2/11/2017

→ Υπάρχουν άπειροι πρώτοι αριθμοί

→ Μπορώ να βρω ν-διαδοχικούς αριθμούς που κανείς από αυτούς δεν είναι πρώτος

ΘΕΩΡΗΜΑ Κάθε σύνθετος αριθμός $a>1$ έχει τουλάχιστον ένα πρώτο διαιρέτη $p\leq\sqrt{a}$

Απόδειξη

a-σύνθετος: $a=c\cdot d$ $\quad 1<c<a$
$\quad 1<d<a.$

Χ.β.γ. $c\leq d.$

Τότε $c\leq d \Rightarrow c^2\leq c\cdot d=a \Rightarrow c\leq\sqrt{a}$

$c>1. \xRightarrow[\text{θεωρ.}]{\text{από}} \exists p$ πρώτος τ.ω. $p|c.$

$\left.\begin{matrix} p|c \\ c|a \end{matrix}\right\} \Rightarrow p|a$, p πρώτος

και αφού $p|c \Rightarrow p\leq c\leq\sqrt{a}$

ΘΕΩΡΗΜΑ: Αν ένας φυσικός αριθμός $a>1$ δεν διαιρείται από κάποιο πρώτο αριθμό $p\leq\sqrt{a}$, τότε ο a είναι πρώτος αριθμός.

$a>1 \Rightarrow$ a ~~σύνθετος~~ γιατί δεν έχει κάποιο πρώτο διαιρέτη
ή
a πρώτος

Άρα ο a πρώτος.

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	28	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	58	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	86	~~87~~	88	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Κόσκινο
του
Ερατοσθένη

Μαθηματικός
Αστρονόμος
Φιλόλογος.

Θα βρούμε τους πρώτους.
Το 2 είναι. Τα πολ/σια του 2 όχι.
Το 3 είναι. Τα πολ/σια του όχι.
Όμοια για το 7 και τα πολ/σια του.
→ Όσοι αριθμοί έμειναν είναι ~~[illegible]~~ πρώτοι.

δεκαδικό σύστημα αρίθμησης.

$$\begin{array}{r|l} 345 & 10 \\ \cline{2-2} 30 & 34 \\ \cline{1-1} 45 & \\ 5 & \end{array}$$

Άρα $345 = 34 \cdot \underline{\underline{10}} + 5. = \cancel{34}(3 \cdot 10 + 4) \cdot 10 + 5$
$= 3 \cdot 10^2 + 4 \cdot 10 + 5$

$$\begin{array}{r|l} 34 & 10 \\ \cline{2-2} 30 & 3 \\ \cline{1-1} 4 & \end{array}$$

$34 = 3 \cdot 10 + 4.$

εφταδικό σύστημα αρίθμησης

Άρα $345 = 49 \cdot 7 + 2$

$$\begin{array}{r|l} 345 & 7 \\ \cline{2-2} 28 & 49 \\ \cline{1-1} 65 & \\ 63 & \\ \cline{1-1} 2 & \end{array}$$

$$\begin{array}{r|l} 49 & 7 \\ \hline 49 & 7 \\ 0 & \end{array} \qquad \begin{array}{r|l} 7 & 7 \\ \hline 7 & 1 \\ 0 & \end{array} \qquad \begin{array}{r|l} 1 & 7 \\ \hline 1 & \end{array}$$

$345 = 49 \cdot 7 + 2 = 7^3 + 2$

$(1002)_7$ → τα υπόλοιπα.

$= 7^3 + 0 \cdot 7^2 + 0 \cdot 7 + 2$

δυαδικό σύστημα αρίθμησης

$$\begin{array}{r|l} 345 & 2 \\ \hline 2 & 172 \\ 14 & \\ 14 & \\ 005 & \\ 4 & \\ 1 & \end{array} \qquad \begin{array}{r|l} 172 & 2 \\ \hline 16 & 86 \\ 12 & \\ 12 & \\ 0 & \end{array} \qquad \begin{array}{r|l} 86 & 2 \\ \hline 8 & 43 \\ 06 & \\ 6 & \\ 0 & \end{array} \qquad \begin{array}{r|l} 43 & 2 \\ \hline 4 & 21 \\ 03 & \\ 2 & \\ 1 & \end{array} \qquad \begin{array}{r|l} 21 & 2 \\ \hline 2 & 10 \\ 01 & \end{array}$$

$(345)_{10} = 2 \cdot 172 + 1 = 2^2 \cdot (86) + 1$

$= 2^3 (43) + 1$

$= 2^3 (2 \cdot 21 + 1) + 1$

$= 2^4 \cdot 21 + 2^3 + 1$

$= 2^4 (2 \cdot 10 + 1) + 1 \cdot 2^3 + 1$

$= 2^5 \cdot (10) + 1 \cdot 2^4 + 2^3 + 1$

$= 2^5 (2 \cdot 5 + 0) + 2^4 + 2^3 + 1$

$= 2^6 \cdot (5) + 2^4 + 2^3 + 1$

$= 2^6 (2 \cdot 2 + 1) + 2^4 + 2^3 + 1$

$= 2^8 + 2^6 + 2^4 + 2^3 + 1$

$= (101011001)_2$

Άσκηση 10 / Φυλ. #3

$(2052)_6 = 2\cdot 6^3 + 0\cdot 6^2 + 5\cdot 6 + 2$ → στο δεκαδικό.

Μέγιστος Κοινός Διαιρέτης

Ορισμός: Έστω $a_1, a_2, \dots, a_n$ ακέραιοι αριθμοί από τους οποίους ένας τουλάχιστον είναι διάφορος του μηδενός. Ο μέγιστος κοινός διαιρέτης των $a_1, \dots, a_n$ είναι ένας φυσικός αριθμός d τ.ω.

i) $d | a_1, d | a_2, \dots, d | a_n$.

ii) Αν $\delta | a_1, \delta | a_2, \dots, \delta | a_n$ τότε το $\delta \le d$

→ Δεν θέλω όλοι οι $a_1, \dots, a_n$ να είναι μηδέν γιατί έχει διαιρέτες όλους τους αριθμούς άρα δεν υπάρχει ΜΚΔ.

Μ.Κ.Δ(35, 25, 65)

1	1	1	κοινοί διαιρέτες
5	5	5	→ μέγιστος κοινός διαιρέτης
7	25	13	
35		65	

ΘΕΩΡΗΜΑ: Αν $d = \mu.\kappa.\delta(a_1, a_2, \dots, a_n)$ τότε υπάρχουν ακέραιοι $\lambda_1, \dots, \lambda_n$ τέτοιοι ώστε $d = \lambda_1 \cdot a_1 + \lambda_2 \cdot a_2 + \dots + \lambda_n \cdot a_n$.

π.χ. $5 = \boxed{3} \cdot 35 + \boxed{-4} 25 + \boxed{0} 65$

ή $5 = \boxed{-1} 35 + \boxed{-1} 25 + \boxed{1} 65$

υπάρχουν άπειροι συνδυασμοί.

Απόδειξη

$S = \{x_1 \cdot a_1 + x_2 \cdot a_2 + \dots + x_n \cdot a_n \mid x_i \in \mathbb{Z}, 1 \le i \le n\} \subseteq \mathbb{Z}$

Υπάρχει $a_i \neq 0$ $\quad a_i = \boxed{0} a_1 + \boxed{0} a_2 + \dots + \boxed{1} a_i + \dots \in S$

$-a_i \neq 0 \quad -a_i = \boxed{0} a_1 + \boxed{0} a_2 + \dots + \boxed{-1} a_i + \dots \in S$

$$\left.\begin{array}{l} a_i \in S \text{ και } -a_i \in S \\ a_i \neq 0 \end{array}\right\} \Rightarrow$$

$\Rightarrow S \cap \mathbb{N} \neq \emptyset$ γιατί ή a_i ή $-a_i \in \mathbb{N}$.

Αρχής καλής διάταξης $\Rightarrow$ το $S \cap \mathbb{N}$ έχει ελάχιστο στοιχείο l.

$\Rightarrow l \in \mathbb{N}$

Θ.δ.ο. $l = d$

$l \in S \Rightarrow l = \lambda_1 a_1 + \lambda_2 \cdot a_2 + \dots + \lambda_n \cdot a_n$

Ισχυρίζομαι ότι $S \overset{?}{=} l \cdot \mathbb{Z} = \{l \cdot m \mid m \in \mathbb{Z}\}$

$(\supseteq)$ $l \cdot m \in l \cdot \mathbb{Z} \Rightarrow l \cdot m = (\lambda_1 \cdot a_1 + \lambda_2 \cdot a_2 + \dots + \lambda_n a_n) m$
$= \lambda_1 \cdot m \cdot a_1 + \lambda_2 \cdot m \cdot a_2 + \dots + \lambda_n \cdot m \cdot a_n \in S$

(C) Έστω $k \in S \Rightarrow k = k_1 \cdot a_1 + k_2 \cdot a_2 + \ldots + k_n \cdot a_n$

$k, l \in \mathbb{Z}$, $l \neq 0$ (αφού $l \in \mathbb{N}$)

$\xrightarrow{\text{Ευκλ.}}$ $k = l \cdot q + r$, $0 \leq r < l$

Θ.δ.ο. $r = 0$

$r = k - l \cdot q = (k_1 a_1 + \ldots + k_n \cdot a_n) - (\lambda_1 a_1 + \ldots + \lambda_n a_n)$

$(k_1 - \lambda_1 \cdot q) a_1 + \ldots + (k_n - \lambda_n \cdot q) \cdot a_n$

$\Rightarrow r \in S$

$0 \leq r < l <$ i) $0 < r < l$, ii) $r = 0$

i) Έστω $0 < r < l$. Ξέρω ότι $r \in S \Rightarrow$ $r \in \mathbb{N}$ άρα $r \in S \cap \mathbb{N}$

και $r < l$ το l είναι το ελάχιστο στοιχείο του $S \cap \mathbb{N}$ Άτοπο

Συνεπώς, $r = 0 \Rightarrow k = l q$

Άρα $S = l \cdot \mathbb{Z}$.

$a_1 = 1 \cdot a_1 + 0 \cdot a_2 + \ldots + 0 \cdot a_n \Rightarrow a_1 \in S$
$\Rightarrow l / a_1$

$a_2 = 0 \cdot a_1 + 1 \cdot a_2 + \ldots + 0 \cdot a_n \Rightarrow a_1 \in S \Rightarrow l / a_2$

$\vdots$

$a_n = 0 \cdot a_1 + 0 \cdot a_2 + \ldots + 1 a_n \Rightarrow l / a_n$.

Άρα l κοινός διαιρέτης.

Έστω $\delta / a_1, \delta / a_2, \ldots, \delta / a_n$ (Θ.δ.ο $\delta \leq l$)

$\delta / \ell \Longrightarrow \delta \leq \ell$.

Άρα το ℓ είναι ο Μ.Κ.Δ. των $a_1, a_2, \dots, a_n$.

$\Rightarrow d = \ell = \lambda_1 \cdot a_1 + \lambda_2 \cdot a_2 + \dots + a_n \cdot \lambda_n$.

Παράδειγμα

μ.κ.δ (35,25)

$35 = 1 \cdot \underbrace{25} + \underbrace{10}$

$25 = 2 \cdot \underbrace{10} + \underbrace{5} \longrightarrow$ Το τελευταίο μη μηδενικό υπόλοιπο είναι ο Μ.Κ.Δ.

$10 = 2 \cdot 5 + 0$

$5 = 25 - 2 \cdot 10 = 25 - 2 \cdot (35 - 25)$

$= 25 - 2 \cdot 35 + 2 \cdot 25$

$= 3 \cdot 25 - 2 \cdot 35$