26-10-16

Previously on Beligiannis

- **Θεμελιώδες Θεώρημα Αριθμητικής (Ύπαρξη)**

Κάθε θετικός ακέραιος $\alpha > 1$ μπορεί να γραφεί ως γινόμενο πεπερασμένου πλήθους πρώτων αριθμών

- **Λήμμα του Ευκλείδη**: Αν $\alpha, b \in \mathbb{Z}$ και p: πρώτος τότε: $p \mid ab \Rightarrow p \mid a$ ή $p \mid b$

- **Πόρισμα**: Αν p: πρώτος και $a_1, a_2, \dots, a_n \in \mathbb{Z}$, τότε:

$p \mid a_1 a_2 \dots a_n \Rightarrow \exists i = 1, \dots, n : p \mid a_i$ (*)

Απόδειξη: • Αν $n=1$, η (*) ισχύει τετριμμένα

• Αν $n=2$, τότε η (*) προκύπτει απ' το Λήμμα του Ευκλείδη

Επαγωγική Υπόθεση: Η σχέση (*) είναι αληθής για $k (= n-1)$ πλήθος ακεραίων όπου $k \geq 1$

Για n το πλήθος ακέραιους, θα έχουμε:

$p \mid a_1 a_2 \dots a_n \Rightarrow p \mid (a_1 a_2 \dots a_{n-1}) a_n \xrightarrow[\text{Ευκλείδη}]{\text{Λήμμα του}}$

$\Rightarrow p \mid a_1 a_2 \dots a_{n-1}$ ή $p \mid a_n \xrightarrow[\text{Υπόθεση}]{\text{Επαγωγική}}$

$\exists\, i=1,\dots,n-1$ ή $p \mid a_n$ $\Rightarrow p \mid a_i$

Άρα, $\exists\, i=1,2,\dots,n \Rightarrow p \mid a_i$

Οπότε, η (*) ισχύει $\forall\, n \in \mathbb{N}$

- <u>Πόρισμα</u>: Αν $p_1, p_2, \dots, p_n$ είναι πρώτοι, τότε αν $p \mid p_1 p_2 \dots p_n \Rightarrow \exists\, i=1,\dots,n \Rightarrow p = p_i$

- <u>Θεμελιώδες Θεώρημα Αριθμητικής (Μοναδικότητα)</u>

Έστω $a>1$ και υποθέτουμε ότι:

$a = p_1 p_2 \dots p_m$, $p_1, \dots, p_m$: πρώτοι
$= q_1 q_2 \dots q_n$, $q_1, \dots, q_m$: πρώτοι
} Τότε:

Διατάσσοντας τους p_i, q_j κατά σειρά μεγέθους θα έχουμε $m=n$ και $p_i = q_i$, $\forall\, i=1,\dots,n$ (*)

<u>Απόδειξη</u>: • Αν $a=2$, πρώτος, τότε: η (*) αληθής διότι $n=m=1$ και $p_1 = q_1 = 2$

<u>Επαγωγική Υπόθεση</u>: Η σχέση (*) είναι αληθής $\forall\, b \in \mathbb{N}$, όπου $2 \le b < a$

<u>Γενική Περίπτωση</u>: i) Αν a: πρώτος, τότε η (*) ισχύει

ii) Υποθέτουμε ότι ο α είναι σύνθετος. Ισοδύναμα τότε $n, m > 1$

Έστω ότι $\alpha = p_1 p_2 \dots p_m$, p_i : πρώτοι , $1 \le i \le m$

$= q_1 q_2 \dots q_n$, q_j : πρώτοι , $1 \le j \le n$

$p_1 \le p_2 \le \dots \le p_m$ Θδο: $n = m$ και $p_i = q_i$, $\forall i = 1, \dots, n = m$

$q_1 \le q_2 \le \dots \le q_n$

- $p_1 | \alpha \Rightarrow p_1 | q_1 q_2 \dots q_n \xrightarrow{\text{Πόρισμα}} \Rightarrow \exists\, r = 1, \dots, n : p_1 = q_r$

- $q_1 | \alpha \Rightarrow q_1 | p_1 p_2 \dots p_m \xrightarrow{\text{Πόρισμα}} \Rightarrow \exists\, s = 1, \dots, m : q_1 = p_s$

$\Rightarrow$

$p_1 \le p_s = q_1 \le q_r = p_1 \Rightarrow \boxed{p_1 = q_1}$ (1)

Τότε , $\dfrac{\alpha}{p_1} = p_2 p_3 \dots p_m$

$\dfrac{\alpha}{q_1} = q_2 q_3 \dots q_n$

$\Rightarrow \dfrac{\alpha}{p_1} = \dfrac{\alpha}{q_1} < \alpha$

Από την Επαγωγική Υπόθεση, έπεται ότι:

$m-1 = n-1 \Rightarrow m = n$ (2) και $p_2 = q_2, \dots, p_m = q_n$ (3)

Συνδυάζοντας τις (1), (2), (3) προκύπτει η (*)

• Θεμελιώδες Θεώρημα Αριθμητικής

Κάθε $\alpha > 1$ θετικός ακέραιος μπορεί να γραφεί ως εξής:

$\alpha = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, $p_1, \dots, p_k$: πρώτοι όπου $i \neq j$ και $a_i \geq 1$, $i = 1, \dots, k$. Η γραφή αυτή είναι μοναδική!

Αν $\alpha = q_1^{b_1} q_2^{b_2} \dots q_\lambda^{b_\lambda}$, $q_1, \dots, q_\lambda$: πρώτοι,

$i \neq j \Rightarrow q_i \neq q_j$, $\beta_i \geq 1$, $1 \leq i \leq \lambda$

Τότε, $k = \lambda$, $p_i = q_i$, $i = 1, \dots, k$ και $a_i = \beta_i$

(*) Η παραπάνω γραφή ($\alpha = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$) ονομάζεται πρωτογενής ανάλυση του α.

• Παράδειγμα: $2013 = 3 \cdot 11 \cdot 61$

$2014 = 2 \cdot 19 \cdot 53$

$2015 = 5 \cdot 13 \cdot 31$

$3960 = 2^3 \cdot 3^2 \cdot 5 \cdot 11$

Έστω $a, b > 1$ και $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$ και $b = q_1^{\beta_1} q_2^{\beta_2} \dots q_m^{\beta_m}$. Τότε, θέτοντας $\kappa = \max\{n, m\}$ θα έχουμε:

$$a = p_1^{\alpha_1} \dots p_n^{\alpha_n} p_{n+1}^{\alpha_{n+1}} \dots p_\kappa^{\alpha_\kappa}, \quad p_{n+1} = q_1, \dots, p_\kappa = q_m$$

$$\alpha_{n+1} = \dots = \alpha_\kappa = 0$$

$$b = p_1^{\beta_1} \dots p_n^{\beta_n} p_{n+1}^{\beta_{n+1}} \dots p_\kappa^{\beta_\kappa}, \quad \beta_1 = \dots = \beta_n = 0$$

⊛ <u>Παρατήρηση</u>: Οι παραπάνω χρήσεις των a, b δεν αποτελούν πρωτοχρονιάτικες αναλύσεις.

• <u>Θεώρημα</u>: Έστω $a > 1$ και $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$ η πρωτογενής ανάλυση του a.

Τότε, $d \mid a \iff d = p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n}$, $0 \le \beta_i \le \alpha_i$, $i = 1, \dots, n$

<u>Απόδειξη</u>: ($\Leftarrow$) Έστω ότι $d = p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n}$, $0 \le \beta_i \le \alpha_i$ $i = 1, \dots, n$

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n} = p_1^{\alpha_1 - \beta_1 + \beta_1} p_2^{\alpha_2 - \beta_2 + \beta_2} \dots p_n^{\alpha_n - \beta_n + \beta_n} =$$

$$= p_1^{\alpha_1 - \beta_1} p_1^{\beta_1} p_2^{\alpha_2 - \beta_2} p_2^{\beta_2} \dots p_n^{\alpha_n - \beta_n} p_n^{\beta_n} =$$

$$= p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n} \dots p_1^{\alpha_1 - \beta_1} p_2^{\alpha_2 - \beta_2} \dots p_n^{\alpha_n - \beta_n}$$

$\underbrace{\qquad d \qquad}$ $\underbrace{\qquad\qquad a' \qquad\qquad}$

$= d\alpha' \Rightarrow d|\alpha$

($\Rightarrow$) Έστω $d|\alpha$

- Αν $\underline{d=1}$, τότε $d = p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n}$, $\beta_1 = \dots = \beta_n = 0$
- Έστω ότι $\underline{d>1}$. Έστω $p|d$, όπου p: πρώτος

Επειδή $\left.\begin{matrix} d|\alpha \\ p|d \end{matrix}\right\} \Rightarrow$ $p|\alpha = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$ Πόρισμα $\Rightarrow$

$\exists\, i = 1, \dots, n \Rightarrow p = p_i$

Άρα, κάθε πρώτος διαιρέτης του d είναι και πρώτος διαιρέτης του α.

Τότε μπορούμε να γράψουμε τον d ως εξής

$d = p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n}$, όπου $\beta_i \geq 0$

Μένει να δω $\beta_i \leq \alpha_i$ (Άσκηση)

Παράδειγμα: Διαιρέτες του 2015

$2015 = 5^{\alpha_1} \cdot 13^{\alpha_2} \cdot 31^{\alpha_3}$

Οι διαιρέτες είναι $d = 5^{\beta_1} \cdot 13^{\beta_2} \cdot 31^{\beta_3}$, $0 \le \beta_i \le \alpha_i = 1$

Το d είναι κάποιος απ' τους εξής:

$d_1 = 5, 13, 31, 1, 5 \cdot 13, 5 \cdot 31, 13 \cdot 31, 5 \cdot 13 \cdot 31 = 2015$

Άσκηση: Να δειχθεί ότι υπάρχουν άπειροι πρώτοι της μορφής $6k+5$

Θεώρημα Dirichlet: Αν $a, b \in \mathbb{N}$, $\text{ΜΚΔ}(a,b) = 1$ τότε υπάρχουν άπειροι πρώτοι αριθμοί της μορφής $ak+b$, $k \in \mathbb{N}$

Λύση: Υπάρχει πεπερασμένο πλήθος πρώτων της μορφής $6k+5$ και έστω ότι αυτοί είναι:

$p_1, p_2, \dots, p_n$. Θεωρούμε $A = 6 \cdot p_1 p_2 \dots p_{n-1}$

Ο $A > 1$, είναι της μορφής:

$A = 6 p_1 p_2 \dots p_n - 6 + 5 = 6(p_1 p_2 \dots p_{n-1}) + 5$

Αν p: πρώτος διαιρέτης του A, τότε: ο p έχει μια από τις παρακάτω μορφές:

$6k, 6k+1, 6k+2, 6k+3, 6k+4, 6k+5$

Επειδή p: πρώτος $\Rightarrow p = 6k+1$ ή $p = 6k+5$

Αν όλοι οι πρώτοι διαιρέτες του A είναι της μορφής $6k+1$, τότε, επειδή

α) Ο A είναι το γινόμενο των πρώτων διαιρετών του

β) Το γινόμενο αριθμών της μορφής $6k+1$, είναι της μορφής $6k+1$

Προκύπτει ότι ο A θα είναι της μορφής $6k+1$

Άτοπο, καθώς υποθέσαμε ότι ο A είναι της μορφής $6k+5$

Άρα, υπάρχει τουλάχιστον ένας πρώτος διαιρέτης p του A που θα είναι της μορφής $6k+5$

Οπότε, $p = p_k$, $k = 1, \dots, n$

Τότε $\left.\begin{matrix} p = p_k \mid 6p_1 \dots p_n \\ p \mid A \end{matrix}\right\} \Rightarrow p \mid 1$: Άτοπο

Συνεπώς, υπάρχει άπειρο πλήθος πρώτων της μορφής $6k+5$.