02-11-12

Πρόταση: Αν $a_1, a_2, \dots, a_n \in \mathbb{Z}$, υπάρχει $k = 1, \dots, n$ $a_k \neq 0$, τότε:

$(a_1, a_2, \dots, a_n) = (a_1, a_2, \dots, a_{m-1}, (a_m, a_{m+1}, \dots, a_n))$, όπου $m < n$

Απόδειξη: Θέτουμε $d = (a_1, a_2, \dots, a_n)$, $\delta = (a_m, a_{m+1}, \dots, a_n)$

$d' = (a_1, a_2, \dots, a_{m-1}, \delta)$. Θδο: $d = d'$

$$d \mid a_i \Rightarrow \begin{cases} d \mid a_i \\ 1 \le i \le m-1 \end{cases} \Rightarrow \begin{cases} d \mid a_i \\ 1 \le i \le m-1 \\ d \mid \delta = (a_m, \dots, a_n) \end{cases} \Rightarrow$$
$$1 \le i \le n \qquad \begin{cases} d \mid a_i \\ m \le i \le n \end{cases}$$

$\Rightarrow d \mid d' = (a_1, \dots, a_{m-1}, \delta) \Rightarrow d \mid d'$ (1)

$$\bullet\ d' \mid a_i \Rightarrow \begin{cases} d' \mid a_i \\ 1 \le i \le m-1 \\ d' \mid a_i \\ m \le i \le n \end{cases} \Rightarrow \begin{cases} d' \mid a_i \\ 1 \le i \le n \end{cases} \Rightarrow$$
$1 \le i \le m-1$
και
$d' \mid \delta = (a_m, \dots, a_n)$

$\Rightarrow d' \mid d$ (2)

Απ' τις (1),(2) $\Rightarrow$ $d = d'$

πχ $(20, 35, 90) = (90, (20, 35))$ Πρόταση

$= (90, (4 \cdot 5, 5 \cdot 7)) = (90, 5) = (18 \cdot 5, 5) = 5$

• Λήμμα του Ευκλείδη

Αν $a,b,c \in \mathbb{Z}$ και $a \mid b \cdot c$, $(a,b)=1$ $\Rightarrow a \mid c$

Απόδειξη: $a \mid b \cdot c \Rightarrow bc = az$, για $z \in \mathbb{Z}$

$(a,b)=1 \Rightarrow \exists\, x,y \in \mathbb{Z} : ax+by=1 \Rightarrow$

$\Rightarrow c \cdot ax + c \cdot by = c \Rightarrow c = a \cdot c \cdot x + azy \Rightarrow$

$\Rightarrow c = a(cx+zy) \Rightarrow a \mid c$

• Πόρισμα (Λήμμα του Ευκλείδη): Αν p: πρώτος και $p \mid a \cdot b$, τότε $p \mid a$ ή $p \mid b$

Απόδειξη: Αν $p \nmid a \Rightarrow (p,a)=1 \xrightarrow[\text{Ευκλείδη}]{\text{Λήμμα του}} p \mid b$

(ομοίως για $p \nmid b$)

• Παρατήρηση: $15 \mid 45 = 5 \cdot 9$ όμως $15 \nmid 5$, $15 \nmid 9$

Ο λόγος είναι ότι δεν ισχύει $(15,9)=1$, $(15,5)=1$

• Πρόταση: Αν $a,b,c \in \mathbb{Z}$ και

$b \mid a$ και $c \mid a$, $(b,c)=1$ $\Rightarrow bc \mid a$

Απόδειξη: $b|a \Rightarrow a = bk$, για κάποιο $k \in \mathbb{Z}$

Αναλόγα, $c|a \Rightarrow a = c \cdot \lambda$, —ιι— $\lambda \in \mathbb{Z}$

$(b,c) = 1 \Rightarrow \exists\, x,y \in \mathbb{Z} : bx + cy = 1 \Rightarrow$

$\Rightarrow a \cdot b \cdot x + a \cdot c \cdot y = a \Rightarrow c \cdot \lambda \cdot b \cdot x + b \cdot k \cdot c \cdot y = a \Rightarrow$

$\Rightarrow bc(\lambda x + ky) = a \Rightarrow bc|a$

Παρατήρηση: $10|20$, $5|20$ και $5 \cdot 10 \nmid 20$

Ο λόγος είναι $(10,5) = 5 \neq 1$

Θεώρημα: Έστω $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$

όπου, $p_1 p_2, \ldots, p_n$: πρώτοι και $\alpha_i, \beta_i \geq 0$. Τότε:

$(a,b) = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \cdots p_k^{\min(\alpha_k, \beta_k)}$

Απόδειξη: Θέτουμε $d = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}$, όπου $\gamma_i = \min\limits_{1 \leq i \leq k} \{\alpha_i, \beta_i\}$

Θδο: $d = (a,b)$. Θα έχουμε

$\gamma_i = \min\{\alpha_i, \beta_i\} \begin{cases} \rightarrow \gamma_i \leq \alpha_i \\ \rightarrow \gamma_i \leq \beta_i \end{cases} \quad \forall\, i = 1, \ldots, k \xRightarrow{\circledast}$

$\circledast \begin{cases} a = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \text{ και } d \in \mathbb{Z} \\ d|a \Leftrightarrow d = p_1^{\beta_1} \cdots p_k^{\beta_k}, \quad 0 \leq \beta_i \leq \alpha_i, \quad i = 1, \ldots, k \end{cases}$

$\circledast \Rightarrow d|a$ και $d|b$ (1)

Έστω $\delta|a$ και $\delta|b$. Πρέπει να δω $\delta \le d$

Τότε: $\delta = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_k^{\lambda_k}$, $\lambda_i \ge 0$, $i = 1, \dots, k$

$\delta|a \overset{\circledast}{\Rightarrow} \lambda_i \le \alpha_i$, $i = 1, \dots, k$

$\delta|b \overset{\circledast}{\Rightarrow} \lambda_i \le b_i$, $i = 1, \dots, \lambda$ $\Bigg\} \Rightarrow$

$\lambda_i \le \min\{\alpha_i, \beta_i\} = \gamma_i$

Έπεται από την $\circledast$ ότι $\delta|d \Rightarrow \delta \le d$ (2)

Άρα, από τις (1), (2) $\Rightarrow d = (a, b)$

Παράδειγμα: $(2013, 2016) = ?$

$2013 = 3 \cdot 11 \cdot 61 = 2^0 \cdot 3^1 \cdot 7^0 \cdot 11^1 \cdot 61^1$

$2016 = 2^5 \cdot 3^2 \cdot 7 = 2^5 \cdot 3^2 \cdot 7^1 \cdot 11^0 \cdot 61^0$

$(2013, 2016) = 2^0 \cdot 3^1 \cdot 7^0 \cdot 11^0 \cdot 61^0 = 3$

Άσκηση: Αν $\{f_n\}_{n\geq 1}$: η ακολουθία Fibonacci

τότε : $(f_n, f_{n+1}) = 1 \quad \forall n \geq 1$ (*)

Λύση:

• για $n=1 \Rightarrow (F_1, F_2) = (1,1) = 1$

Επαγωγική Υπόθεση: $(f_n, f_{n+1}) = 1$, $\forall n \geq 2$

$(f_{n+1}, f_{n+2}) = d$. Θδο $d=1$

$f_{n+2} = f_n + f_{n+1}$

Όμως $\left.\begin{matrix} d \mid f_{n+1} \\ d \mid f_{n+2} \end{matrix}\right\} \Rightarrow \left.\begin{matrix} d \mid f_n \\ d \mid f_{n+1} \end{matrix}\right\} \Rightarrow d \mid (f_n, f_{n+1}) = 1$

$\Rightarrow d = 1$

Άρα από (ΑΜΕ) , η (*) ισχύει $\forall n \geq 1$

Άσκηση: Έστω $\alpha, n, m \in \mathbb{N}$ και n: περιττός . Τότε

$(\alpha^n - 1, \alpha^m + 1)$

Λύση: Έστω $d = (\alpha^n - 1, \alpha^m + 1) \Rightarrow \left\{\begin{matrix} d \mid \alpha^n - 1 \\ d \mid \alpha^m + 1 \end{matrix}\right.$

Έστω $\alpha^n - 1 = d \cdot r$, για $r \in \mathbb{Z}$

$\alpha^m + 1 = d \cdot s$, για $s \in \mathbb{Z}$ $\Rightarrow$

$\Rightarrow \left\{\begin{matrix} \alpha^n = d \cdot r + 1 \\ \alpha^m = d \cdot s - 1 \end{matrix}\right. \Rightarrow \left\{\begin{matrix} i) \ (\alpha^n)^m = (d \cdot r + 1)^m \overset{*}{\Rightarrow} \end{matrix}\right.$

* Διώνυμο Νεύτωνα: $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$

$\binom{n}{k} = \frac{n!}{k!(n-k)!}$

$\overset{*}{\Rightarrow} a^{nm} = \sum_{k=0}^{m} \binom{n}{k} (d\kappa)^k \Rightarrow$

$\Rightarrow a^{nm} = 1 + \sum_{k=1}^{n} \binom{n}{k} (d\kappa)^k = 1 + d\cdot A \quad (1)$

ii) $(a^m)^n = (ds-1)^n = (-(1-ds))^n = (-1)^n (1-ds)^n =$

n: περιττός $\quad -(1-ds)^n \overset{*}{=} -\sum_{k=0}^{n} \binom{n}{k} (-ds)^k =$

$= -\left(1 + \sum_{k=1}^{n} \binom{n}{k} (-ds)^k\right) = -(1 + dB') =$

$= -1 - dB' = -1 + dB \quad (2)$

$1 + dA = -1 + dB \Rightarrow 2 = d(B-A) \Rightarrow$

$\Rightarrow d \mid 2 \Rightarrow d = 1 \text{ ή } d = 2$

Άρα $(a^n - 1, a^m + 1) = 1 \text{ ή } 2$

• Αν α: περιττός τότε α^n, α^m: περιττοί

$$\Rightarrow \begin{cases} \alpha^n - 1 \\ \alpha^m + 1 \end{cases} \text{: άρτιοι} \Rightarrow \begin{matrix} 2 \mid \alpha^n - 1 \\ 2 \mid \alpha^m + 1 \end{matrix}$$

$$\Rightarrow 2 \mid (\alpha^n - 1, \alpha^m + 1) \Rightarrow 2 \leq (\alpha^n - 1, \alpha^m + 1) \leq 2$$

$\Rightarrow (\alpha^n - 1, \alpha^m + 1) = 2$ και αντίστροφα αν

$(\alpha^n - 1, \alpha^m + 1) = 2$, ο α: περιττός

Άρα, $(\alpha^n - 1, \alpha^m + 1) = 2 \iff \alpha$: περιττός

$(\alpha^n - 1, \alpha^m + 1) = 1 \iff \alpha$: άρτιος

Άσκηση: Να βρεθούν όλοι οι θετικοί ακέραιοι n οι οποίοι έχουν

α) 2
β) 3 } διαιρέτες
γ) 4

Λύση: α) Όλοι οι πρώτοι αριθμοί

β) Προφανώς $n > 1$ και $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ (πρωτ. ανάλυση)

Αν $k \geq 2$ τότε θα έχουμε ως διαιρέτες τους $1, p_1, p_2, n$ Άτοπο.

Άρα, $k = 1 \Rightarrow n = p_1^{\alpha_1}$

Αν $\alpha_1 \geq 3$ τότε θα έχουμε ως διαιρέτες τους $1, p_1, p_1^2, n$: Άτοπο

Άρα, $\alpha_1 = 2$, δηλαδή : $n = p_1^2$

γ) $n = p_1 \cdot p_2$, όπου p_1, p_2: πρώτοι και $p_1 \neq p_2$