ΠΑΡΑΤΗΡΗΣΗ: Έστω A το σύνολο των πρώτων, B_0 το σύνολο των άρτιων πρώτων, B_1 το σύνολο των περιττών πρώτων έχουμε $A = B_0 \cup B_1$ κ' $B_0 = \{2\}$.
Αφού από Θεώρημα το A είναι άπειρο σύνολο, έχουμε ότι κ' το B_1 είναι άπειρο σύνολο. Συνεπώς $\exists$ άπειροι στο πλήθος περιττοί πρώτοι.

ΠΑΡΑΤΗΡΗΣΗ: Έστω A το σύνολο των πρώτων, B_0 το σύνολο των πρώτων της μορφής $3k+0$, B_1 το σύνολο των πρώτων της μορφής $3k+1$ κ' B_2 το σύνολο των πρώτων της μορφής $3k+2$

Φανερά, $A = B_0 \cup B_1 \cup B_2$ κ' $B_0 = \{3\}$.
Αφού A άπειρο σύνολο, έπεται τουλάχιστον ένα από τα σύνολα B_1 κ' B_2 είναι άπειρο.

Στόχος. Νδο B_2 άπειρο σύνολο, δηλαδή ότι $\exists$ άπειροι στο πλήθος πρώτοι της μορφής $3k+2$. ($\exists$ τουλάχιστον ένα, το 5. Επίσης το $11 = 3\cdot 3+2$, $17 = 5\cdot 3+2$, $23 = 7\cdot 3+2$)

Πρόταση: Το γινόμενο δύο ακεραίων "της μορφής $3k+1$" είναι της ίδιας μορφής.

είναι λάθος να γράφω κ αντί

Απόδειξη: Έστω $a, b \in \mathbb{Z}$ "της μορφής $3k+1$". Συνεπώς $\exists\, k_1, k_2 \in \mathbb{Z}$ ώστε $a = 3k_1+1$
$b = 3k_2+1$

Συνεπώς, $ab = (3k_1+1)(3k_2+1) = 3(3k_1k_2 + k_1 + k_2) + 1$. Το αποτέλεσμα έπεται.

ΠΑΡΑΤΗΡΗΣΗ: Ο ίδιος σχεδόν υπολογισμός δείχνει ότι το γινόμενο ενός ακεραίου "της μορφής $3k+1$" με έναν της μορφής "$3k+2$", είναι της μορφής $3k+2$ κ' το γινόμενο δύο ακεραίων "της μορφής $3k+2$" είναι της μορφής "$3k+1$"

π.χ. Το 5 είναι "της μορφής $3k+2$", ενώ το $5^2 = 25$ είναι "της μορφής $3k+1$", γιατί $25 = 8\cdot 3+1$.

Πόρισμα: Έστω $a \geq 2$ ακέραιος "της μορφής $3k+2$". Τότε έχει πρώτο διαιρέτη "της μορφής $3k+2$".

Απόδειξη: Έστω $n \in \mathbb{Z}$ με $a = 3n+2$.
Από Θεμελιώδες Θεώρημα Αριθμητικής, $\exists$ πρώτοι $p_1, \dots, p_r$ ώστε $a = p_1 \cdots p_r$

Υποθέτουμε ότι κανένα p_i δεν είναι "της μορφής $3k+2$"
Άρα δύο περιπτώσεις:
(i) Όλα τα p_i "της μορφής $3k+1$". Από την προηγούμενη πρόταση κ' επαγωγή, ο a είναι "της μορφής $3k+1$", αντίφαση.
(ii) Κάποιο από τα p_i να είναι ίσο με 3. Τότε ο a είναι πολλαπλάσιο του 3, άρα είναι "της μορφής $3k$", αντίφαση.

Θεώρημα: $\exists$ άπειροι το πλήθος πρώτοι "της μορφής $3k+2$".

Απόδειξη: Έστω ότι δεν ισχύει κ' ότι $\{p_1, p_2, \dots, p_N\}$ είναι το σύνολο όλων των πρώτων "της μορφής $3k+2$". Θέτουμε $m = 3p_1p_2 \cdots p_N - 1 \in \mathbb{N}$
Αφού το 5 είναι κάποιο από τα p έχουμε $m \geq 14$.
Αφού το $m \geq 14$ είναι "της μορφής $3k+2$", από το πόρισμα $\exists$ πρώτος "της μορφής $3k+2$" που να διαιρεί το m. Άρα $\exists$ με $1 \leq i \leq N$, ώστε p_i / m. Άρα $\exists\, u \in \mathbb{Z}$ με $3p_1p_2 \cdots p_N - 1 = u p_i \Rightarrow 1 = 3p_1p_2 \cdots p_N - u p_i \Rightarrow p_i / 1$, αντίφαση.

Ερώτημα: $\exists$ άπειροι το πλήθος πρώτοι "της μορφής $3k+1$" ή όχι;

Απάντηση: Ο Dirichlet (1837) απέδειξε το εξής:
Έστω $a, b \in \mathbb{Z}$ με $a, b \geq 1$ κ' $\text{ΜΚΔ}(a,b) = 1$. Τότε $\exists$ άπειροι το πλήθος πρώτοι "της μορφής $ka+b$".
π.χ. για $a=3$, $b=1$ ή 2 $\exists$ άπειροι το πλήθος πρώτοι της μορφής $3k+1$ κ' το ίδιο της μορφής $3k+2$ (το δείξαμε)
Για $a=4, b=1$ το ίδιο της μορφής $4k+1$
$a=4, b=3$ —//— $4k+3$
$a=5, b=1$ —//— $5k+1$
$a=5, b=2$ —//— $5k+2$ κτλ.

Υπενθύμιση: Ισχύει ότι οι ρητοί αριθμοί $\mathbb{Q}$ έχουν την ιδιότητα.
$\mathbb{Q} = \{a \in \mathbb{R} \,/\, \exists N \geq 1$ με $N \in \mathbb{Z}$ ώστε $Na \in \mathbb{Z}\}$

Πρόταση: Έστω $a, b \in \mathbb{Z}$ με $(a,b) \neq (0,0)$ κ' $d = ΜΚΔ(a,b)$. Τότε $ΜΚΔ\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

Απόδειξη: Φανερά $\frac{a}{d}, \frac{b}{d} \in \mathbb{Z}$, γιατί d/a κ' d/b. Έστω $e = ΜΚΔ\left(\frac{a}{d}, \frac{b}{d}\right)$
Αφού $ΜΚΔ(a,b) = d$, $\exists x, y \in \mathbb{Z}$ με $d = xa + yb$. Άρα,
$1 = x\frac{a}{d} + y\frac{b}{d}$. Αφού $e / \frac{a}{d}$ κ' $e / \frac{b}{d} \Rightarrow e / x\frac{a}{d} + y\frac{b}{d} = 1 \Rightarrow e = 1$
(αφού $e \geq 1$)

Πρόταση: Έστω $a \in \mathbb{Q}$ με $a \neq 0$. Τότε $\exists$ μοναδικά $n, m \in \mathbb{Z}$ με $n \geq 1$ κ' $ΜΚΔ(n,m) = 1$ ώστε (στο $\mathbb{R}$) $a = \frac{m}{n}$.

Απόδειξη (Ύπαρξη): Αφού $a \in \mathbb{Q} - \{0\}$, $\exists N \in \mathbb{Z}$, $N \geq 1$, ώστε $Na \in \mathbb{Z}$.
Θέτουμε $M = Na$ (*). Αφού $a \neq 0$, $N \neq 0$ έχουμε $M \neq 0$. Θέτουμε $d = ΜΚΔ(M, N)$ κ' $m = ΜΚΔ\left(\frac{M}{d}, \frac{N}{d}\right)$. Από την πρόταση $ΜΚΔ(m,n) = 1$ κ' από (*) στο $\mathbb{R}$ έχουμε $a = \frac{M}{N} = \frac{\left(\frac{M}{d}\right)}{\left(\frac{N}{d}\right)} = \frac{m}{n}$

(Μοναδικότητα): Έστω $m, n, m', n' \in \mathbb{Z}$ με $m \neq 0$, $m' \neq 0$, $n \geq 1$, $n' \geq 1$. $ΜΚΔ(m,n) = 1$, $ΜΚΔ(m',n') = 1$ κ' $\frac{m}{n} = \frac{m'}{n'}$ στο $\mathbb{R}$. Άρα $mn' = nm' \Rightarrow n'/n$
$ΜΚΔ(n',m') = 1$.

Επίσης, $mn' = nm' \Rightarrow n / mn' \Rightarrow n / n'$
$ΜΚΔ(n,m) = 1$.

$(1) + (2) + (n \geq 1) + (n' \geq 1) \Rightarrow n = n'$. Άρα $\frac{m}{n} = \frac{m'}{n} \Rightarrow m = m'$

π.χ. Αν $a = \frac{10}{4}$, τότε $a = \frac{5}{2}$ με $2 \geq 1$ κ' $ΜΚΔ(5,2) = 1$

ΥΠΕΝΘΥΜΙΣΗ: Έστω $a \in \mathbb{R}$, $a \geq 0$. Η εξίσωση (στο $\mathbb{R}$) $x^2 = a$ έχει μοναδική λύση $x_0 \geq 0$ που τη συμβολίζουμε $\sqrt{a} \in \mathbb{R}$. Πιο γενικά, αν $n \geq 2$, η εξίσωση (για $a \in \mathbb{R}$, $a \geq 0$) $x^n = a$ έχει μοναδική μη αρνητική λύση στο $\mathbb{R}$, που συμβολίζεται $\sqrt[n]{a}$

Ερώτημα: Έστω $a \in \mathbb{Z}$ με $a \geq 2$ κ' $n \geq 2$. Δώστε ικανές κ' αναγκαίες συνθήκες ώστε $\sqrt[n]{a} \in \mathbb{Q} \subseteq \mathbb{R}$.

Στόχος: Έστω $a, n \in \mathbb{Z}$ με $a, n \geq 2$. Πότε $\sqrt[n]{a} \in \mathbb{Q}$.

Πρόταση: Έστω $a, n \in \mathbb{Z}$ με $a, n \geq 2$. Υποθέτουμε ότι στην πρωτογενή ανάλυση του n $a = p_1^{d_1} p_2^{d_2} \dots p_r^{d_r}$ με p_i πρώτους $p_i \neq p_j$ για $i \neq j$ κ' $d_i \in \mathbb{Z}$ με $d_i > 0$, το $n | d_i$ $\forall i$. Θέτουμε $b = p_1^{d_1/n} p_2^{d_2/n} \dots p_r^{d_r/n}$. Τότε $b \in \mathbb{Z}$ (άρα $b \in \mathbb{Q}$) κ' $b^n = a$, άρα $b = \sqrt[n]{a}$

Απόδειξη: Αφού $\frac{d_i}{n}$ θετικός ακέραιος $\forall i$, $b \in \mathbb{Z}$ κ' $b^n = b \cdot b \dots b =$
$= (p_1^{\frac{d_1}{n}} p_2^{\frac{d_2}{n}} \dots p_r^{\frac{d_r}{n}})^n = (p_1^{\frac{d_1}{n}})^n \dots (p_r^{\frac{d_r}{n}})^n = p_1^{d_1} \dots p_r^{d_r} = a$

(π.χ.) i) Αν $a = 3^2 \cdot 7^6$ κ' $n = 2$, τότε $\sqrt[2]{a} = 3^{2/2} 7^{6/2} = 3 \cdot 7^3$

ii) Αν $a = 100 = 2^2 5^2$ κ' $n = 2$, τότε $\sqrt[2]{a} = 2^{2/2} 5^{2/2} = 2 \cdot 5 = 10$

Πρόταση: Έστω $a, n \in \mathbb{Z}$ με $a \geq 2$ κ' $n \geq 2$. Υποθέτουμε $\sqrt[n]{a} = \frac{b}{c} \in \mathbb{Q}$ με $b, c \in \mathbb{Z}$, $c > 0$ κ' $\text{ΜΚΔ}(b, c) = 1$.
Τότε $c = 1$

Απόδειξη: Έστω $c > 1$. Τότε $\exists$ πρώτος p με $p | c$ $\qquad$ p πρώτος
$\sqrt[n]{a} = \frac{b}{c} \Rightarrow c \cdot \sqrt[n]{a} = b \Rightarrow (c \sqrt[n]{a})^n = b^n \Rightarrow c^n \cdot a = b^n \Rightarrow p | b^n \Rightarrow p | b$.
Άρα $p | b$ κ' $p | c$ $\Rightarrow p | \text{ΜΚΔ}(b, c) = 1$, αντίφαση.

(!) Πρόταση: Έστω $a, n \in \mathbb{Z}$ με $a \geq 2$, $n \geq 2$ κ' $a = p_1^{d_1} p_2^{d_2} \dots p_r^{d_r}$ η πρωτογενής ανάλυση του a. Υποθέτουμε $\sqrt[n]{a} \in \mathbb{Q}$. Τότε $n | d_i$ $\forall i = 1, 2, \dots, r$

Απόδειξη: Αφού $\sqrt[n]{a} \in \mathbb{Q}$ από την προηγούμενη πρόταση $\exists b \in \mathbb{Z}$ με $\sqrt[n]{a} = b \Rightarrow a = b^n$ (*)
Η (*) μας λέει ότι ένας πρώτος p διαιρεί το a αν διαιρεί το b. Συνεπώς, υπάρχουν ακέραιοι e_i με $e_i > 0$, ώστε $b = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$
Άρα $(*) \Rightarrow p_1^{d_1} \dots p_r^{d_r} = (p_1^{e_1} \dots p_r^{e_r})^n = p_1^{ne_1} p_2^{ne_2} \dots p_r^{ne_r}$

Από τη μοναδικότητα της γραφής σε γινόμενο πρώτων έχουμε $d_i = \nu e_i$ $\forall i$
Άρα $\nu | d_i$ $\forall i$

<u>Απόδειξη</u> (⇐): Άμεση από τις προηγούμενες προτάσεις

<u>Π.χ.</u> (i) Έστω $a = 3^6 7^8 11^3$
Για $\nu = 2$ έχουμε $\nu \nmid 3$. Συνεπώς $\sqrt{a} \notin \mathbb{Q}$.
Για $\nu = 3$ έχουμε $\nu \nmid 8$. Συνεπώς $\sqrt[3]{a} \notin \mathbb{Q}$

(ii) $a = 2 = 2^1$
Για $\nu = 2$. $2 \nmid 1$ άρα από το θεώρημα $\sqrt{2} \in \mathbb{R} - \mathbb{Q}$

Πιο γενικά, για $\nu \in \mathbb{Z}$, $\nu \geq 2$ έχουμε $\nu \nmid 1$. Συνεπώς $\sqrt[\nu]{2} \in \mathbb{R} - \mathbb{Q}$.

(iii) Βρείτε μια τιμή του $y \in \mathbb{Z}$ με $y > 0$ ώστε $\sqrt[3]{3^6 7^{8+y} 11^3} \in \mathbb{Q}$.

<u>Λύση</u>: Από το θεώρημα $\sqrt[3]{3^6 7^{8+y} 11^3} \in \mathbb{Q}$ ανν $\begin{cases} 3|6 \\ 3|8+y \\ 3|3 \end{cases} \Leftrightarrow 3|8+y$.

Άρα για $y = 1$ ισχύει.

<u>Πρόταση</u>: Έστω $a \in \mathbb{Q}$ με $a > 0$ κ' $\nu \geq 2$. Τότε υπάρχουν πρώτοι $p_1, p_2, \ldots, p_r$ κ' ακέραιοι (που μπορεί να είναι αρνητικοί) $d_i \in \mathbb{Z}$ ώστε $a = p_1^{d_1} p_2^{d_2} \cdots p_r^{d_r}$ κ' $p_i \neq p_j$ για $i \neq j$. Τότε $\sqrt[\nu]{a} \in \mathbb{Q}$ ανν $\nu | d_i$ $\forall i$.

<u>Απόδειξη</u>: Παρόμοια με τις προηγούμενες.

<u>Π.χ.</u> $\frac{15}{2}$. Έχουμε $15 = 3^1 \cdot 5^1$, $2 = 2^1$. Συνεπώς $\frac{15}{2} = 2^{-1} 3^1 5^1$ κ' $\sqrt[\nu]{\frac{15}{2}} \notin \mathbb{Q}$ $\forall \nu \geq 2$

<u>Ορισμός</u>: Έστω $a, b \in \mathbb{Z}$ με $a > 0$ κ' $b > 0$. Ο ακέραιος $e > 0$ λέγεται το ελάχιστο κοινό πολλ/σιο των a κ' b αν είναι το ελάχιστο κοινό πολλαπλάσιο των a κ' b (δηλαδή $a|e$, $b|e$ κ' κάθε θετικό κοινό πολλαπλάσιο των a κ' b είναι μεγαλύτερο ή ίσο του e

Πρόταση: Έστω $p_1, \dots, p_r$ πρώτοι με $p_i \neq p_j$ για $i \neq j$ κ' $c_i \geq 0$ $d_i \geq 0$ ακέραιοι.
Τότε ΕΚΠ$(p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r}, p_1^{d_1} p_2^{d_2} \cdots p_r^{d_r}) = p_1^{\max(c_1,d_1)} p_2^{\max(c_2,d_2)} \cdots p_r^{\max(c_r,d_r)}$

Απόδειξη: Θέτουμε $f = p_1^{\max(c_1,d_1)} p_2^{\max(c_2,d_2)} \cdots p_r^{\max(c_r,d_r)}$ κ' έστω g ένα θετικό κοινό πολλαπλάσιο των $a = p_1^{c_1} \cdots p_r^{c_r}$, κ' $d = p_1^{d_1} \cdots p_r^{d_r}$. Αφού $d_i \leq \max(c_i,d_i)$ $\forall i$, ομοίως
Αφού $c_i \leq \max(c_i,d_i)$ $\forall i$, από πρόταση $a|f$.
$b|f$. Άρα f κοινό πολλαπλάσιο των a κ' b.
Αφού g θετικό κοινό πολλαπλάσιο, για $i \in \{1, \dots, r\}$ έχουμε $p_i^{c_i}|a \Rightarrow$ $p_i^{c_i}|g$ κ' ομοίως $p_i^{d_i}|g$. Αφού $\max(c_i,d_i) \in \{c_i, d_i\} \Rightarrow$ $p_i^{\max(c_i,d_i)}|g$. Άρα αφού p_i πρώτοι με $p_i \neq p_j$ για $i \neq j$ έπεται $f|g \Rightarrow$ $f \leq g$. Συνεπώς $f =$ ΕΚΠ(a,b)

πρόταση

π.χ. ΕΚΠ$(40, 12) =$ ΕΚΠ$(2^3 \cdot 5^1, 2^2 \cdot 3) =$ ΕΚΠ$(2^3 3^0 \cdot 5^1, 2^2 3^1 \cdot 5^0) =$
$2^{\max(3,2)} 3^{\max(0,1)} 5^{\max(1,0)} = 2^3 \cdot 3 \cdot 5 = 120$

Πρόταση: Έστω $x, y \in \mathbb{R}$. Τότε $\min(x,y) + \max(x,y) = x + y$.

Απόδειξη: Περίπτωση 1. Αν $x \leq y$, τότε $\min(x,y) = x$, $\max(x,y) = y$ κ' ισχύει.
Περίπτωση 2. Αν $x > y$, τότε $\min(x,y) = y$, $\max(x,y) = x$ κ' πάλι ισχύει

Πρόταση: (Σχέση ΕΚΠ κ' ΜΚΔ). Έστω $a, b \in \mathbb{N}$. (δηλαδή $a, b \in \mathbb{Z}$, $a \geq 1$, $b \geq 1$)
Τότε ΕΚΠ(a,b)ΜΚΔ$(a,b) = a \cdot b$.

Απόδειξη: Υπάρχουν πρώτοι $p_1, \dots, p_r$ με $p_i \neq p_j$ για $i \neq j$ κ' ακέραιοι c_i, d_i με $c_i \geq 0, d_i \geq 0$ ώστε $a = p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r}$ κ' $b = p_1^{d_1} p_2^{d_2} \cdots p_r^{d_r}$

Από προτάσεις έχουμε:
ΕΚΠ$(a,b) \cdot$ ΜΚΔ$(a,b) = p_1^{\max(c_1,d_1)} p_2^{\max(c_2,d_2)} \cdots p_r^{\max(c_r,d_r)} p_1^{\min(c_1,d_1)} p_2^{\min(c_2,d_2)} \cdots p_r^{(c_r,d_r)} =$

$= p_1^{\max(c_1,d_1)} p_1^{\min(c_1,d_1)} p_2^{\max(c_2,d_2)} p_2^{\min(c_2,d_2)} \cdots p_r^{\max(c_r,d_r)} p_r^{\min(c_r,d_r)} =$

$= p_1^{\max(c_1,d_1)+\min(c_1,d_1)} p_2^{\max(c_2,d_2)+\min(c_1,d_1)} \cdots p_r^{\max(c_r,d_r)+\min(c_r,d_r)}$

Πρόταση: $p_1^{c_1+d_1} p_2^{c_2+d_2} \cdots p_r^{c_r+d_r} = p_1^{c_1} p_1^{d_1} p_2^{c_2} p_2^{d_2} \cdots p_r^{c_r} p_r^{d_r} =$

$= (p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r})(p_1^{d_1} p_2^{d_2} \cdots p_r^{d_r}) = ab$

π.χ. Αν $a=40$ κ' $b=12$, είδαμε ΕΚΠ$(12,40)=120$. Συνεπώς, από την πρόταση ΕΚΠ$(12,40)$ ΜΚΔ$(12,40) = 12 \cdot 40 \Rightarrow$ ΜΚΔ$(12,40) = \frac{12 \cdot 40}{ΕΚΠ(12,40)} = \frac{480}{120} = 4$.

ΠΑΡΑΤΗΡΗΣΗ: Ένας αποτελεσματικός αλγόριθμος για την εύρεση ΕΚΠ(a,b) είναι ο εξής (για $a, b \in \mathbb{N}$):

Βήμα 1º: Υπολογίζουμε με Ευκλείδειο Αλγόριθμο τον ΜΚΔ(a,b)

Βήμα 2º: Έχουμε ΕΚΠ$(a,b) = \frac{a \cdot b}{ΜΚΔ(a,b)}$

Φυλλάδιο 5 άσκηση 5.
Έστω $a, b \in \mathbb{N}$. Ν.Ο. αν ΜΚΔ$(a,b)=1$, τότε ΜΚΔ$(a-b, a^{11}b^{12})=1$

Λύση: Θέτουμε $d=$ ΜΚΔ$(a-b, a^{11}b^{12})$
Υποθέτουμε $b>1$ κ' θα βρούμε αντίφαση. Αφού $d>1$ $\exists$ πρώτος p με $p|d$
Αφού $d|a^{11}b^{12} \Rightarrow d|a^{11}b^{12} \xrightarrow{p \text{ πρώτος}} p|a$ ή $p|b$

Περίπτωση 1η: $p|a$. Αφού $d|a-b$ κ' $p|d \Rightarrow p|a-b$

Άρα $\left.\begin{matrix} p|a \\ p|a-b \end{matrix}\right\} \Rightarrow p|a-(a-b) \Rightarrow p|b$

Άρα $p|a$ κ' $p|b \Rightarrow p|$ΜΚΔ$(a,b)=1$, αντίφαση

Περίπτωση 2η: $p|b$. Αφού $d|a-b$ κ' $p|d \Rightarrow p|a-b$.

Άρα $\left.\begin{matrix} p|b \\ κ' \\ p|a-b \end{matrix}\right\} \Rightarrow p|b+(a-b) \Rightarrow p|a$. Άρα $p|a$ κ' $p|b$

Συνεπώς, $p|$ΜΚΔ$(a,b)=1$, αντίφαση

Φυλλάδιο 4 άσκηση 3: Έστω $m \in \mathbb{Z}$. Ν.δ.ο. $ΜΚΔ(2m+1, 9m+4) = 1$.

<u>Λύση</u>: $ΜΚΔ(2m+1, 9m+4) = ΜΚΔ(2m+1, (9m+4) - 4(2m+1)) \overset{(*)}{=}$ (γιατί $ΜΚΔ(a,b) = ΜΚΔ(a, b - xa)\ \forall x \in \mathbb{Z}$.

$\overset{(*)}{=} ΜΚΔ(2m+1, m) = ΜΚΔ(2m+1-2m, m) = ΜΚΔ(1, m) = 1$.

<u>Πρόταση</u>: Έστω a, b, c φυσικοί αριθμοί με $a|c$ κ' $b|c$. Αν $ΜΚΔ(a,b) = 1$, τότε $ab|c$

<u>Απόδειξη</u>: Αφού $a|c$ $\exists k_1 \in \mathbb{Z}$ με $c = k_1 a$ (1)
Αφού $b|c$ $\exists k_2 \in \mathbb{Z}$ με $c = k_2 b$ (2)
Αφού $ΜΚΔ(a,b) = 1$, υπάρχουν $x, y \in \mathbb{Z}$ με $1 = xa + yb$ (3)
$(3) \Rightarrow c = xac + ybc \overset{(1),(2)}{=} xak_2b + ybk_1a = ab(xk_2 + yk_1)$
Συνεπώς $ab|c$.

ΠΡΟΣΟΧΗ! Η πρόταση <u>δεν</u> ισχύει γενικά αν $ΜΚΔ(a,b) \neq 1$. Π.χ. $a=2, b=2, c=2$.
Τότε $a|c$, $b|c$ αλλά $ab = 4 \nmid 2 = c$