12/11/2018

Πρόταση: Έστω p, q πρώτοι με $p|q$. Τότε $p=q$

Απόδειξη: Αφού p πρώτος $p \geq 2$. Αφού q πρώτος, οι μόνοι θετικοί διαιρέτες του q είναι οι 1 και q. Άρα αφού $p|q$ και $p \geq 2$ έπεται $p=q$.

Υπενθύμιση: Έστω ότι αν p πρώτος, $a_1 \dots a_s \in \mathbb{Z}$ και $p|a_1 a_2 \dots a_s$, τότε υπάρχει i με $p|a_i$.

Πρόταση: Έστω $r, s \geq 1$, $p_1 \dots p_r, q_1 \dots q_s$ πρώτοι και $p_1 \cdot p_2 \dots p_r = q_1 q_2 \dots q_s$

Τότε $r=s$ και υπάρχει $\sigma : \{1 \dots r\} \to \{1 \dots s\}$ "1-1" και "επί" ώστε $q_i = p_{\sigma(i)}$, για $i = 1 \dots r$

(Με άλλα λόγια, απλοϊζοντας ενδεχομένως τη σειρά των p_i έπεται ότι τα αντίστοιχα p_i, p_j είναι ίσα).

Απόδειξη: Με επαγωγή στο r

→ Περίπτ. $r=1$, δηλ. $p_1 = q_1 q_2 \dots q_s$ (1) Από την προηγούμενη πρόταση υπάρχει $i \in \{1 \dots s\}$ με $p_1 = q_i$

Άρα θέτοντας $A = q_1 \dots q_{i-1}, q_s$ η (1) $\Rightarrow p_1 = A \cdot p_1 \Rightarrow p_1(A-1) = 0 \Rightarrow A=1$. Άρα $s=1$.

Υποθ. ότι $r \geq 1$ και η πρόταση ισχύει για r. Έστω $p_1 p_{r+1} = q_1 \dots q_s$. Τότε $p_1 | q_1 \cdot \dots \cdot q_s$. άρα υπάρχει i ώστε $p_1 = q_i$. Θέτουμε $A = q_1 q_2 \cdot \dots \cdot q_{i-1} q_{i+1} \cdot \dots \cdot q_s$. Τότε $p_1 (p_2 \dots p_{r+1}) = A p_1 \Rightarrow p_2 \dots p_{r+1} = A$ και η υπόθεση της επαγωγής μας δίνει το ζητούμενο

ΠΑΡΑΤΗΡΗΣΗ: Η πρόταση μας λέει ότι αν ένας ακέραιος $n \geq 2$ είναι γινόμενο πρώτων, η γραφή είναι μοναδική αν δεν λάβουμε υπόψη τη σειρά των παραγόντων.

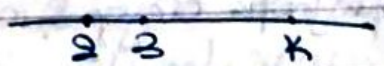
ΘΕΩΡΗΜΑ: (Θεμελ. Θεώρημα της Αριθμητικής)
Έστω $n \geq 2$ ακέραιος. Τότε υπάρχει $s \geq 1$ και πρώτοι $p_1, p_2 \dots p_s$ ώστε $n = p_1 p_2 \dots p_s$ (*)
Η γραφή (*) είναι μοναδική, αν δεν λάβουμε υπόψη την σειρά των p.

ΑΠΟΔΕΙΞΗ:
Ύπαρξη: Υποθέτουμε ότι δεν ισχύει η πρόταση, και άρα υπάρχει $n \in \mathbb{Z}$ με $n \geq 2$ που δεν είναι (πεπερασμένο) γινόμενο πρώτων. Θα βρούμε αντίφαση.
Θέτουμε $S = \{m \in \mathbb{Z} / m \geq 2$ και m δεν γινόμενο πρώτων$\}$.
Έχουμε υποθέσει $S \neq \emptyset$. Άρα από θεώρημα το S έχει ελάχιστο στοιχείο, έστω n_0
Το n_0 δεν είναι πρώτος, γιατί $n_0 \in S$ και κανένας πρώτος δεν είναι στο S. Άρα n_0 σύνθετος. Συνεπώς υπάρχουν r_1, r_2 ακέραιοι με $2 \leq r_1 \leq n_0 - 1$, $2 \leq r_2 \leq n_0 - 1$ ώστε
$n_0 = r_1 \cdot r_2$.

Αφού $r_1 < k_0 \Rightarrow r_1 \notin S$ άρα r_1 (πιεπερ) γινόμενο πρώτων
Αφού $r_2 < k_0 \Rightarrow r_2 \notin S$ άρα r_2 (πιεπερ) γινόμενο πρώτων
Συνεπώς και $k_0 = r_1 r_2$ (πιεπερ) γινόμενο πρώτων, άρα $k_0 = r_1 r_2$ (πιεπερ) γινόμενο πρώτων άρα $k_0 \notin S$, αντίφαση
ΜΟΝΑΔΙΚΟΤΗΤΑ: Την είχουμε δείξει.

ΠΑΡΑΤΗΡΗΣΗ: Έστω $k \geq 2$ ακέραιος. Φυσικά, υπάρχουν αλγόριθμοι, που υπολογίζουν την γραφή του k σαν γινόμενο πρώτων.

ΠΑΡΑΔΕΙΓΜΑ: Ξεκινάμε από το 2 μέχρι το $k-1$. Αν κάποιο d σε αυτό το διάστημα διαιρεί το k, συνεχίζουμε με την παραγοντοποίηση των ακεραίων d και k/d
Αν δεν υπάρχει τέτοιος d, ο k είναι πρώτος.



Για μεγάλα k ο παραπάνω αλγόριθμος απαιτεί υπερβολικά πολύ μεγάλο αριθμό πράξεων.

ΑΝΟΙΧΤΟ ΕΡΩΤΗΜΑ: Υπάρχει αλγόριθμος που παραγοντ. ακεραίους σε πολυωνυμικό χρόνο;

ΘΕΩΡΗΜΑ: Υπάρχει αλγόριθμος που σε πραγματικό χρόνο αποφαίνεται αν ένας δοθέν ακέραιος k είναι πρώτος.

Πρόταση: Έστω $k \geq 2$ ακέραιος. Αν κανένας πρώτος p με $p \leq \sqrt{k}$ δεν διαιρεί το k, τότε ο k είναι πρώτος.

Απόδειξη: Έστω ότι ο k δεν είναι πρώτος. Τότε υπάρχει $s \geq 2$ και πρώτοι $p_1, p_2 \dots p_s$ με $p_1 \leq p_2 \leq \dots \leq p_s$ ώστε
$$k = p_1 p_2 \dots p_s$$
Άρα $p_1^s \leq k \Rightarrow p_1^s \leq k \Rightarrow p_1 \leq \sqrt{k}$ αντίφαση.

Αλγόριθμος: Υπολογίζει αν ένας δοθέν ακέραιος $k \geq 2$ είναι πρώτος ή σύνθετος.
Βήμα - 1ο: Υπολογίζουμε ακέραιο $n \geq 1$ με $n^2 \leq k < (n+1)^2$
Βήμα - 2ο: Αν υπάρχει πρώτος $p \leq n$ με $p | k$ τότε ο k είναι σύνθετος. Αλλιώς ο k είναι πρώτος.

Παράδειγμα: Είναι ο 101 πρώτος; Εφαρμόζουμε αλγόριθμο.
Βήμα - 1ο: Θέτουμε $n = 10$ Τότε $n^2 \leq 101 < (n+1)^2$
Βήμα - 2ο: Οι πρώτοι ≤ 10 είναι οι εξής 2, 3, 5, 7.

2: Δεν διαιρεί 101, γιατί 101 περιττός
3: Δεν διαιρεί 101, γιατί $101 = 3 \cdot 33 + 2$, δηλαδή το υπόλοιπο της Ευκ. Διαιρ. του 101 με το 3 είναι $2 \neq 0$.
(β' τρόπος $1+0+1 = 2$ που δεν διαιρείται από το 3)
5: Δεν διαιρεί το 101 γιατί το τελευταίο δεκαδικό ψηφίο του 101 είναι το 1, άρα όχι 0 ή 5.
7: Ευκ. Διαιρ. 101 με 7

101	7
31	14
3	

άρα $101 = 14 \cdot 7 + 3$, άρα $7 \nmid 101$
Συνεπώς 101 πρώτος

Αλγόριθμος: Έστω $k \geq 2$ ακέραιος. Ο αλγόριθμος (που λέγεται Κόσκινο του Ερατοσθένη) υπολογίζει όλους τους πρώτους $\leq k$.

Βήμα-1ο: Γράφουμε με τη σειρά όλους τους ακεραίους από το 2 έως το k.
Βήμα-2ο: Υπογραμμίζουμε τον πρώτο 2, διαγράφουμε τα γνήσια πολλαπλάσια του (δηλ. 4, 6, 8)
Βήμα-3ο: Υπογραμμ. τον επόμενο ακέραιο που δεν έχει διαγραφεί και διαγράφουμε τα γνήσια πολ/σια του.
Βήμα-4ο: Συνεχίζουμε την ίδια διαδικασία μέχρι το μεγαλύτερο ακέραιο που είναι μικρότερος ή ίσος με το $\sqrt{k}$.
Βήμα-5ο: Οι ακέραιοι που δεν έχουν διαγραφεί είναι ακριβώς οι πρώτοι p με $p \leq k$.

Παράδειγμα: Για $k=25$. 2, 3, ~~4~~, 5, ~~6~~, 7, ~~8~~, ~~9~~, ~~10~~, 11, ~~12~~, 13, ~~14~~, ~~15~~, ~~16~~, 17, ~~18~~, 19, ~~20~~, ~~21~~, ~~22~~, 23, ~~24~~, ~~25~~

→ Στο παράδειγμα $k=25$ άρα $\sqrt{25}=5$.

Παρατήρηση: Έστω $k \geq 2$. Τότε ο k είναι της μορφής $2q$ (δηλ. άρτιος) ή της μορφής $2q+1$ (δηλ. περιττός)
Ο μόνος άρτιος πρώτος είναι το 2.
Δείξαμε ότι υπάρχουν άπειροι το πλήθος πρώτοι. Επομένως, υπάρχουν άπειροι το πλήθος περιττοί πρώτοι, δηλ. πρώτοι της μορφής $2q+1$.

Έρώτημα: Έστω ότι αν k περιττός, πρώτος, ο k είναι της μορφής $4q+1$ ή της μορφής $4q+3$
(γιατί το υπόλοιπο της Ευκ. Διαιρ. του k με το 4 είναι 0 ή 1 ή 2 ή 3 και αν είναι 0 ή 2 ο k είναι άρτιος).

Έστω Α το σύνολο των περιττών πρώτων B_1 το σύνολο των πρώτων της μορφής $4q+1$, B_2 το σύνολο των πρώτων της μορφής $4q+3$. Έχουμε $A = B_1 \cup B_2$.
Άρα, αφού Α άπειρο σύνολο τουλάχιστον ένα από τα B_1, B_2 είναι άπειρο σύνολο.
Θα δείξουμε ότι το B_2 είναι άπειρο σύνολο. Ισχύει ότι και B_1 είναι άπειρο σύνολο, αλλά η αποδείξη είναι πιο δύσκολη.

Πρόταση: Αν $m_1, m_2 \dots, m_s$ (για $s \geq 1$) ακέραιοι της μορφής $4q+1$, τότε και το γινόμενο $m_1, m_2 \dots m_s$ είναι της μορφής $4q+1$.

Απόδειξη: Για $s=1$ έχουμε μόνο m_1 και η πρόταση ισχύει.
Έστω $s \geq 1$ και υπόθ. ότι η πρόταση ισχύει για γινόμενο s ακεραίων. Θα δείξουμε ότι ισχύει για γινόμενο $s+1$ ακεραίων.
Έστω $m_1, m_2 \dots m_{s+1}$ ακέραιοι της μορφής $4q+1$.
Έχουμε $m_1, m_2 \dots m_s m_{s+1} = (m_1 \dots m_s) m_{s+1}$. Από υπόθεση, υπάρχει $k_1 \in \mathbb{Z}$ με $m_{s+1} = 4k_1 + 1$ και από επαγ. υπόθεση υπάρχει $k_2 \in \mathbb{Z}$ με $(m_1 \dots m_s) = 4k_2 + 1$. Συνεπώς, $m_1 m_2 \dots m_s m_{s+1} =$
$= (4k_1+1)(4k_2+1) = 16k_1k_2 + 4k_1 + 4k_2 + 1 = 4(4k_1k_2 + k_1 + k_2) + 1$
και το αποτέλεσμα ισχύει.

Πόρισμα: Έστω ότι $k \geq 2$ είναι της μορφής $4q+3$. Τότε ο k έχει πρώτο διαιρέτη της μορφής $4q+3$.

Απόδειξη: Έστω $K = p_1 p_2 \dots p_s$ η γραφή του K σαν γινόμενο πρώτων. Αφού K της μορφής $4q+3$, ο K είναι περιττός. Επομένως, κάθε p_i είναι περιττός. Αν όλοι τα p_i ήταν της μορφής $4q+1$, οπότε την πρόταση και το γινόμενο τους θα ήταν της ίδιας μορφής. Αντίφαση. γιατί K της μορφής $4q+3$. Άρα τουλάχιστον ένα από τα p_i είναι της μορφής $4q+3$.

Θεώρημα: Το σύνολο B_2 των πρώτων της μορφής $4q+3$ είναι άπειρο.

Απόδειξη: Έστω ότι δεν ισχύει και $p_1, p_2 \dots p_m$ είναι όλοι πρώτοι της μορφής $4q+3$. (Υπάρχει τουλάχιστον ένας, ο 3). Θέτουμε $K = 4p_1 p_2 \dots p_m - 1$. Αφού 3 είναι από τα p_i, έπεται $K \geq 4 \cdot 3 - 1 = 11$.

Αφού $K = 4(p_1 p_2 \dots p_m + 1) + 3$. Ο K είναι της μορφής $4q+3$. Άρα από το πόρισμα έχει πρώτο διαιρέτη της μορφής $4q+3$ άρα υπάρχει i με $1 \leq i \leq m$ ώστε $p_i | K$. Αλλά $p_i | 4p_1 p_2 \dots p_m$ άρα $p_i | K - 4p_1 p_2 \dots p_m = -1$, αντίφαση.

Ερώτημα: Τι γίνεται με το σύνολο B_1 των πρώτων της μορφής $4q+1$. Τι γίνεται με το σύνολο των πρώτων της μορφής $5q+1$; Της μορφής $5q+2$ κτλ; Της μορφής $3q+1$ ή $3q+2$;

Θεώρημα: (Dirichlet, 1837) Έστω m, r ακέραιοι με $q \geq 2$ και $\text{ΜΚΔ}(q, r) = 1$. Θέτουμε $B = \{p$ πρώτος της μορφής $mq + r\}$
Τότε το B είναι άπειρο σύνολο.

Ορισμός: Έστω $n \geq 2$ ακέραιος. Η έκφραση $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ λέγεται **πρωτογενής αναπτυγμα** του n αν κάθε p_i είναι πρώτος $p_1 < p_2 < \cdots < p_r$ και κάθε εκθέτης a_i είναι ακέραιος ≥ 1.

Παραδείγματα:
(1): Αν p πρώτος, $p = p^1$ είναι η πρωτογενής ανάπτυγμα του.
(2): Η πρωτογενής ανάπτυγμα του 12 είναι $12 = 2^2 \cdot 3^1$ του 27 είναι $27 = 3^3$ του 30 είναι $30 = 2^1 \cdot 3^1 \cdot 5^1$.

Παρατήρηση: Δείξαμε ότι κάθε ακέραιος $n \geq 2$ έχει μοναδική πρωτογενή ανάπτυγμα.

ΘΕΤΙΚΟΙ ΔΙΑΙΡΕΤΕΣ ΑΚΕΡΑΙΟΥ:

Πρόταση: Έστω $n \in \mathbb{Z}$ με πρωτογενή ανάπτυγμα $n = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$ (όπου $p_1 < p_2 < \ldots < p_m$ πρώτοι, $a_i \geq 1$). Έστω $b_1, \ldots b_m$ ακέραιοι με $0 \leq b_i \leq a_i$ για κάθε i. Τότε ο αριθμός $p_1^{b_1} p_2^{b_2} \cdots p_m^{b_m} | n$

Απόδειξη: $n = \left(p_1^{b_1} \cdots p_m^{b_m}\right) \cdot \left(p_1^{a_1 - b_1} p_2^{a_2 - b_2} \cdots p_m^{a_m - b_m}\right)$

και $p_1^{a_1 - b_1} \cdots p_m^{a_m - b_m} \in \mathbb{Z}$ γιατί $b_i \leq a_i$ $\forall i$.

Πρόταση: Έστω $n \in \mathbb{Z}$ με πρωτογενή ανάπτυγμα $n = p_1^{a_1} \cdots p_m^{a_m}$ και $d \geq 1$ διαιρέτης του n. Τότε υπάρχουν $b_i \in \mathbb{Z}$ με $0 \leq b_i \leq a_i$ ώστε $d = p_1^{b_1} \cdots p_m^{b_m}$.

Απόδειξη:

Βήμα - 1ο: Αν $d=1$ ισχύει για $b_i=0$ $\forall i$. Άρα υποθέτουμε $d \geq 2$.

Βήμα - 2ο: Έστω q πρώτος με $q|d$. Τότε το q είναι ένας από τους $p_1, p_2 \dots p_m$.

Προκύπτει $q|d$ και $d|k$ $\Big\} \rightarrow q|k$ και αφού q πρώτος το ολοκλήρωμα έπεται.

Βήμα - 3ο: Από βήμα - 2ο υπάρχουν $b_i \in \mathbb{Z}$ με $b_i \geq 0$ ώστε $q = p_1^{b_1} \dots p_m^{b_m}$. Αφού $q|d$ υπάρχει $n \in \mathbb{Z}$ με $n = qd$. Από τις πρωταρχ. έπεται ότι $b_i \leq a_i$ $\forall i$.

Πόρισμα: Έστω $k \in \mathbb{Z}$ με πρωτογενή ανάλυση $k = p_1^{a_1} \dots p_m^{a_m}$

Τότε το σύνολο S των θετικών διαιρετών του k είναι το εξής

$S = \{ p_1^{b_1} \dots p_m^{b_m} : b_i$ ακέραιοι και $0 \leq b_i \leq a_i \ \forall i \}$

Άρα ο αριθμός $\tau(k)$ των θετικών διαιρετών του k είναι ίσος με $(a_1+1)(a_2+1) \dots (a_m+1)$

Παράδειγμα: Βρείτε όλους τους θετικούς διαιρέτες του.

(1) $k = 2^5$.

Λύση: Από πόρισμα οι θετικοί διαιρέτες του k είναι $\{ 2^{b_i} : 0 \leq b_1 \leq 5 \} =$

$= \{ 2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 16, 2^5 = 32 \}$ και

$\tau(k) = 5+1 = 6$ Δηλ. το 2^5 έχει 6 θετ. διαιρέτες.

(2) $k = 44$. Έχουμε $44 = 4^1 \cdot 11^1$ πρωτογ. ανάλυση. Συνεπώς, από το πόρισμα το σύνολο S των θετικών διαιρετών του k είναι

$S = \{ 4^{b_1} 11^{b_2}$ με $0 \leq b_1 \leq 1$, $0 \leq b_2 \leq 1 \} = \{ 4^0 11^0 = 1, 4^0 \cdot 11^1 = 11,$

$4^1 \cdot 11^0 = 4, 4^1 \cdot 11^1 = 44 \}$ και $\tau(44) = (1+1)(1+1) = 4$