Θεμέλια των Μαθηματικών

Ελένη Τζανάκη & Θεόδουλος Γαρεφαλάκης

Εαρινο εξάμηνο 2019-20

Θεωρημα [Αλγόριθμος διαίρεσης για φυσικούς]

Εάν $m,\ n \in \mathbb{N}_0$ και $n \neq 0$, τότε υπάρχουν μοναδικοί φυσικοί αριθμοί, $q,\ r \in \mathbb{N}_0$, τέτοιοι ώστε $m = qn + r$ και $0 \leq r < n$.

Θα αποδείξουμε την πρόταση με την Αρχή του Ελαχίστου. Δεδομένων $m, n \in \mathbb{N}_0$, $n \neq 0$, ορίζουμε το σύνολο $S = \{m - qn \ : \ q \in \mathbb{N}_0\} \cap \mathbb{N}_0$. Τότε

- $m = m - 0 \cdot n \in S$, οπότε $S \neq \emptyset$ και εξ' ορισμού $S \subseteq \mathbb{N}_0$.
- Έστω $r = \min S$. Τότε $r = m - qn$ για κάποιο $q \in \mathbb{N}_0$ και $r \geq 0$.

Μένει να δείξουμε ότι $r < n$. Ας υποθέσουμε ότι $r \geq n$. Ας εξετάσουμε το στοιχείο

$$r' = r - n = m - (q + 1)n.$$

Τότε ισχύουν τα παρακάτω:

- $r' \in S$,
- $r' < r$,
- το r είναι το ελάχιστο στοιχείο του συνόλου S. Άτοπο!

Θα δείξουμε ότι τα q και r είναι μοναδικά. Ας υποθέσουμε ότι υπάρχουν $q, r, q', r' \in \mathbb{N}_0$ τέτοιοι ώστε

$$m = qn + r = q'n + r' \quad \text{με} \quad 0 \leq r < n \ \text{ και } \ 0 \leq r' < n.$$

Θα αποδείξουμε ότι $q = q'$ και $r = r'$. Οι παραπάνω συνθήκες μας δίνουν:

- $(q - q')n = r' - r \implies |q - q'|\, n = |r - r'|$.
- Αν $q \neq q'$ τότε $|q - q'| \geq 1$.
- Τότε $|r - r'| \geq n$.
- Οι συνθήκες $0 \leq r, r' < n$ συνεπάγονται $|r - r'| < n$.

Άτοπο!

Θεωρημα [Αλγόριθμος διαίρεσης για ακεραίους]

Εάν $m,\ n \in \mathbb{Z}$ και $n \neq 0$, τότε υπάρχουν μοναδικοί ακέραιοι αριθμοί, $q,\ r \in \mathbb{Z}$, τέτοιοι ώστε

$$m = qn + r \quad \text{και} \quad 0 \leq r < |n|. \tag{1}$$

Γνωρίζουμε ότι τα q, r υπάρχουν όταν $m \geq 0$ και $n > 0$. Μένουν να εξετάσουμε τρεις περιπτώσεις:

- Έστω ότι $m \geq 0$ και $n < 0$. Τότε υπάρχουν $q', r' \in \mathbb{N}_0$ τέτοιοι ώστε

  $$m = q'(-n) + r', \quad \text{με} \quad 0 \leq r' < -n.$$

  Οπότε η ταυτότητα (1) ισχύει για $q = -q'$ και $r = r'$.

- Έστω ότι $m < 0$ και $n > 0$. Τότε υπάρχουν $q', r' \in \mathbb{N}_0$ τέτοιοι ώστε

  $$-m = q'n + r', \quad \text{με} \quad 0 \leq r' < n.$$

  Αν $r' = 0$,τότε η ταυτότητα (1) ισχύει για $q = -q'$ και $r = r' = 0$.
  Αν $0 < r' < n$ τότε

  $$m = (-q')n - r' = (-q' - 1)n + (n - r'), \quad \text{με} \quad 0 < n - r' < n.$$

  Οπότε η ταυτότητα (1) ισχύει για $q = -q' - 1$ και $r = n - r'$.

- Έστω ότι $m < 0$ και $n < 0$. Άσκηση...

Μοναδικότητα: Άσκηση...

Ορισμός Σχέσης Διαιρετότητας

Λέμε οτι $k \in \mathbb{Z}$ είναι παράγοντας ή διαιρέτης του $m \in \mathbb{Z}$ εάν υπάρχει $s \in \mathbb{Z}$ τέτοιος ώστε $m = k \cdot s$. Συμβολίζουμε $k \mid m$.

Παρατηρήσεις:

- Παραπάνω ορίσαμε μία σχέση, όχι μία πράξη!
- Ο αριθμός $k \neq 0$ διαιρεί τον αριθμό m ανν το υπόλοιπο της διαίρεσης του m με τον k είναι 0.
- Οι ± 1 και $\pm m$ είναι διαιρέτες του m. Κάθε άλλος διαιρέτης ονομάζεται γνήσιος διαιρέτης.
- $0 \mid m \iff m = 0$.
- $k \mid 0$ για κάθε $k \in \mathbb{Z}$.
- Αν $k \mid m$ ισχύουν και τα $k \mid -m$, $-k \mid m$, $-k \mid -m$.
- Αν $k \mid m$ και $m \mid k$ τότε $k = m$ ή $k = -m$.

- Αν $k \mid m$ και $k \mid n$, τότε $k \mid sm + tn$ για κάθε $s, t \in \mathbb{Z}$.

Ορισμός πρώτων αριθμών

Ένας φυσικός αριθμός m ονομάζεται πρώτος εάν $m > 1$ και ο m δεν έχει γνήσιους διαιρέτες.

Παρατηρήσεις/Παραδείγματα:

- Οι αριθμοί $0, 1$ εξ' ορισμού *δεν* είναι πρώτοι.
- Μπορούμε να ελέγξουμε ότι οι αριθμοί $2, 3, 5, 7$ είναι όλοι οι πρώτοι αριθμοί μικρότεροι του 10.
- Ο αριθμός 10 δεν είναι πρώτος, αφού $10 = 2 \cdot 5$, δηλαδή το 2 είναι γνήσιος διαιρέτης του 10.

Σύμφωνα με τον ορισμό, ένας φυσικός αριθμός m *δεν* είναι πρώτος αν και μόνο αν μπορεί να γραφεί ως γινόμενο $m = a \cdot b$, με $a, b \in \mathbb{N}$, $1 < a, b < m$.

Πρόταση

Κάθε φυσικός αριθμός $m > 1$ είναι γινόμενο πρώτων αριθμών.

θέλουμε να δείξουμε ότι το παρακάτω σύνολο είναι κενό

$$M = \{n \in \mathbb{N} \ : \ n > 1 \ \text{ και ο } \ n \ \text{ δεν είναι γινόμενο πρώτων}\}.$$

Ας υποθέσουμε ότι $M \neq \emptyset$.

- Από την Αρχή Ελαχίστου υπάρχει ελάχιστο στοιχείο $m \in M$.
- Ο m είναι μεγαλύτερος από το 1 και δεν είναι πρώτος (αφού δεν είναι γινόμενο πρώτων).
- Συνεπώς υπάρχουν φυσικοί αριθμοί a και b τέτοιοι ώστε $1 < a < m$, $1 < b < m$ και $m = a \cdot b$.
- Αφού m είναι το ελάχιστο στοιχείο του M, οι a και b δεν ανήκουν στο M, και συνεπώς είναι γινόμενα πρώτων αριθμών.
- Αν $a = p_1 \cdots p_s$ και $b = q_1 \cdots q_t$, όπου $p_1, \ldots, p_s, q_1, \ldots, q_t$ είναι πρώτοι,
- τότε $m = a \cdot b = p_1 \cdots p_s \cdot q_1 \cdots q_t$ είναι επίσης γινόμενο πρώτων αριθμών. Ατοπο!

Άρα $M = \emptyset$, δηλ. κάθε φυσικός αριθμός μεγαλύτερος από τον 1 είναι γινόμενο πρώτων αριθμών.

Θεώρημα ύπαρξης άπειρων πρώτων

Υπάρχουν άπειροι πρώτοι αριθμοί.

- Ας υποθέσουμε ότι υπάρχει πεπερασμένο πλήθος πρώτων, $p_1 < p_2 < \ldots < p_r$.
- Εξετάζουμε το φυσικό αριθμό $m = p_1 p_2 \cdots p_r + 1$
- $m > 1$, άρα είναι γινόμενο πρώτων.
- Αν $p_i \mid m$ τότε $p_i \mid m - p_1 \cdots p_r$.
- Άρα $p_i \mid 1$, άτοπο!