Υπενθύμιση: Αν $a, b \in \mathbb{Z}$ κ' $ab \neq 0$, τότε $(a-kb, a) \neq (0,0)$ κι

1) $(\text{ΜΚΔ}) = \text{ΜΚΔ}((a-kb), a)$

2) Αν $a \in \mathbb{Z}$, τότε $\text{ΜΚΔ}(a, 0) = \text{ΜΚΔ}(a)$

3) $\text{ΜΚΔ}(b, a) = \text{ΜΚΔ}(a, b)$

SOS Ευκλείδειος αλγόριθμος

Έστω $a, b \in \mathbb{Z}$ με $(a, b) \neq (0,0)$ ο παρακάτω αλγόριθμος υπολογίζει το $\text{ΜΚΔ}(a, b)$ κ' $x, y \in \mathbb{Z}$ ώστε $\text{ΜΚΔ} = xa + yb$

<u>Βήμα 1ο</u>: Θέτουμε $a_1 = a$ κ' $a_2 = b$. Εκτελούμε ευκλείδεια διαίρεση $a_1 = q_1 a_2 + a_3$ με $0 \le a_3 \le |q_1| - 1$

Έχουμε $ΜΚΔ(a,b) = ΜΚΔ(a_1,a_2) = ΜΚΔ(a_1 - q_1 a_2, a_2) = ΜΚΔ(a_3, a_2)$ κ'
$a_3 = a_1 - q_1 a_2 = a - q_1 b$

Αν $a_3 = 0$ $ΜΚΔ(a,b) = ΜΚΔ(a_3,a_2) = ΜΚΔ(0,b) = b$ κ' $b = 0\cdot a + 1\cdot b$ κ' σταματάμε

<u>Βήμα 2ο</u>: Έστω $a_3 \neq 0$ κάνουμε ευκλείδεια διαίρεση
$a_2 = q_2 a_3 + a_4$ με $0 \le a_4 < a_3 - 1$

Τότε: $ΜΚΔ(a_3 - a_2) = ΜΚΔ(a_3, a_2 - q_2 a_3) = ΜΚΔ(a_3, a_4)$ κ' $a_4 = a_2 - q_2 a_3 \overset{(x)}{=}$
$b - q_2(a - q_1 b) = (1 - q_2)a + (1 + q_1)b$

Αν $a_4 = 0$, τότε $ΜΚΔ(a,b) = a_3$ αν όχι, συνεχίζουμε την ίδια διαδικασία για το ζεύγος (a_3, a_4)

Ο αλγόριθμος τελειώνει γιατί $|a_2| > |a_3| > |a_4| >$ κ' επίσης δεν υπάρχει άπειρη γνησίως φθίνουσα ακολουθία μη αρνητικών ακεραίων, γιατί υπάρχουν ακριβώς $|a_2| + 1$ μη αρνητικοί ακέραιοι μεταξύ 0 κ' $|a_2|$

<u>π.χ.</u> Έστω $d = ΜΚΔ(104, 50)$ υπολογίστε το d κ' υπολογίστε $x, y \in \mathbb{Z}$ με
$$d = x104 + y50$$

<u>Ευκλείδειες διαιρέσεις</u>

$$\underset{a_1}{104} = 2\cdot \underset{a_2}{50} + \underset{a_3}{4} \quad (1)$$

$$50 = 12 \cdot \underset{a_3}{4} + \underset{a_4}{2} \quad (2)$$

$$4 = 2\cdot 2 + \underset{a_5}{0} \quad (3)$$

Αφού $a_5 = 0$ έχουμε $ΜΚΔ(104,50) =$ το τελευταίο μη μηδενικό υπόλοιπο της διαδικασίας = 2.

Υπολογισμός x, y

$(2) \Rightarrow 2 = 50 - 12\cdot 4 \overset{(1)}{=} 50 - 12(104 - 2\cdot 50) = 50(-12)\cdot 104 + (25)\,50$

Άρα θέτουμε $x = -12$, $y = 25$, άρα $d = -12x + 25y$

Πρόταση: Έστω $a, b \in \mathbb{Z}$ με $(a,b) \neq (0,0)$. Τότε ο ΜΚΔ(a,b) είναι ο ελάχιστος θετικός ακέραιος που μπορεί να γραφεί στη μορφή $xa + yb$ με $x, y \in \mathbb{Z}$

Απόδειξη: Θέτουμε $d =$ ΜΚΔ(a,b). Από τον ευκλείδιο αλγόριθμο υπάρχουν $x, y \in \mathbb{Z}$ με $d = xa + yb$. Έστω τώρα e θετικός ακέραιος με την ιδιότητα ότι υπάρχουν $x', y' \in \mathbb{Z}$ με $e = x'a + y'b$. ΝΔΟ $d \leq e$.
Πράγματι,

$$\left.\begin{array}{l} d / a \\ d / b \\ e = x'a + y'b \end{array}\right\} \xRightarrow{\text{πρόταση}} d / e \xrightarrow[e>0]{d>0} d \leq e$$

π.χ. Βρείτε τον ελάχιστο θετικό ακέραιο που γράφεται στη μορφή $x\cdot 104 + y\cdot 50$ με $x, y \in \mathbb{Z}$

Λύση: Από την πρόταση, αυτός ο ΜΚΔ$(104, 50)$ που είναι ίσος με 2 από το προηγούμενο παράδειγμα

Ορισμός: Έστω $a, b \in \mathbb{Z}$ με $(a,b) \neq (0,0)$. Οι a, b λέγονται πρώτοι μεταξύ τους αν ΜΚΔ$(a,b) = 1$.

π.χ. Αφού ΜΚΔ$(10,3) = 1$ οι $3, 10$ είναι πρώτοι μεταξύ τους.
ΜΚΔ$(104,50) = 2$. Οι 104 κ' 50 δεν είναι πρώτοι μεταξύ τους.

Πρόταση: Έστω $a,b,c \in \mathbb{N}$ κ' a/bc. Αν $ΜΚΔ(a,b)=1$, τότε a/c

Απόδειξη: Αφού a/bc $\exists \kappa \in \mathbb{Z}$ με $bc=\kappa a$. Αφού $ΜΚΔ(a,b)=1$

$\exists x,y \in \mathbb{Z}$ με $1 = xa+yb$ (1)

(2) $\Rightarrow c = xac + ybc \overset{(1)}{=} xac + y\kappa a = a(xc+y\kappa)$, άρα a/c

Προσοχή. ΠΑΡΑΤΗΡΗΣΗ: Η υπόθεση $ΜΚΔ(a,b)=1$ δεν μπορεί να παραληφθεί.

Για π.χ $a=4, b=2, c=2$, έχουμε a/bc, αλλά $a \nmid c$, γιατί $4 \nmid 2$

ΠΑΡΑΤΗΡΗΣΗ: Η απόδειξη της προηγούμενης πρότασης είναι το γενικό τύπο.
Έστω $a,b,c \in \mathbb{Z}$ με $a \neq 0$ κ' a/bc. Αν $ΜΚΔ(a,b)=1$, τότε a/c

Πρόταση: Έστω $a,b,c \in \mathbb{Z}$ με $a \neq 0$ κ' $b \neq 0$. Αν ab/c κ' $ΜΚΔ(b,c)=1$
τότε a/c

ΠΡΩΤΟΙ ΑΡΙΘΜΟΙ

Ορισμός: Έστω $\kappa \in \mathbb{Z}$. Ο κ λέγεται πρώτος αν $\kappa \geq 2$ κ' οι μόνοι θετικοί διαιρέτες είναι οι 1 κ' "κ".

ΠΡΟΣΟΧΗ: Το 1 δεν είναι πρώτος.

π.χ. $2,3$ πρώτοι 4 όχι πρώτος
$5,7,11$ πρώτοι

ΠΑΡΑΤΗΡΗΣΗ: Έστω $p \in \mathbb{Z}$ κ' πρώτος κ' $a \in \mathbb{Z}$.
(i) Αν a είναι πολλαπλάσιο του p, τότε $ΜΚΔ(a,p)=p$.
(ii) Αν το a δεν είναι πολλαπλάσιο του p, τότε $ΜΚΔ(p,a)=1$.

Απόδειξη: (i) Αφού $p|a$ $\exists \kappa \in \mathbb{Z}$ με $a=\kappa p$. Συνεπώς, $ΜΚΔ(p,a) = ΜΚΔ(p, a-\kappa p)$
$= ΜΚΔ(p,0) = p$.

(ii) Υποθέτουμε α όχι πολλαπλάσιο του p. Θέτουμε $d = ΜΚΔ(p,\alpha)$. Άρα $d \geq 1$ κ' $d|p$ κ' p πρώτος έχουμε $d=p$ ή $d=1$

Αν $d=p$, αφού $d|\alpha$ έπεται $p|\alpha$, άτοπο. Άρα $d=1$

<u>Πρόταση</u>: Έστω p πρώτος $\alpha, b \in \mathbb{Z}$ κ' $p|\alpha b$, τότε $p|\alpha$ ή $p|b$

<u>Απόδειξη</u>: Αν $p|\alpha$ η πρόταση ισχύει.
Υποθέτουμε $p \nmid \alpha$, τότε από την προηγούμενη πρόταση $ΜΚΔ(p,\alpha)=1$. Συνεπώς, από πρόταση $p|\alpha b$ συνεπάγεται $p|b$

<u>Πόρισμα</u>: Έστω p πρώτος κ' $n \geq 1$ κ' $\alpha_1, \dots, \alpha_n \in \mathbb{Z}$. Αν $p|(\alpha_1 \alpha_2 \dots \alpha_n)$, τότε $\exists i$ με $1 \leq i \leq n$, ώστε $p|\alpha_i$.

<u>Απόδειξη</u>: Με επαγωγή στο $n \geq 1$

<u>Βήμα 1ο</u>: Έστω $n=1$. Τότε $p|\alpha_i$, άρα $p|\alpha_1$

<u>Βήμα 2ο</u>: Υποθέτουμε $n \geq 1$ κ' ότι αν το p διαιρεί το γινόμενο n ακεραίων τότε διαιρεί τουλάχιστον έναν από αυτούς.
Έστω $\alpha_1, \dots, \alpha_n, \alpha_{n+1} \in \mathbb{Z}$ κ' $p|(\alpha_1 \alpha_2 \dots \alpha_n \alpha_{n+1})$.

Τότε $p|\alpha_1(\alpha_2 \dots \alpha_{n+1})$. Άρα η πρόταση: $p|\alpha_1$ ή $p|(\alpha_2 \alpha_3 \dots \alpha_{n+1})$

Αν $p|\alpha_1$ τελειώσαμε. Αν $p|\alpha_2 \dots \alpha_{n+1}$ από την υπόθεση της επαγωγής $\exists i$ με $2 \leq i \leq n+1$, ώστε $p|\alpha_i$. Συνεπώς από την αρχή της μαθηματικής επαγωγής το πόρισμα ισχύει.

<u>ΠΑΡΑΤΗΡΗΣΗ</u>: Άρα αν ο πρώτος διαιρεί ένα γινόμενο ακεραίων, τότε διαιρεί τουλάχιστον έναν από αυτούς τους παράγοντες

<u>Ορισμός</u>: Ένας ακέραιος λέγεται σύνθετος αν δεν είναι πρώτος. Αν $\alpha \geq 2$ κ' δεν είναι πρώτος

<u>πχ.</u>: Αριθμοί $4, 6, 8, 9, 10, 12, 14, 15$ είναι σύνθετοι.

Έστω $\alpha \in \mathbb{Z}$ σύνθετος, τότε $\exists\, b, b' \in \mathbb{Z}$ με $2 \leq b$ κ' $2 \leq b'$ ώστε $\alpha = bb'$

πχ $\quad 4 = 2 \cdot 2 \quad 12 = 3 \cdot 4$

<u>Στόχοι</u>: 1) Υπάρχουν άπειροι το πλήθος πρώτοι.
2) Κάθε ακέραιος ≥ 2 γράφεται με ουσιαστικά μοναδικό τρόπο σαν γινόμενο πρώτων

<u>Πρόταση</u>: Έστω $\alpha \in \mathbb{Z}$ με $\alpha \geq 2$. Τότε υπάρχει πρώτος p, με $p \mid \alpha$

<u>Απόδειξη</u>: Έστω ότι δεν ισχύει. Τότε το σύνολο $S = \{\alpha \in \mathbb{Z}$, με $\alpha \geq 2$ κ' δεν έχει πρώτο διαιρέτη$\}$ είναι μη κενό.
Αφού S φραγμένο κάτω, αυτό το 1, μη κενό υποσύνολο του $\mathbb{Z}$ το S έχει ελάχιστο στοιχείο, έστω $\alpha_0 \in S$
→ Αν το α_0 είναι πρώτος, τότε έχει πρώτους διαιρέτες το α_0, άρα $\alpha_0 \notin S$, άτοπο.
→ Συνεπώς, α_0 σύνθετος. Άρα $\exists\, b_1, b_2 \in \mathbb{Z}$ με $b_1 \geq 2, b_2 \geq 2$ ώστε $\alpha_0 = b_1 b_2$

Άρα $b_1 < \alpha_0$. Όμως αφού α_0 το ελάχιστο στοιχείο του S, τότε $b_1 \notin S$, άρα $\exists$ πρώτος p με $p \mid b_1$

Συνεπώς, $\left.\begin{matrix} b_1 \mid \alpha_0 \\ p \mid b_1 \end{matrix}\right\} p \mid \alpha_0$, άρα $\alpha_0 \notin S$, άτοπο.

<u>Πρόταση</u>: Έστω $\alpha_1, \alpha_2, \ldots, \alpha_s$ ακέραιοι μεγαλύτεροι ή ίσοι του δύο. Τότε $\forall i$, με $1 \leq i \leq s$, ισχύει α_i <u>δεν διαιρεί</u> το $(\alpha_1 \cdot \alpha_2 \cdots \alpha_s) + 1$

Απόδειξη: Έστω i με $1 \le i \le 5$.
Τότε $a_1 \cdots a_5 + 1 = (a_1 \cdots a_{i-1} a_{i+1} \cdots a_5) a_i + 1$

Συνεπώς, το υπόλοιπο της Ευκλείδειας διαίρεσης του $a_1 \cdots a_5 + 1$ με το a_i είναι ίσο με 1. Άρα $a_i \nmid (a_1 \cdots a_5) + 1$.

π.χ. Έστω $k = 4 \cdot 5 \cdot 9 + 1$. Τότε $4 \nmid k$ κ' $5 \nmid k$ κ' $9 \nmid k$

Θεώρημα: Το σύνολο των πρώτων αριθμών είναι άπειρο (ισοδύναμα, δεν είναι φραγμένο άνω).

Απόδειξη: Έστω ότι B όχι άπειρο σύνολο. Τότε $\exists$ πρώτοι αριθμοί $p_1, p_2, \dots, p_r$ ώστε $B = \{p_1, p_2, \dots, p_r\}$. (φανερά $B \neq \emptyset$, γιατί $2 \in B$)

Θέτουμε $k = (p_1 \cdot p_2 \cdots p_r) + 1$
Αφού κάποιο p_i είναι ίσο με 2, έχουμε $k \geq 3 > 2$

Από πρόταση $\exists$ πρώτος p με $p \mid k$.
Άρα $p \in B$, συνεπώς $\exists\, i$ με $1 \le i \le r$ ώστε $p = p_i$. Άρα από πρόταση, $p \nmid k$, άτοπο.

Πόρισμα: Έστω $k \in \mathbb{Z}$. Τότε $\exists$ πρώτος p με $p > k$.

Ερώτημα: Ποιος είναι ο μεγαλύτερος πρώτος αριθμός που ξέρουμε μέχρι τώρα;

Απάντηση: (25/1/2013): $a = 2^{57885161} - 1$
(τότε ήταν ο μεγαλύτερος. Έχει βρεθεί μεγαλύτερος)

Έχει 17.425.170 ψηφία