ΓΥΜΝΑΣΜΑΤΑ ΑΡΙΘΜΟΘΕΩΡΙΑΣ
Κασαπίδης Γεώργιος – Μαθηματικός
geokasap@sch.gr

Το θεμελιώδες θεώρημα της αριθμητικής

Κάθε φυσικός αριθμός μεγαλύτερος της μονάδας αναλύεται σε γινόμενο πρώτων_παραγόντων κατά ένα και μοναδικό τρόπο, αν δεν λάβουμε υπόψιν μας την σειρά των παραγόντων στο γινόμενο.

απόδειξη

Ανάλυση σε γινόμενο πρώτων: Έστω $k>1$· εφαρμόζουμε τη μέθοδο της μαθηματικής επαγωγής:

1) Για $k = 2$ το πρώτο σκέλος είναι προφανές.

2) Έστω ότι για κάθε φυσικό αριθμό n με $2 \leq n \leq k-1$, υπάρχουν πρώτοι αριθμοί $p_1, \dots, p_m$, όχι αναγκαστικά διαφορετικοί, έτσι ώστε $n = p_1 \cdots p_m$. Αν ο αριθμός k είναι πρώτος ο ισχυρισμός μας ισχύει. Αν ο k είναι σύνθετος, τότε υπάρχουν $b, c \in N$ τέτοια ώστε:

$$k = bc \text{ και } 1 < b \leq c < k$$

Τότε, σύμφωνα με την υπόθεση της επαγωγής, μπορούμε να γράψουμε $b = p_1 \cdots p_a$ και $c = q_1 \cdots q_d$, όπου $p_1, \dots, p_a$ και $q_1, \dots, q_d$ είναι πρώτοι. Επομένως

$$k = bc = p_1 \dots p_a q_1 \dots q_d$$

Δηλαδή αποδείξαμε με την μέθοδο της μαθηματικής επαγωγής ότι κάθε φυσικός αριθμός μεγαλύτερος της μονάδας αναλύεται σε γινόμενο πρώτων.

Μοναδικότητα ανάλυσης: Έστω $p_1 \cdots p_a = k = q_1 \cdots q_d$, με $a \leq d$, δύο πρωτογενείς αναλύσεις του k. Παρατηρούμε ότι το p_1 διαιρεί το k. Επομένως, $p_1 | q_1 \cdots q_d$. Από το λήμμα του Ευκλείδη αυτό συνεπάγεται ότι $p_1 | q_j$ για κάποιο δείκτη j. Και επειδή ο q_j είναι πρώτος, $p_1 = q_j$. Χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι $q_j = q_1$ Συνεπώς,

$$p_2 \dots p_a = q_2 \dots q_d$$

Με την ίδια διαδικασία βρίσκουμε ότι ο πρώτος p_2 ταυτίζεται με κάποιον από τους πρώτους $q_2 \dots q_d$ που και πάλι χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι αυτός είναι ο q_2. Συνεχίζοντας αυτή την διαδικασία συμπεραίνουμε ότι οι $p_1, \dots p_a$ ταυτίζονται με κάποιους από τους $q_1, \dots, q_d$. Χωρίς βλάβη της γενικότητας

$$p_i = q_i \text{ για κάθε } 1 \leq i \leq a$$

Επιπλέον, $1 = q_1 \dots q_{d-a}$. Αν $d > a$ η ισότητα αυτή είναι αδύνατο να ισχύει, άρα αναγκαστικά $a = d$.