25-10-16

Άσκηση: Αν $p_n$ είναι ο $n$-οστός πρώτος αριθμός $n \geq 1$, τότε:

$$p_n \leq 2^{2^{n-1}} \quad (*)$$

Απόδειξη: • Για $n=1$, $p_1 = 2$ και $2^{2^{n-1}} = 2^{2^0} = 2$ άρα η $(*)$ ισχύει ως ισότητα

• Επαγωγική Υπόθεση: Υποθέτω ότι $p_m \leq 2^{2^{m-1}}$, $\forall m: 2 \leq m < n$

Ισχυρισμός: $p_n \leq p_1 p_2 \dots p_{n-1} + 1$

Απόδειξη: Ο αριθμός $p_1 p_2 \dots p_{n-1} + 1 > 1$, άρα $\exists p$: πρώτος έτσι ώστε $p \mid p_1 p_2 \dots p_{n-1} + 1$

Αν $p = p_k$, $1 \leq k \leq n-1$, τότε $p = p_k \mid p_1 p_2 \dots p_{n-1}$ και τότε $p \mid 1$. Άτοπο

Αν $p = p_k$, $k \geq n$, τότε $p_n \leq p_k = p$

$$\left.\begin{array}{l} p \mid p_1 p_2 \dots p_{n-1} + 1 \\ p_n \leq p_1 p_2 \dots p_{n-1} + 1 \end{array}\right\} \Rightarrow p \leq p_1 \dots p_{n-1} + 1$$

Τότε: $p_n \leq p_1 p_2 \dots p_{n-1} + 1 \leq 2 \cdot 2^2 \dots 2^{2^{n-2}} + 1 =$

$$= 2^{1+2+\dots+2^{n-2}} + 1 = 2^{2^{n-1}-1} + 1 = 2^{2^{n-1}-1} + 2^{2^{n-1}-1} =$$

$$= 2 \cdot 2^{2^{n-1}-1} = 2^{2^{n-1}},$$ άρα η $(*)$ ισχύει $\forall n \geq 1$

Παρατήρηση: Υπάρχουν οσοδήποτε μεγάλα χάσματα στην κατανομή των πρώτων αριθμών

Πράγματι, $\forall\, n \geq 1$ θεωρούμε τους εξής διαδοχικούς ακεραίους:

$$(n+1)! + 2,\ (n+1)! + 3,\ (n+1)! + 4,\ \ldots,\ (n+1)! + (n+1)$$

Κανένας απ' τους παραπάνω δεν είναι πρώτος, διότι:

$\forall\, k = 2, 3, 4, \ldots, n+1$ : $k \mid (n+1)!$ (επειδή $k \leq n+1$) και

$$k \mid (n+1)! + k$$

• Κάθε θετικός ακέραιος $\alpha > 1$ έχει ένα πρώτο διαιρέτη $p \leq \sqrt{\alpha}$

• Έστω $\alpha > 1$ και δεν υπάρχει πρώτος $p \leq \sqrt{\alpha}$ έτσι ώστε : $p \mid \alpha$

Τότε $\alpha$: πρώτος

Παράδειγμα: $\alpha = 10^{100}$ : Χρειαζόμαστε περίπου $10^{25}$ χρόνια να βρούμε πόσοι πρώτοι υπάρχουν με το παραπάνω κριτήριο

Παράδειγμα: $a=643$ , $b=583$

→ Για τον $a$: $25 < \sqrt{643} < 26$

Πρώτοι $\leq 25$ : 2, 3, 5, 7, 11, 13, 17, 19, 23

Έπειτα από δοκιμές, προκύπτει ότι κανένας απ'τους παραπάνω δε διαιρεί το 643

→ Για τον $b$: $24 < \sqrt{583} < 25$

Πρώτοι $\leq 24$ : 2, 3, 5, 7, 11, 13, 17, 19, 23

Έπειτα από δοκιμές, προκύπτει ότι το 11 διαιρεί τον 583

Άρα, ο $b$ δεν είναι πρώτος

• Κόσκινο του Ερατοσθένη: Εύρεση όλων των πρώτων αριθμών $p$: $p \leq \alpha$, όπου $\alpha \in N$, $\alpha > 1$

α) Γράφουμε τους αριθμούς: $2, 3, \ldots, \alpha-2, \alpha-1, \alpha$

β) Βρίσκουμε όλους τους πρώτους $p$: $p \leq \sqrt{\alpha}$

γ) Διαγράφουμε από τους αριθμούς τα θετικά ακέραια πολλαπλάσια του $p$, $\forall p$: πρώτο, $p \leq \sqrt{\alpha}$

δ) Οι αριθμοί που μένουν μετά το τρίτο βήμα, είναι όλοι οι πρώτοι, $p \leq \sqrt{\alpha}$

Παράδειγμα: Όλοι οι πρώτοι $\leq 30$ :

(2) (3) 4 (5) 6 (7) 8 9 10 (11) 12 (13) 14 15

16 (17) 18 (19) 20 21 22 (23) 24 25 26 27 28 (29) 30

• Θεμελιώδες Θεώρημα της Αριθμητικής

Έστω $\alpha > 1$. $\alpha = p_1 p_2 \dots p_\kappa$, $p_i$: πρώτοι, $i = 1, \dots, \kappa$ $\Big\} \Rightarrow$

$= q_1 q_2 \dots q_\lambda$, $q_j$: πρώτοι, $j = 1, \dots, \lambda$

$\underline{\kappa = \lambda}$ και μετά από αναδιάταξη θα έχουμε

$p_1 = q_1$, $p_2 = q_2$, ..., $p_\kappa = q_\kappa$

Παράδειγμα: $X = \{2, 4, 6 \dots\}$, σύνολο θετικών, άρτιων ακεραίων

$\alpha \in X$, καλείται πρώτο στοιχείο του $X \Leftrightarrow$

$\alpha$ δε μπορεί να γραφεί ως γινόμενο $\alpha = \kappa \cdot \lambda$, $\kappa, \lambda \in X$

$10 \in X$ και 10: πρώτο στοιχείο του $X$

$8 \in X$ και 8: όχι πρώτο, διότι $8 = 4 \cdot 2$

$60 \in X$ και $60 = 2 \cdot 30 = 6 \cdot 10$

Άρα, στο $X$ δεν υπάρχει πάντα η μοναδικότητα της γραφής ενός στοιχείου ως γινόμενο πρώτων στοιχείων

• Πρόταση: Κάθε θετικός ακέραιος $\alpha > 1$ μπορεί να γραφεί ως γινόμενο πεπερασμένου πλήθους πρώτων αριθμών

Απόδειξη: Αν $\alpha = 2$, τότε είναι γινόμενο πρώτων με τετριμμένο τρόπο

• Έστω $\alpha > 2$. Επαγωγική Υπόθεση: Για κάθε $b \in \mathbb{N}$ $2 \leq b < \alpha$, ο $b$ μπορεί να γραφεί ως γινόμενο πρώτων αριθμών

Δηλαδή: $b = p_1 p_2 \dots p_k$, $p_i$: πρώτοι, $i = 1, \dots, k$

Για τον $\alpha$: i) $\alpha$: πρώτος, τότε ο $\alpha$ είναι γινόμενο πρώτων, κατά τετριμμένο τρόπο

ii) $\alpha$: σύνθετος, τότε μπορούμε να γράψουμε ότι ο $\alpha$ είναι: $\alpha = r \cdot s$, $1 < r, s < \alpha$

Από την επαγωγική υπόθεση, μπορούμε να γράψουμε

$r = p_1 \dots p_k$, $p_1, \dots, p_k$: πρώτοι

$s = q_1 q_2 \dots q_\lambda$, $q_1, \dots q_\lambda$: πρώτοι

Άρα, $\alpha = r \cdot s = p_1 p_2 \dots p_k q_1 q_2 \dots q_\lambda$, γινόμενο πρώτων

Λήμμα του Ευκλείδη: Αν $a, b \in \mathbb{Z}$ και $p$: πρώτος τότε: $p \mid a \cdot b \Rightarrow p \mid a$ ή $p \mid b$ (*)

Απόδειξη: Αν $a=0$ ή $b=0$, τότε η (*) ισχύει άμεσα

Έστω $a\neq 0$ και $b\neq 0$

Επειδή $p|x \Leftrightarrow p||x|$, μπορούμε να υποθέσουμε ότι $a,b\in\mathbb{N}$

Υποθέτουμε ότι $a,b\in\mathbb{N}$ και $p|ab$

Θεωρούμε το $X=\{x\in\mathbb{N} \mid p|ax\}$

Το $X\neq\emptyset$, διότι: $\begin{cases} i)\ b\in X, \text{ διότι: } p|ab \\ ii)\ p\in X, \text{ διότι: } p|ap \end{cases}$ ①

Από την (ΑΔΕ), το $X$ έχει ελάχιστο στοιχείο

Έστω $\vartheta=\min X$. Τότε $\vartheta\in\mathbb{N}$ και $p|a\vartheta$ ②

Ισχυρισμός: $\forall x\in X : \vartheta|x$

Αν $x\in X$, απ' την Ευκλείδεια Διαίρεση του $x$ με το $\vartheta$ θα έχουμε: $x=\vartheta q+r$, $0\leq r<\vartheta$

Αν $r\neq 0$, τότε $x-a=a\cdot\vartheta\cdot q+a\cdot r$

$$\left.\begin{array}{l} x\in X \Rightarrow p|ax \\ \vartheta\in X \Rightarrow p|a\vartheta \Rightarrow p|a\vartheta q \end{array}\right\} \begin{array}{l} \Rightarrow p|ax-a\vartheta q=ar \\ \Rightarrow p|ar \end{array}$$

Αρα, $r \in X$. Όμως $r < \theta = \min X$. Άτοπο

Συνεπώς $\boxed{r=0} \Rightarrow x = \theta q \Rightarrow \theta | x$ ③

Τότε : ① $\Rightarrow p \in X \xrightarrow[x=p \quad p:\text{πρώτος}]{③} \theta | p$ $\Bigg\} \Rightarrow$

$\Rightarrow \quad \theta = 1 \quad$ ή $\quad \theta = p$

$\downarrow$ $\qquad$ $\downarrow$

$p | a \qquad p | b$