdots p_k^{\gamma_k}$, όπου $0 \leq \gamma_i \leq a_i$, $1 \leq i \leq k$

Έστω $\delta|a, \delta|b$, Τότε $\delta = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_k^{\lambda_k}$, όπου $0 \le \lambda_i \le a_i$
$0 \le \lambda_i \le \beta_i$, $1 \le i \le k$

Τότε: $\lambda_i \le \min\{a_i, \beta_i\} = \gamma_i$. Τότε: $\left.\begin{array}{l} \delta = p_1^{\lambda_1} \cdots p_k^{\lambda_k} \\ 0 \le \lambda_i \le \gamma_i \\ 1 \le i \le k \end{array}\right\} \Rightarrow \delta | d$

Άρα $(a,b) = d$

ΘΕΩΡΗΜΑ: Έστω $a_1, a_2, \dots, a_k$ θετικοί ακέραιοι και έστω: $\forall j = 1, \dots, k$: $a_j = p_1^{a_{j1}} p_2^{a_{j2}} \cdots p_k^{a_{jk}}$, $0 \le a_{ji}$, $\forall i = 1, \dots, k$ και οι $p_1, \dots, p_k$ είναι ανά δύο διαφορετικοί πρώτοι αριθμοί.

Τότε: $(a_1, a_2, \dots, a_k) = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$, όπου $\beta_i = \min\{a_{1i}, \dots, a_{ki}\}$, $\forall i = 1, \dots, k$

ΛΗΜΜΑ ΤΟΥ ΕΥΚΛΕΙΔΗ

Έστω $a, b, c \in \mathbb{N}$. Αν $(a,b) = 1$, και $a|bc$, τότε $a|c$

Απόδειξη

Επειδή $(a,b) = 1 \Rightarrow \exists\, x, y \in \mathbb{Z}: 1 = ax + by$

$a|bc \Rightarrow bc = az$, για κάποιο $z \in \mathbb{Z}$

$1 = ax + by \Rightarrow c = acx + bcy = acx + azy =$
$= a \cdot (cx + zy) \Rightarrow a|c$

Παράδειγμα:

$15 | 45 = 5 \cdot 9$ και $15 \nmid 5$ κ' $15 \nmid 9$

ΕΦΑΡΜΟΓΗ

Έστω $b|a$ και $(b,c) = 1$
$c|a$
Τότε $bc|a$

$10 | 20$
$5 | 20$
Τότε $10 \cdot 5 \nmid 20$

Μπορούμε να γράψουμε
$a = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, $b = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$,

$c = p_1^{\gamma_1} p_2^{\gamma_2}, \dots, p_k^{\gamma_k}$, όπου $a_i, \beta_i, \gamma_i \geq 0$, $1 \leq i \leq k$
$p_1, \dots, p_k$ ανά δύο διαφορετικοί πρώτοι

$1 = (b,c) = p_1^{\min\{\beta_1,\gamma_1\}} \dots p_k^{\min\{\beta_k,\gamma_k\}} \Rightarrow \{\beta_i, \gamma_i\} = 0$ (*)
$1 \leq i \leq k$

$b | a \Rightarrow \beta_i \leq a_i, \forall i = 1, \dots, k$
$c | a \Rightarrow \gamma_i \leq a_i, \forall i = 1, \dots, k$ $\Big\}$ (**)

~~[illegible]~~ $bc = p_1^{\beta_1} \dots p_k^{\beta_k} p_1^{\gamma_1} \dots p_k^{\gamma_k} = p_1^{\beta_1+\gamma_1} \dots p_k^{\beta_k+\gamma_k}$

Από τη σχέση (*) $\min\{\beta_i, \gamma_i\} = 0$ → αν $\min\{\beta_i, \gamma_i\} = \beta_i = 0$
$\Rightarrow \beta_i + \gamma_i = \gamma_i \leq a_i$ από τις σχέσεις (**)

↳ αν $\min\{\beta_i, \gamma_i\} = \gamma_i = 0 \Rightarrow$
$\Rightarrow \beta_i + \gamma_i = \beta_i \leq a_i$, από τις σχέσεις (**)

Άρα $\forall i = 1, \dots, k: \beta_i + \gamma_i \leq a_i \Rightarrow bc | a$

Παράδειγμα:
$(1998, 2004, 2016) = d$
Η πρωτογενής ανάλυση των:
$1998 = 2 \cdot 3^3 \cdot 37$
$2004 = 2^2 \cdot 3 \cdot 167$ $\longrightarrow d = 2 \cdot 3 = 6$
$2016 = 2^5 \cdot 3^2 \cdot 37$

Άσκηση: $(b,c) = 1 \Rightarrow (a, b \cdot c) = (a,b)(a,c)$
Θέτουμε $d = (a, b \cdot c)$ δδο $d = d_1 d_2$
$d_1 = (a,b)$
$d_2 = (a,c)$

Έστω $x=(d_1,d_2)$. Τότε

$$\Rightarrow \left\{ \begin{array}{l} x|d_1 \text{ κ' } d_1|b \Rightarrow x|b \\ \text{κ'} \\ x|d_2 \text{ κ' } d_2|c \Rightarrow x|c \end{array} \right\} \Rightarrow$$

Τότε: $x|(b,c)=1 \Rightarrow x=1$

Άρα: $(d_1,d_2)=1$ ⊛

Τότε $d_1=(a,b) \Rightarrow \exists x_1,y_1 \in \mathbb{Z}: d_1=ax_1+by_1$

$d_2=(a,c) \Rightarrow \exists x_2,y_2 \in \mathbb{Z}: d_2=ax_2+cy_2$

$$\Rightarrow d_1d_2=a^2x_1x_2+acx_1y_2+aby_1x_2+bcy_1y_2$$
$$=a(ax_1x_2+cx_1y_2+by_1x_2)+bcy_1y_2$$

$$\left.\begin{array}{l} \left.\begin{array}{l} d_1|b \\ d_2|c \end{array}\right\} \Rightarrow d_1d_2|bc \\ \left.\begin{array}{l} d_1|a \text{ και } (d_1,d_2)=1 \\ d_2|a \end{array}\right\} \xrightarrow{\text{ΕΦΑΡΜΟΓΗ}} d_1d_2|a \end{array}\right| \Longrightarrow$$

$\Rightarrow d_1d_2=d$