

4/11/2015

Έστω $a_1, a_2, \dots, a_n \in \mathbb{Z}$ και έστω ότι $a_i \neq 0$, για κάποιο $i=1, \dots, n$.
 Ο θετικός ακέραιος d कहैται ο πρότος κοινός διαιρέτης των $a_1, \dots, a_n$:
 $d = (a_1, a_2, \dots, a_n) \Leftrightarrow$ ① $d|a_1, \dots, d|a_n$ και ② $\delta|a_1, \dots, \delta|a_n \Rightarrow \delta \leq d$

ΘΕΩΡΗΜΑ: Έστω $a_1, a_2, \dots, a_n \in \mathbb{Z}$ και αλτ0, για κάποιο $i=1, \dots, n$. Αν $d = (a_1, \dots, a_n)$
 τότε: υπάρχουν $k_1, k_2, \dots, k_n \in \mathbb{Z}$: $d = k_1 a_1 + \dots + k_n a_n$

Απόδειξη: Οεμπνίτε το ανώτατο κοινό ακέραιο:

$$S = \{ x_1 a_1 + \dots + x_n a_n \in \mathbb{Z} \mid x_i \in \mathbb{Z}, 1 \leq i \leq n \}$$

Επειδή $a_n = 0 \cdot a_1 + \dots + 0 \cdot a_{n-1} + 1 \cdot a_n + 0 \cdot a_{n+1} + \dots + 0 \cdot a_n \in S$

Άρα το $S \neq \emptyset$ και πάντα περιέχει πρό-φθευμνός ακέραιος.

Αν $a_n > 0$, τότε το $a_n \in S$. Αν $a_n < 0$, τότε $-a_n > 0$ και $-a_n \in S$,

διότι: $-a_n = 0 \cdot a_1 + \dots + (-1) \cdot a_n + \dots + 0 \cdot a_n \in S$

Άρα το S περιέχει θετικούς ακέραιους $\Rightarrow S \cap \mathbb{N} \neq \emptyset$.

Από την Αρχή Καλής Αιτάσεως, έπεται ότι το $S \cap \mathbb{N}$ έχει ελάχιστο

στοχείο, έστω $d = \min(S \cap \mathbb{N})$. Θα δείξουμε ότι $d = (a_1, a_2, \dots, a_n)$.

Επειδή $d \in S \cap \mathbb{N}$, θα έχουμε: υπάρχουν $k_1, \dots, k_n \in \mathbb{Z}$:

$$d = k_1 a_1 + \dots + k_n a_n$$

Έστω $m \in S$, τότε υπάρχουν $\xi_1, \dots, \xi_n \in \mathbb{Z}$: $m = \xi_1 a_1 + \dots + \xi_n a_n$. Από την Ευκλείδεια

Διαίρεση του m με το d , μπορούμε να γράψουμε: $m = dq + r$, όπου $0 \leq r < d$

$$\begin{aligned} \text{Τότε } r &= m - dq = \xi_1 a_1 + \dots + \xi_n a_n - (k_1 a_1 + \dots + k_n a_n)q \\ &= (\xi_1 - qk_1) a_1 + \dots + (\xi_n - qk_n) a_n \in S \end{aligned}$$

Αν $r > 0$, τότε επειδή $r \in S$, θα έχουμε ότι $r \in S \cap \mathbb{N}$. Όμως $r < d = \min(S \cap \mathbb{N})$

Αυτό είναι άτοπο, και άρα $r = 0$. Τότε: $m = dq$

Έτσι δείχνουμε ότι $m \in S$, τότε $\exists q \in \mathbb{Z}$: $m = dq$

Αρα $S = \{d, q \in \mathbb{Z} \mid q \in \mathbb{Z}\}$

Έστω $q \in \mathbb{Z}$ και τότε: $dq = (k_1 a_1 + \dots + k_n a_n)q = (qk_1)a_1 + \dots + (qk_n)a_n \in S$

Επομένως δείξαμε ότι $S = \{dq \in \mathbb{Z} \mid q \in \mathbb{Z}\}$
 Επειδή $a_i \in S \Rightarrow a_i = dq_i$, για κάποιο $q_i \in \mathbb{Z}$
 $1 \leq i \leq n$ $1 \leq i \leq n$

Αρα $d \mid a_i, \forall i = 1, \dots, n$ ①

Έστω $d \mid a_1, \dots, a_n \Rightarrow d \mid k_1 a_1, \dots, k_n a_n \Rightarrow d \mid k_1 a_1 + \dots + k_n a_n = d$

Αρα $d \mid d \Rightarrow d \leq d$ ②

Από ①, ② $\Rightarrow d = (a_1, a_2, \dots, a_n)$

ΠΡΟΤΙΣΜΑ: Έστω $a_1, a_2, \dots, a_n \in \mathbb{Z}$ και $a_k \neq 0$, για κάποιο $k = 1, \dots, n$. Τότε:

$d = (a_1, a_2, \dots, a_n) \Leftrightarrow$ ① $d \mid a_1, \dots, d \mid a_n$

② $d \mid a_1, \dots, d \mid a_n \Rightarrow d \mid d$

Απόδειξη: Προκύπτει από την Απόδειξη του ΘΕΩΡΗΜΑΤΟΣ

ΠΡΟΤΙΣΜΑ: Έστω $a_1, \dots, a_n \in \mathbb{Z}$, $a_k \neq 0$ για κάποιο $k = 1, \dots, n$. Τότε αν $d \in \mathbb{N}$, θα έχουμε

Αν $d \mid a_1, \dots, d \mid a_n$, και $d = k_1 a_1 + \dots + k_n a_n$ για κάποια $k_1, k_2, \dots, k_n \in \mathbb{Z}$,
 τότε: $d = (a_1, a_2, \dots, a_n)$

Απόδειξη Έστω $d \mid a_1, \dots, d \mid a_n \Rightarrow d \mid k_1 a_1, \dots, d \mid k_n a_n \Rightarrow d \mid k_1 a_1 + \dots + k_n a_n = d$

Αρα από το προηγούμενο Πρόσφα $\Rightarrow d = (a_1, a_2, \dots, a_n)$

ΠΑΡΑΤΗΡΗΣΗ: ① $d = (a_1, a_2, \dots, a_n) \Rightarrow d = k_1 a_1 + \dots + k_n a_n$, για κάποια $k_i \in \mathbb{Z}, 1 \leq i \leq n$

② $d = k_1 a_1 + \dots + k_n a_n$, για κάποια $k_i \in \mathbb{Z}, 1 \leq i \leq n$
 $d \mid a_1, \dots, d \mid a_n$

③ $d = (a_1, \dots, a_n) \Leftrightarrow$ ① $d \mid a_1, \dots, d \mid a_n$

② $d \mid a_1, \dots, d \mid a_n \Rightarrow d \mid d$

$d \mid a_1, \dots, d \mid a_n \Rightarrow$
 $d \mid (a_1, a_2, \dots, a_n)$

Ορισμοί: ① Οι αριθμοί $a_1, \dots, a_n$ कहलवतल प्रलतल परलतल $\Leftrightarrow (a_1, a_2, \dots, a_n) = 1$

② Οι αριθμοί $a_1, \dots, a_n$ कहलवतल प्रलतल परलतल सरलल $\Leftrightarrow (a_i, a_j) = 1, \text{ αν } 1 \leq i \neq j \leq n$

Αν οι $a_1, \dots, a_n$ εलναι प्रलतल परलतल सरलल, तलतल εलναι कल प्रलतल परलतल तलस, डलतल αν $(a_i, a_j) = 1$, तलन $i \neq j$ कल $d = (a_1, \dots, a_n)$, तलतल: $d | a_i \Rightarrow d | a_j$

$\Rightarrow d | (a_i, a_j) = 1 \Rightarrow d = 1 \Rightarrow$ οι $a_1, \dots, a_n$ εलναι प्रलतल परलतल सरलल

ΠΑΡΑΔΕΙΓΜΑ: $d = (6, 14, 21) = 1 \Rightarrow$ οι 6, 14, 21 εलναι प्रलतल परलतल सरलल
 $(6, 14) = 2, (6, 21) = 3, (14, 21) = 7$, οι 6, 14, 21 डलन εलναι प्रलतल परलतल सरलल

ΠΟΡΙΣΜΑ: Εστω $a_1, \dots, a_n \in \mathbb{Z}$ कल $a_k \neq 0$ गल कलतल $k = 1, \dots, n$. तलतल:
 Οι $a_1, \dots, a_n$ εलναι प्रलतल परलतल सरलल εल $1 = k_1 a_1 + \dots + k_n a_n$,
 गल कलतल $k_i \in \mathbb{Z}, 1 \leq i \leq n$
 Δलतलतल: $(a_1, a_2, \dots, a_n) = 1$

Απόδειξη: $\Rightarrow$ Αποδεικνलतल στο Θεώρημα.

$\Leftarrow$ $1 = k_1 a_1 + \dots + k_n a_n \mid \text{ΠΟΡΙΣΜΑ } 1 = (a_1, \dots, a_n) \mid a_1, \dots, a_n$

ΠΑΡΑΔΕΙΓΜΑ: $(2011, 9014) = ;$

$$\forall a \in \mathbb{Z} \quad 9(2011) + (-8)(9014) = 18099 - 72112 = -54013 \neq 1$$

$$\Rightarrow (2011, 9014) = 1$$

ΑΣΚΗΣΗ: Να υπολογलतल ο ελτλτοσ κολνός Δलतलतल $d = (2^k + 3^k, 2^{k+1} + 3^{k+1})$
 $k \in \mathbb{Z}$ (ΘΕΜΑ ΣΕΠΤΕΜΒΡΙΟΥ)

Exaφc $d | 2^k + 3^k \mid \Rightarrow d | 2^{k+1} + 3^{k+1} - 2^k - 3^k$

$\Rightarrow d | 2^{k+1} - 2^k + 3^{k+1} - 3^k \Rightarrow d | 2^k + 2 \cdot 3^k \mid \Rightarrow d | 2^k + 2 \cdot 3^k - 2^k - 3^k \Rightarrow d | 3^k$

$\begin{matrix} d | 3^k \textcircled{1} \\ d | 2^k + 3^k \end{matrix} \Rightarrow d | 2^k \textcircled{2}$

Αρα $d | 2^k \mid \Rightarrow d: \text{ίσος} : \text{Ατομο}, \text{Αρα } d=1. \text{Ενδεχως}$
 $d | 3^k \mid \Rightarrow d: \text{πρώτος}$
 $(2^k + 3^k, 2^{k+1} + 3^{k+1}) = 1$

ΠΡΟΤΑΣΗ: Έστω $a_1, a_2, \dots, a_n \in \mathbb{Z}, a_i \neq 0$, για κάποιο $k=1, \dots, n$

① $(a_1, \dots, a_n) = (|a_1|, \dots, |a_n|)$

② Αν $y = a_1 x_1 + \dots + a_n x_n$, τότε: $(a_1, \dots, a_n) = (a_1, \dots, a_n, y)$
 όπου $x_1, \dots, x_n \in \mathbb{Z}$

Απόδειξη: Έστω $d = (a_1, \dots, a_n)$ Τότε $d | a_1, \dots, a_n \Rightarrow d | |a_1|, \dots, |a_n| \Rightarrow$
 $\Rightarrow d | (|a_1|, \dots, |a_n|) \Rightarrow d | \delta \textcircled{1}$

$\Rightarrow d | (|a_1|, \dots, |a_n|)$ Ανάλογα: $\delta | |a_1|, \dots, |a_n| \Rightarrow \delta | a_1, \dots, a_n \Rightarrow$
 $\delta | (a_1, \dots, a_n) \Rightarrow \delta | d \textcircled{2}$
 Από τα $\textcircled{1}, \textcircled{2} \Rightarrow \delta = d$