Πρόταση: Έστω $p, p_1, p_2, \dots, p_r$ πρώτοι.
Υποθέτουμε ότι $p \mid (p_1 \cdot p_2 \cdots p_r)$

Τότε $\exists i$ με $1 \le i \le r$ ώστε $p = p_i$

Απόδειξη: Έχουμε δείξει ότι αν p πρώτος, $a_1, \dots, a_r \in \mathbb{Z}$ κ' $p \mid (a_1 a_2 \cdots a_r)$, τότε $\exists i$ με $p \mid a_i$

Άρα $\exists i$ με $1 \le i \le r$ ώστε $p \mid p_i$. Αλλά p_i πρώτος κ' p πρώτος, άρα $p \ge 2$. Συνεπώς, $p = p_i$, γιατί αφού p_i πρώτος, οι μόνοι θετικοί διαιρέτες του p_i είναι το 1 κ' το p_i.

π.χ. Αν $p_1, p_2, \dots, p_{10}$ πρώτοι κ' $7 \mid (p_1 \cdot p_2 \cdots p_{10})$, τότε κάποιο p_i είναι ίσο με 7 (επειδή 7 πρώτος)

ΠΡΟΣΟΧΗ: Η πρόταση δεν ισχύει αν p όχι πρώτος.

π.χ. $6 \mid 6 \Rightarrow 6 \mid 2 \cdot 3$ Αλλά $6 \neq 2$ κ' $6 \neq 3$

Πρόταση: Έστω $a \in \mathbb{Z}$ με $a \ge 2$. Τότε $\exists r \in \mathbb{Z}$ με $r \ge 1$ κ' πρώτοι $p_1, p_2, \dots, p_r$ με $a = p_1 \cdot p_2 \cdots p_r$

Απόδειξη: Έστω ότι δεν ισχύει.

Συνεπώς το σύνολο $S = \{a \in \mathbb{Z}, a \ge 2$ κ' a όχι γινόμενο πρώτων$\}$
είναι μη κενό κ' φραγμένο κάτω (από το 1).
Άρα είναι υποσύνολο του $\mathbb{Z}$, οπότε έχει ελάχιστο στοιχείο $a_0 \in \mathbb{Z}$.

Το a_0 δεν είναι πρώτος, γιατί αλλιώς $a_0 = a_0$ κ' άρα $a_0 \notin S$, άτοπο.

→ Συνεπώς το a_0 είναι σύνθετος. Άρα $\exists b_1, b_2 \in \mathbb{Z}$ με $b_1 \ge 2$ κ' $b_2 \ge 2$, ώστε $a_0 = b_1 \cdot b_2$

Έχουμε $b_1 < a_0$. άρα $b_1 \notin S$ κ' άρα $b_1 = q_1 \cdot q_2 \cdots q_r$ με αί πρώτοι

Ομοίως, $b_2 < a_0$ άρα $b_2 \notin S$ κ' άρα $b_2 = q_1' q_2' \cdots q_s'$ με q_i' πρώτοι.

Άρα $a_0 = q_1 \cdots q_r q_1' \cdots q_s'$ γινόμενο πρώτων
Άρα $a_0 \notin S$, άτοπο.

<u>Πρόταση</u>: Έστω $r, t \geq 1$, $p_1, \ldots, p_r$ πρώτοι με $p_1 \leq p_2 \leq \cdots \leq p_r$ κ' $q_1, \ldots, p_t$ πρώτοι με $q_1 \leq q_2 \leq \cdots \leq q_t$.

Υποθέτουμε $p_1 \cdot p_2 \cdots p_r = q_1 \cdot q_2 \cdots q_t$
Τότε, $r = t$ κ' $p_i = q_i \ \forall i$

<u>Απόδειξη</u>: Επαγωγή στο r.
(i) Έστω $r = 1$. Άρα $p = q_1 \cdot q_2 \cdots q_t$. Συνεπώς $\exists i \in \{1, \ldots, t\}$ ώστε $p = q_i$ κ' $p \mid (q_1 \cdot q_2 \cdots q_i \cdots q_t)$

Άρα αν $t \geq 2$ έχουμε $p = q_1 \cdots q_{i-1} \cdot p \cdot q_{i+1} \cdots q_t$

$\Rightarrow q_1 \cdot q_2 \cdots q_{i-1} q_{i+1} \cdots q_t = 1$, <u>άτοπο</u> γιατί $t \geq 2$ κ' q_i πρώτοι

Άρα $t = 1$ κ' $p_1 = q_1$

(ii) Έστω $r, t \geq 1$ κ' έστω $p_1 \cdot p_2 \cdots p_r = q_1 \cdot q_2 \cdots q_t$

(iii) Θδο ισχύει $p_1 \cdot p_2 \cdots p_r \cdot p_{r+1} = q_1 \cdot q_2 \cdots q_s$

Αφού $p_{r+1} \mid q_1 \cdot q_2 \cdots q_s \xrightarrow{\text{πρόταση}} \exists i$ με $p_{r+1} = q_i$

Συνεπώς $p_{r+1} \overset{(1)}{\leq} q_s$. Αφού $q_s \mid p_1 \cdot p_2 \cdots p_r p_{r+1}$

$\xrightarrow{\text{πρόταση}} \exists i$ με $q_s = p_i$. Συνεπώς $q_s \leq p_{r+1}$ (2)
Άρα (1), (2) $\rightarrow$ $p_{r+1} = q_s$

Άρα $p_1 p_2 \cdots p_r \cdot \cancel{p_{r+1}} = q_1 \cdot q_2 \cdots q_{s-1} \cdot \cancel{q_s}$

$p_1 p_2 \cdots p_r = q_1 \cdot q_2 \cdots q_{s-1}$ ισχύει από υπόθεση

π.χ. Έστω $q_1, q_2, \ldots, q_t$ πρώτοι με $q_1 \le q_2 \le \ldots \le q_t$ κ' $q_1 \cdot q_2 \cdots q_t = 36$. Βρείτε το t κ' τα $q_1 \ldots q_t$

Λύση: Έχουμε $2 \cdot 2 \cdot 3 \cdot 3 = 36 = q_1 \cdot q_2 \cdots q_t$
Συνεπώς (από την τελευταία πρόταση) $t = 4$ με $q_1 = q_2 = 2$ κ' $q_3 = q_4 = 3$

Θεώρημα (Θεμελιώδες Θεώρημα Αριθμητικής)
Έστω $a \in \mathbb{Z}$ με $a \ge 2$. Τότε $\exists$ μοναδικός ακέραιος t κ' μοναδικοί πρώτοι $p_1, p_2, \ldots, p_t$ με $p_1 \le p_2 \le \ldots \le p_t$ ώστε $a = p_1 \cdot p_2 \cdots p_t$.

Απόδειξη: Συνδυασμός των δύο παραπάνω προτάσεων.

Ορισμός: Έστω $x \in \mathbb{R}$.
Ορίζουμε $\Pi(x)$ = ο αριθμός των πρώτων p με p.

π.χ. $\Pi\left(\frac{3}{2}\right) = 0$, $\Pi(4) = 2$, $\Pi(9) = 4$

Θεώρημα: (Θεώρημα πρώτων αριθμών) (Hadamard - de la Vallée Poussin 1896)

$$\lim_{x \to +\infty} \frac{\Pi(x)}{\left(\frac{x}{\ln x}\right)} = 1$$

Με άλλα λόγια, για $x \in \mathbb{R}$ με x αρκετά μεγάλο,
το $\frac{x}{\ln x}$ είναι περίπου ίσο με τον αριθμό των πρώτων που είναι μικρότεροι ή ίσοι του x.

Απόδειξη παραλείπεται

Πρόταση: Έστω $\alpha \in \mathbb{Z}$ με $\alpha \geq 2$, σύνθετος κ' p_1 ο μικρότερος πρώτος διαιρέτης του. Τότε $p_1 \leq \sqrt{\alpha}$.

Απόδειξη: Αφού α όχι πρώτος, $\exists\, t \geq 2$ κ' πρώτοι $p_1, p_2, \ldots, p_t$ με $p_1 \leq p_2 \leq \ldots \leq p_t$ ώστε $\alpha = p_1 \cdot p_2 \cdots p_t \geq p_1^2$. Άρα $p_1 \leq \sqrt{\alpha}$.

π.χ. Δείξτε ότι το 53 είναι πρώτος.
$\sqrt{53} < \sqrt{64} = 8$, άρα $\sqrt{53} < 8$.

Έστω 53 σύνθετος. Τότε από την πρόταση $\exists$ μικρότερος πρώτος διαιρέτης $p \leq 8$ με $p \mid 53$

Οι πρώτοι ≤ 8 είναι οι 2, 3, 5, 7. Φανερά κανένας δεν διαιρεί το 53. Οπότε, άτοπο.
Άρα 53 → πρώτος

Υπενθύμιση: Έστω $\alpha \in \mathbb{Z}$ με $\alpha \geq 2$. Τότε $\exists$ μοναδικό $t \geq 1$ κ' πρώτοι $p_1, p_2, \ldots, p_t$ με $p_1 \leq p_2 \leq p_3 \leq \ldots \leq p_t$, ώστε $\alpha = p_1 \cdot p_2 \cdots p_t$

π.χ. $4 = 2 \cdot 2$, άρα $t = 2$, $p_1 = 2$, $p_2 = 2$.

Υπενθύμιση: Έστω $\alpha \geq 2$ ακέραιος. Αν μπορέσουμε να δω κανένας πρώτος $\leq \sqrt{\alpha}$ δεν διαιρεί το α, τότε έπεται ότι α πρώτος

π.χ. Νδο 101 πρώτος: Έχουμε $\sqrt{101} \simeq 10$ κ' τότε < 11. Οι πρώτοι < 11 είναι 2, 3, 5, 7. Κανένας δεν διαιρεί το 101.

Το 2 όχι, γιατί 101 περιττός

Το 3 όχι, γιατί $1+0+1=2$.

Το 5 όχι, γιατί το 101 δεν λήγει σε 0 ή 5.

Το 7 όχι, γιατί $101 = 14 \cdot 7 + 3$

Άρα 101 πρώτος.