

## ΠΡΩΤΟΙ ΑΡΙΘΜΟΙ

Ορισμός: Ένας θετικός ακέραιος  $P > 1$  καλείται πρώτος  $\Leftrightarrow$   
 $\Leftrightarrow$  οι μόνοι διαιρέτες του είναι:  $1, P$ .

Ένας θετικός ακέραιος  $\alpha$  καλείται εύνθετος  $\Leftrightarrow$  δεν είναι  
 πρώτος  $\Leftrightarrow \exists (b, c) \in \mathbb{Z}^2 : \alpha = b \cdot c \text{ κ' } 1 < b, c < \alpha$ .

Θεώρημα: Κάθε θετικός ακέραιος ( $\alpha > 1$ ) έχει πάντα έναν  
 πρώτο διαιρέτη!

Απόδειξη: Θεωρούμε το ακόλουθο σύνολο  $S = \{m \in \mathbb{N} \mid m/\alpha \wedge 1 < m < \alpha\}$   
 Τότε  $S \neq \emptyset$  διότι  $\alpha \in S$  (διότι  $\alpha/\alpha \wedge \alpha > 1$ ).

Άρα από (ΑΚΔ) το  $S$  έχει ελάχιστο στοιχείο, έστω  $P = \min S$ .  
 Ιδιαίτερα  $P \in S : P/\alpha \text{ κ' } P > 1$ .

Υποθέτουμε ότι  $P$  είναι εύνθετος  $\Rightarrow \exists b, c \in \mathbb{N} : P = b \cdot c$

Είναι  $b|P$  κ'  $b|\alpha \Rightarrow b|\alpha \text{ κ' } b > 1 \Rightarrow b \in S$  με  $1 < b < P$ .

$\Rightarrow b \in S$  άτοπο διότι  $b < P = \min S$  ΑΤΟΠΟ

Άρα  $P$  πρώτος κ' επομένως ο  $\alpha$  έχει πάντα έναν  
 πρώτο διαιρέτη.

**(\*) ΘΕΩΡΗΜΑ**: (Ευκλείδης - Στοιχεία του Ευκλείδη - 9<sup>ο</sup> βιβλίο).

Το πλῆθος των πρώτων αριθμών είναι άπειρο! §20

Απόδειξη: Υποθέτουμε ότι το πλῆθος των πρώτων αριθμών είναι  
 πεπερασμένο, έστω  $n$ , κ' έστω:  $P_1, \dots, P_n$  όλοι οι πρώτοι αριθμοί.

Θεωρούμε τον αριθμό  $\alpha = P_1 \cdot P_2 \cdot \dots \cdot P_n + 1$ . Τότε  $\alpha > 1$

Από το προηγούμενο θεώρημα ο  $\alpha$  έχει έναν πρώτο διαιρέτη  
 έστω  $P$ . Άρα  $P|\alpha$ . Επειδή  $P_1, \dots, P_n$  όλοι οι πρώτοι αριθμοί  $\Rightarrow$

$\Rightarrow P = P_k$  για κάποιο  $k = 1, \dots, n$ . Τότε  $P = P_k |\alpha$

κ'  $\alpha = P_1 \cdot P_2 \cdot \dots \cdot P_n + 1$

Έχουμε ότι  $\left. \begin{array}{l} P_k | P_1 \cdot \dots \cdot P_n + 1 \\ P_k | P_1 \cdot \dots \cdot P_n \end{array} \right\} \Rightarrow P_k | \alpha - P_1 \cdot \dots \cdot P_n \Rightarrow$

$\Rightarrow P_k | 1$  ΑΤΟΠΟ (οι μόνοι διαιρέτες του 1 είναι το 1 κ'  $P_k > 1$  δίνει πρώτος)

Άρα το πλήθος των πρώτων αριθμών είναι άπειρο!!

Σύνολο των πρώτων αριθμών:  $\mathbb{P} = \{p \in \mathbb{N} \mid p \text{ πρώτος}\}$ .

$$p_1=2, p_2=3, p_3=5, p_4=7, p_5=11, p_6=13, \dots$$

Πρόταση: Αν  $p_n$  ο  $n$ -οστος πρώτος αριθμός τότε:

$$p_n \leq 2^{2^{n-1}}, \quad \forall n \geq 1$$

Απόδειξη: Θα γίνει με χρήση της ΑΜΕ των πρώτων

$$P(n) : p_n \leq 2^{2^{n-1}}, \quad \forall n \geq 1.$$

- Για  $n=1 \Rightarrow p_1=2 \leq 2=2^1$ , άρα  $P(1)$  αληθής.
- Επαγωγική υπόθεση: Η πρόταση  $P(m) : p_m \leq 2^{2^{m-1}}$ ,  $1 \leq m < n$ .
- Θα  $n$  πρόταση  $P(n)$  είναι αληθής.

Ισχυρισμός:  $p_n \leq p_1 \cdot p_2 \cdot \dots \cdot p_{n-1} + 1$  (\*).

Απόδειξη του ισχυρισμού

Ο αριθμός  $\alpha = p_1 \cdot p_2 \cdot \dots \cdot p_{n-1} + 1 > 1$  και άρα ο  $\alpha$  έχει έναν πρώτο διαιρέτη, έστω  $p$ :  $p \mid \alpha \Rightarrow p \mid (p_1 \cdot \dots \cdot p_{n-1} + 1)$

Τότε  $p \neq p_1, p_2, \dots, p_{n-1}$  διότι διαφορετικά αν  $p = p_k$ ,  $1 \leq k \leq n-1$

$$\begin{aligned} \text{τότε } p &= p_k \mid p_1 \cdot \dots \cdot p_{n-1} \\ p &= p_k \mid p_1 \cdot \dots \cdot p_{n-1} + 1 \end{aligned} \Rightarrow p_k \mid 1 \text{ άρα } p_k = 1 \text{ αφού } p_k \text{ πρώτος.}$$

$$\text{Άρα } p = p_k \mid \alpha, k \geq n \Rightarrow p_n \leq p_k \leq \alpha = (p_1 \cdot \dots \cdot p_{n-1} + 1)$$

$p_k \mid \alpha \Rightarrow p_k \leq \alpha$

Άρα αποδείχθηκε η (\*)

Από τον ισχυρισμό είναι:  $p_n \leq p_1 \cdot \dots \cdot p_{n-1} + 1 \leq$

$$p_1 \leq 2^{2^{1-1}}$$

$$p_2 \leq 2^{2^{2-1}}$$

$$p_{n-1} \leq 2^{2^{n-2}}$$

$$\begin{aligned} &\leq 2^{2^0} \cdot 2^{2^1} \cdot \dots \cdot 2^{2^{n-2}} + 1 = \\ &= 2^1 \cdot 2^2 \cdot \dots \cdot 2^{2^{n-2}} + 1 = \\ &= 2^{1+2+2^2+\dots+2^{n-2}} + 1 = \\ &= 2^{2^{n-1}-1} + 1 \leq 2^{2^{n-1}-1} + 2^{2^{n-1}-1} = \end{aligned}$$

$$p_m \leq 2^{2^{m-1}}, \quad 1 \leq m < n.$$

Επαδ. υπόθεσ.

$$\begin{aligned} &1 + 2 + 2^2 + \dots + 2^{n-2} = \\ &= 2^{n-1} - 1 \end{aligned}$$

$$= 2 \cdot 2^{2^{n-1}-1} = 2^{2^{n-1}}$$

$$\text{Άρα } P_n \leq 2^{2^{n-1}} \Rightarrow P(n) : \text{αριθμός}$$

$$\text{Άρα } \boxed{n | P(n) \text{ αριθμός, } \forall n \geq 1}$$

$$2 = P_1 \leq 2^{2^1-1} = 2^{2^0} = 2^1 = 2$$

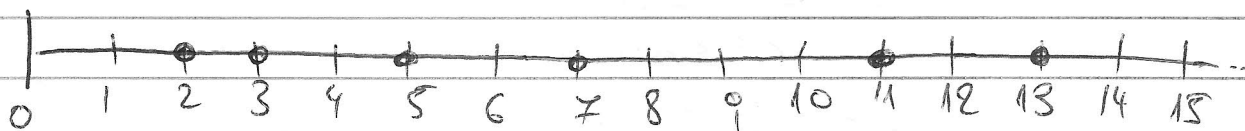
$$3 = P_2 \leq 2^{2^2-1} = 4$$

$$5 = P_3 \leq 2^{2^3-1} = 2^4 = 16$$

$$P_4 = 7 \leq 2^{2^4-1} = 256$$

1-1

Ο Μεγαλύτερος γνωστός Πρώτος αριθμός:  $2^{57.885.161} - 1 \rightarrow$   
 $\rightarrow$  έχει περίπου 17.425.140 ψηφία.



Κύρια προβλήματα που αφορούν τους Πρώτους αριθμούς:

① Υπάρχουν αλγόριθμοι οι οποίοι να αποφασίζουν αν ένας αριθμός είναι Πρώτος; ΝΑΙ σε πολυωνομικό χρόνο (ή) σε ανώτερο χρόνο

② Υπάρχουν αλγόριθμοι να αναζητήσω έναν αριθμό σε γνώστο Πρώτο Παράγονση; ΟΧΙ προς το παρόν

Αν ένας αριθμός της μορφής  $2^n - 1$  είναι πρώτος  $\Rightarrow$  τότε καλούμε Πρώτοι του Mersenne.

Πρόταση: Υπάρχουν ομοδομήσις μεγάλα διακεμήλα φυσικών αριθμών τα οποία δεν περιέχουν κανέναν πρώτο αριθμό.

$\forall n \geq 1$ : οι αριθμοί  $(n+1)! + 2, (n+1)! + 3, \dots, (n+1)! + n+1$   
 δεν είναι πρώτοι, διότι το  $2 \mid [(n+1)! + 2]$ , το  $3 \mid [(n+1)! + 3], \dots$ , το  $(n+1) \mid [(n+1)! + n+1]$

- Για  $n=2 \Rightarrow (n+1)! + 2 = 1 \cdot 2 \cdot 3 + 2 = 8$ ,  $6 + 3 = 9$  (όχι πρώτοι)
- $n=3 \Rightarrow (n+1)! = 24$   $24 + 2 = 26$ ,  $24 + 3 = 27$ ,  $24 + 4 = 28$  (+/-)
- $n=4 \Rightarrow (n+1)! = 120$ ,  $122, 123, 124, 125$ .

+

(Πρόβλημα του Ερατοσθένη) Θεώρημα: Κάθε σύνθετος αριθμός  $\alpha > 1$ , έχει έναν πρώτο διαιρέτη  $p \leq \sqrt{\alpha}$ .

Απόδειξη: Ο αριθμός  $\alpha$ : σύνθετος  $\Rightarrow \alpha = b \cdot c$   $1 < b, c < \alpha$ .

Λογισ βλίζη ως γενικότερας έσω ότι  $c \leq b$ .

$$\text{Τότε } \alpha = b \cdot c \leq b^2 \quad (1)$$

$$c^2 \leq b \cdot c = \alpha \quad (2)$$

Επειδή  $c > 1$ , ο  $c$  έχει πρώτο διαιρέτη, έσω  $p$ . Τότε  $p \mid c \Rightarrow \Rightarrow p \leq c$ . Τότε

$$\left. \begin{array}{l} p \mid c \\ c \mid \alpha \end{array} \right\} \Rightarrow p \mid \alpha \text{ κ' } p \leq \sqrt{\alpha}$$

Πρόταση: Αν  $\alpha \in \mathbb{N}$  με  $\alpha > 1$  κ' δεν  $\exists p$  πρώτος έτσι ώστε  $p \mid \alpha$  κ'  $p \leq \sqrt{\alpha}$  τότε  $\alpha$ : πρώτος.

[Κριτήριο απόφασης για τον αν ένας αριθμός είναι πρώτος ή όχι].

Παράδειγμα: (α)  $\alpha = 643$ , (β) ~~583~~,  $\alpha = 583$ .

$$(α) \quad 25 < \sqrt{643} < 26$$

$$p \leq \sqrt{643} ?$$

Πρώτοι  $\Rightarrow p = 2, 3, 5, 7, 11, 13, 17, 19, 23$ .

Δοκιμάζοντας, κανένας από αυτούς τους αριθμούς δεν διαιρεί  $\rightarrow$

τον 643, άρα ο 643 είναι πρώτος με βάση το παραπάνω κριτήριο.

(b)  $\alpha = 583. \Rightarrow 24 < \sqrt{583} < 25$

η άρα οι ίδιοι  $P \in \alpha$

Τότε δοκιμάζοντας  $\Rightarrow 11/583$  κ'  $11 \leq \sqrt{583} \Rightarrow 583$  όχι πρώτος

## ΚΟΣΚΙΝΟ ΕΡΑΤΟΣΘΕΝΗ

Η μέθοδος συνίσταται στο εύρεση όλων των πρώτων  $P \leq \alpha$  όπου  $\alpha > 1$ .

Βάση της μεθόδου: Αν ο  $\alpha$  δεν διαιρείται από κανέναν  $P \leq \sqrt{\alpha}$  τότε  $\alpha$  : πρώτος.

Μέθοδος: θεωρούμε τους αριθμούς:  $2, 3, \dots, \alpha$

α' κέραια

• για κάθε πρώτο  $P \leq \sqrt{\alpha}$ , διαγράφουμε όλα τα πολλαπλάσια του  $P$

• αυτοί που μένουν θα είναι όλοι οι πρώτοι οι οποίοι είναι  $\leq \alpha$ .

—/

Παράδειγμα: ~~2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20~~

(2) (3) (5) (7) (11) (13) (17) (19) (23) (29) (31) (37) (41) (43) (47) (53)

Όλοι οι = είναι  
οι πρώτοι

$\alpha = 50$

$P \leq \sqrt{50}$

↓  
πρώτος ( $P = 2, 3, 5, 7$ )

OK OK OK OK