

2/11/2015

(Συνέχεια απόδειξης Θ.Θ.Α)

①, ②, ③: Από το προηγούμενο βήμα.

- ① Κάθε θετικός ακέραιος $a > 1$ μπορεί να γραφεί ως γινόμενο πρώτων αριθμών.
- ② Αν p : πρώτος και $p | a_1 \dots a_n$, τότε $\exists i = 1, \dots, n: p | a_i$
- ③ Αν $p_1, p_2, \dots, p_n$: πρώτοι αριθμοί και $p | p_1 \dots p_n$, τότε $\exists i = 1, \dots, n: p = p_i$

ΘΕΜΕΛΙΩΔΕΣ ΘΕΩΡΗΜΑ ΑΡΙΘΜΗΤΙΚΗΣ: Κάθε θετικός ακέραιος $a > 1$ μπορεί να γραφεί μοναδικά ως γινόμενο πρώτων αριθμών, δηλαδή.

αν $a = p_1 p_2 \dots p_m = q_1 q_2 \dots q_n$, όπου p_i, q_j : πρώτοι, όπου
 $1 \leq i \leq m$ τότε: $n = m$ και κάθε p_i είναι ίσο με κάποιο q_j , $\forall i = 1, \dots, m$.
 $1 \leq j \leq n$

Απόδειξη: Υποθέτουμε ότι:

$$a = p_1 \cdot p_2 \dots p_m, \text{ όπου } p_i, q_j \text{ είναι πρώτοι αριθμοί } \begin{matrix} 1 \leq i \leq m \\ 1 \leq j \leq n \end{matrix}$$
$$= q_1 \cdot q_2 \dots q_n$$

Αν $a = 2$, τότε προφανώς $n = m = 1$ και $q_1 = p_1 = 2$.

Επαγωγικό Υπόθεση: Υποθέτουμε ότι το αλγόριθμο ισχύει για κάθε θετικό ακέραιο b : $2 \leq b < a$

Μπορούμε να υποθέσουμε ότι: $p_1 \leq p_2 \leq \dots \leq p_m$ και $q_1 \leq q_2 \leq \dots \leq q_n$
Τότε $p_1 | a = q_1 q_2 \dots q_n \xrightarrow{③} \exists r = 1, \dots, n: p_1 = q_r$. Παρόμοια $q_1 | a = p_1 p_2 \dots p_n \xrightarrow{③} \exists s = 1, \dots, m: q_1 = p_s$

$$p_1 \leq p_s = q_1 \leq q_r = p_1 \Rightarrow p_1 = q_1 = p_s = q_r. \text{ Άρα } p_1 = q_1$$

Τότε επειδή $p_1, q_1 | a \Rightarrow \frac{a}{p_1} = \frac{a}{q_1} \in \mathbb{N}$ και $\frac{a}{p_1} < a$.

Από την επαγωγική υπόθεση, για τον δευτερεύοντα ακέραιο

$$\frac{a}{p_1} = \frac{a}{q_1} = p_2 \cdots p_m, \text{ θα έχουμε: } m-1 = n-1 \text{ και } p_2 = q_2, \dots, p_m = q_m = q_n$$

$$\text{Τότε } n=m \text{ και } p_1 = q_1, p_2 = q_2, \dots, p_m = q_m.$$

Άρα ισχύει η μοναδικότητα στο πρώτο.

□

Έστω $a > 1$ και $a = p_1 p_2 \cdots p_m$, όπου $p_1, \dots, p_m$ πρώτοι τότε:
κάποιοι από τους p_i πρέπει να είναι ίσοι μεταξύ τους

$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$, όπου $p_1, \dots, p_n$ είναι ανα δύο
διαφορετικοί πρώτοι αριθμοί (δηλαδή αν $i \neq j, 1 \leq i, j \leq n$, τότε
 $p_i \neq p_j$) και $a_i \geq 1$. Η γραφή αυτή του $a > 1$ καλείται:
ΠΡΩΤΟΓΕΝΗΣ ΑΝΑΛΥΣΗ του a .

ΒΑΣΙΚΟ ΠΡΟΒΛΗΜΑ: Δοθέντος δευτερεύοντα ακέραιου $a > 1$, να βρεθεί η
πρωτογενής του ανάλυση.

Παράδειγμα: $a = 2015$. Επειδή $\sqrt{2015} \sim 44.8$. Τότε οι πρώτοι
αριθμοί < 44 είναι: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43.
Οι πρώτοι διαιρέτες του 2015 είναι 5, 13, 31 και τότε $2015 = 5 \cdot 13 \cdot 31$

Παράδειγμα: $720 = 2^4 \cdot 3^2 \cdot 5$

Έστω $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$: πρωτογενής ανάλυση του $a > 1$
 $b = q_1^{b_1} q_2^{b_2} \cdots q_m^{b_m}$: $\neq$ $\neq$ $b > 1$

Τότε υποθέτουμε ότι $p_1 = q_1, \dots, q_k = q_k$, όπου $k \leq n, k \leq m$
 $a = p_1^{a_1} \cdots p_k^{a_k} p_{k+1}^{a_{k+1}} \cdots p_n^{a_n} = p_1^{a_1} \cdots p_k^{a_k} p_{k+1}^{a_{k+1}} \cdots p_n^{a_n} \cdot q_{k+1}^{b_{k+1}} \cdots q_m^{b_m}$, όπου $b_{k+1} = \dots = b_m = 0$
 $b = p_1^{b_1} \cdots p_k^{b_k} q_{k+1}^{b_{k+1}} \cdots q_m^{b_m} = p_1^{b_1} \cdots p_k^{b_k} q_{k+1}^{b_{k+1}} \cdots q_m^{b_m} p_{k+1}^{a_{k+1}} \cdots p_n^{a_n}$, όπου $a_{k+1} = \dots = a_n = 0$

ΘΕΩΡΗΜΑ: Έστω $a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$ η πρωτεύουσα ανάλυση του $a > 1$.

Τότε:
 $\forall d \in \mathbb{N} : d | a \Leftrightarrow d = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$, όπου $0 \leq b_i \leq a_i, i = 1, \dots, n$

Απόδειξη

$\Leftarrow$ Έστω $d = p_1^{b_1} \dots p_n^{b_n}$, όπου $0 \leq b_i \leq a_i, i = 1, \dots, n$

Τότε:

$$a = p_1^{a_1} \dots p_n^{a_n} = p_1^{a_1 - b_1 + b_1} \dots p_n^{a_n - b_n + b_n} = p_1^{a_1 - b_1} p_1^{b_1} \dots p_n^{a_n - b_n} p_n^{b_n} =$$

$$= p_1^{a_1 - b_1} \dots p_n^{a_n - b_n} p_1^{b_1} \dots p_n^{b_n}$$

$\Rightarrow a = b \cdot d \Rightarrow d | a$

$\Rightarrow$ Έστω $d | a$. Αν $d = 1$, τότε $d = 1 = p_1^{b_1} \dots p_n^{b_n}$, όπου $b_1 = \dots = b_n = 0$.

Έστω ότι $d > 1$.

Αν p πρώτος διαιρέσει τα d , σημαίνει p πρώτος κ' $p | a$.

Τότε γενικά $d | a$, θα έχουμε:

$p | a = p_1^{a_1} \dots p_n^{a_n} \Rightarrow \exists i = 1, \dots, n : p = p_i$. Άρα κάθε πρώτος διαιρέων τα d είναι και πρώτος διαιρέων τα a , δηλαδή είναι κειμένος από τους $p_1, \dots, p_n$. Άρα η πρωτεύουσα ανάλυση των d θα είναι της μορφής: $d = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$, όπου $b_i \geq 0, i = 1, 2, \dots, n$

Μένει να δείξουμε ότι: $b_i \leq a_i, i = 1, \dots, n$

$d | a \Rightarrow a = d \cdot d'$ και τότε όπως πριν θα έχουμε: $d' = p_1^{c_1} p_2^{c_2} \dots p_n^{c_n}$, όπου $0 \leq c_i, i = 1, \dots, n$

Τότε: $a = p_1^{a_1} \dots p_n^{a_n} = p_1^{b_1} \dots p_n^{b_n} p_1^{c_1} \dots p_n^{c_n} = p_1^{b_1 + c_1} \dots p_n^{b_n + c_n}$

Από το θεμελιώδες θεώρημα της αριθμικής θα έχουμε

$a_i = b_i + c_i, 1 \leq i \leq n \Rightarrow \begin{cases} b_i \leq a_i \\ c_i \leq a_i \end{cases}$



Παράδειγμα: $a = 720 = 2^4 \cdot 3^2 \cdot 5$

$d | 720 \Leftrightarrow d = 2^{b_1} \cdot 3^{b_2} \cdot 5^{b_3}$, όπου $0 \leq b_1 \leq 4 \rightarrow 5$
 $0 \leq b_2 \leq 2 \rightarrow 3$
 $0 \leq b_3 \leq 1 \rightarrow 2$

Ετσι προκύπτουν $5 \cdot 3 \cdot 2 = 30$

διαίρεται του 720

π.χ. $2^3 \cdot 3^2$

Παράδειγμα: $a = 2015 = 5 \cdot 13 \cdot 31$

$1, 5, 13, 31, 5 \cdot 13, 5 \cdot 31, 13 \cdot 31, 5 \cdot 13 \cdot 31$

ΜΕΓΙΣΤΟΣ ΚΟΙΝΟΣ ΔΙΑΙΡΕΤΗΣ

Έστω $a_1, a_2, \dots, a_n \in \mathbb{Z}$. Αν $a_1 = a_2 = \dots = a_n = 0$, τότε κάθε ακέραιος είναι κοινός διαιρέτης των $a_1 = \dots = a_n = 0$ και τότε κατά ούτως ορίζουμε ότι ο μέγιστος κοινός διαιρέτης των $a_1 = \dots = a_n = 0$ να είναι το 0. Αν τύχει και στο εξής υποθέτουμε ότι $a_k \neq 0$, για κάποιο $k = 1, \dots, n$.

Έστω $S = \{m \in \mathbb{N} \mid m | a_i, i = 1, \dots, n\} \subseteq \mathbb{N}$. Τότε $S \neq \emptyset$ διότι $1 \in S$ και το S είναι πεπερασμένο διότι $\forall m \in S: m \leq |a_k|$. Ο μεγαλύτερος κοινός διαιρέτης των $a_i, i = 1, \dots, n$ δηλαδή το μέγιστο στοιχείο του S καλείται ο Μέγιστος Κοινός Διαιρέτης των $a_i, i = 1, \dots, n$, $(a_1, a_2, \dots, a_n)$.

$d = (a_1, a_2, \dots, a_n) \Leftrightarrow$ ① $d | a_1, \dots, d | a_n$
 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 έστω ότι $a_k \neq 0$, για κάποιο $k = 1, \dots, n$.

Αν $d = (a_1, a_2, \dots, a_n) \Rightarrow \exists k_1, \dots, k_n \in \mathbb{Z} : d = k_1 a_1 + \dots + k_n a_n$

Απόδειξη (στο άλλο φύλλο)