30/10/2017

Θεώρημα: (Ευκλείδεια διαίρεση)
Για κάθε ζεύγος φυσικών a, b ($a \in \mathbb{N}_0$ κ' $b \in \mathbb{N}_0$) υπάρχει μοναδικό ζεύγος ακεραίων q, r έτσι ώστε

$$\underbrace{a = bq + r}_{q:\ \text{πηλίκο},\ r:\ \text{υπόλοιπο}} \quad \text{και} \quad 0 \leq r < b$$

Απόδειξη: $S = \{\underbrace{a - bx}_{\in \mathbb{Z}}\}$ $x \in \mathbb{N}$ και $a - bx \geq 0$

$\boxed{S \subseteq \mathbb{N}_0}$

για $x = 0$: $a = a - b \cdot 0 \geq 0 \Rightarrow a \in S$ $\quad S \neq \emptyset$

Άρα από αρχή καλής διάταξης γνωρίζουμε ότι το S έχει ελάχιστο στοιχείο.

Το ελάχιστο στοιχείο του S το συμβολίζουμε με r.

$r \in S \Rightarrow r = a - bq \Rightarrow a = bq + r$

$r \in S \Rightarrow r \geq 0$

$r - b \in \mathbb{Z}$, $r - b = a - bq - b = a - b(q+1)$

$r - b < r$

1η περίπτωση: $r - b \geq 0 \Rightarrow r - b \in S \Rightarrow r - b < r =$ το ελάχιστο στοιχείο του $S \Rightarrow$ ΑΤΟΠΟ

2η περίπτωση: $r - b < 0 \Rightarrow r < b$

Έστω ότι $a = bq' + r'$ $\quad 0 \leq r' < b$

$-a = bq + r$

$a - a = bq - bq' + r - r'$

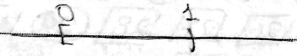
Έστω ότι το r είναι μεγαλύτερο ή ίσο από το r'

$0 = bq - bq' + r - r'$

$0 \le r - r' = b(q'-q)$ (1)

$$0 \le r - r' \le r < b \Rightarrow 0 \le b(q'-q) \le r < b \Rightarrow 0 \le b(q'-q) < b \quad , b \in \mathbb{N}$$

$$0 \le q'-q < 1$$



$q'-q \in [0,1)$ Επίσης q', q ακέραιοι $\Rightarrow q'-q \in \mathbb{Z}$

Άρα $q'-q = 0 \Rightarrow q' = q$

(1) $\Rightarrow r - r' = b(q-q') \overset{q'-q=0}{\Rightarrow} r - r' = 0 \Rightarrow r = r'$

Άρα τα q, r είναι μοναδικά

Θεώρημα: Για κάθε ζεύγος ακεραίων a, b με $b \neq 0$ υπάρχει μοναδικό ζεύγος ακεραίων q, r έτσι ώστε

$$a = bq + r \quad 0 \le r < |b|.$$

Απόδειξη: $a, b \in \mathbb{Z} \Rightarrow |a| \in \mathbb{N}_0$ και $|b| \in \mathbb{N}$

$\Rightarrow$ Υπάρχει μοναδικό ζεύγος q, r έτσι ώστε

$$|a| = |b|q + r \quad 0 \le r < |b|.$$

Περιπτώσεις:

i.) $a \ge 0 \ , b > 0 \Rightarrow a = bq + r \quad 0 \le r < b = |b|$

ii.) $a \ge 0 \ , b < 0 \Rightarrow a = -bq + r \Rightarrow 0 \le r < |b| = -b$

$a = b(-q) + r \quad 0 \le r < |b| = -b$

iii.) $a < 0 \ , b > 0 \quad -a = bq + r \quad 0 \le b < |b|.$

$a = b(-q) - r \quad -b < -r \le 0$

iiiα.) $r = 0 \quad : a = b(-q) + 0 = b(-q)$

iiiβ.) $0 < r < b \quad : a = b(-q) + r$ (*)

$-b < -r < 0 \overset{\text{προσθέτω } b}{\Rightarrow} b - b < b - r < b \Rightarrow 0 < b - r < b$

(*) $\Rightarrow a = b(-q) - r \Rightarrow a = b(-q) - b + b - r$

$a = b(-q-1) + b - r \qquad 0 \le b - r < b$

iv.) $a < 0 \quad , b < 0 \qquad |a| = |b|q + r \qquad 0 \le r < |b|$

$-a = -bq + r$

$a = bq - r \cdot a \quad , \quad -|a| < -r < 0$

iva.) $r = 0 \qquad a = bq + 0 = bq + r$

iv.β.) $0 < r < b \Rightarrow$ αφαιρώ b

$b < -r \le 0$

• $b - b < -r - b < -b$

$0 < -r - b < |b|$

(a) $\Rightarrow a + bq + b - r - b \Rightarrow b(q+1) - r - b$

Παραδείγματα:

1.) $25 = 7 \cdot \boxed{3} + \boxed{4}$

$25 = -7 \cdot \boxed{-3} + \boxed{4}$

$-25 = 7 \cdot \boxed{-4} + \boxed{3}$

$-25 = -7 \cdot \boxed{4} + \boxed{3}$

Θεώρημα:

$b \neq 0 \qquad b, a \in \mathbb{Z}$

$b|a \Leftrightarrow$ το υπόλοιπο της διαίρεσης του a με το b είναι 0.

Απόδειξη: $(\Leftarrow)$ $a = bq \Rightarrow b|a$

$(\Rightarrow)$ $b|a$

$a = bq + r \qquad 0 \le r < |b|$

$b | a = bq + r$ \
$b | bq$ > Η διαφορά τους θα είναι πολ/σιο του b.

Άρα $b|r \Rightarrow r = b \cdot c$ (1)

$0 \le r < |b| \overset{(1)}{\Rightarrow}$

$0 \le b \cdot c < |b| \Rightarrow$

$0 \le |b \cdot c| < |b| \Rightarrow 0 \le |c| < 1 \qquad c \in \mathbb{Z}$

Άρα $|c| = 0 \Rightarrow$

Άρα (1) $\Rightarrow r = 0$.

Οι σύνθετοι αριθμοί μπορούν να γράφουν στην μορφή $\omega = c \cdot d$ $\quad 1 < c < \omega$

$1 < d < \omega$

Θεώρημα: Κάθε φυσικός αριθμός $a > 1$ έχει τουλάχιστον ένα διαιρέτη που είναι πρώτος αριθμός

$S = \{\omega \mid \omega \in \mathbb{N},\ \omega \mid a$ και $\omega \neq 1\}$

Απόδειξη: Το $a \in S \Rightarrow S \neq \emptyset$. Άρα από αρχή καλής διάταξης έχει ελάχιστο στοιχείο το p.

p ελάχιστο στοιχείο του $S \Rightarrow p \in S \Rightarrow p \neq 1,\ p \in \mathbb{N},\ p \mid a$

Έστω p σύνθετος $\Rightarrow p = c \cdot d$ $\quad 1 < c < p$

$1 < d < p$

Ξέρουμε $c > 1$ $\quad c \mid p \mid a$ άρα $c \mid a$

$c \in S$ και $c < p$ Άτοπο

γιατί το p ελάχιστο στοιχείο

$p \neq 1$, p δεν είναι σύνθετος. Άρα p πρώτος

Θεώρημα: (Ευκλείδη): Το πλήθος των πρώτων αριθμών είναι άπειρο.

Απόδειξη: Έστω ότι το πλήθος των πρώτων αριθμών είναι πεπερασμένο και έστω ότι αυτοί είναι $p_1, p_2, p_3,$ p_4, p_5, p_n

$a = p_1, p_2, \ldots, p_{n+1}$

$a > 1 \Rightarrow$ Το a έχει τουλάχιστον ένα διαιρέτη που είναι πρώτος αριθμός έστω το p_s

$p_s \mid a = p_1 p_2 \cdots p_{n+1}$ $\Big\}$ $\quad$ διαφορά τους $= 1$ πολλ/σιο το p_s $\rightarrow$

$p_s \mid p_1 p_2 \cdots p_s \cdots p_n$

$p_s \mid 1 \Rightarrow p_s = 1$ το p_s δεν είναι πρώτος Άτοπο! Άρα το πλήθος των πρώτων αριθμών είναι άπειρο

Θεώρημα: Για κάθε φυσικό αριθμό "n" σε πλήθος διαδοχικών φυσικοί αριθμοί
$(n+1)!+2,\ (n+1)!+3 \ldots (n+1)!\,(n+1)$ είναι σύνθετοι αριθμοί
↳ τυχαίο $(n+1)!+k$
$2 \leq k \leq n+1$

Απόδειξη: $2 \mid (n+1)!+2$ $\quad 1 < 2 < (n+1)!+2$
Άρα $(n+1)!+2$ σύνθετος

Ομοίως $3 \mid (n+1)!+3$ $\quad 1 < 3 < (n+1)!+3$

Άρα $(n+1)!+3$ σύνθετος

$k \mid (n+1)!+k$ $\quad 1 < k \leq n+1 < (n+1)!+k$
$(n+1) \mid (n+1)!+(n+1)$ $\quad 1 < n+1 < (n+1)!+(n+1)$