

12/03/15.

ΘΕΜΕΛΙΩΔΕΣ ΘΕΩΡΗΜΑ ΤΗΣ ΑΡΙΘΜΗΤΙΚΗΣ

Θεώρημα: Κάθε θετικός ακεραίος $\alpha > 1$ μπορεί να γραφεί μοναδικά ως γινόμενο πεπερασμένου πλήθους πρώτων αριθμών.

Παρένθεση: $X =$ όλοι οι άρτιοι θετικοί ακεραίοι.

Ένας αριθμός ο οποίος ανήκει στο X , δηλ ένας άρτιος, καλείται "πρώτος" ($\Rightarrow$) δεν μπορεί να γραφεί ως γινόμενο δύο άλλων αριθμών στο X .

$10 = 2 \cdot 5 \Rightarrow 10$ πρώτος στο σύνολο X (αφού $5 \notin X$)

$8 = 2 \cdot 4 \Rightarrow 8$ σύνθετος στο σύνολο X .

$60 = 6 \cdot 10$ (γινόμενο "πρώτων") } γινόμενα "πρώτων" (στο X) και η γραφή
 $60 = 2 \cdot 30$ (-// -) } δεν είναι μοναδική.

Απόδειξη: (Υπαρξη): Αν $\alpha = 2$, τότε 20α είναι γινόμενο πρώτων αριθμών κατά τετραγώνον τρόπο.

• Επαγωγική υπόθεση: Υποθέτουμε ότι το θεώρημα ισχύει (αφορά την ύπαρξη) $\forall m \in \mathbb{N}: 2 \leq m < \alpha$.

• Γενική περίπτωση: Έστω $\alpha \geq 2$. Αν α πρώτος τότε ο α γράφεται κατά τετραγώνον τρόπο ως γινόμενο πρώτων αριθμών.

Έστω ότι α : σύνθετος. $\Rightarrow \alpha = \lambda \cdot \kappa$, $\lambda, \kappa \neq 1$ και $\lambda, \kappa \in (1, \alpha)$

Από την επαγωγική υπόθεση $\Rightarrow \kappa = p_1 \cdot \dots \cdot p_n$, όπου $p_1, \dots, p_n$ πρώτοι
 $\lambda = q_1 \cdot \dots \cdot q_s$, όπου $q_1, \dots, q_s$ πρώτοι } $\Rightarrow$

$\Rightarrow \alpha = p_1 \cdot \dots \cdot p_n \cdot q_1 \cdot \dots \cdot q_s$ γινόμενο πρώτων αριθμών.

Άρα το θεώρημα (ως προς την ύπαρξη) ισχύει $\forall \alpha \geq 1$.

Θεώρημα: Έστω p : πρώτος και $(a, b) \in \mathbb{Z}^2$. Τότε $p \mid a \cdot b \Rightarrow$
(Ευκλείδης) $\Rightarrow p \mid a$ ή $p \mid b$.

Απόδειξη: • Αν $a=0$ ή $b=0$ τότε ο ιερχυρισμός ιεχθεί κατ'ε
τεταγμένο τρόπο.

• Επειδή $\forall x \in \mathbb{Z} : P|x \Leftrightarrow P| |x|$, μπορούμε να περιοριστούμε σε θε-
τικούς ακέραιους a, b .

Έστω $a, b \geq 1$. Θεωρούμε το σύνολο $X = \{x \in \mathbb{N} : P|ax\}$

Θα έχουμε ότι $X \neq \emptyset$ διότι $\underbrace{P \in X}$ κ' $\underbrace{b \in X}$
άρα υποθέτουμε

Από (ΑΚΔ) $\Rightarrow$ το X έχει ελάχιστο στοιχείο: $\theta = \min X$.

δηλαδή $\theta \in X \Rightarrow P|a \cdot \theta$ κ' $\forall x \in X \Rightarrow \theta \leq x$.

Ιεχυρισμός: $\forall x \in X : \theta | x$

Απόδειξη ιεχυρισμού: Από την ευκλείδεια διαίρεση του x με το θ
ιεχθεί: $\exists x = \theta \cdot q + r$, με $0 \leq r < \theta$. Αρκεί νδο $r=0$.

Έστω $r \neq 0$. Αρκεί νδο $r \in X$ κ' θα έχω άτοπο.

Είναι: $x = \theta \cdot q + r \Rightarrow ax = a\theta \cdot q + a \cdot r$
 $x \in X \Rightarrow P|ax$
 $\theta \in X \Rightarrow P|a \cdot \theta \Rightarrow P|a \cdot \theta \cdot q$ } $\Rightarrow$ (το P θα διαίρει
τη διαφορά τους).

$\Rightarrow P|a \cdot r$
 $r \geq 1$ } $\Rightarrow r \in X$ άτοπο αφού $r < \theta$ κ' $\theta = \min X$.

άρα $r=0$ δηλ $x = \theta \cdot q \Rightarrow \theta | x$
άρα αποδείξαμε τον ιεχυρισμό.

Επειδή $P \in X$, από τον ιεχυρισμό $\Rightarrow \theta | P$
 P : πρώτος } $\Rightarrow \theta = 1$ ή $\theta = P$

$\theta = 1 \Rightarrow P|a \cdot \theta \Rightarrow P|a \cdot 1 \Rightarrow P|a$ (διότι $\theta \in X$). Άρα αν $\theta = 1 \Rightarrow P|a$

$\theta = P \Rightarrow$ επειδή $b \in X$ θα έχουμε, από τον ιεχυρισμό ότι: $P = \theta | b \Rightarrow$
 $\Rightarrow \theta = P \Rightarrow P|b$.

Πρόταση: Έστω P πρώτος και $a_1, \dots, a_n \in \mathbb{Z}$. Τότε:

$P|a_1 \dots a_n \Rightarrow \exists i = 1, \dots, n : P|a_i$

Απόδειξη: • Αν $n=1$, τότε $P|a_1$, ιεχθεί

• Αν $n=2$, τότε το αποτέλεσμα ιεχθεί από το θεωρήμα.

• Επαγωγική Υπόθεση: Το αποτέλεσμα ιεχθεί για n το πλήθος

$\rightarrow$

ακεραίους $\alpha_1, \dots, \alpha_m$ όντα $1 \leq m \leq n$. Δηλαδή $P | \alpha_1 \dots \alpha_m \Rightarrow$
 $\Rightarrow \exists i=1, \dots, m : p | \alpha_i$

• První napřewy : $P \mid d_1 \dots d_n = (d_1 \dots d_{n-1}) \cdot d_n \Rightarrow$
 En zp. wšedem $\rightarrow$ $\left\{ \begin{array}{l} P \mid d_1 \dots d_{n-1} \Rightarrow \exists k=1, \dots, n-1 : P \mid d_k \quad (1) \\ d_n \end{array} \right.$
 $\left\{ \begin{array}{l} P \mid d_n \quad (2) \end{array} \right.$

доказано 1, 2 $\Rightarrow \exists i=1, \dots, n : P/d_i$

Πορίσματα: Έστω P πρόταση κ' $P_1, \dots, P_n$ πρότασις. Τότε:

$$P \wedge P_1 \wedge \dots \wedge P_n \Rightarrow \exists i=1, \dots, n: P = P_i$$

Απόδειξη : Έχουμε $P \mid P_1 \dots P_n \xrightarrow{\text{Παρίσταται}} \exists i=1, \dots, n : P \mid P_i$ Επειδή P_i : πρώτος
έπεται ότι $P = P_i$. $\square$

Θεώρημα: [Θεμελιώδες Θεώρημα Αριθμητικής] (Μοναδικότητα)
 Η γραφή ενός θετικού ακεραίου $a > 1$ σε γινόμενο πρώτων
 αριθμών είναι μοναδική, δηλαδή:

$\alpha = p_1 \cdot p_2 \cdot \dots \cdot p_m$, όπου $p_1, \dots, p_m$ πρώτοι

$\alpha = q_1 \cdot \dots \cdot q_m$, όπου $q_1, \dots, q_m$ πρώτοι.

$\Rightarrow n = m$
και κάθε ηρώος $P_i = q_j$
 $\hat{c} = 1, \dots, m$
 $\hat{j} = 1, \dots, n$

Ανέδειξη: Μπορούμε να υποθέσουμε ότι $P_1 \leq P_2 \leq \dots \leq P_m$
 $q_1 \leq q_2 \leq \dots \leq q_n$ } (*)
 & μπορούμε ότι P_i, q_j πρώτοι $\forall i=1, \dots, m, j=1, \dots, n$.

• Av $\alpha=2$ zolt enedh 2 nplwos $\Rightarrow \alpha=2=P_1=q, \kappa' n=w=1$

• Αν $n \geq 2$, θα έχουμε την ΕΠΑΓΟΓΙΚΗ ΥΠΟΘΕΣΗ: Υποθέτουμε ότι το ευκλείδειο ισχύει μέχρι $n-1$ ακέραιοι $m: 2 \leq m < n$.

- Permutation $\alpha = p_1 \dots p_m = q_1 \dots q_n$

Tότε το $p_1 | q_1, \dots, q_n$. Αν το όμοιο $\Rightarrow \exists r=1, \dots, n$
τέτοιος ώστε $p_1 = q_r$ ①

Παρόμοια $q_1, p_2, \dots, p_m \Rightarrow JS = 1, \dots, m : q_1 = p_s. \textcircled{2}$

Τότε: $p_1 \cdot \textcircled{*} p_s \cdot \textcircled{2} = q_1 \cdot \textcircled{*} q_r = p_1 \Rightarrow \boxed{p_1 = q_1} = p_s = q_r$

Επειδή $p_1 = q_1$ κ' $\alpha = \cancel{p_1} \cdot \dots \cdot p_m = \cancel{q_1} \cdot \dots \cdot q_n$ και άρα θα έχω

$b = p_2 \cdot \dots \cdot \cancel{p_m} = q_2 \cdot \dots \cdot \cancel{q_n}$ κ' $b < \alpha$ και άρα από
επαγωγική υπόθεση θα είναι $m-1 = n-1 \Rightarrow \boxed{m=n}$

Επίσης κάθε πρώτος από τους $p_2, \dots, p_m$ είναι ίσος με κάποιον
από τους πρώτους $q_2, \dots, q_n$

Άρα λαμβάνοντας υπ' όψη και τη σχέση $\textcircled{*}$ θα έχουμε
το ζητούμενο.

Έστω $\alpha > 1$ θετικός ακέραιος. Τότε ο α μπορεί να γραφεί
γονιδικά ως εξής: $\alpha = p_1 \cdot p_2 \cdot \dots \cdot p_m$, όπου $p_1, \dots, p_m$ πρώτοι κριθοί.
 $= p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$, όπου $p_1, \dots, p_k$ πρώτοι
και $\alpha_1, \dots, \alpha_k \geq 1$

Η πρωτογενής ανάλυση ενός θετικού $\alpha > 1$ είναι:

$\alpha = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}$, όπου $p_1, \dots, p_k$ διαφορετικοί ανά δύο πρώτοι
και $\alpha_i \geq 1, \forall i=1, \dots, k$.

Παράδειγμα: Πρωτογενής ανάλυση του 2015.

$$2015 = 5 \cdot 403$$

Εύκολα βλέπουμε ότι $403 = 13 \cdot 31$ (από κόσκινο του Ερωτοδότη)

$$\text{άρα } 2015 = 5 \cdot 13 \cdot 31$$

$$k=3, p_1=5, p_2=13, p_3=31 \text{ και } \alpha_1=\alpha_2=\alpha_3=1.$$

Παρατηρήσεις: Έστω $\alpha, b > 1$ και έστω οι πρωτογενείς αναλύσεις
 $\alpha = p_1^{\alpha_1} \cdot \dots \cdot p_n^{\alpha_n}$ κ' $b = q_1^{b_1} \cdot \dots \cdot q_m^{b_m}$, όπου $p_1, \dots, p_n$ ανά 2 διαφορε-

τικοί πρώτοι κ' όλοια $q_1, \dots, q_m$ κ' $\alpha_i, b_i \geq 1 \forall i=1, \dots, n, 1, \dots, m$.

Θέτουμε $k = \max\{n, m\}$

$$\alpha = p_1^{\alpha_1} \cdot \dots \cdot p_n^{\alpha_n} \cdot p_{n+1}^{\alpha_{n+1}} \cdot \dots \cdot p_{n+m}^{\alpha_{n+m}} \text{ με } p_{n+1} = q_1, \dots, p_k = q_m \text{ με } \alpha_{n+1} = \dots = \alpha_k = 0$$

$$b = p_1^{\delta_1} \dots p_n^{\delta_n} p_{n+1}^{\delta_{n+1}} \dots p_k^{\delta_k}, \text{ όπου } \delta_1 = \dots = \delta_n = 0 \text{ κ' } p_{n+1} = q_1, \dots, p_k = q_k \\ \text{και } \delta_{n+1} = b_1, \dots, \delta_k = b_k.$$

Άρα έχουμε ότι οι a, b είναι γινώμενα δυνάμεων των ίδιων
πρώτων αριθμών. (ΔΙΟΡΘΩΣΗ!!
όπου $k = n + m$)

Παράδειγμα:

$$\left. \begin{array}{l} 12 = 2^2 \cdot 3^1 = 2^2 \cdot 3 \\ 20 = 2^2 \cdot 5^1 = 2^2 \cdot 5 \end{array} \right\} \Rightarrow \left. \begin{array}{l} 12 = 2^2 \cdot 3^1 \cdot 5^0 \\ 20 = 2^2 \cdot 3^0 \cdot 5^1 \end{array} \right\} \begin{array}{l} (\Delta \epsilon \nu \epsilon \iota \nu \alpha \iota \eta \mu \epsilon \rho \epsilon \nu \alpha \nu \alpha \lambda \iota \sigma \mu \epsilon \nu \alpha \iota) \\ (\delta \alpha \nu \iota \varsigma \alpha \nu \alpha \lambda \iota \sigma \mu \epsilon \nu \alpha \iota) \end{array}$$

→ ηρωτογενείς αναλύσεις!

(2) Αν $\alpha \in \mathbb{Z}$, $\alpha \neq 0, 1$, τότε:

$$\alpha = \varepsilon \cdot \alpha', \text{ όπου } \pm 1 \text{ κ' } \alpha' > 1 \text{ άρα } \alpha' = p_1^{\alpha_1} \dots p_k^{\alpha_k} \text{ ηρωτ. αναλ.} \\ \text{και } \alpha = (\pm 1) \cdot p_1^{\alpha_1} \dots p_k^{\alpha_k} \left(\begin{array}{l} + \rightarrow \alpha^0 \text{ θετικός} \\ - \rightarrow \alpha \text{ αρνητικός} \end{array} \right).$$

Θεώρημα: (Εύρεως διαιρετών αριθμών των ηρωτογενών αναλύσεων)

Έστω $\alpha = p_1^{\alpha_1} \dots p_n^{\alpha_n}$ η ηρωτογενής ανάλυση του $\alpha > 1$.

Τότε: $d | \alpha \Leftrightarrow d = p_1^{b_1} \dots p_n^{b_n}$, όπου $0 \leq b_i \leq \alpha_i$, $i = 1, \dots, n$.

Απόδειξη: (⇒) Έστω $d = p_1^{b_1} \dots p_n^{b_n}$ όπου $0 \leq b_i \leq \alpha_i$, $i = 1, \dots, n$.

Τότε: $\alpha_i = b_i + \delta_i$ όπου $\delta_i \geq 0$, $i = 1, \dots, n$.

$$\alpha = p_1^{\alpha_1} \dots p_n^{\alpha_n} = p_1^{b_1 + \delta_1} \dots p_n^{b_n + \delta_n} = p_1^{b_1} \cdot p_1^{\delta_1} \dots p_n^{b_n} \cdot p_n^{\delta_n} = \\ = (p_1^{b_1} \dots p_n^{b_n}) (p_1^{\delta_1} \dots p_n^{\delta_n}) = d (p_1^{\delta_1} \dots p_n^{\delta_n}) \Rightarrow d | \alpha.$$

(⇒) Υποθέτω ότι: $d | \alpha$

• Αν $d = 1$, τότε $d = p_1^0 \dots p_n^0$, δηλ. για ποινή του θέλω
κ' $b_1 = \dots = b_n = 0$.

• Έστω $d > 1$. Τότε ο d είναι ηρώτος διαιρέτης, έστω p .

Δηλαδή p ηρώτος κ' $p | d$ } $\Rightarrow p | \alpha = p_1^{\alpha_1} \dots p_n^{\alpha_n} \Rightarrow$

ΠΟΡΙΣΜΑ → $p \in \{p_1, \dots, p_n\}$. Άρα κάθε ηρώτος διαιρέτης του d
είναι και ηρώτος διαιρέτης του α δηλ. είναι κάποιος απ'
τους $\{p_1, \dots, p_n\}$. Άρα $d = p_1^{b_1} \dots p_n^{b_n}$ με $0 \leq b_i \leq \alpha_i$, $i = 1, \dots, n$.
Διότι $\sim \exists k \in \{1, \dots, n\} : b_k > \alpha_k \Rightarrow p_k^{b_k} \nmid d \Rightarrow d \nmid \alpha$ } $\Rightarrow$

$$\Rightarrow p_k^{b_k} \mid \alpha = p_1^{\alpha_1} \dots p_n^{\alpha_n}$$

$$\text{Ση). } \alpha = p_1^{\alpha_1} \dots p_n^{\alpha_n} = p_k^{b_k} \cdot \lambda \Rightarrow p_1^{\alpha_1} \dots p_{k-1}^{\alpha_{k-1}} p_{k+1}^{\alpha_{k+1}} \dots p_n^{\alpha_n} = p_k^{b_k - d_k} \cdot \lambda$$

$$\text{Άρα } p_k \mid p_1^{\alpha_1} \dots p_{k-1}^{\alpha_{k-1}} p_{k+1}^{\alpha_{k+1}} \dots p_n^{\alpha_n} \Rightarrow$$

$\Rightarrow p_k$ είναι κάποιος από τους πρώτους: $p_1, p_{k-1}, p_{k+1}, \dots, p_n$

άρα $0 \leq b_i \leq \alpha_i, \forall i=1, \dots, n$.

Παράδειγμα: $720 = 2^4 \cdot 3^2 \cdot 5^1$

$$d \mid 720 \Rightarrow d = 2^{\alpha} \cdot 3^{\beta} \cdot 5^{\gamma} \quad \mu \epsilon \quad 0 \leq \alpha \leq 4$$

$$0 \leq \beta \leq 2$$

$$0 \leq \gamma \leq 1$$

Οι διαφορετικοί διαιρέτες του 720 είναι: $5 \cdot 3 \cdot 2 = 30$
(το α παίρνει 5 τιμές, το β 3 και το γ 2).