19/11/2018

ΠΡΟΤΑΣΗ: Έστω $a,b\in\mathbb{N}$ και $k\in\mathbb{Z}$, $k\neq 0$. Τότε $\text{ΜΚΔ}(ka,kb) = |k|\,\text{ΜΚΔ}(a,b)$

ΑΠΟΔΕΙΞΗ: Θέτουμε $d=\text{ΜΚΔ}(a,b)$, $d_1=\text{ΜΚΔ}(ka,kb)$.

Έχουμε $\left.\begin{matrix} d|a \\ |k|\,|k \end{matrix}\right\} \Rightarrow d|k|\,|ak$. Όμοια $d|k|\,|kb$.

Επομένως, $d|k|$ κοινός θετικός διαιρέτης των $ka, kb \Rightarrow d|k| \le d_1$ (1)

Έχουμε ότι υπάρχουν $x,y\in\mathbb{Z}$ με $d=xa+yb$.

Συνεπώς (2) $|k|d = x|k|a + y|k|b = \begin{cases} xka+ykb & \text{αν } k>0 \\ (-x)ka+(-y)kb & \text{αν } k<0 \end{cases}$

Αφού $d_1|ka$ και $d_1|kb \overset{(2)}{\Rightarrow} d_1\,|\,|k|d \Rightarrow d_1 \le |k|d$ (3)

Από (1) και (3) $\Rightarrow d_1 = |k|d$.

ΠΑΡΑΔΕΙΓΜΑ: Αν $\text{ΜΚΔ}(a,b) = 2 \Rightarrow \text{ΜΚΔ}(2018a, 2018b) = 2018\cdot 2 = 4036$.

ΟΡΙΣΜΟΣ: Έστω $a, b \in \mathbb{Z}$ όχι και οι δύο μηδέν. Οι a, b λέγονται πρώτοι μεταξύ τους ή σχετικά πρώτοι αν $ΜΚΔ(a,b) = 1$.

ΠΡΟΤΑΣΗ: Έστω $a, b \in \mathbb{N}$ και $d = ΜΚΔ(a,b)$. Τότε $\frac{a}{d} \in \mathbb{N}$, $\frac{b}{d} \in \mathbb{N}$ και $ΜΚΔ\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

ΑΠΟΔΕΙΞΗ: Αφού $d | a$ και $d, a > 0$ έπεται $\frac{a}{d} \in \mathbb{N}$. Ομοίως $\frac{b}{d} \in \mathbb{N}$

Από προηγούμενη πρόταση για $k = d$ έχουμε

$$ΜΚΔ\left(k\left(\frac{a}{d}\right), k\left(\frac{b}{d}\right)\right) = k\, ΜΚΔ\left(\frac{a}{d}, \frac{b}{d}\right) \Rightarrow$$

$$ΜΚΔ(a,b) = k\, ΜΚΔ\left(\frac{a}{d}, \frac{b}{d}\right) \Rightarrow d = d \cdot ΜΚΔ\left(\frac{a}{d}, \frac{b}{d}\right) \overset{d \neq 0}{\Rightarrow}$$

$$ΜΚΔ\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

ΠΑΡΑΔΕΙΓΜΑ: $ΜΚΔ(6, 9) = 3$. Άρα η πρόταση λέει $ΜΚΔ\left(\frac{6}{3}, \frac{9}{3}\right) = 1$ που ισχύει.

$ΜΚΔ(2,3)$

(Στόχος: $\sqrt{2} \notin \mathbb{Q}$)

ΟΡΙΣΜΟΣ: $\mathbb{Q} = \{u \in \mathbb{R}$ υπάρχει $e \in \mathbb{N}$ με $ue \in \mathbb{Z}\}$. Τα στοιχεία του $\mathbb{Q}$ λέγονται ρητοί αριθμοί.

ΠΡΟΤΑΣΗ: Έχουμε $\mathbb{Z} \subseteq \mathbb{Q}$, δηλαδή κάθε ακέραιος αριθμός είναι ρητός.

ΑΠΟΔΕΙΞΗ: Έστω $u \in \mathbb{Z}$. Για $e = 1 \in \mathbb{N}$, $u = u e \in \mathbb{Z}$. Άρα από τον ορισμό $u \in \mathbb{Q}$

ΠΑΡΑΔΕΙΓΜΑ: $u = \frac{1}{2} \in \mathbb{Q}$, γιατί $2 \in \mathbb{N}$ και $u \cdot 2 = 1 \in \mathbb{Z}$

ΠΡΟΤΑΣΗ: Έστω $u \in \mathbb{Q}$

(i) Αν $u > 0$, τότε υπάρχουν $a, b \in \mathbb{N}$ με $\text{ΜΚΔ}(a, b) = 1$ ώστε
$u = \frac{a}{b}$.

(ii) Αν $u < 0$, τότε υπάρχουν $a, b \in \mathbb{N}$ με $\text{ΜΚΔ}(a, b) = 1$ ώστε
$u = -\frac{a}{b}$

ΑΠΟΔΕΙΞΗ:

(1) Έστω $u \in \mathbb{Q}$ με $u > 0$. Τότε υπάρχει $e \in \mathbb{N}$ με $e u \in \mathbb{Z}$.
Θέτουμε $f = e u$. Αφού $u, e > 0 \Rightarrow f > 0$, άρα $f \in \mathbb{N}$.
Θέτουμε $d = \text{ΜΚΔ}(e, f)$. Θέτουμε $b = \frac{e}{d}$, $a = \frac{f}{d}$. Τότε από πρόταση $\text{ΜΚΔ}(a, b) = 1$ και $f = e u \Rightarrow da = dbu \overset{d \neq 0}{\Rightarrow} a = bu$
$\Rightarrow u = \frac{a}{b}$.

(2) Αφού $u < 0$ έχουμε $-u > 0$. Από το (1) υπάρχουν $a, b \in \mathbb{N}$ με $\text{ΜΚΔ}(a, b) = 1$ ώστε $-u = \frac{a}{b} \Rightarrow u = -\frac{a}{b}$

ΠΑΡΑΔΕΙΓΜΑ: Ο $u = \frac{6}{9} \in \mathbb{Q}$, γιατί $9u \in \mathbb{Z}$. Έχουμε $d = \text{ΜΚΔ}(6, 9) = 3$
Θέτουμε $a = \frac{6}{d} = 2$, $b = \frac{9}{d} = 3$, και $u = \frac{2}{3}$ με $2, 3 \in \mathbb{N}$
και $\text{ΜΚΔ}(2,3) \overset{d}{=} 1$.

ΟΡΙΣΜΟΣ: Έστω $y \in \mathbb{R}$ με $y>0$. Συμβολίζουμε με $\sqrt{y}$ (τετραγ. ρίζα του y) τον μοναδικό $x \in \mathbb{R}$ ώστε $x>0$ και $x^2=y$.

ΑΠΟΔΕΙΞΗ: Υποθέτουμε ότι $\sqrt{2} \in \mathbb{Q}$ και θα βρούμε αντίφαση. Αφού υποθέσαμε $\sqrt{2} \in \mathbb{Q}$ και $\sqrt{2}>0$, από Πρόταση υπάρχουν $a,b \in \mathbb{N}$ με $\text{ΜΚΔ}(a,b)=1$ και $\sqrt{2} = \frac{a}{b}$ (1).

Άρα (1) $\Rightarrow b\sqrt{2} = a \Rightarrow (b\sqrt{2})^2 = a^2 \Rightarrow 2b^2 = a^2$ (2)

Άρα $2 \mid a^2 \xRightarrow{2 \text{ πρώτος}} 2 \mid a$. Συνεπώς υπάρχει $k \in \mathbb{N}$ με $a = 2k$

Τότε η (2) $\Rightarrow 2b^2 = 4k^2 \Rightarrow 2k^2 = b^2 \Rightarrow 2 \mid b^2 \xRightarrow[2 \text{ πρώτος}]{} 2 \mid b$

$$\text{Άρα } \left.\begin{array}{l} 2 \mid a \\ \text{και } 2 \mid b \end{array}\right\} \Rightarrow 2 \mid \text{ΜΚΔ}(a,b) = 1 \text{ αντίφαση.}$$

ΠΑΡΑΤΗΡΗΣΗ: Αν $u = 16 \in \mathbb{N}$, $\sqrt{u} = 4 \in \mathbb{Q}$

ΕΡΩΤΗΜΑ: Έστω $k \in \mathbb{Z}$, $k \geq 2$. Πότε $\sqrt{k} \in \mathbb{Q}$ και πότε $\sqrt{k} \notin \mathbb{Q}$;

ΠΡΟΤΑΣΗ: Έστω $k \in \mathbb{Z}$, $k \geq 2$ με πρωτογενή ανάλυση $k = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ (δηλαδή p_i πρώτοι, $p_1 < p_2 < \dots < p_r$ και $a_i \in \mathbb{N}$).

(α) Αν $2 \mid a_i$ για κάθε i, τότε $\sqrt{k} \in \mathbb{Q}$, και μάλιστα $\sqrt{k} \in \mathbb{N}$.

(β) Αν υπάρχει i, με $1 \leq i \leq r$ ώστε a_i περιττός, τότε $\sqrt{k} \notin \mathbb{Q}$.

ΑΠΟΔΕΙΞΗ:

(1) Αφού $2 | a_i$ για κάθε i υπάρχει $b_i \in \mathbb{N}$ με $a_i = 2b_i$. Θέτουμε $x = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$. Τότε $x \in \mathbb{N}$, άρα $x \in \mathbb{Q}$ και $x^2 = (p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r})^2 = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r} p_1^{b_1} \cdots p_r^{b_r} = p_1^{b_1} \cdot p_1^{b_1} \cdot p_2^{b_2} \cdot p_2^{b_2} \cdots p_r^{b_r} p_r^{b_r} = p_1^{2b_1} \cdot p_2^{2b_2} \cdots p_r^{2b_r} = p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r} = K$

(Παράδειγμα: $K = 16 = 2^4$. Τότε $x = 2^2$)

(2) Υποθ. ότι υπάρχει i με $1 \leq i \leq r$ ώστε a_i περιττός. Υποθέτουμε ότι υπάρχει $q \in \mathbb{Q}$ με $q^2 = K$, και θα βρούμε αντίφαση.
Αφού $q \in \mathbb{Q}$ και $q > 0$, από πρόταση υπάρχουν $d, f \in \mathbb{N}$ με $ΜΚΔ(d,f) = 1$ ώστε $q = \frac{d}{f}$. Άρα $q \cdot f = d \Rightarrow (q \cdot f)^2 = d^2 \Rightarrow q^2 \cdot f^2 = d^2 \Rightarrow K f^2 = d^2$
Έστω $r_1 \geq 0$ η μέγιστη δύναμη του p_i που διαιρεί το f και
$r_2 \geq 0$ " " " " " " " d

Από $Kf^2 = d^2$ και μοναδικ. πρωτογενούς ανάλυσης έχουμε ότι $a_i + 2r_1 = 2r_2$. Άρα $a_i = 2r_2 - 2r_1$ άρτιος, αντίφαση.

ΠΑΡΑΔΕΙΓΜΑ:

(1) Είναι $\sqrt{20} \in \mathbb{Q}$ ή όχι. Έστω $K = 20$ - ΟΚ έχει πρωτογενή ανάλυση $K = 2^2 \cdot 5^1$. Αφού ο εκθέτης του 5 είναι 1 που είναι περιττός, έχουμε $\sqrt{K} \notin \mathbb{Q}$.

(2) Έστω $K = 9 \cdot 16$. Είναι $\sqrt{K} \in \mathbb{Q}$ ή όχι;
→ Η πρωτογενής ανάλυση του K είναι $K = 2^4 \cdot 3^2$
Κάθε εκθέτης άρτιος, άρα $\sqrt{K} \in \mathbb{Q}$ και μάλιστα $\sqrt{K} = 2^2 \cdot 3 = 12$.

ΦΥΛΛΑΔΙΟ 5 - ΑΣΚΗΣΗ 1.

Δείξτε ότι ο 211 είναι πρώτος

ΛΥΣΗ:

Βήμα - 1º: $14^2 = 196 \le 211 < 15^2 = 225$

Βήμα - 2º: Υπολογίζουμε όλους τους πρώτους ≤ 14. Είναι
$2, 3, 5, 7, 11, 13$

Βήμα - 3º: $2 \nmid 211$ προφανές
$3 \nmid 211$ γιατί $3 \nmid (2+1+1) = 4$
$5 \nmid 211$ γιατί το 211 δεν λήγει σε 0 ή 5
$7 \nmid 211$ Ευκλ. Διαίρεση $211 = 30 \cdot 7 + 1$
$11 \nmid 211$ " " $211 = 19 \cdot 11 + 2$
$13 \nmid 211$ " " $211 = 16 \cdot 13 + 3$

Άρα το 211 → πρώτος

ΦΥΛΛΑΔΙΟ 5 - ΑΣΚΗΣΗ 3.

Έστω $p, q, a \in \mathbb{N}$ με $p \neq q$ και p, q πρώτοι. Υποθέτουμε $p|a$ και $q|a$. Δείξτε ότι $p \cdot q | a$
(Επίσης δείξτε ότι δεν ισχύει γενικά αν p πρώτος αλλά q σύνθετος).

ΛΥΣΗ: Αφού p πρώτος, $p \geq 2$ και αφού $p|a \Rightarrow a \geq 2$. Άρα ο a έχει πρωτογενή ανάλυση, έστω $a = p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r}$

Αφού $p|a \Rightarrow p | p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r} \Rightarrow$ υπάρχει i_1 ώστε $p | p_{i_1} \Rightarrow p = p_{i_1}$

Αφού $q|a \Rightarrow q | p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r} \Rightarrow$ υπάρχει i_2 ώστε $q | p_{i_2} \Rightarrow q = p_{i_2}$

Αφού $p \neq q \Rightarrow i_1 \neq i_2$

Άρα $a = (p_1^{g_1} p_2^{g_2} \cdots p_r^{g_r})(p \cdot q)$ (*) όπου $g_i = c_i$ αν $i \neq i_1$ και $i \neq i_2$
και $g_i = c_i - 1$ αν $i = i_1$ ή $i = i_2$. Από (*) $p \cdot q | a$
(παράδ. αν $p = 5$, $q = 7$, $a = 3 \cdot 5^2 \cdot 7$ τότε $a = (3 \cdot 5)(5 \cdot 7)$)

Έστω τώρα $p = 2$, $q = 6$, $a = 6$. Ισχύει $p|a$, ισχύει $q|a$ αλλά
$p \cdot q = 12 \nmid a$

ΦΥΛΛΑΔΙΟ 5 - ΑΣΚΗΣΗ 4

Έστω $p, a, b \in \mathbb{N}$ με p πρώτο και $pb = a^2$ $(*)$. Δείξτε ότι $p|b$.

ΛΥΣΗ:

Αφού $p|a^2$ και p πρώτος $\Rightarrow p|a$. Άρα υπάρχει $k \in \mathbb{N}$ ώστε $a = kp$. Συνεπώς $(*) \Rightarrow pb = (kp)^2 \Rightarrow pb = k^2p^2 \underset{p\neq 0}{\Rightarrow}$ $b = k^2 p \Rightarrow p|b$.

ΥΠΕΝΘΥΜΙΣΗ: Έστω $a \in \mathbb{Z}$. Ο a λέγεται σύνθετος αν $a \geq 2$ και a όχι πρώτος.
πχ 4, 6, 8, 9...

ΠΡΟΤΑΣΗ: Έστω $a \geq 4$ άρτιος. Τότε a σύνθετος, αν $a \geq 2$.
Αφού άρτιος, υπάρχει $k \in \mathbb{Z}$ με $a = 2k$. Αφού $a \geq 4$ έπεται $k \geq 2$.
Άρα a σύνθετος.

ΦΥΛΛΑΔΙΟ 5 - ΑΣΚΗΣΗ 10

Έστω $k \in \mathbb{Z}$ με $k > 11$. Δείξτε ότι ο k είναι άθροισμα δύο σύνθετων.

ΛΥΣΗ:

Περίπτωση - 1: a άρτιος. Τότε $a > 11 \Rightarrow a - 4 > 7$ άρα
$a = 4 + (a-4)$ και $4, a-4$ σύνθετοι (γιατί $a-4$ άρτιος ≥ 4)

Περίπτωση - 2: a περιττός. Τότε $a-9$ άρτιος και $a > 11 \Rightarrow a - 9 > 2$
Άρα $a = 9 + (a-9)$ και $9, a-9$ σύνθετοι (γιατί $a-9$ άρτιος > 2)

ΥΠΕΝΘΥΜΙΣΗ: Αν $k \in \mathbb{Z}$ με $k \geq 2$ και πρωτογενή ανάλυση
$k = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$ από πρόταση το σύνολο S των θετικών διαιρετών του k είναι το $S = \{p_1^{b_1}, p_2^{b_2} \dots p_r^{b_r} : 0 \leq b_i \leq a_i \ \forall i\}$
και $\#S = (a_1+1) + (a_2+1) \dots (a_r+1)$ (όπου $\#S$ συμβολίζουμε τον αριθμό στοιχείων του S)
και γράφουμε $\tau(k) = \#S$

ΦΥΛΛΑΔΙΟ 5 - ΑΣΚΗΣΗ 7

Βρείτε όλους τους φυσικούς διαιρέτες του 28

ΛΥΣΗ

Έχουμε πρωτογενή ανάλυση $28 = 2^2 \cdot 7$. Από υπενθ. το σύνολο S των φυσικών διαιρετών του 28 είναι
$S = \{2^{b_1} \cdot 7^{b_2} : 0 \le b_1 \le 2,\ 0 \le b_2 \le 1\} =$
$= \{2^0 7^0 = 1,\ 2^0 7^1 = 7,\ 2^1 7^0 = 2,\ 2^1 7^1 = 14,\ 2^2 7^0 = 4,$
$2^2 \cdot 7^1 = 28\}$ και $\tau(28) = \#S = (2+1)(1+1) = 6$

$10! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 = 2 \cdot 3 \cdot 2^2 \cdot 5 \cdot 2 \cdot 3 \cdot 7 \cdot 2^3 \cdot 3^2 \cdot 2 \cdot 5 =$
$= 2^{(1+2+1+3+1)} \cdot 3^4 \cdot 5^2 \cdot 7^1 = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7.$

Άρα το σύνολο S των θετικών διαιρετών του $10!$ έχει $\tau(10!) =$
$= (8+1)(4+1)(2+1)(1+1) = 9 \cdot 5 \cdot 3 \cdot 2 = 270$ στοιχεία
και είναι $S = \{2^{b_1} \cdot 3^{b_2} \cdot 5^{b_3} \cdot 7^{b_4} : 0 \le b_1 \le 8,\ 0 \le b_2 \le 4,$
$0 \le b_3 \le 2,\ 0 \le b_4 \le 1\}$

ΦΥΛΛΑΔΙΟ 5 - ΑΣΚΗΣΗ 8

Να περιγραφούν όλοι οι φυσικοί αριθμοί οι οποίοι έχουν ακριβώς 2 ή 3 ή 4 θετικούς διαιρέτες

ΛΥΣΗ:

Ισχυρισμός - 1: Έστω κ φυσικός. Ο κ έχει ακριβώς 2 θετικούς διαιρέτες αν και μόνο αν κ πρώτος.

ΑΠΟΔΕΙΞΗ: Αν $\kappa = p$ πρώτος, έχει ακριβώς 2 φυσικούς διαιρέτες, το 1 και το p. Υποθέτουμε τώρα ότι κ φυσικός με ακριβώς 2 φυσικούς διαιρέτες. Φανερά $\kappa \neq 1$, γιατί το 1 έχει μόνο ένα φυσικό διαιρέτη. Άρα $\kappa \geq 2$. Αν κ σύνθετος υπάρχει d με $2 \le d \le \kappa - 1$ με $d | \kappa$. Άρα ο κ έχει τουλάχιστον 3 φυσικούς διαιρέτες το 1, το d και το κ. Άρα κ πρώτος.

Ισχυρισμός - 2: Έστω κ φυσικός. Ο κ έχει ακριβώς 3 φυσικούς διαιρέτες αν-ν υπάρχει πρώτος p με $k = p^2$.

ΑΠΟΔΕΙΞΗ: Έστω p πρώτος και $k=p^2$. Τότε $k=p^2$ είναι η πρωτογενής ανάλυση του κ. Άρα η πρόταση $\tau(k) = (2+1) = 3$ δηλ. ο κ έχει ακριβώς 3 φυσικούς διαιρέτες.

Υποθέτουμε τώρα ότι κ φυσικός με $\tau(k)=3$. Αφού $\tau(1) = 1 \Rightarrow k \geq 2$. Έστω $p_1, \dots, p_r$ οι πρώτοι διαιρέτες του κ και

$$k = p_1^{a_1} \dots p_r^{a_r}$$ η πρωτογενής ανάλυση (Υπενθ. $a_i > 0 \ \forall i$)

Από πρόταση $\tau(k) = (a_1+1)(a_2+1)\dots(a_r+1)$. Από υπόθεση $\tau(k)=3$. Άρα έχουμε γινόμενο ακεραίων καθένας ≥ 2 που είναι ίσο με 3. Αν το γινόμενο έχει ≥ 2 όρους, το γινόμενο είναι ≥ 4 και όχι ≥ 3. Αντίφαση.

Άρα $r=1$ και $a_1 + 1 = 3 \Rightarrow a_1 = 2$.

Συνεπώς $k = p_1^{a_1} = p_1^2$, δηλαδή κ τετραγ. πρώτου.

Ισχυρισμός - 3: Έστω κ φυσικός. Τότε ο κ έχει ακριβώς 4 φυσικούς διαιρέτες αν-ν κ γινόμενο δύο διαφορετικών πρώτων ή κ 3η δύναμη πρώτου.

ΑΠΟΔΕΙΞΗ: Έστω p, q διαφ. πρώτοι και $k = pq = p^1 q^1$

Τότε $\tau(k) = (1+1)(1+1) = 4$

Έστω p πρώτος και $k=p^3$. Τότε $\tau(k) = (3+1) = 4$.

Αντίστροφα, όπως προηγουμένως $k \geq 2$. Έστω $k = p_1^{a_1} \dots p_r^{a_r}$ η πρωτογενής ανάλυση. Τότε $4 = \tau(k) = (a_1+1)(a_2+1)\dots(a_r+1)$ και καθε $a_i + 1 \geq 2$.

Άρα αφού $2 \cdot 2 \cdot 2 = 8 > 4$, αναγκαστικά $r \leq 2$.

Περίπτωση 1: $r=2$.
Τότε $(a_1+1)(a_2+1)=4 \Rightarrow a_1=a_2=1$ και a κ γινόμενο δύο διαφορετικών πρώτων.

Περίπτωση 2: $r=1$
Άρα $a_1+1=4 \Rightarrow a_1=3$. Συνεπώς, και $3^{η}$ δύναμη πρώτου.