

18/11/2016

ΑΣΚΗΣΗ ① Ο αριθμός $\sqrt{2}$ είναι άρρητος.

Έστω ότι $\sqrt{2} = \frac{a}{b}$, όπου $a, b \in \mathbb{Z}$ και $b \neq 0$.

Αν $d = (a, b)$ τότε $\begin{cases} d|a \Rightarrow a = d \cdot a' \\ d|b \Rightarrow b = d \cdot b' \end{cases} \Rightarrow$

$$\Rightarrow \sqrt{2} = \frac{a}{b} = \frac{d \cdot a'}{d \cdot b'} = \frac{a'}{b'} \text{ και τότε } (a', b') = 1 \Rightarrow$$

$$(\text{διότι: } d = (a, b) = (d \cdot a', d \cdot b') = d(a', b') \Rightarrow (a', b') = 1)$$

Αρα προπαίτε να υποθέσουμε ότι $\sqrt{2} = \frac{a}{b}$, όπου $a, b \in \mathbb{Z}$, $b \neq 0$
και $(a, b) = 1$

$$2 = \frac{a^2}{b^2} \Rightarrow a^2 = 2 \cdot b^2 \Rightarrow \begin{matrix} 2|a^2 \\ 2 \text{ πώτες} \end{matrix} \Rightarrow 2|a \text{ (*)} \Rightarrow a = 2 \cdot c \text{ για κάποιον } c$$

$$\text{Τότε } a^2 = 2b^2 \xrightarrow{(*)} (2c)^2 = 2b^2 \Rightarrow 4c^2 = 2b^2 \Rightarrow b^2 = 2 \cdot c^2 \Rightarrow$$

$$\Rightarrow \begin{matrix} 2|b^2 \\ 2 \text{ πώτες} \end{matrix} \Rightarrow 2|b \text{ (**)}$$

$$\text{Τότε (*), (**) } \Rightarrow \begin{matrix} 2|a \\ 2|b \end{matrix} \Rightarrow 2|(a, b) = 1 \Rightarrow 2|1 \text{ άτοπο.}$$

Αρα $\sqrt{2}$ άρρητος.

ΑΣΚΗΣΗ ② Το σύνολο των πρώτων επιδεικνύει τις προπαι (S OS)

(a) $3k+2$

(β) $4k+3$

(γ) $6k+5$

είναι άμειρο.

(α) Έστω ότι το γινόμενο των πρώτων της μορφής $3k+2$ είναι
 περιττός και έστω ότι έτσι οι πρώτοι της μορφής $3k+2$
 είναι οι $p_1, p_2, \dots, p_n$
 διαγράψτε τον αριθμό:

$$A = 3p_1 p_2 \dots p_{n-1} = 3p_1 p_2 \dots p_n - 3 + 2 = 3(p_1 p_2 \dots p_{n-1}) + 2 \quad \left(\begin{array}{l} \text{αριθμός} \\ \text{της μορφής} \\ 3k+2 \end{array} \right)$$

Έστω p : πρώτος διαρέτης του A . Τότε ο p δίνει
 τη μορφή $\begin{cases} 3k \\ 3k+1 \\ 3k+2 \end{cases}$

Αρραδιότητα διότι p πρώτος

Αν έτσι οι πρώτοι διαρέτες του A ήταν της μορφής $3k+1$, τότε
 από πρωτογενή ανάλυση του A , θα είχε πρώτους της μορφής $3k+1$.

$$\begin{aligned} \text{Όμως έχουμε } (3k_1+1)(3k_2+1) &= 3(3k_1 k_2) + 3k_1 + 3k_2 + 1 = \\ &= 3(3k_1 k_2 + k_1 + k_2) + 1 \end{aligned}$$

τότε ο A ως
 γινόμενο πρώτων της μορφής $3k+1$, θα ήταν της μορφής $3k+1$.
 Αυτό είναι άτοπο διότι ο A είναι της μορφής $3k+2$.

Άρα ο A θα έχει ταλάχιστον έναν πρώτο διαρέτη p της
 μορφής $3k+2$. Άρα $p = p_k, 1 \leq k \leq n$

$$\begin{aligned} \text{Τότε: } p &= p_k \mid A = 3p_1 \dots p_k p_{n-1} \\ p &= p_k \mid p_1 \dots p_k p_n \Rightarrow \\ p &= p_k \mid 3p_1 \dots p_k p_n \end{aligned} \quad \left\{ \begin{array}{l} p = p_k \mid 1: \text{ άτοπο} \\ \text{Άρα το γινόμενο των} \\ \text{πρώτων της μορφής} \\ 3k+2 \text{ είναι άπειρο.} \end{array} \right.$$

$$(6) A = 4p_1 \dots p_n - 1$$

$$(7) A = 6p_1 \dots p_{n-1} = 6p_1 \dots p_n - 6 + 5 = 6(p_1 \dots p_{n-1}) + 5$$

ΘΕΩΡΗΜΑ [Dirichlet] Αν $(a,b)=1$, τότε υπάρχουν άπειροι πρώτοι
 αριθμοί της μορφής $ak+b$.

ΑΣΚΗΣΗ 3 $(a,b)=1 \Rightarrow (a+b, a-b)=1$ n 2 (In repetition)
 $\Rightarrow (a+b, a-b, ab)=1$ n 2 (In repetition)
 Έστω $d=(a+b, a-b) \Rightarrow d|a+b$ $\left\{ \begin{array}{l} d|2a \\ d|2b \end{array} \right\} \Rightarrow$
 $d|a-b$

$\Rightarrow d|(2a, 2b) \Rightarrow d|2 \Rightarrow d=1$ n $d=2$
 $(2a, 2b)=2(a,b)=2$

• Αν a, b : άρτιοι $\Rightarrow a+b, a-b$: άρτιοι $\Rightarrow d \neq 1$ (όπως $(a,b)=1 \Rightarrow$
 $\Rightarrow$ άρα ας η η περίπτωση δει εφ' όσον

• Αν a, b : περιττοι $\Rightarrow$ $4|$ $\Rightarrow d=2$

• Αν a : άρτιος, b : περιττος, τότε $d \neq 2$, διότι τότε αν η a
 b : περιττος b : άρτιος $2|b$ άτονο n
 $2|a$: άτονο

Άρα $d=1$.

Παράδειγμα περίπτωση:

$(a_1, a_2, \dots, a_n) = (a_1, \dots, a_i, a_{i+1}, \dots, a_n)$, ~~$(a_1, a_2, \dots, a_n) = (a_1, \dots, a_i, a_{i+1}, \dots, a_n)$~~

$(a+b, a-b, ab) = ((a+b, a-b), ab) \xrightarrow{(a+b, a-b)=1} (1, ab) = 1$
 $\xrightarrow{(a+b, a-b)=2} (2, ab) = 1$ n 2

- a, b : άρτιοι $\Rightarrow$ d : άρτιος $(a,b)=1$
- ~~a, b~~ a, b : περιττοι, τότε $(2, ab)=1$
- αν a : άρτιος n a : περιττος
 b : περιττος b : άρτιος

ΑΣΚΗΣΗ 4 Αν $a, n, m \in \mathbb{N}$ και ο n είναι περιττός, να βρεθεί ο $d = (a^n - 1, a^m + 1)$

$$d \mid a^n - 1 \Rightarrow a^n - 1 = d \cdot r, \text{ για κάποιο } r \in \mathbb{Z} \Rightarrow a^n = d \cdot r + 1$$

$$d \mid a^m + 1 \Rightarrow a^m + 1 = d \cdot s, \text{ για κάποιο } s \in \mathbb{Z} \Rightarrow a^m = d \cdot s - 1$$

Αιώνιο του Νεύτωνα:

$$(x+y)^n = \sum_{k=0}^n \binom{n}{k} x^k y^{n-k}$$

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

$$\begin{aligned} (a^n)^m &= a^{n \cdot m} = (d \cdot r + 1)^m = \sum_{k=0}^m \binom{m}{k} (d \cdot r)^k = 1 + \sum_{k=1}^m \binom{m}{k} (d \cdot r)^k = \\ &= 1 + d \cdot A, \text{ για κάποιο ακέραιο } A. \end{aligned}$$

$$\begin{aligned} (a^m)^n &= a^{m \cdot n} = (d \cdot s - 1)^n = (-1)^n (1 - d \cdot s)^n = -(1 - d \cdot s)^n = - \sum_{k=0}^n \binom{n}{k} (-d \cdot s)^k = \\ &= - \left(1 + \sum_{k=1}^n \binom{n}{k} (-d \cdot s)^k \right) = -(1 + d \cdot B), \text{ όπου } B: \text{ακέραιος} \end{aligned}$$

$$\begin{aligned} a^{n \cdot m} &= 1 + d \cdot A \\ a^{n \cdot m} &= -(1 + d \cdot B) = -1 - d \cdot B \end{aligned} \quad \left| \Rightarrow 1 + d \cdot A = -1 - d \cdot B \Rightarrow 2 = d(-A - B) \Rightarrow \right.$$

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

$$\text{Άρα: } d = (a^n - 1, a^m + 1) = \begin{cases} 1 \\ 2 \end{cases}$$

• Αν a περιττός τότε, το a^n και το a^m περιττά, άρα $a^n - 1, a^m + 1$ άρτια $\Rightarrow d = (a^n - 1, a^m + 1) = 2$

• Αν a άρτιος τότε $d = (a^n - 1, a^m + 1) = 1$

ΛΗΜΜΑ: Έστω a, b ακέραιοι και $b \neq 0$. Τότε για το χ αναδικο
 ζεύγος ακεραίων q, r ισχύει: $a = bq + r$, $0 \leq r < |b|$

ισχύει ότι: $(a, b) = (b, r)$

Απόδειξη: Έστω $d = (a, b)$ Τότε: $d | a$
 $\delta = (b, r)$ $d | b \Rightarrow d | bq$ $\left. \vphantom{\begin{matrix} d | a \\ d | bq \end{matrix}} \right\} \Rightarrow$

$$\left\{ \begin{array}{l} d | a - bq = r \\ d | b \end{array} \right\} \Rightarrow d | (b, r) = \delta \Rightarrow d | \delta \quad (1)$$

$$\text{Τότε: } \begin{array}{l} \delta | b \\ \delta | r \end{array} \Rightarrow \begin{array}{l} \delta | bq \\ \delta | r \end{array} \Rightarrow \delta | bq + r = a \Rightarrow \delta | a \left\{ \begin{array}{l} \delta | a \\ \delta | b \end{array} \right\} \Rightarrow \delta | (a, b)$$

Άρα $\delta | d$ (2)

ΑΠΟΡΙΣΜΟΣ ΤΟΥ ΕΥΚΛΕΙΗ

για την εύρεση του ΜΚΔ δύο ακεραίων

Έστω $a \in \mathbb{Z}$ και έστω $b \neq 0$. Γνωρίζοντας $(a, b) = (|a|, |b|)$, μπορούμε
 να υποθέσουμε ότι $a, b > 0$.

Τυπικά επιλέγουμε την γενικότερη υποθέτουμε ότι: $a \geq b > 0$. Θέτουμε $r_0 = a$
 $r_1 = b$

$$r_0 = r_1 q_1 + r_2, \quad 0 \leq r_2 < r_1$$

$$r_4 < r_3 < r_2 < r_1 \neq b$$

$$r_1 = r_2 q_2 + r_3, \quad 0 \leq r_3 < r_2$$

$$r_2 = r_3 q_3 + r_4, \quad 0 \leq r_4 < r_3$$

$\vdots$

Από τη διαδοχική Ευκλείδεια διαίρεση, θα σταματήσει διότι
 η πορεία φθάνει ακολουθία των υπολοίπων r_k , θα φθάσει
 να μηδενιστεί και έτσι αν από βγει γίνει $r_{n+1} = 0$

$$r_{n-2} = r_{n-1} q_{n+1} + r_n, \quad 0 \leq r_n < r_{n-1}$$

$$r_{n-1} = r_n q_n + \cancel{r_{n+1}^0}$$

$$(a, b) = (r_0, r_1) = (r_1, r_2) = (r_2, r_3) = \dots = (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n) = \\ = (r_n q_n, r_n) = r_n (q_n, 1) = r_n$$

Ο ΜΚΔ των a, b είναι το τελευταίο μη μηδενικό υπόλοιπο στη
 ακολουθία των διαδοχικών Ευκλείδειων διαίρεσεων.