05/11/2018

Υπενθύμιση - 1: Αν $a \neq 0$ $ΜΚΔ(a,0) = |a|$

Υπενθύμιση - 2: Αν a, b όχι και τα δύο μηδέν, και $k \in \mathbb{Z}$, τότε

$ΜΚΔ(b,a) = ΜΚΔ(a,b) = ΜΚΔ(|a|,|b|)$

$ΜΚΔ(a,b) = ΜΚΔ(a, b-ka)$

Εφαρμογή.

$ΜΚΔ(10,32) = ΜΚΔ(10, 32-1\cdot10) = ΜΚΔ(10,2) = ΜΚΔ(2,10) =$

$= ΜΚΔ(2, 10-5\cdot2) = ΜΚΔ(2,0) = 2.$

Ευκλείδεια διαίρεση

Έστω $a, b \geq 1$ ακέραιοι. Ο ευκλείδειος αλγόριθμος υπολογίζει το $ΜΚΔ(a,b)$ και υπολογίζει $x, y \in \mathbb{Z}$ με $ΜΚΔ(a,b) = xa + yb$.

Βήμα -1ο: Θέτουμε $\alpha_1 = a$, $\alpha_2 = b$. Εκτελούμε Ευκλ. Διαίρεση
$\alpha_1 = r_1 \cdot \alpha_2 + \alpha_3$ με $0 \le \alpha_3 < \alpha_2$.
Άρα ΜΚΔ(a,b) = ΜΚΔ(α_1, α_2) = ΜΚΔ(α_2, α_3) και
(1) $\alpha_3 = \alpha_1 - r_1 \cdot \alpha_2$
Αν $\alpha_3 = 0$ τότε ΜΚΔ$(a,b) = \alpha_2$ και $\alpha_2 = 1 \cdot b$

Βήμα-2ο: Αν $\alpha_3 \neq 0$ Ευκλ. Διαίρεση του α_2 με το α_3
άρα $\alpha_2 = r_2 \alpha_3 + \alpha_4$ με $0 \le \alpha_4 < \alpha_3$.
Αν $\alpha_4 = 0$, τότε ΜΚΔ$(a,b) = \alpha_3$ και η (1) δίνει
γραμμή του ΜΚΔ(a,b) σαν γραμμή και $+yb$.

Βήμα-3ο: Αν $\alpha_4 \neq 0$ συνεχίζουμε με Ευκλ. Διαίρεση του α_3 με
το α_4 όπως στο βήμα 2.
Επειδή $\alpha_2 > \alpha_3 > \alpha_4 > \dots \ge 0$, ο αλγόρ. τερματίζει.

ΠΑΡΑΔΕΙΓΜΑ.
Βρείτε το ΜΚΔ$(104, 50)$ και $x, y \in \mathbb{Z}$ ώστε ΜΚΔ$(104,50) = x \cdot 104 + y \cdot 50$.

ΛΥΣΗ.
(Ευκλ. Αλγόριθμος)
Βήμα -1ο: Ευκλ Διαίρεση 104 με 50
Δηλ. $\alpha_1 = 104$, $\alpha_2 = 50$
$\alpha_3 = 4$, $\alpha_4 = 2$, $\alpha_5 = 0$.

$104 = 2 \cdot 50 + 4$ (1)
$50 = 12 \cdot 4 + 2$ (2)
$4 = 2 \cdot 2 + 0$ (3).

Συμπέρασμα -1: ΜΚΔ(104, 50) = 2 (γιατί 2 το τελευταίο υπόλοιπο που δεν είναι μηδέν)

(2) ⇒ 2 = 50 - 12·4 (1)⇒ 50 - 12(104 - 2·50) = (-12)·104 + 25·50

Άρα βρήκαμε x = -12, y = 25.

ΠΑΡΑΤΗΡΗΣΗ.

Τα x, y δεν είναι μοναδικά, αλλά εμείς πρόσεξε χρειαζόμαστε έναν μόνο ζεύγος x, y με ΜΚΔ(a, b) = xa + yb.

ΠΡΟΤΑΣΗ:

Έστω a, b ∈ ℕ και d_1 = ΜΚΔ(a, b) και d_2 ο ελάχιστος φυσικός που μπορεί να γραφεί στη μορφή $x_2 a + y_2 b$ με $x_2, y_2 \in \mathbb{Z}$

Τότε $d_1 = d_2$.

ΑΠΟΔΕΙΞΗ:

Από Ευκλ. Αλγόριθμο, υπάρχουν $x, y \in \mathbb{Z}$ με $xa + yb = d_1$. Συνεπώς,

$d_2 \leq d_1$ (1)

Έστω $d_2 = x_2 a + y_2 b$ με $x_2, y_2 \in \mathbb{Z}$

Αλλά $\left.\begin{matrix} d_2 / a \\ \text{και} \\ d_2 / b \end{matrix}\right\} \Rightarrow d_2 / x_2 a + y_2 b \Rightarrow \frac{d_1}{d_2} \Rightarrow d_1 \leq d_2$ (2)

Από (1), (2) ⇒ $d_1 = d_2$.

ΕΡΩΤΗΜΑ:

Έστω $a,b,c \in \mathbb{N}$ με $a|c$ και $b|c$. Ισχύει:

$ab|c$;

ΑΠΑΝΤΗΣΗ:

Όχι, για $a=b=c=2$.

ΠΡΟΤΑΣΗ:

Έστω $a,b,c \in \mathbb{N}$ με $a|c$ και $b|c$. Αν $ΜΚΔ(a,b)=1$, τότε $a,b|c$.

Απόδειξη: Αφού $ΜΚΔ(a,b)=1$ από Θεώρημα Bezout υπάρχουν $x,y \in \mathbb{Z}$ με $1=x\cdot a+yb$ (1).

Αφού $a|c$ υπάρχει $k_1 \in \mathbb{Z}$ με $c=k_1\cdot a$ (2)

Αφού $b|c$ " $k_2 \in \mathbb{Z}$ με $c=k_2\cdot b$ (3).

$(1) \Rightarrow c=c\cdot x\cdot a+cyb \overset{(2),(3)}{=} k_2bxa+k_1ayb =$

$=ab(k_2x+k_2y)$.

Άρα $a\cdot b|c$.

ΟΡΙΣΜΟΣ:

Έστω $p \in \mathbb{Z}$. Ο p λέγεται πρώτος αν $p \geq 2$ και οι μόνοι θετικοί διαιρέτες του p είναι οι αριθμοί 1 και p.

ΠΑΡΑΔΕΙΓΜΑ:

2: πρώτος, 3: πρώτος, 4: όχι πρώτος διότι $4=2\cdot 2$

5: πρώτος.

Πρόταση:

Έστω p πρώτος και $a \in \mathbb{Z}$. Έχουμε δύο περιπτώσεις.

- Περίπτωση 1: $p \mid a$. Τότε $\text{ΜΚΔ}(p,a) = p$
- Περίπτωση 2: $p \nmid a$ (δηλ. p ΔΕΝ διαιρεί το a). Τότε $\text{ΜΚΔ}(p,a) = 1$.

Απόδειξη

- Περίπτωση 1: Προφανώς αφού $p \mid a$ υπάρχει $k \in \mathbb{Z}$ με $a = kp$

άρα $\text{ΜΚΔ}(p,a) = \text{ΜΚΔ}(p, kp) = \text{ΜΚΔ}(p, kp - kp) =$
$\text{ΜΚΔ}(p,0) = |p| = p.$

- Περίπτωση 2: Υποθέτουμε $p \mid a$. Έστω $d = \text{ΜΚΔ}(p,a)$.

Αφού p πρώτος $d \mid p$ και $d \geq 1 \Rightarrow d = 1$ ή $d = p$.
Αν $d = p$, τότε $p \mid a$ αντίφαση. Άρα $d = 1$.

Πρόταση:

Έστω $a, b, c \in \mathbb{N}$ με $a \mid bc$ και $\text{ΜΚΔ}(a,b) = 1$. Τότε $a \mid c$.

Απόδειξη:

Αφού $\text{ΜΚΔ}(a,b) = 1$, υπάρχουν $x, y \in \mathbb{Z}$ με $1 = xa + yb$
Άρα $c = xac + ybc$ (1)
Αφού $a \mid bc$ υπάρχει $k \in \mathbb{Z}$ με $bc = ka$ (2)
(1) + (2) $\Rightarrow c = xac + yka = a(xc + yk) \Rightarrow a \mid c$.

Προσοχή:

Για $a = 4$, $b = c = 2$, έχουμε $a \mid b \cdot c$ αλλά $a \nmid b$ και $a \nmid c$.
Γιατί δεν εφαρμόζεται η πρόταση, γιατί $\text{ΜΚΔ}(a,b) = 2 \neq 1$.

Πόρισμα:
Έστω p πρώτος, $a, b \in \mathbb{N}$. Αν $p \mid a \cdot b$ τότε $p \mid a$ ή $p \mid b$
Με άλλα λόγια αν ένας πρώτος διαιρεί το γινόμενο δύο φυσικών, τότε διαιρεί τουλάχιστον έναν από αυτούς.

Απόδειξη
Έστω $p \nmid a$. Τότε $\text{ΜΚΔ}(p, a) = 1$, γιατί p πρώτος. Άρα από την προηγούμενη πρόταση $p \mid b$.

Παρατήρηση
Με ίδιο συλλογισμό αποδείξη το πόρισμα ισχύει και για $a, b \in \mathbb{Z}$.
Δηλαδή p πρώτος, $a, b \in \mathbb{Z}$ και $p \mid ab \Rightarrow p \mid a$ ή $p \mid b$.

Παρατήρηση:
Με επαγωγή έπαιρνε το εξής, Έστω p πρώτος και $a_1, \dots a_n \in \mathbb{Z}$.
Αν $p \mid a_1 a_2 \dots a_n$ τότε υπάρχει i με $p \mid a_i$.

Υπόμνηση. Τα παραπάνω χρειάζονται $p \neq$ Πρώτος.

Στόχος: Θεμελ. Θεώρημα Αριθμητικής.
Κάθε φυσικός $n \geq 2$ είναι πεπερ. γινόμενο πρώτων.

Ορισμός:
Έστω $m > 0$ και $a \in \mathbb{Z}$. Λέμε ότι ο a έχει "τη μορφή" $qm + r$, για $0 \leq a < r$. Αν r είναι το υπόλοιπο της Ευκλ. Διαίρεσης του a με το m.

ΠΑΡΑΔΕΙΓΜΑ-1:

$m=2$ και $a \in \mathbb{Z}$.

Τότε οι εκτός της μορφής $2q+0$ είναι οι άρτιοι

" οι " " " $2q+1$ " οι περιττοί

ΠΑΡΑΔΕΙΓΜΑ-2:

$m=4$.

Ο 1 έχει τη μορφή $4q+1$

Ο 15 " " " $4q+3$

Ο 22 " " " $4q+2$.

ΠΑΡΑΤΗΡΗΣΗ:

Έστω $m>0$ και $a \in \mathbb{Z}$. Τότε ο a έχει ακριβώς μια από τις ακόλουθες μορφές.

$$qm+0,\ qm+1,\ \ldots,\ qm+(m-1)$$

ΑΠΟΔΕΙΞΗ: Άμεσο από την ιδιαιτερότητα στην Ευκ. Διαίρεση.

ΠΡΟΤΑΣΗ: Το γινόμενο δύο ακεραίων της μορφής $2k+1$ είναι της μορφής $2k+1$.

ΑΠΟΔΕΙΞΗ: Αυτό σημαίνει ότι το γινόμενο δύο περιττών είναι περιττός που ισχύει.

ΠΑΡΑΔΕΙΓΜΑ: Το γινόμενο δύο ακεραίων της μορφής $6q+5$ είναι της μορφής $6q+1$.

Απόδειξη: Έστω a, b της μορφής $6q+5$

Άρα υπάρχουν $k_1, k_2 \in \mathbb{Z}$ με $a = 6k_1 + 5$

$b = 6k_2 + 5$

Άρα $a \cdot b = (6k_1+5)(6k_2+5) = 36k_1k_2 + 30k_1 + 30k_2 + 25$

$= 36k_1k_2 + 30k_1 + 30k_2 + 4 \cdot 6 + 1 = 6(6k_1k_2 + 5k_1 + 5k_2 + 4) + 1$

Άρα το ab είναι της μορφής $6q+1$.

Πρόταση: Έστω a περιττός. Τότε το a^2 είναι της μορφής $8k+1$.

Απόδειξη: Ο a διαιρούμενος με το 4 έχει μια από τις ακόλουθες μορφές: $4q$, $4q+1$, $4q+2$, $4q+3$.

Αφού ο a περιττός, ο a είναι της μορφής: $4q+1$ ή $4q+3$

Περίπτωση 1: Υπάρχει $k \in \mathbb{Z}$ με $a = 4k+1$. Τότε

$a^2 = (4k+1)^2 = 16k^2 + 8k + 1 = 8(2k^2+k) + 1$

Περίπτωση 2: Υπάρχει $k \in \mathbb{Z}$ με $a = 4k+3$. Τότε

$a^2 = (4k+3)^2 = 16k^2 + 24k + 9 = 16k^2 + 24k + 8 + 1 =$

$= 8(2k^2 + 3k + 1) + 1$

Άρα σε κάθε περίπτωση ο a^2 είναι της μορφής $8q+1$.