

19/10/2015

Έστω $a, b \in \mathbb{Z}$. Πότε $a \mid b$ (ο a διαιρεί τον b) $\Leftrightarrow \exists c \in \mathbb{Z} : b = c \cdot a$

ΠΡΟΤΑΣΗ:

- ① $\forall a \in \mathbb{Z} : a \mid 0 \wedge 0 \mid b \Rightarrow b = 0 \ (\forall b \in \mathbb{Z})$
- ② $a \mid b \Leftrightarrow -a \mid b \Leftrightarrow -a \mid -b \Leftrightarrow a \mid -b \Leftrightarrow |a| \mid |b|$
- ③ $\forall a \in \mathbb{Z} : a \mid a$
- ④ $\begin{matrix} a \mid b \\ b \mid c \end{matrix} \Rightarrow a \mid c$
- ⑤ $\begin{matrix} a \mid b \\ a \mid c \end{matrix} \Rightarrow a \mid bx + cy$ ΓΕΝΙΚΟΤΕΡΑ: $\forall a, b_1, \dots, b_n \in \mathbb{Z}$ και $a \mid b_1, a \mid b_2, \dots, a \mid b_n$
 $\forall x, y \in \mathbb{Z}$ τότε $a \mid b_1 x_1 + \dots + b_n x_n, \forall x_1, x_2, \dots, x_n \in \mathbb{Z}$
- ⑥ $\begin{matrix} a \mid b \\ c \mid d \end{matrix} \Rightarrow ac \mid bd$
- ⑦ $a \mid b \Rightarrow ax \mid bx, \forall x \in \mathbb{Z}$
- ⑧ $a \mid b \wedge b \neq 0 \Rightarrow |a| \leq |b|$
- ⑨ $a \mid b$ και $b \mid a \Rightarrow |a| = |b|$

Απόδειξη

- ① $a \mid 0$ διότι $a \cdot 0$ και αν $0 \mid b \Rightarrow \exists c \in \mathbb{Z} : b = 0 \cdot c = 0$
- ② $a \mid b \Leftrightarrow \exists c \in \mathbb{Z} : b = a \cdot c \Leftrightarrow b = (-a) \cdot (-c) \Leftrightarrow -b = (-a) \cdot c \Leftrightarrow -b = a \cdot (-c)$
 $\Leftrightarrow -a \mid b \Leftrightarrow -a \mid -b \Leftrightarrow a \mid -b$
- ③ $a \mid a$, διότι $a = a \cdot 1$
- ④ $\begin{matrix} a \mid b \Rightarrow \exists x \in \mathbb{Z} : b = ax \\ b \mid c \Rightarrow \exists y \in \mathbb{Z} : c = by \end{matrix} \Rightarrow c = by = a \cdot xy = a \cdot k$
- ⑤ $a \mid b_i, 1 \leq i \leq n \Rightarrow b_i = a \cdot c_i$, για κάποιες ακεραίες $c_1, \dots, c_n \Rightarrow$
 $\Rightarrow b_i x_i = a c_i x_i \Rightarrow b_1 x_1 + \dots + b_n x_n = a(c_1 x_1 + \dots + c_n x_n)$. Άρα $a \mid b_1 x_1 + \dots + b_n x_n$
 $1 \leq i \leq n$

$$\textcircled{6} \begin{aligned} a|b &\Rightarrow \exists x \in \mathbb{Z} : b = ax \\ c|d &\Rightarrow \exists y \in \mathbb{Z} : d = cy \end{aligned} \Rightarrow bd = acxy \Rightarrow a|bd$$

$$\textcircled{7} a|b \Rightarrow \exists c \in \mathbb{Z} : b = a \cdot c \Rightarrow bx = axc \Rightarrow ax|bx$$

$$\textcircled{8} a|b \Rightarrow \exists c \in \mathbb{Z} : b = a \cdot c \Rightarrow |b| = |a||c| \geq |a|$$

$b \neq 0$ $\Rightarrow$ τότε $c \neq 0$, διότι διαφορετικά $b=0$, το οποίο δεν ισχύει.
Άρα $|a| \leq |b|$

$\textcircled{9}$ Έστω $a|b$ ή $b=0$, τότε έχουμε $b|a$, διότι έχουμε $a=0$ και τότε $a=b=0$
 $b|a$ $\Rightarrow$ $a=0$ τότε $b=0$, δηλαδή $a=b=0$

Έστω $a \neq 0, b \neq 0$, τότε από το $\textcircled{8}$:

$$\begin{aligned} a|b &\Rightarrow |a| \leq |b| \\ b|a &\Rightarrow |b| \leq |a| \end{aligned} \Rightarrow |a| = |b|$$

□

ΠΑΡΑΤΗΡΗΣΗ: $\textcircled{1} \frac{a|b}{c|d} \nRightarrow a+c|b+d$ ΔΕΝ ΙΣΧΥΕΙ, διότι $2|4$ και $2+3=5$
 $3|12$ $\nRightarrow 12+4=16$

$$\textcircled{2} \bullet \perp n, \forall n \in \mathbb{Z} \text{ και } n|1 \Leftrightarrow n = \pm 1$$

$$\bullet \text{ad} \frac{a|c}{a \neq 0} \Rightarrow \exists x \in \mathbb{Z} : ac = adx \Rightarrow a(c-dx) = 0 \xrightarrow{a \neq 0} c-dx=0 \Rightarrow c=dx \Rightarrow d|c$$

$$\bullet a \in \mathbb{Z} \text{ και } a|1$$

$$\frac{d|a}{d|a+1} \Rightarrow d=1 \text{ διότι } d|(a+1-a) = d|1 \Rightarrow d=1, \text{ διότι } d \geq 1$$

ΠΡΟΤΑΣΗ: $\forall n \geq 0 : 9 | 10^n + 3 \cdot 4^{n+2} + 5 : P(n)$

$\textcircled{1}$ Για $n=0$: $10^0 + 3 \cdot 4^2 + 5 = 1 + 3 \cdot 16 + 5 = 54$ και προφανώς $9 | 54 \Rightarrow n P(0)$ ισχύει.

$\textcircled{2}$ Για $n=1$: $10^1 + 3 \cdot 4^3 + 5 = 207 = 9 \cdot 23 \Rightarrow 9 | 207 \Rightarrow P(1)$ ισχύει

$\textcircled{3}$ ΕΠΑΓΓΕΛΙΚΗ ΥΠΟΘΕΣΗ: Υποθέτουμε ότι $n P(n)$ ισχύει: $9 | 10^n + 3 \cdot 4^{n+2} + 5$

$$10^{n+1} + 3 \cdot 4^{n+3} + 5 = 10^{n+1} + 3 \cdot 4^{n+2} \cdot 4 + 5 = 10^n \cdot 10 + 3 \cdot 4 \cdot 4^{n+2} + 5 =$$

$$= 10^n(9+1) + 12 \cdot 4^{n+2} + 5 = 10^n + 9 \cdot 10^n + 3 \cdot 4^{n+2} + 9 \cdot 4^{n+2} + 5 =$$

$$= (10^n + 3 \cdot 4^{n+2} + 5) + 9(10^n + 4^{n+2}) \stackrel{P(n)}{=} \text{δα διασπείρει από το 9}$$

με χρήση της επαγωγικής υπόθεσης.

ΑΣΚΗΣΗ ① $\forall n \in \mathbb{Z} : 4 \nmid n^2 + 2$ (ΝΔΟ)

α. Έστω n άρτιος $\Rightarrow \exists k \in \mathbb{Z} : n = 2k \Rightarrow n^2 + 2 = 4k^2 + 2 = 2(2k^2 + 1)$

Αν $4 \mid n^2 + 2 \Rightarrow 4 \mid 2(2k^2 + 1) \Rightarrow 2 \mid 2k^2 + 1$: άτοπο διότι $2k^2 + 1$ περιττός $\Rightarrow 2 \nmid 2k^2 + 1$

Αρα n άρτιος $\Rightarrow 4 \nmid n^2 + 2$

β. Έστω n περιττός $\Rightarrow n = 2k + 1 \Rightarrow n^2 + 2 = (2k + 1)^2 + 2 = 4k^2 + 4k + 1 + 2 = 4k^2 + 4k + 3$

Αν $4 \mid n^2 + 2 \Rightarrow 4 \mid 4k^2 + 4k + 3 \Rightarrow 4 \mid 4k^2 + 4k + 4 - 1 \Rightarrow 4 \mid 4(k^2 + k + 1) - 1 \Rightarrow 4 \mid 1$
 Όπως $4 \mid 4(k^2 + k + 1)$: άτοπο

□

ΑΣΚΗΣΗ ② Ποιοι ακέραιοι m ικανοποιούν την σχέση: $m+1 \mid m^2+1$;

Έστω $m+1 \mid m^2+1 \Rightarrow m+1 \mid m^2+m+2 \Rightarrow m+1 \mid m(m+1)+2$
 Όπως $m+1 \mid m+1$: Όπως $m+1 \mid m+1 \Rightarrow m+1 \mid m(m+1)$

$\Rightarrow m+1 \mid 2 \Rightarrow m+1 = 0, \pm 1, \pm 2$
 $\searrow$
 $|m+1| \leq |2| = 2$

- Τότε :
- ① $m+1=0 \Rightarrow m=-1 : 0 \nmid 2$ δεν ισχύει
 - ② $m+1=1 \Rightarrow m=0 : 1 \mid 2$ ισχύει
 - ③ $m+1=-1 \Rightarrow m=-2 : -1 \mid 2$ ισχύει
 - ④ $m+1=2 \Rightarrow m=1 : 2 \nmid 2$ ισχύει
 - ⑤ $m+1=-2 \Rightarrow m=-3 : -2 \nmid 2$ ισχύει

Αρα οι ζητούμενες τιμές του m που τις οποίες $m+1 \mid m^2+1$
 είναι: $m=0, m=-2, m=1, m=-3$

□

ΘΕΩΡΗΜΑ [ΕΥΚΛΕΙΔΕΙΑ ΔΙΑΙΡΕΣΗ]:

Έστω $a, b \in \mathbb{Z}, b \neq 0$. Τότε υπάρχουν μοναδικοί ακέραιοι $q, r \in \mathbb{Z}$:
 $a = bq + r, 0 \leq r < |b|$

Απόδειξη: Θεωρούμε το σύνολο: $S = \{a - bx \in \mathbb{Z} \mid x \in \mathbb{Z} \text{ και } a - bx \geq 0\} \subseteq \mathbb{N}_0$
Θα δείξουμε ότι: $S \neq \emptyset$,

Ξεχωρίζουμε περιπτώσεις:

- α) $b > 0$, τότε δέχουμε $x = -(1 + |a|)$, και τότε: $a - bx = a + b(1 + |a|) \geq a + 1 + |a| \geq 1$
 $\Rightarrow a - bx \in S$, όπου $x = -(1 + |a|) \Rightarrow S \neq \emptyset$
- β) $b < 0$, τότε δέχουμε $x = 1 + |a|$, και τότε: $a - bx = a + (-b)(1 + |a|) \geq a + 1 + |a| \geq 1$
 $\Rightarrow a - bx \in S$, όπου $x = 1 + |a| \Rightarrow S \neq \emptyset$

Επειδή $S \neq \emptyset$, από την ΑΡΧΗ ΚΑΙΗΣ ΔΙΑΤΑΞΗΣ $\Rightarrow$ το S έχει ένα ελάχιστο στοιχείο. Έστω r : το ελάχιστο στοιχείο του $S \Rightarrow r = a - bq \geq 0$, για κάποιο $q \in \mathbb{Z}$. Άρα: $a = bq + r$, και $0 \leq r$. Μένει να δείξουμε ότι $r < |b|$

$$\begin{aligned} \text{Θεωρούμε τον αριθμό: } r - |b| &= a - bq - |b| = \\ &= \begin{cases} \xrightarrow{b > 0} a - bq - b = a - b(q+1) \\ \xrightarrow{b < 0} a - bq + b = a - b(q-1) \end{cases} \end{aligned}$$

Άρα ο αριθμός $r - |b|$ είναι της μορφής $a - bx$, όπου $x \in \mathbb{Z}$

Αν $r - |b| \geq 0$, τότε $r - |b| \in S$, αυτό όμως είναι άτοπο διότι: $r - |b| < r$ και το r ελάχιστο στοιχείο του S . Άρα $r - |b| < 0 \Rightarrow r < |b|$

ΜΟΝΑΔΙΚΟΤΗΤΑ: Έστω $q', r' \in \mathbb{Z} : a = bq' + r'$ και $0 \leq r' < |b|$ | Θεωρούμε $\begin{cases} q = q' \\ r = r' \end{cases}$
 $q, r \in \mathbb{Z} : a = bq + r$ και $0 \leq r < |b|$

$$r' - r = b(q - q') \Rightarrow |r' - r| = |b(q - q')| = |b| \cdot |q - q'| \quad ①$$

$$\begin{aligned} 0 \leq r' < |b| \Rightarrow -|b| < -r \leq 0 & \Rightarrow -|b| < r' - r < |b| \Rightarrow |r' - r| < |b| \quad ② \\ 0 \leq r < |b| & \quad 0 \leq r' < |b| \end{aligned}$$

$$\text{Τότε από τα } ①, ② \Rightarrow |q' - q| < 1 \Rightarrow |q' - q| = 0 \Rightarrow \boxed{q' = q}$$

$$\text{Τότε } r' = a - bq' = a - bq = r \Rightarrow \boxed{r' = r}$$