19-10-16

Παράδειγμα: $\forall n \in N: 4 \nmid n^2+2$

Έστω ότι $\exists n \in N: 4 | n^2+2$. Τότε $\exists k \in N$

$n^2+2 = 4k$

α) Αν n: άρτιος $\Rightarrow n = 2\lambda, \lambda \in N$ και τότε

$4\lambda^2 + 2 = 4k \Rightarrow \underbrace{2\lambda^2+1}_{\text{περιττός}} = \underbrace{2k}_{\text{άρτιος}}$ : Άτοπο

β) Έστω n: περιττός $\Rightarrow n = 2\lambda+1, \lambda \in N$ και τότε

$(2\lambda+1)^2 + 2 = 4k \Rightarrow 4\lambda^2 + 4\lambda + 1 + 2 = 4k \Rightarrow$

$\Rightarrow 4\lambda^2 + 4\lambda + 4 - 1 = 4k \Rightarrow 4(\lambda^2+\lambda+1) - 1 = 4k \Rightarrow$

$$\left.\begin{array}{l} 4|4k \Rightarrow 4|4(\lambda^2+\lambda+1)-1 \\ 4|4(\lambda^2+\lambda+1) \end{array}\right\} \Rightarrow 4|1 : \text{Άτοπο}$$

Άρα, η υπόθεση ότι υπάρχει $n \in N: 4|n^2+2$, μας οδήγησε σε άτοπο.

Συνεπώς, $\forall n \in N: 4 \nmid n^2+2$

• Άσκηση: $\forall n \geq 0 : 9 | 10^n + 3 \cdot 4^{n+2} + 5$

Λύση: για $n=0$ : $10^n + 3\cdot 4^{n+2} + 5 = 1+5+48 = 54 = 6\cdot 9$

Άρα, $9 \mid 10^0 + 3\cdot 4^{0+2} + 5$

• Υποθέτουμε ότι ισχύει για $n \geq 1$ και $9 \mid 10^n + 3\cdot 4^{n+2} + 5$

• Θδο: $9 \mid 10^{n+1} + 3\cdot 4^{n+1+2} + 5$

$10^{n+1} + 3\cdot 4^{n+1+2} + 5 = 10^n \cdot 10 + 3\cdot 4^{n+2}\cdot 4 + 5 =$

$= 10\cdot 10^n + 12\cdot 4^{n+2} + 5 = 9\cdot 10^n + 10^n + 9\cdot 4^{n+2} + 3\cdot 4^{n+2} + 5 =$

$= 9(10^n + 4^{n+2}) + (10^n + 3\cdot 4^{n+2} + 5)$ $\dfrac{9 \mid 10^n + 3\cdot 4^{n+2} + 5}{9 \mid 9(10^n + 4^{n+2})}$

Συνεπώς, $9 \mid 9(10^n + 4^{n+2}) + (10^n + 3\cdot 4^{n+2} + 5)$

Από την $(AME)_1 \Rightarrow 9 \mid 10^n + 3\cdot 4^{n+2} + 5$, $\forall\, n \geq 0$

Άσκηση: Για κάθε $n \in \mathbb{N}$, το γινόμενο n το πλήθος διαδοχικών ακεραίων διαιρείται απ' το n.

Απόδειξη: Για κάθε ακέραιο k, θα έχουμε τους εξής n το πλήθος διαδοχικούς ακεραίους

$k, (k+1), (k+2), \ldots, (k+n-1)$

Θδο: $n \mid A$, όπου $A = k(k+1)(k+2)\ldots(k+n-1)$

Από την Ευκλείδεια διαίρεση του k με το n, έχουμε

$k = nq + r$, $0 \leq r \leq n-1$

- Αν $r=0 \Rightarrow k=nq \Rightarrow \left.\begin{matrix} n|k \\ k|A \end{matrix}\right\} \Rightarrow n|A$

- Αν $r \neq 0 \Rightarrow 1 \leq r \leq n-1$

Τότε : $1 \leq n-r \leq n-1$

$A = k(k+1)(k+2)\dots(k+n-r)\dots(k+n-1)$

Όμως $(k+n-r) = nq + \cancel{r} + n - \cancel{r} = n(q+1)$

$\Rightarrow \left.\begin{matrix} n|(k+n-r) \\ (k+n-r)|A \end{matrix}\right\} \Rightarrow n|A$

- Πρώτοι Αριθμοί

- Ορισμός: Ένας θετικός ακέραιος $p$ καλείται πρώτος $\Leftrightarrow$
  $\Leftrightarrow$ οι μόνοι (θετικοί) διαιρέτες είναι: $1, p$

Ένας θετικός ακέραιος $p$ καλείται σύνθετος $\Leftrightarrow$

$\Leftrightarrow$ αν δεν είναι πρώτος $\Leftrightarrow$ $p$: σύνθετος αν-ν:
$\exists\, r, s \in \mathbb{N} : p = rs,\ 1 < r, s < p$

Παράδειγμα: 2 3 5 7 11 13 17 19 23 29

Οι παραπάνω είναι όλοι οι πρώτοι απ' το 2 ως το 30

**Θεώρημα:** Κάθε θετικός ακέραιος μεγαλύτερος της μονάδας, έχει ένα πρώτο διαιρέτη.

Απόδειξη: Θεωρούμε το σύνολο $S$

$S=\left\{ m\in \mathbb{N} \;\middle|\; \begin{matrix} m>1 \\ m|a \end{matrix} \right\}$. Τότε, $S\neq\emptyset$, διότι $a\in S$

Από την (ΑΚΔ) $\Rightarrow$ Το $S$ έχει ελάχιστο στοιχείο

Έστω $p=\min S$. Τότε $\begin{matrix} p>1 \\ p|a \end{matrix}$

Αν $p$: σύνθετος $\Rightarrow p=r\cdot s$, $1<r,s<p$

Τότε: $\left.\begin{matrix} r>1 \text{ και } r|p \\ p|a \end{matrix}\right\} \Rightarrow \left.\begin{matrix} r>1 \\ r|a \end{matrix}\right\} \Rightarrow r\in S$

Συνεπώς, $p=\min S$ και $r<p$. Άτοπο

Άρα, ο $p$ είναι πρώτος

**Θεώρημα:** {9ο Βιβλίο στοιχείων του Ευκλείδη}

Το πλήθος των πρώτων αριθμών είναι άπειρο

Απόδειξη: Υποθέτουμε ότι το $\mathbb{P}$(σύνολο πρώτων αριθμών) είναι πεπερασμένο

Τότε μπορούμε να υποθέσουμε ότι: $\mathbb{P}=\{P_1,P_2,\dots,P_n\}$

Θεωρούμε τον $a = p_1 p_2 \dots p_n + 1$

$a > 1$ και απ' το προηγούμενο θεώρημα, ο $a$ έχει έναν πρώτο διαιρέτη $p$

Τότε $p \in \mathbb{P} \Rightarrow \exists\, k = 1, \dots, n : p = p_k$

Όμως, $\left.\begin{array}{l} p \mid a = p_1 p_2 \dots p_k \dots p_n + 1 \\ p = p_k \mid p_1 \dots p_k \dots p_n \end{array}\right\} \Rightarrow p_k \mid a - p = 1$

$p = 1$ : Άτοπο, διότι $p \geq 2$

Άρα, το πλήθος των πρώτων αριθμών είναι άπειρο

$\vartheta : \mathbb{R} \to \mathbb{R}$, $\vartheta(x) =$ πλήθος πρώτων αριθμών $\leq x$

• Θεώρημα πρώτων αριθμών: $\forall x \in \mathbb{R}$

$\vartheta(x) \sim \frac{x}{\log x}$ $\left[\lim_{x \to \infty} \vartheta(x) \frac{\log x}{x} = 1\right]$

• Εικασία του Bertrand: $\forall\, n \geq 2$, $\exists\, p$: πρώτος $\Rightarrow n < p < 2n$

Πόρισμα: Αν $\forall\, n \geq 1$ $p_n =$ ο n-οστός πρώτος αριθμός

$p_n \leq 2^n$

(*) Θα αποδείξουμε ότι: $p_n \leq 2^{2^{n-1}}$

Θεώρημα: Κάθε θετικός σύνθετος ακέραιος $\alpha>1$ έχει πάντα ένα πρώτο διαιρέτη $p$, $p \leq \sqrt{\alpha}$

Απόδειξη: Επειδή $\alpha$: σύνθετος

$\alpha = b \cdot c$, όπου $b, c \in \mathbb{N}$ και $1 < b, c < \alpha$

Χωρίς βλάβη της γενικότητας, έστω ότι $c \leq b$

$c \leq b \Rightarrow c^2 \leq bc = \alpha \Rightarrow c \leq \sqrt{\alpha}$

$c > 1 \Rightarrow c$: έχει ένα πρώτο διαιρέτη $p$

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

$$\left.\begin{array}{l} p \mid c \\ c \mid \alpha \end{array}\right\} \Rightarrow p \mid \alpha$$

Άρα, $p$: πρώτος διαιρέτης του $\alpha$ και $p \leq \sqrt{\alpha}$

• Κριτήριο για το αν ένας θετικός ακέραιος $\alpha > 1$ είναι πρώτος

α) Υπολογίζουμε τη ρίζα του $\alpha$ ($\sqrt{\alpha}$)

β) Βρίσκουμε ποιοι απ' τους πρώτους αριθμούς $p \leq \sqrt{\alpha}$, διαιρούν τον $\alpha$.

i) Αν δεν υπάρχει $p$ έτσι ώστε $p \mid \alpha \Rightarrow \alpha$: πρώτος

ii) Αν υπάρχει $p \leq \sqrt{\alpha}$ και $p \mid \alpha \Rightarrow \alpha$: σύνθετος