

26/10/2015

ΚΡΙΤΗΡΙΟ ΓΙΑ ΤΟ ΑΝ Ο $a > 1$ ΕΙΝΑΙ ΠΡΩΤΟΣ: Αν a θετικός ακεραίος

όπου $a > 1$, και αν ο a δεν διαιρείται από κανέναν πρώτο p με $p \leq \sqrt{a}$, τότε ο a : πρώτος.

ΚΟΣΚΙΝΟ ΤΟΥ ΕΡΑΤΟΣΘΕΝΗ: Μέθοδος εύρεσης όλων των πρώτων αριθμών $p \leq a$, όπου $a \in \mathbb{N}$, $a > 1$.

- Γράψαμε τις αριθμούς: $2, 3, 4, \dots, a-1, a$.
- Διαγράψαμε όλα τα γινόμενα πολλαπλασιασμού του 2: $2 \cdot 2, 2 \cdot 3, \dots$.
Ο πρώτος στη σειρά που βέβαια είναι ο 3, ο οποίος είναι πρώτος.
- Διαγράψαμε όλα τα γινόμενα πολλαπλασιασμού του 3: $3 \cdot 3, 3 \cdot 5, \dots$ (τα $3 \cdot 2, 3 \cdot 4$ έχουν ήδη διαγραφεί).
- Ο πρώτος στη σειρά που βέβαια είναι ο 5, ο οποίος είναι πρώτος.
- Συνεχίζουμε αυτή τη διαδικασία θα έχουμε διαγράψει όλα τα γινόμενα πολλαπλασιασμού του p , $\forall p$: πρώτος $\leq \sqrt{a}$.
- Οι αριθμοί που θα μείνουν θα είναι οι πρώτοι $\leq a$.

Σαν άσκηση: η ίδια διαδικασία μέχρι το 100

2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19
20	21	23	24	25	26	27	29	30

Σε αυτή κρυπτογραφία χρησιμοποιούνται αριθμοί $n \sim 10^{100}$ και γίνεται την εύρεση των πρώτων διαιρετών του n και τότε θα πρέπει να ελεγχάμε περίπου: $8 \cdot 10^{47}$ πρώτους αριθμούς
↳ είναι περίπου

ΘΕΜΕΛΙΩΔΕΣ ΘΕΩΡΗΜΑ ΑΡΙΘΜΗΤΙΚΗΣ: Κάθε θετικός ακέραιος $a > 1$,

μπορεί να γραφεί ως γινόμενο πρώτων αριθμών, όχι κατ'αύστην διαφορετικών με μοναδικό τρόπο

ΘΕΩΡΗΜΑ: Κάθε θετικός ακέραιος $a > 1$, μπορεί να γραφεί ως γινόμενο πρώτων αριθμών.

Απόδειξη: (1) Αν $a=2$ τότε ο a είναι κατα προφανή τρόπο γινόμενο πρώτων αριθμών.

(2) Έστω $a > 2$.

Επαγωγική Υπόθεση: Υποθέτουμε ότι το ζητούμενο ισχύει για κάθε θετικό ακέραιο $< a$

Τότε: (α) Αν ο a είναι πρώτος, τότε όπως και πριν ο a γράφεται κατα προφανή τρόπο ως γινόμενο πρώτων αριθμών.

(β) Αν ο a είναι σύνθετος, τότε $a = bc$, όταν $1 < b, c < a$

Από την επαγωγική υπόθεση θα έχουμε: $b = p_1 \dots p_k$ και $c = q_1 \dots q_l$

όπου p_i, q_j : πρώτοι αριθμοί.

Τότε $a = p_1 \dots p_k \cdot q_1 \dots q_l$: γινόμενο πρώτων αριθμών. Άρα από την Αρχή Μαθηματικής Επαγωγής το ζητούμενο ισχύει $\forall a > 1$.

Αν $a = p_1 \dots p_k$ όπου $p_1, \dots, p_k, q_1, \dots, q_l$ είναι πρώτοι αριθμοί $= q_1 \dots q_l$, τότε θα λέμε ότι έχουμε μοναδικότητα στη γραφή του a ως γινόμενο πρώτων.

αν: $k=l$ και κάθε p_i είναι ίσος με ένα q_j [10 = 2 · 5]

□

ΠΑΡΑΜΕΤΡΙΑ: $X = \text{όλοι οι θετικοί άρτιοι αριθμοί} = \{2, 4, 6, 8, \dots\}$
 Ένας "πρώτος" άρτιος a είναι ένας άρτιος ο οποίος δεν μπορεί να γραφεί ως $a = b \cdot c$, όπου b, c άρτιοι.
 Για παράδειγμα 6, 10, 14... είναι "πρώτοι" άρτιοι.
 8, 16, ... δεν είναι "πρώτοι" άρτιοι.
 $60 = 6 \cdot 10$ } 2 διαγώνως γράφει στο 60 ως γινόμενο
 $= 2 \cdot 30$ } "πρώτων" άρτιων.

ΘΕΩΡΗΜΑ: Αν p : πρώτος άρτιος, και $a, b \in \mathbb{Z}$, έτσι ώστε $(p|a \cdot b)$, τότε:
 $p|a$ ή $p|b$

Απόδειξη: Αν $a=0$ ή $b=0$, τότε προφανώς $p|0$ και άρα το συμπέρασμα ισχύει. Έστω $p|x \Leftrightarrow p||x|$, μπορούμε να υποθέσουμε ότι $(a, b \in \mathbb{N})$ θεωρούμε το αλγόριθμο αλγόριθμο:

$$X = \{x \in \mathbb{N} \mid p|ax\}$$

Τότε το $X \neq \emptyset$ διότι: $b \in X$ (διότι $p|ab$, από την υπόθεση)
 $p \in X$ ($p|ap$)

* Από την ΑΡΧΗ ΚΑΛΗΣ ΔΙΑΤΑΞΗΣ το X έχει ελάχιστο στοιχείο, έστω $\theta = \min X$. Τότε ιδιαιτέρως: $p|a\theta$
 $\theta \theta_0: \theta|x, \forall x \in X$ *

Από την Ευκλείδεια Διαιρέση: $x = \theta q + r$, όπου $0 \leq r < \theta$

Τότε: $ax = a\theta q + ar$ και $x \in X \Rightarrow p|ax$
 $\theta \in X \Rightarrow p|a\theta \Rightarrow p|a\theta q$ $\Rightarrow$

$\Rightarrow p|ax - a\theta q \Rightarrow p|ar$

Αν $r \neq 0$, τότε $r \in \mathbb{N}$ και $plar \Rightarrow r \in X$. Αυτό είναι άτοπο διότι $r < \delta = \min X$

Άρα $r=0$ και τότε: $x = \delta q \Rightarrow \delta | x$. Άρα: $(\delta | x, \forall x \in X)$ ②

Τότε $p \in X, \delta | x, \forall x \in X \Rightarrow \delta | p \stackrel{p: \text{πρώτος}}{=} \begin{cases} \delta=1 \Rightarrow \text{Επειδή } \delta \in X \Rightarrow p | \delta \stackrel{\delta=1}{=} 1 \Rightarrow p | a \\ \delta=p \Rightarrow \text{Επειδή } \delta \in X \Rightarrow \delta | b \stackrel{\delta=p}{=} p | b \end{cases}$

$\left\{ \begin{array}{l} b \in X \\ p \in X \end{array} \right\} \text{ ①}$
 $\Rightarrow p | a$
 $\Rightarrow p | b$

ΠΟΡΙΣΜΑ: Αν p πρώτος και $a_1, \dots, a_k \in \mathbb{Z}$ έτσι ώστε: $p | a_1 a_2 \dots a_k$, τότε $p | a_i$ για κάποιο $i=1, \dots, k$

Απόδειξη:

• Αν $k=1$ τότε $p | a_1$ και δεν έχουμε να αποδείξουμε τίποτα.

• Αν $k=2$, το αποτέλεσμα είναι το προηγούμενο λήμμα.

Επαγωγική υπόθεση: Υποθέτουμε ότι το αποτέλεσμα ισχύει για κάθε $m: 2 \leq m < k$.

Τότε: $p | a_1 \dots a_k \Rightarrow p | (a_1 \dots a_{k-1}) a_k \stackrel{\text{ΛΗΜΜΑ}}{\Rightarrow} \begin{cases} p | a_1 \dots a_{k-1} \\ p | a_k \end{cases} \Rightarrow$

$\Rightarrow \begin{cases} p | a_i, \text{ για κάποιο } i=1, \dots, k-1 \\ p | a_k \end{cases} \Rightarrow p | a_i, \text{ για κάποιο } i=1, \dots, k$

ΠΟΡΙΣΜΑ: Αν $p, p_1, \dots, p_k$ πρώτοι αριθμοί και $p | p_1 \dots p_k$, τότε

$$p = p_i, \text{ για κάποιο } i = 1, \dots, k$$

Απόδειξη: Έστω $p | p_1 \dots p_k$ ^{ΠΟΡΙΣΜΑ} $p | p_i$ για κάποιο $i = 1, \dots, k \implies$

$$p_i \text{ πρώτος} \implies \begin{cases} p_i = 1 & : \text{άτοπο} \\ p = p_i \end{cases}$$

ΘΕΩΡΗΜΑ: (Θεώρημα ισοδυναμίας Αριθμητικής) Κάθε θετικός

ακέραιος $a > 1$ μπορεί να γραφεί κατά μοναδικό τρόπο ως γινόμενο πρώτων αριθμών.

Απόδειξη: Έχουμε ήδη αποδείξει ότι $a = p_1 \dots p_m$, όπου $p_1, \dots, p_m$ πρώτοι αριθμοί.

Υποθέτουμε ότι $a = q_1 \dots q_n$, όπου $q_1, \dots, q_n$ πρώτοι αριθμοί.
Θέω: $n = m$ και κάθε πρώτος p_i είναι ίσος με έναν πρώτο q_j , $\forall i = 1, \dots, m, \forall j = 1, \dots, n$