

26/02/15

AME1: Έστω $P(n)$ πρόταση η οποία εξαρτάται από το $n \in \mathbb{N}$.

- $P(1) : \alpha \lambda \eta \theta \iota \varsigma$ (16 x 6)
 - $\forall n \geq 1 : P(n) : \alpha \lambda \eta \theta \iota \varsigma$ (unódexen) $\Rightarrow P(n+1) \alpha \lambda \eta \theta \iota \varsigma$
- $\Rightarrow \text{~~But~~ } P(n) : \alpha \lambda \eta \theta \iota \varsigma, \forall n \in \mathbb{N}.$

AME2: Έστω $P(n)$ πρόταση η οποία εξαρτάται ~~from~~ από το $n \in \mathbb{N}$.

- $P(1) : \alpha \lambda \eta \theta \iota \varsigma$
- $\forall n > 1, P(k) : \alpha \lambda \eta \theta \iota \varsigma, 1 \leq k < n \Rightarrow P(n) : \alpha \lambda \eta \theta \iota \varsigma$

$\Rightarrow P(n) : \alpha \lambda \eta \theta \iota \varsigma, \forall n \in \mathbb{N}.$

AME3: Έστω P πρόταση η οποία εφάρζεται από το $n \in \mathbb{N}$, $\forall n \geq n_0$.

$$\left. \begin{array}{l} \bullet P(n_0) : \alpha \lambda \eta \theta \eta \varsigma \\ \left\{ \begin{array}{l} \forall n \geq n_0, P(n) : \alpha \lambda \eta \theta \eta \varsigma \Rightarrow P(n+1) : \alpha \lambda \eta \theta \eta \varsigma \\ \forall n > n_0, P(k) : \alpha \lambda \eta \theta \eta \varsigma, n_0 \leq k < n \Rightarrow P(n) : \alpha \lambda \eta \theta \eta \varsigma \end{array} \right\} \end{array} \right\} \Rightarrow$$

$$\Rightarrow P(n) : \alpha \lambda \eta \theta \eta \varsigma, \forall n \geq n_0.$$

↪

Παράδειγμα: Ακολουθία Fibonacci: $F_1=1, F_2=1, F_3=2, F_4=3, \dots$
 $\text{Οπότε } F_{n+1} = F_n + F_{n-1}, \forall n \geq 2$

Έχουμε δείξει ότι $F_n < 2^n, \forall n \geq 1$.

Θ.δ.ο. : $F_n < \left(\frac{7}{4}\right)^n, \forall n \geq 1. \quad \left(\frac{7}{4} = 1,75\right)$

• $\forall n \geq 1 : P(n) : F_n < \left(\frac{7}{4}\right)^n$

• Αν $n=1$, τότε $F_1=1 < 1,75 = \frac{7}{4} = \left(\frac{7}{4}\right)^1$

Άρα $n P(1)$ είναι αληθής

• Υποθέτουμε ότι $n P(k)$ είναι αληθής, $1 \leq k < n, n > 1$.

Τότε $F_k < \left(\frac{7}{4}\right)^k, 1 \leq k < n$.

Τότε $F_n = F_{n-1} + F_{n-2} < \left(\frac{7}{4}\right)^{n-1} + \left(\frac{7}{4}\right)^{n-2} =$

$= \left(\frac{7}{4}\right)^{n-2} \left(\frac{7}{4} + 1\right) = \left(\frac{7}{4}\right)^{n-2} \cdot \frac{11}{4} \overset{\substack{\text{επειδή} \\ \text{για } k=n-1, n-2}}{<} \left(\frac{7}{4}\right)^{n-2} \cdot \left(\frac{7}{4}\right)^2 = \left(\frac{7}{4}\right)^n$

⊗ $11/4 < \left(\frac{7}{4}\right)^2 \Rightarrow P(n) \text{ αληθής}$

Άρα από AME2 $\Rightarrow F_n < \left(\frac{7}{4}\right)^n, \forall n \geq 1$.

Θ.δ.ο. $f_n = \frac{\alpha^n - b^n}{\sqrt{5}}$, με $\alpha = \frac{1+\sqrt{5}}{2}$, $b = \frac{1-\sqrt{5}}{2} // \frac{1+\sqrt{5}}{2} \approx 1,618$

α b $\Rightarrow \frac{\alpha+b}{\alpha} = \frac{\alpha}{b} \Rightarrow$ ~~$\frac{\alpha+b}{\alpha} = \frac{\alpha}{b}$~~ $\downarrow$ $x \text{ πολλαπλασιάζω}$

$\Rightarrow 1 + \frac{b}{\alpha} = \frac{\alpha}{b} \xrightarrow{\alpha/b = \varphi} 1 + \frac{1}{\varphi} = \varphi \Rightarrow \varphi + 1 = \varphi^2 \Rightarrow$

$\Rightarrow \varphi^2 - \varphi - 1 = 0 \Rightarrow \begin{cases} \alpha = \frac{1+\sqrt{5}}{2} \\ b = \frac{1-\sqrt{5}}{2} \end{cases}$

Παράδειγμα: ①: $f(x) = x^2 - x + 41$ (Gauss-Euler)

Για $x = 1, 2, \dots, 40 \Rightarrow f(x)$ πρώτος αριθμός !!

Όμως $f(41) = (41)^2$ ΔΕΝ ΕΙΝΑΙ ΠΡΩΤΟΣ.

②: $\Phi_n(x) = \prod_{1 \leq k \leq n} (x - e^{2\pi i \frac{k}{n}})$

$(k, n) = 1$ (πρώτος με προς n)

π.χ. $\Phi_1(x) = x - 1$

$\Phi_2(x) = x + 1$

$\Phi_3(x) = x^2 + x + 1$

$\Phi_4(x) = x^2 + 1 \dots$

Οι συντελεστές του $\Phi_m(x)$: $n \leq 104$ είναι ± 1 .

Όμως $\Phi_{105}(x)$ έχει ως όρο x^{47}

ΘΕΩΡΗΜΑ [Ευκλείδεια Διαίρεση Ακεραίων]. : Έστω $a, b \in \mathbb{Z}$
όπου $b \neq 0$. Τότε $\exists!$ ζεύγος ακεραίων $(q, r) \in \mathbb{Z}^2$:
 $a = b \cdot q + r$ και $0 \leq r < |b|$.

Απόδειξη : Θεωρούμε το σύνολο $S = \{a - bx \in \mathbb{Z} \mid x \in \mathbb{Z} \text{ και } (a - bx) \geq 0\}$

Είναι $S \subseteq \mathbb{N} \cup \{0\}$

Ισχυρισμός : $S \neq \emptyset$.

Απόδειξη ισχυρισμού : (α) Έστω $b > 0$. Τότε θέτουμε $x = -(1 + |a|)$
Τότε ~~$a - bx$~~ $a - bx = a - b(-1 - |a|) = a + b(1 + |a|) >$
 $> a + 1 + |a| \geq 1$

(δίδει (i) αν $a \geq 0 \Rightarrow a + 1 + |a| = 2a + 1 \geq 1$
(ii) αν $a < 0 \Rightarrow a + 1 + |a| = ~~a + 1~~ a + 1 - a = 1 \geq 1$)

Άρα αν $b > 0$ τότε για $x = -(1 + |a|)$ έχουμε $a - bx \geq 0$
και ιδίαιτερα $(a - bx) \in S \Rightarrow S \neq \emptyset$.

(β) $b < 0$. Θέτουμε $x = 1 + |a|$. Τότε $a - bx = a + (-b)x =$
 $= a + (-b)(1 + |a|) \geq a + (1 + |a|) \geq 1$

Άρα $a - bx \geq 0 \Rightarrow (a - bx) \in S \Rightarrow S \neq \emptyset$.

Αν $a \in \mathbb{N}$, το S έχει ελάχιστο στοιχείο, έστω r .

Άρα $r \in \mathbb{Z}$ και $r = a - b \cdot q \geq 0$, δηλαδή $a = b \cdot q + r$ και $0 \leq r$.

Θ.δ.ο. $r < |b|$. Θεωρούμε την διαφορά $r - |b| = a - b \cdot q - |b| =$

$$= \begin{cases} (b > 0) = a - bq - b = a - b(q + 1) \\ (b < 0) = a - bq + b = a - b(q - 1) \end{cases}$$

Άρα $(r - |b|) \in \mathbb{Z}$ της μορφής $a - bx$

Αν $r - |b| \geq 0$, τότε $(r - |b|) \in S$ άτοπο, διότι $r = \min S$
και $r - |b| < r$ (διότι $b \neq 0$)

Άρα $r - |b| < 0 \Rightarrow r < |b|$

Συνοψίζουμε : $\exists (q, r) \in \mathbb{Z}^2 : a = b \cdot q + r, 0 \leq r < |b|$.

Έστω $(q', r') \in \mathbb{Z}^2 : a = b \cdot q' + r', 0 \leq r' < |b|$

$$r' - r = \alpha - bq' - (\alpha - bq) = b(q - q') \Rightarrow \boxed{r' - r = b(q - q')} \Rightarrow$$

$$\Rightarrow \boxed{|r' - r| = |b| \cdot |q - q'|} \quad (1)$$

$$\text{Επίσης: } \left. \begin{array}{l} 0 \leq r' < |b| \\ -|b| < -r \leq 0 \end{array} \right\} \Rightarrow -|b| < r' - r < |b| \Rightarrow \boxed{|r' - r| < |b|} \quad (2)$$

$$\text{Από (1), (2)} \Rightarrow \left. \begin{array}{l} |b| \cdot |q - q'| < |b| \\ b \neq 0 \end{array} \right\} \Rightarrow |q - q'| < 1 \Rightarrow$$

$$\Rightarrow 0 \leq |q - q'| < 1. \quad \left. \begin{array}{l} \text{Επειδή } q, q' \in \mathbb{Z} \end{array} \right\} \Rightarrow |q - q'| = 0 \Rightarrow \boxed{q = q'}$$

$$\text{Τότε } r' = \alpha - bq' = \alpha - bq = r \text{ Άρα } \boxed{r = r'}$$

Οπότε τα $(q, r) \in \mathbb{Z}^2$ είναι μοναδικά!

Πορίσμα: Έστω $\alpha, b \in \mathbb{Z}$, $b \neq 0$. Τότε από Ευκλείδεια Διαίρεση
 $\exists!$ ζεύγος $(q, r) \in \mathbb{Z}^2$: $\alpha = b \cdot q + r$, $0 \leq r < |b|$.

Ο αρέματος q καθορίζει το ημίτιο της διαίρεσης του α με το b .
 $\begin{array}{ccccccc} r' & -11- & r & -11- & \text{το συνολικό } -11- & -11- & \end{array}$

Παράδειγμα: $\alpha \in \mathbb{Z}$ κ' $b = 2$. Τότε $\alpha = 2q + r$, $0 \leq r < 2 \Rightarrow \boxed{r = 0} \text{ ή } \boxed{r = 1}$

$$\text{Άρα: } \alpha = \begin{cases} 2 \cdot q, & \alpha \text{ άρτιος} \\ 2 \cdot q + 1, & \alpha \text{ περιττός} \end{cases}$$

Παρατήρηση: Έστω $\alpha \in \mathbb{Z}$ κ' $m \in \mathbb{N}$. Τότε :

$$\alpha = m \cdot q + r, \quad 0 \leq r < m \Rightarrow 0 \leq r \leq m-1$$

Άρα ο τυχόν $\alpha \in \mathbb{Z}$ έχει μία από τις παρακάτω μορφές :

$$\alpha = mq, \alpha = mq + 1, \dots, \alpha = mq + m - 1$$

$$r = 0 \quad r = 1 \quad \dots \quad r = m - 1.$$

Παράδειγμα : Αν α περιζώος ακέραιος τότε ο αριθμός α^2 είναι
της μορφής $\frac{2k+1}{2k+1}$ $k \in \mathbb{N}$.

0 & 8 & einen aus drei anderen koppelte: ~~4.9~~, ~~4.9+1~~, 4.9, 4.9+1, 4.9+2, 4.9+3.
 2.9205

Oμως α περιττός $\Rightarrow \alpha \nrightarrow \alpha$ ~~α~~ $\partial \alpha$ είναι 2ης μορφής
 $\alpha = 4 \cdot 9 + 1$ ή $\alpha = 4 \cdot 9 + 3$

(i) Av $\alpha = 4.9 + 1 \Rightarrow \alpha^2 = 8(2.9^2) + 8.9 + 1 =$
 $= \underline{\underline{8(2.9^2 + 9) + 1 = 8k + 1}}$
 k

(ii) Av $\alpha = 4 \cdot 9 + 3$ tout $\alpha^2 = \underbrace{(2 \cdot 9^2 + 3 \cdot 9 + 1)}_K = 8k + 1$.

Ορισμός: Έστω $a, b \in \mathbb{Z}$. Λέμε: ο a διαιρεί τον b και θα γράφουμε $a | b \Leftrightarrow \exists k \in \mathbb{Z} : b = k \cdot a$

Παράδειγμα : $4 \mid -20$ διότι $\exists (-5) \in \mathbb{Z} : -20 = (-5) \cdot 4$
 $15 \nmid 10$ διότι $\nexists k \in \mathbb{Z} : 10 = k \cdot 15$.

Αν $0 \neq \alpha$ δεν διαιρεί τον b , δηλ $\nexists k \in \mathbb{Z} : b = k \cdot \alpha$ και γράφουμε $\alpha \nmid b$.

Πρόσθευ: (Ιδιόμματα & διαπρεζόμενα)

① $\forall a \in \mathbb{Z} : a \neq 0 \wedge 0 \nmid b \Rightarrow b \neq 0$.

(2) $a|b \Leftrightarrow -a|b \Leftrightarrow a|-b \Leftrightarrow -a|-b \Leftrightarrow \cancel{a|a|b|}$

③ $\forall \alpha \in \mathbb{Z} : \alpha \mid \alpha$

(4) $A \vee a/b \wedge b/c \Rightarrow a/c$

⑤ Av $\alpha/b_i, i=1, \dots, n$, zot $\forall x_i, i=1, \dots, n, x_i \in \mathbb{Z} \Rightarrow$
 $\Rightarrow \alpha | (b_1 x_1 + \dots + b_n x_n)$

(6) $a/b \text{ e } c/d \Rightarrow a \cdot c / b \cdot d$

⑦ $a|b \Rightarrow a \cdot x | b \cdot x \quad \forall x \in \mathbb{Z}$.

⑧ $a|b$ & $b \neq 0 \Rightarrow |a| \leq |b|$

⑨ $a|b$ & $b|a \Rightarrow |a|=|b| \Rightarrow a=\pm b$.

Απόδειξη:

$$\begin{aligned} 5) \alpha | b_i, i=1, \dots, n &\Rightarrow \exists c_i \in \mathbb{Z} : b_i = c_i \alpha, 1 \leq i \leq n. \Rightarrow \\ &\Rightarrow \sum_{1 \leq i \leq n} b_i x_i = \sum_{1 \leq i \leq n} c_i x_i \cdot \alpha \Rightarrow b_1 x_1 + \dots + b_n x_n = c_1 x_1 \alpha + \dots + c_n x_n \alpha = \\ &= (c_1 x_1 + \dots + c_n x_n) \alpha \Rightarrow \\ &\Rightarrow \alpha | (b_1 x_1 + \dots + b_n x_n) \end{aligned}$$

$$7) \alpha | b \Rightarrow \exists c \in \mathbb{Z} : b = c \cdot \alpha \Rightarrow b \cdot x = c \cdot x \cdot \alpha \Rightarrow \alpha \cdot x | b \cdot x$$

$$88) \alpha | b \Rightarrow \exists c \in \mathbb{Z} : b = \alpha \cdot c \Rightarrow |b| = |\alpha \cdot c| = |\alpha| \cdot |c| \geq |\alpha| \quad (\text{δίνει } b \neq 0)$$

$\forall \alpha \in \mathbb{Z} : \alpha \alpha$	Ορίστε μια σχέση στο $\mathbb{Z}$:
$\begin{cases} \alpha b \\ b c \end{cases} \Rightarrow \alpha c$	
	$\alpha \sim b \Leftrightarrow \alpha b$
	Εκεί α ~ α (ανακλινόμενη)
	$\left. \begin{array}{l} \alpha \sim b \\ b \sim c \end{array} \right\} \Rightarrow \alpha \sim c \text{ (μεταβινητή)}$
	$\alpha \sim b \Leftrightarrow \alpha b \Leftrightarrow b \alpha \Leftrightarrow b \sim \alpha \text{ (δεν είναι αντικατασκευαστική)}$
	άρα δεν είναι σχέση ισοδυναμίας.

Παράδειγμα: α, b : περιζωτοί α κέραιοι $\Rightarrow 8 | \alpha^2 - b^2$.

$$\left. \begin{array}{l} \alpha : \text{περιζωτός} \Rightarrow \alpha^2 = 8k + 1, k \in \mathbb{N} \text{ (προηγ. παράδειγμα)} \\ b : \text{περιζωτός} \Rightarrow b^2 = 8\lambda + 1, \lambda \in \mathbb{N} \end{array} \right\} \Rightarrow$$

$$\Rightarrow \alpha^2 - b^2 = 8(k - \lambda) \Rightarrow 8 | \alpha^2 - b^2$$

Παράδειγμα: Να βρεθούν όλοι οι κέραιοι $m \in \mathbb{Z} : m+1 | m^2+1$.

Έστω ότι $\exists m \in \mathbb{Z} : m+1 | m^2+1$.

Όπως $m+1 | m+1$

$$\Rightarrow m+1 | m^2+1 + (m+1) = m^2+m+2 \Rightarrow$$

$$\Rightarrow m+1 | m(m+1)+2$$



$$\begin{aligned} m+1/m+1 &\Rightarrow m+1/m(m+1) \\ m+1/m(m+1)+2 &\Rightarrow m+1/(m+1)m+2-m(m+1) \rightarrow \end{aligned}$$

$$\Rightarrow m+1/2 \Rightarrow m+1/2 \leq 2$$

$$\text{Άρα } m+1=0 \quad m+1=1 \quad m+1=-1 \quad m+1=2 \quad m+1=-2 \Rightarrow$$

$$\Rightarrow m=-1 \quad m=0 \quad m=-2 \quad m=1 \quad m=-3$$

$$\bullet m=-1 \Rightarrow m+1=0$$

$$m^2+1=2 \Rightarrow 0/2 \Rightarrow 2=0 \text{ αλυσή}$$

$$m=0 \Rightarrow m+1=1$$

$$m^2+1=1 \quad | \text{6xδει}$$

$$\bullet m=-2 \Rightarrow m+1=-1$$

$$m^2+1=5 \quad | \text{6xδει}$$

... (όλες οι υποδοχές 6xδει)

Παράδειγμα: Νδo $9 \mid 10^{2015} + 3 \cdot 4^{2017} + 5$

$$10^{2015} + 3 \cdot 4^{2+2015} + 5$$

Γενικά Ο.δ.ο. $\forall n \geq 0$ 6xδει:

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

$$\bullet \text{Av } n=0 \text{ τότε } (10)^0 + 3 \cdot 4^{0+2} + 5 = 1 + 3 \cdot 4 + 5 = 17 \neq 6 \cdot 9 \Rightarrow$$

$$\Rightarrow 9 \mid 10^0 + 3 \cdot 4^2 + 5 \Rightarrow P(0) \text{ αληθής}$$

$$\bullet \text{Av } n=1 \text{ τότε } 10^1 + 3 \cdot 4^{1+2} + 5 = 207 = 23 \cdot 9 \Rightarrow$$

$$\Rightarrow 9 \mid 10^1 + 3 \cdot 4^{1+2} + 5 \Rightarrow P(1) \text{ αληθής}$$

Επαγωγική Υπόθεση: $9 \mid 10^k + 3 \cdot 4^{k+2} + 5, \forall k=1, \dots, n. (P(k) \text{ αληθής})$

Αρκεί νδo ότι $P(k+1)$ αληθής

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

$$= (9+1) \cdot 10^n + 12 \cdot 4^{n+2} + 5 =$$

$$= \cancel{(9+1)} \cdot 10^n + 9 \cdot 10^n + 10^n + 9 \cdot 4^{n+2} + 3 \cdot 4^{n+2} + 5$$

$$P(n) : 9 \mid 10^n + 3 \cdot 4^{n+2} + 5 \quad (1)$$

$$9 \mid 10^n \cdot 9 + 9 \cdot 4^{n+2} \quad (2)$$

$$\left. \begin{array}{l} (1) \\ (2) \end{array} \right\} \Rightarrow$$

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

$$= 10^{n+1} + 3 \cdot 4^{n+3} + 5 : P(n+1)$$

→

Αρα $P(n+1)$: αληθής κ' ανδ $AN \in \mathbb{Z} \rightarrow P(n)$ αληθής $\forall n \geq 0$.

ΠΑΡΑΤΗΡΗΣΗ : ① $\left. \begin{array}{l} \alpha | b \\ c | d \end{array} \right\} \Rightarrow \alpha + c | b + d$

π.χ. $\left. \begin{array}{l} 2 | 4 \\ 3 | 12 \end{array} \right\} \Rightarrow 2+3 | 4+12 \Rightarrow 5 | 16$ ΑΤΟΝΟ!

② • $1 | n, \forall n \in \mathbb{Z}$
 • $n | 1 \Leftrightarrow n = \pm 1$
 • $\alpha d | \alpha n \Rightarrow d | n$

• $\left. \begin{array}{l} d, n \in \mathbb{N} \\ d | n \end{array} \right\} \Rightarrow d \leq n$

③ $\left. \begin{array}{l} d | \alpha \\ d | \beta \end{array} \right\} \Rightarrow d | \alpha \pm \beta$

④ $\left. \begin{array}{l} \alpha, d \in \mathbb{N} \\ d | \alpha \\ d | \alpha + 1 \end{array} \right\} \Rightarrow \boxed{d = 1}$