Θεμέλια των Μαθηματικών

Ελένη Τζανάκη & Θεόδουλος Γαρεφαλάκης

Εαρινο εξάμηνο 2019-20

Κανονική Ανάλυση σε πρώτους

Κάθε φυσικός $n > 1$ μπορεί να γραφεί με μοναδικό τρόπο ως γινόμενο $n = p_1^{a_1} \cdots p_s^{a_s}$, όπου p_i είναι διακεκριμένοι πρώτοι και $a_i \geq 1$ για $1 \leq i \leq s$.

Παρατηρήσεις:

- Η πρόταση σημαίνει: εάν $n = p_1^{a_1} \cdots p_s^{a_s} = q_1^{b_1} \cdots b_t^{b_t}$ με
  - $p_i,\ 1 \leq i \leq s$ διακεκριμένους πρώτους και $q_j,\ 1 \leq j \leq t$ διακεκριμένους πρώτους,
  - $a_i \geq 1,\ 1 \leq i \leq s$ και $b_j \geq 1,\ 1 \leq j \leq t$,

  τότε

  - $s = t$ και
  - $p_i = q_{\sigma(i)}, a_i = b_{\sigma(i)}$, για κάποια αμφιμονοσήμαντη συνάρτηση $\sigma : \{1, \ldots, s\} \to \{1, \ldots, s\}$.
- Οι δύο απαιτήσεις είναι απαραίτητες:
  - Αν οι p_i δεν είναι διακεκριμένοι ή οι q_j δεν είναι διακεκριμένοι,
  - αν κάποιοι εκθέτες είναι ίσοι με 0,

  τότε το συμπέρασμα δεν είναι αληθές.
- Κάποιες φορές είναι βολικό να επιτρέπουμε εκθέτες = 0.

Διαιρέτες

Έστω $a = p_1^{a_1} \cdots p_s^{a_s}$. Τότε $d \mid a$ αν και μόνο αν $d = p_1^{d_1} \cdots p_s^{d_s}$ με $0 \leq d_i \leq a_i$ για $1 \leq i \leq s$.

Έστω ότι $d \mid a$.

- $a = d \cdot c$, άρα κάθε πρώτος που διαιρεί τον d διαιρεί και τον a.
- Άρα $d = p_1^{d_1} \cdots p_s^{d_s}$ για κάποια $d_i \geq 0$
- Αν ήταν $d_i > a_i$
    - $p_1^{a_1} \cdots p_s^{a_s} = p_1^{d_1} \cdots p_s^{d_s} \cdot c$
    - $p_1^{a_1} \cdots p_{i-1}^{a_{i-1}} p_{i+1}^{a_{i+1}} \cdots p_s^{a_s} = p_1^{d_1} \cdots p_{i-1}^{d_{i-1}} p_i^{d_i - a_i} p_{i+1}^{d_{i+1}} \cdots p_s^{d_s} \cdot c.$
    - Άρα $p_i = p_j$ για κάποιο $j \in \{1, \ldots, s\} \setminus \{i\}$. Άτοπο!
- Άρα $0 \leq d_i \leq a_i$ για κάθε $1 \leq i \leq s$.

Έστω ότι $d = p_1^{d_1} \cdots p_s^{d_s}$, με $d_i \leq a_i$ για $1 \leq i \leq s$.

- $a = p_1^{a_1} \cdots p_s^{a_s} = \left(p_1^{d_1} \cdots p_s^{d_s}\right) \cdot \left(p_1^{a_1 - d_1} \cdots p_s^{a_s - d_s}\right)$
- Άρα $a = d \cdot c$, με $c = p_1^{a_1 - d_1} \cdots p_s^{a_s - d_s} \in \mathbb{N}$.

Μέγιστος Κοινός Διαιρέτης

Έστω $a = p_1^{a_1} \cdots p_s^{a_s}$ και $b = p_1^{b_1} \cdots p_s^{b_s}$, όπου p_i διακεκριμένοι πρώτοι και $a_i \geq 0$, $b_i \geq 0$ για $1 \leq i \leq s$. Τότε

$$(a, b) = p_1^{c_1} \cdots p_s^{c_s}, \quad \text{όπου} \quad c_i = \min\{a_i, b_i\}.$$

Ας ονομάζουμε $d = p_1^{c_1} \cdots p_s^{c_s}$, με $c_i = \min\{a_i, b_i\}$.

- $0 \leq c_i \leq a_i$ άρα $d \mid a$.
- $0 \leq c_i \leq b_i$ άρα $d \mid b$.
- Έστω $f \in \mathbb{N}$ τέτοιος ώστε $f \mid a$ και $f \mid b$.
- Τότε $f = p_1^{f_1} \cdots p_s^{f_s}$ με $0 \leq f_i \leq a_i$ και $0 \leq f_i \leq b_i$.
- Άρα $0 \leq f_i \leq \min\{a_i, b_i\}$.
- Άρα $f \mid d$.

Παράδειγμα

Έστω $a = 2^3 \cdot 3^4 \cdot 11$ και $b = 2 \cdot 5^2 \cdot 11^2 \cdot 13$. Θέλουμε να υπολίσουμε το (a, b).

Γράφουμε

$$\begin{aligned} a &= 2^3 \cdot 3^4 \cdot 5^0 \cdot 11 \cdot 13^0 \\ b &= 2 \cdot 3^0 \cdot 5^2 \cdot 11^2 \cdot 13 \end{aligned}$$

Άρα $(a, b) = 2^1 \cdot 3^0 \cdot 5^0 \cdot 11 \cdot 13^0 = 2 \cdot 11 = 22$.

Παρατήρηση

Αυτή *δεν* είναι η καλύτερη μέθοδος για να υπολογίζουμε το μκδ δύο αριθμών, διότι η παραγοντοποίηση ακεραίων είναι γενικά δύσκολη. Είναι όμως χρήσιμο θεώρημα για να αποδεικνύουμε προτάσεις ή όταν η παραγοντοποίηση των αριθμών είναι γνωστή.

Ελάχιστο Κοινό Πολλαπλάσιο

Έστω φυσικοί αριθμοί a, b. Ένας αριθμός m ονομάζεται ελάχιστο κοινό πολλαπλάσιο των a, b εάν

1. $a \mid m$ και $b \mid m$
2. Για κάθε $m' \in \mathbb{N}$, αν $a \mid m'$ και $b \mid m'$ τότε $m \mid m'$.

Ύπαρξη ΕΚΠ

Έστω $a = p_1^{a_1} \cdots p_s^{a_s}$, $b = p_1^{b_1} \cdots p_s^{b_s}$, με $a_i \geq 0$ και $b_i \geq 0$ για $1 \leq i \leq s$. Τότε ο αριθμός

$$m = p_1^{c_1} \cdots p_s^{c_s}, \quad \text{όπου} \quad c_i = \max\{a_i, b_i\},$$

είναι ελάχιστο κοινό πολλαπλάσιο των a, b.

- $a_i, b_i \leq c_i$, άρα $a \mid m$ και $b \mid m$.
- Άν $f \in \mathbb{N}$ και $a \mid f$ και $b \mid f$, τότε
- $f = p_1^{f_1} \cdots p_s^{f_s} \cdot p_{s+1}^{f_{s+1}} \cdots p_t^{f_t}$, με $a_i \leq f_i$ και $b_i \leq f_i$ για $1 \leq i \leq s$.
- Άρα $\max\{a_i, b_i\} \leq f_i$ για $1 \leq i \leq s$.
- Άρα $m \mid f$.

Θεώρημα

Έστω φυσικοί αριθμοί a, b. Τότε $(a, b) \cdot \text{εκπ}(a, b) = a \cdot b$.

Παρατηρήστε ότι $\min\{x, y\} + \max\{x, y\} = x + y$ για κάθε $x, y \in \mathbb{Z}$.

- $a = p_1^{a_1} \cdots p_s^{a_s}$, $b = p_1^{b_1} \cdots p_s^{b_s}$,
- $(a, b) = p_1^{\min\{a_1, b_1\}} \cdots p_s^{\min\{a_s, b_s\}}$,
- $\text{εκπ}(a, b) = p_1^{\max\{a_1, b_1\}} \cdots p_s^{\max\{a_s, b_s\}}$,
- $a \cdot b = p_1^{a_1 + b_1} \cdots p_s^{a_s + b_s} = p_1^{\min\{a_1, b_1\} + \max\{a_1, b_1\}} \cdots p_s^{\min\{a_s, b_s\} + \max\{a_s, b_s\}} = (a, b) \cdot \text{εκπ}(a, b)$.