25/10/2018

* Ευκλείδια Διαίρεση *

Θεώρημα: Για κάθε ζεύγος $a, b \in \mathbb{N}_0$ με $b \neq 0$, υπάρχει μοναδικό ζεύγος $q, r \in \mathbb{Z}$ έτσι ώστε

$$\underbrace{a = bq + r}_{}\quad \text{και} \quad 0 \leq r < b$$

πηλίκο (q), υπόλοιπο (r)

αφαίρεση φυσικών αριθμών είναι ακέραιος

Απόδειξη: Υπάρχει ζεύγος q, r

$S = \{ a - bx \mid x \in \mathbb{N}_0 \} \cap \mathbb{N}_0$

$a = a - b0 \in S \Rightarrow S \neq \emptyset$

S μη-κενό άρα το S έχει ελάχιστο στοιχείο, έστω το r

$r \in S \Rightarrow r = a - bq$ για κάποιο $q \in \mathbb{N}_0$

$a = bq + r$

$r \in S \Rightarrow 0 \leq r$

Ισχυριζόμαστε $r < b$ (έστω όχι, τότε $b \leq r$

$\Rightarrow 0 \leq \overset{r\in S}{r} - b = a - bq - b = a - b(q+1)$

$\Rightarrow r - b \in S$, $r - b < r$, r ελάχιστο στοιχείο

$\Rightarrow r - b \in S$ και $r - b < r$ Άτοπο!)

Άρα $r < b$

Άρα υπάρχει ζεύγος q, r

(1) $a = bq + r$ και $0 \leq r < b$

(2) $a = bq' + r'$ και $0 \leq r' < b'$

πρέπει να δειχθεί ότι $q = q'$ και $r = r'$

Ένας από τα r, r' είναι μεγαλύτερος ή ίσος από τον άλλον.

Έστω ότι $r \geq r'$

(1) - (2) $0 = Bq - Bq' + r - r' \Rightarrow r - r' = B(q - q')$

$0 \leq r - r' \leq r < B \Rightarrow 0 \leq r - r' < B$

$\Rightarrow 0 \leq B(q' - q) < B \Rightarrow 0 \leq q' - q < 1 \Rightarrow q' - q = 0 \Rightarrow q = q'$

$r - r' = B(q - q') = B0 \Rightarrow \boxed{r = r'}$

Άρα μοναδικοί ακέραιοι

Παρατήρηση - Θεώρημα Για κάθε ακέραιοι $a, B \in \mathbb{Z}$ με $B \neq 0$ υπάρχει μοναδικοί ακέραιοι $q, r \in \mathbb{Z}$ έτσι ώστε $a = Bq + r$ και $0 \leq r < |B|$

Παραδείγματα • $a = 47$, $B = 9$

$\underset{a}{47} = \boxed{5}\,\underset{B}{9} + \boxed{2} \rightarrow 0 \leq r < 9$

$-47 = \boxed{-6}\,9 + \boxed{7}$

$-47 = \boxed{6}(-9) + \boxed{7} \leftarrow -47 = 5(-9) - 2 \rightarrow 0 \leq r < 9$

$47 = 5(-9) - 9 + 9 - 2$

$47 = \boxed{(-5)}(-9) + \boxed{2}$

• $a = 17$ $B = 3$

$17 = \boxed{5}\,3 + \boxed{2} \leftarrow 0 \leq r < |3|$

$17 = \boxed{-5}\,-3 + \boxed{2}$

$-17 = \boxed{-6}\,3 + \boxed{1}$

$-17 = \boxed{6}\,-3 + \boxed{1}$

* ΔΙΑΙΡΕΤΟΤΗΤΑ *

<u>Ορισμός</u> Ο ακέραιος αριθμός a διαιρεί τον ακέραιο αριθμό b αν υπάρχει ακέραιος αριθμός γ τέτοιος ώστε $b = \gamma a$

$a \mid b \rightarrow a$ διαιρεί το b

ή $\iff b = a\gamma$

b πολλαπλάσιο του a

<u>Ιδιότητες</u> (1) $a \mid 0$ για κάθε $a \in \mathbb{Z}$

(2) Αν $0 \mid a \Rightarrow a = 0$ (το 0 διαιρεί το ίδιο το 0)

(3) Αν $a \mid b \iff -a \mid b \iff a \mid -b \iff -a \mid -b \iff |a| \mid |b|$

$a \mid b \Rightarrow b = a\gamma \iff -b = -a\gamma$

Η 3η ιδιότητα μας λέει: Αν καταλάβω τη διαιρετότητα φυσικών, ξέρω τη διαιρετότητα ακεραίων (το πρόσημο δεν μας νοιάζει)

(4) $1 \mid a$ για κάθε $a \in \mathbb{Z}$ (οποιοσδήποτε ακέραιος είναι πολλαπλάσιο του 1)

(5) $a \mid 1 \Rightarrow a = 1$ ή $a = -1$

$a > 0$ και $a \mid 1 \Rightarrow a = 1$

(6) $a \mid a$ για κάθε $a \in \mathbb{Z}$

(7) Αν $a \mid b$ και $b \mid \gamma$ τότε $a \mid \gamma$

(8) Αν $a \mid b$ και $a \mid \gamma$ και $\kappa, \lambda \in \mathbb{Z} \Rightarrow a \mid \kappa b + \lambda$

$b = a\delta$ $\quad \kappa b + \lambda\gamma = a \boxed{\kappa\delta + \lambda\epsilon}$

$\gamma = a\varepsilon$

(9) Αν $a \mid b$ και $\gamma \mid \delta \Rightarrow a\gamma \mid b\delta$

(10) Αν $a \mid b$, $\gamma \mid \gamma \Rightarrow a\gamma \mid b\gamma$

(11) Αν $a \mid b$ και $b \neq 0$ τότε $|a| \leq |b|$

(Αν $a, b \in \mathbb{N}$ και $a \mid b \Rightarrow a \leq b$)

(12) Αν $a, b \in \mathbb{N}$, $a \mid b$ και $b \mid a \Rightarrow a = b$

<u>Ορισμός</u> (πρώτος αριθμός) Ένας φυσικός αριθμός $p>1$ ονομάζεται <u>πρώτος</u> αν οι μοναδικοί φυσικοί αριθμοί που είναι διαιρέτες του είναι ο 1 και ο εαυτός του p

<u>Παραδείγματα</u>: πρώτοι αριθμοί $2, 3, 5, 7, 11$

<u>Ορισμός</u> (σύνθετος αριθμός) Κάθε φυσικός αριθμός μεγαλύτερος του 1 που δεν είναι πρώτος, ονομάζεται <u>σύνθετος</u>
α σύνθετος αν $a>1$
Ένας αριθμός είναι σύνθετος αν μπορεί να γραφεί στην εξής μορφή: $a=\beta\gamma$ $\quad 1<\beta<a$
$1<\gamma<a$

Φυσικοί Αριθμοί

$\{1\} \cup \{\text{πρώτοι}\} \cup \{\text{σύνθετοι}\}$

<u>Πρόταση</u> Κάθε φυσικός αριθμός $a>1$ έχει τουλάχιστον έναν πρώτο διαιρέτη.

$S_a = \{m \mid m\in\mathbb{N},\ m|a \text{ και } m>1\}$
→ όλοι οι φυσικοί διαιρέτες του a που είναι μεγαλύτεροι του 1
$S_a \subseteq \mathbb{N}$ (αν δω ότι είναι μη κενό, τότε έχει ελάχιστο στοιχείο – αρχή καλής διάταξης)

$\left.\begin{array}{l} a|a \\ a>1 \end{array}\right\} \Rightarrow a\in S_a$

$S_a \neq \emptyset$. Άρα το S_a έχει ελάχιστο στοιχείο, έστω το p.
$p\in S_a \Rightarrow p|a,\ p>1$ (p ή $\cancel{1}$ γιατί $p>1$ άρα ή πρώτος ή σύνθετο)

Έστω ότι p σύνθετος $\Rightarrow p = \beta\gamma \quad 1<\beta<p, \ 1<\gamma<p$
$1<\beta<p, \quad \beta | p \quad p|a \Rightarrow \beta | a$
Άρα $\beta \in S_a$ και $\beta < p \rightarrow$ το ελάχιστο στοιχείο το S_a
Άτοπο! Άρα p πρώτος

<u>Θεώρημα Ευκλείδης</u> Το πλήθος των πρώτων αριθμών είναι άπειρο. !

Έστω ότι το πλήθος των πρώτων αριθμών είναι πεπερασμένο και έστω $p_1, p_2, \ldots, p_s$ όλοι οι πρώτοι αριθμοί
$a = p_1 p_2 p_3 \ldots p_s + 1 \quad , a > 1$
Ο a είναι φυσικός αριθμός μεγαλύτερος του 1, άρα έχει τουλάχιστον ένα πρώτο διαιρέτη, τον p

p πρώτος αριθμός, $p \in \{p_1, p_2, \ldots, p_i, \ldots, p_s\} \Rightarrow p = p_i$
$1 \leq i \leq s$

$p_i | a = p_1 p_2 \ldots p_s + 1$
$p_i | p_1 p_2 \ldots p_i \ldots p_s$
$\Rightarrow p_i \,/\, (1)(p_1 p_2 \ldots p_i \ldots p_s + 1) + (-1)(p_1 p_2 \ldots p_i \ldots p_s)$

$\Rightarrow p_i / 1 \Rightarrow p_i = 1$ Άτοπο, γιατί το 1 δεν είναι πρώτος αριθμός

Άρα, το πλήθος των πρώτων αριθμών είναι <u>Άπειρο</u> και όχι πεπερασμένο.