π.χ. μ.κ.δ.(1453, 1204) 9/11/17

$1453 = 1 \cdot 1204 + 249$
$1204 = 4 \cdot 249 + 208$
$249 = 1 \cdot 208 + 41$
$208 = 5 \cdot 41 + 3$
$41 = 3 \cdot 13 + 2$ Άρα μ.κ.δ.$(1453, 1204) = 1$
$3 = 1 \cdot 2 + 1$

$1 = 3 - 2 = 3 - (41 - 3 \cdot 13) = 14 \cdot 3 - 41 = 14(208 - 5 \cdot 41)$
$- 41 = 14 \cdot 208 - 71 \cdot 41 = 14 \cdot 208 - 71(249 - 208) =$
$= 85 \cdot 208 - 71 \cdot 249 = 85(1204 - 4 \cdot 249) - 71 \cdot$
$249 = 85 \cdot 1204 - 411(1453 - 1204) =$
$= 296 \cdot 1204 - 411 \cdot 1453$

Ασκ. π.χ. Βρείτε τον μ.κ.δ.(105, 75, 35) κ' γράψτε τον σαν γραμμικό συνδυασμό των 105, 75 κ' 35.
Λύση: Δηλαδή θέλουμε ν.δ. τον μ.κ.δ.(105, μ.κ.δ.(75, 35))

μ.κ.δ.(75, 35) $\rightarrow 75 = 2 \cdot 35 + 5$
$35 = 7 \cdot 5 + 0$

Άρα μ.κ.δ.(105, 5) $\rightarrow 105 = 21 \cdot 5 + 0$ Άρα
μ.κ.δ.(105, 5) = 5

Θεώρημα: Έστω p πρώτος και a, b ακέραιοι. Αν $p | ab$ τότε $p | a$ ~~και~~ ή $p | b$.
Απόδειξη: μ.κ.δ.$(a, p) = 1$ ή μ.κ.δ.$(a, p) = p$
1η περίπτωση: μ.κ.δ.$(a, \beta) = p \Rightarrow p | a$

2η περίπτωση: μ.κ.δ.$(a, p) = 1 \Rightarrow 1 = \kappa a + \lambda p$

$1 = \kappa a + \lambda p \Rightarrow b = \kappa a b + \lambda p b = p(\kappa q + \lambda b) \Rightarrow p | b$
$p | ab \Rightarrow ab = qp$ (1) $q \in \mathbb{Z}$

Θεώρημα: Έστω p πρώτος αριθμός κ' $a_1, a_2, \dots, a_n$ ακέραιοι. Αν $p | a_1 \dots a_n$ τότε $p | a_1$
ή
⋮
$p | a_n$

$a_1 (a_2 \dots a_n)$

$p | a_1$ ή $p | a_2 \dots a_n$ Απόδειξη με επαγωγή στο n.

Θεώρημα: Κάθε φυσικός αριθμός $n > 1$ μπορεί να γραφτεί σαν γινόμενο πεπερασμένου πλήθους πρώτων αριθμών όχι απαραίτητα διαφορετικών μεταξύ τους.

Απόδειξη: Επαγωγή στο n

• $n = 2$ $2 = 2$ που ισχύει

• Υποθέτω ότι η πρόταση ισχύει για όλους τους αριθμούς m τ.ω. $1 < m < n$ Θ.δ.ο ισχύει για το n.

$n > 1$ i) περίπτωση n πρώτος : $n = p$

ii) περίπτωση n σύνθετος :

$n = ab$ $1 < a < n$

$1 < b < n$

$1 < a < n$ άρα από την υπόθεση της επαγωγής $a = p_1 p_2 \dots p_s$ πρώτοι

$1 < b < n$ ——— ” ——— $b = q_1 q_2 \dots q_k$ —”—

$n = a \cdot b = p_1 p_2 \dots p_s q_1 q_2 \dots q_k$

Άρα το n είναι γινόμενο πεπερασμένου πλήθους πρώτων αριθμών

Άρα η πρόταση ισχύει για το n. Συνεπώς κάθε φυσικός $n > 1$ γράφεται σαν γινόμενο πεπερασμένου πλήθους πρώτων αριθμών.

Θεμελιώδες Θεώρημα της Αριθμητικής:
Κάθε φυσικός $n>1$ γράφεται με μοναδικό τρόπο σαν γινόμενο πρώτων αριθμών, αν δεν λάβουμε υπόψιν τη σειρά των παραγόντων.

Απόδειξη: $n = p_1 p_2 \dots p_s$, $p_1 \le p_2 \le \dots \le p_s$
$n = q_1 q_2 \dots q_s$, $q_1 \le q_2 \le \dots \le q_s$ $\Big\} \overset{\text{Θ.ν.δ.ο.}}{\Rightarrow}$

$p_1 = q_1$, $p_2 = q_2$, $\dots$ $p_s = q_t$, $s = t$

Επαγωγή στο n
Για $n=2$ $2=2$, ισχύει
Υποθέτουμε ότι ισχύει για κάθε $1<m<n$
Θ.δ.ο. ισχύει για n.

$n = p_1 p_2 \dots p_s$, p_i πρώτοι $p_1 \le p_2 \dots \le p_s$
$n = q_1 q_2 \dots q_t$, q_i ~~...~~ πρώτοι $q_1 \le q_2 \dots \le q_t$

$p_1 / n = q_1 q_2 \dots q_t \Rightarrow p_1 / q_j = p_1$ (το $p_1 > 1$, p_1 / q_j κ' το q_j πρώτος $\Rightarrow$ ο διαιρέτης του q_j είναι το 1 και το q_j $\Rightarrow p_1 = q_j$)
πρώτος

$q_1 / n = p_1 p_2 \dots p_s \Rightarrow q_1 / p_\lambda \Rightarrow q_1 = p_\lambda$
πρώτος $1 \le \lambda \le s$

Ξέραμε $p_1 = q_j \geq q_1 = p_\lambda \geq p_1 \Rightarrow p_1 = q_1$ (Επειδή ο πρώτος και ο τελευταίος των ανισοτήτων ταυτίζονται)

κ $\dfrac{n}{p_1} = \dfrac{n}{q_1} < n$ Άρα από την υπόθεση της επαγωγής ο $\frac{n}{p}$ γράφεται με μοναδικό τρόπο ως γινόμενο πρώτων

$n/p_1 = p_2 \dots p_s$
$n/q_1 = q_2 \dots q_t$ $\Big\} \Rightarrow p_2 = q_2 \dots p_s = q_s = q_t$

$n = p_1^{n_1} p_2^{n_2} \dots p_r^{n_s}$
$p_i \ne p_j$ αν $i \ne j$ πρωτογενής ανάλυση του n

6

Παράδειγμα: Βρείτε την πρωτογενή ανάλυση των αριθμών: $999 = 9 \cdot 111 = 3^2 \cdot 3 \cdot 37 = 3^3 \cdot 37 = 37 \cdot 3^3$

$1024 = 2 \cdot 512 = 2 \cdot 2 \cdot 256 = 2^{10}$

$250 = 2 \cdot 125 = 2 \cdot 5 \cdot 25 = 2 \cdot 5^3$

Θεώρημα: Έστω $\alpha = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$ η πρωτογενής ανάλυση ενός φυσικού $\alpha > 1$. Ο φυσικός δ είναι διαιρέτης του αριθμού α αν-ν $\delta = p_1^{\delta_1} p_2^{\delta_2} \cdots p_s^{\delta_s}$ από

$0 \le \delta_1 \le a_1$

$0 \le \delta_2 \le a_2$

$\vdots$

$0 \le 0 \le \delta_s < a_s$

π.χ. $250 = 2^1 \cdot 2^3$

$\delta = 2^{\delta_1} \cdot 5^{\delta_2}$

$0 \le \delta_1 \le 1 \Rightarrow \delta_1 = 0$ ή $\delta_1 = 0$

$0 \le \delta_2 \le 3 \Rightarrow \delta_2 = 0, 1, 2, 3$

Διαιρέτες του 250

$\{ 2^0 \cdot 5^0, 2^0 \cdot 5^1, 2^1 \cdot 5^2, 2^0 \cdot 5^3, 2^1 \cdot 5^0, 2^1 \cdot 5^1, 2^1 5^1, 2^1 \cdot 5^3 \}$