18-10-16

Διαιρετότητα Ακεραίων

• Θεώρημα: {Ευκλείδεια Διαίρεση}: Έστω $a, b \in \mathbb{Z}$, $b \neq 0$

Τότε υπάρχει μοναδικό ζεύγος ακεραίων q, r έτσι ώστε: $a = bq + r$, $0 \leq r < |b|$

Απόδειξη: Θεωρούμε το σύνολο

$$S = \{a - bx \in \mathbb{Z} \mid x \in \mathbb{Z},\ a - bx \geq 0\}$$

⊛ Ισχυρισμός: $S \neq \emptyset$

• 1η περίπτωση: $b > 0$. Τότε θέτουμε $x = -(1 + |a|) \in \mathbb{Z}$ και τότε

$$a - bx = a - b(-(1 + |a|)) = a + b(1 + |a|) \geq a + 1 + |a| \geq 1$$

και $a - bx \in S$

• 2η περίπτωση: $b < 0$. Θέτουμε: $x = 1 + |a| \in \mathbb{Z}$

Τότε: $a - bx = a + (-b)(1 + |a|) \geq a + 1 + |a| \geq 1$

Τότε: $a - bx \in S$

Άρα, σε κάθε περίπτωση: $S \neq \emptyset$

Από την (ΑΔΕ), το S έχει ελάχιστο στοιχείο

$h = \min S \Rightarrow \exists\, q \in \mathbb{Z}: r = a - bq$, $r \geq 0$

Έχουμε προσδιορίσει ακέραιους $q, r \in \mathbb{Z}$: $a = bq + r$, $r \geq 0$

Επιπλέον, θα έχουμε : $r - |b| =$

$$= a - bq - |b| = \begin{cases} b>0 \Rightarrow a - bq - b = a - b(q+1) \\ b<0 \Rightarrow a - bq + b = a - b(q-1) \end{cases}$$

Αν $r - |b| \geq 0$, τότε επειδή $r - |b|$ είναι της μορφής $a - bx \in \mathbb{Z}$, θα έχουμε : $r - |b| \in S$

Όμως, είναι άτοπο, διότι $r = \min S$ και $r - |b| < r$ διότι $b \neq 0$. Άρα, $r < |b|$

Έστω ότι $\exists\, q', r' \in \mathbb{Z} : a = bq' + r'$, $0 \leq r' < |b|$

Θέλω: $q = q'$, $r = r'$

$bq + r = bq' + r' \Rightarrow b(q - q') = r' - r \Rightarrow$

$\Rightarrow |b|\,|q - q'| = |r - r'| \Rightarrow$

$$\left.\begin{array}{l} 0 \leq r < |b| \\ -|b| < -r' \leq 0 \end{array}\right\} \overset{(+)}{\Rightarrow} \left.\begin{array}{l} -|b| \leq r - r' \leq |b| \\ |r - r'| < |b| \end{array}\right\} \Rightarrow$$

$|b|\,|q - q'| = |r - r'| < |b| \Rightarrow |q - q'| < 1$

$\Rightarrow |q - q'| = 0 \Rightarrow q = q'$, άρα $r = r'$

• Ορισμός: Ο αριθμός q καλείται πηλίκο της διαίρεσης του α με το b

Ο αριθμός r καλείται υπόλοιπο της διαίρεσης του b με το α

• Παράδειγμα: Για κάθε ακέραιο α και επιλέγοντας b=2, θα έχουμε ότι:

$\exists\, q, r \in \mathbb{Z} : \alpha = 2q + r$, $0 \le r < 2 \Rightarrow$
$r = 0$ ή $r = 1$

και τότε $\alpha = 2q$ ή $\alpha = 2q + 1$

α: άρτιος α: περιττός

• Εφαρμογή: $\forall\, \alpha \in \mathbb{Z}, \forall\, n \in \mathbb{N}$: ο α έχει μία από τις παρακάτω μορφές:

• $nk,\ nk+1,\ nk+2,\ \dots,\ nk+n-1 \quad k \in \mathbb{Z}$

• Παράδειγμα: Έστω $\alpha \in \mathbb{Z}$ περιττός. Τότε ο α^2 είναι της μορφής: $8k+1$, $k \in \mathbb{N}_0$

Απόδειξη: Από την εφαρμογή, για $n=4$, ο α θα είναι της μορφής: $4k, 4k+1, 4k+2, 4k+3$

Επειδή ο α είναι περιττός, οι $4k, 4k+2$ αποκλείονται

Άρα, ο α είναι της μορφής: $4k+1, 4k+3$

• Αν $a = 4k+1 \Rightarrow a^2 = 16k^2 + 8k + 1 = 8(2k^2+k)+1$

• Αν $a = 4k+3 \Rightarrow a^2 = 16k^2 + 24k + 9 =$

$= 16k^2 + 24k + 8 + 1 = 8(k^2 + 3k$

• <u>Ορισμός</u>: Αν $a, b \in Z$ και $b \neq 0$, θα λέμε ότι ο b διαιρεί τον a και συμβολίζεται ως εξής:

$b|a \iff \exists\, q \in Z : a = bq$

• <u>Παραδείγματα</u>: $4|20$, $-4|20$, $7 \nmid 20$ ⊛

⊛ Ο 7 <u>δεν</u> διαιρεί το 20

• <u>Ιδιότητες Διαιρετότητας</u>

1) $a|0, \forall a \in Z$ και $0|b, b \in Z \Rightarrow b = 0$

2) $a|b \iff -a|b \iff a|-b \iff -a|-b \iff |a|\,|b|$

3) $\forall a \in Z : a|a$ και $1|a$

4) $\left.\begin{matrix} a|b \\ b|c \end{matrix}\right\} \Rightarrow a|c$

5) $\left.\begin{matrix} a|b \\ a|c \end{matrix}\right\} \Rightarrow x, y \in Z \Rightarrow a|bx + cy$

Γενικότερα: $a|b_1, a|b_2, \dots, a|b_k \Rightarrow a|b_1x_1 + \dots + b_kx_k$ $\forall\, x_1, x_2, \dots, x_k$

6) $\left.\begin{matrix} a|b \\ c|d \end{matrix}\right\} \Rightarrow ac|bd$ <u>και</u> $a|b \Rightarrow ax|bx, \forall x \in Z$

7) $a|b \;,\; b\neq 0 \Rightarrow |a| \leq |b|$

8) $\left.\begin{matrix} a,b\neq 0 \\ a|b \\ b|a \end{matrix}\right\} \Rightarrow |a|=|b|$

• Απόδειξη 5ης ιδιότητας

$a|b_i \;,\; i=1,2,\dots,\kappa \Rightarrow \exists\, y_1,y_2,\dots,y_\kappa \in \mathbb{Z}$

$b_i = y_i \cdot a \;,\; \forall\, i=1,\dots,\kappa$

Τότε: $\forall\, x_1,x_2,\dots,x_\kappa : x_i b_i = x_i y_i a \Rightarrow$

$\Rightarrow x_1b_1 + x_2b_2 + \dots + x_\kappa b_\kappa = x_1y_1a + \dots + x_\kappa y_\kappa a =$

$= a(x_1y_1 + \dots + x_\kappa y_\kappa)$

$\Rightarrow a|b_1x_1 + \dots + b_\kappa x_\kappa$

• Απόδειξη 7ης ιδιότητας

Έστω $a,b \in \mathbb{Z}$, $b\neq 0$ και υποθέτουμε ότι

$a|b \Rightarrow \exists\, \kappa \in \mathbb{Z} : b = a\cdot\kappa \xrightarrow{\kappa\neq 0} |b| = |a||\kappa| \geq |a|$

• Ερώτημα: Ισχύει ότι $a+c \,|\, b+d$, εφόσον $\begin{matrix} a|b \\ c|d \end{matrix}$

Απάντηση: Όχι, διότι πχ: $\left.\begin{matrix} 2|4 \\ 3|9 \end{matrix}\right\} \Rightarrow 5 \nmid 13$