11. Ακέραιοι αριθμοί

Παρατηρήσαμε ότι η διαφορά $a-b$ δύο φυσικών αριθμών $a, b \in \mathbb{N}_0$ ορίζεται μόνο αν $a \geq b$, μάλιστα

$$(\alpha)\quad a-b=r \iff a=b+r$$

Επιπλέον παρατηρούμε ότι για $a, b, \gamma, \delta \in$ ώστε $a \geq b$, $\gamma \geq \delta$ ισχύει:

$$(\beta)\quad a-b=\gamma-\delta \iff a+\delta=b+\gamma$$

Πράγματι:

$$a+\delta=b+\gamma \overset{\text{ορισμός}}{\iff} a=(b+\gamma)-\delta \underset{\gamma \geq \delta}{\overset{\text{ιδιοτητα διαφ}}{\iff}}$$

$$a=b+(\gamma-\delta) \overset{\text{ορισμος}}{\iff} a-b=\gamma-\delta$$

Ορίζουμε λοιπόν στο σύνολο $\mathbb{N}_0 \times \mathbb{N}_0$ την σχέση:

$$(a,b)\sim(\gamma,\delta) \iff a+\delta=b+\gamma$$

που ελένχεται εύκολα ότι είναι σχέση ισοδυναμίας. Στη συνέχεια ορίζουμε $\mathbb{Z}$ το σύνολο των κλάσεων ισοδυναμίας της σχέσης $\sim$.

Για $(m,n) \in \mathbb{N}\times\mathbb{N}$ έστω $\langle m,n \rangle$ η κλάση ισοδυναμίας που ανήκει το (m,n), δηλαδή

$$\langle m,n \rangle = \{(a,b) \in \mathbb{N}\times\mathbb{N} : \boxed{a+n=b+m}\}$$

δηλαδή

$$\langle m,n \rangle = \langle a,b \rangle \iff a+n=b+m.$$

Για παράδειγμα:

$$\langle 3,0 \rangle = \langle 8,5 \rangle = \langle 4,1 \rangle = \langle 5,2 \rangle \equiv 3$$

$$\langle 0,3 \rangle = \langle 5,8 \rangle = \langle 1,4 \rangle = \langle 2,5 \rangle \equiv -3$$

(Σκεφτόμαστε την κλάση $\langle a,b \rangle$ ως την διαφορά $a-b$)

Πρόσθεση - Πολλαπλασιασμός στο $\mathbb{Z}$

$$\langle m,n\rangle + \langle a,b\rangle = \langle m+a, n+b\rangle$$

$$\langle m,n\rangle \cdot \langle a,b\rangle = \langle ma+nb, mb+na\rangle$$

Οι πράξεις είναι καλά ορισμένες, δηλαδή
αν $\langle m,n\rangle = \langle m_1, n_1\rangle$ και $\langle a,b\rangle = \langle a_1, b_1\rangle$
τότε:

(i) $\langle m+a, n+b\rangle = \langle m_1+a_1, n_1+b_1\rangle$

[πράγματι, αν $m+n_1 = n+m_1$ και $a+b_1 = b+a_1$
τότε $(m+a)+(n_1+b_1) = (m+n_1)+(a+b_1) =$
$= (n+m_1)+(b+a_1) = (m_1+a_1)+(n+b)$]

(ii) $\langle ma+nb, nb+na\rangle = \langle m_1a_1+n_1b_1, n_1b_1+n_1a_1\rangle$
(άσκηση)

Πρόταση

Ισχύουν οι ακόλουθες ιδιότητες για τις πράξεις της πρόσθεσης και του πολ/σμού:

(i) $a+b = b+a \quad \forall\, a,b \in \mathbb{Z}$

(ii) $a+(b+\gamma) = (a+b)+\gamma \quad \forall\, a,b,\gamma \in \mathbb{Z}$

(iii) Υπάρχει $0 \in \mathbb{Z}$ ώστε $0+a = a \quad \forall\, a \in \mathbb{Z}$

(iv) Για κάθε $a \in \mathbb{Z}$ υπάρχει στοιχείο το $-a \in \mathbb{Z}$ ώστε $a+(-a) = 0$

(i′) $a \cdot b = b \cdot a \quad \forall\, a,b \in \mathbb{Z}$

(ii′) $a \cdot (b \cdot \gamma) = (a \cdot b) \cdot \gamma \quad \forall\, a,b,\gamma \in \mathbb{Z}$

(iii′) Υπάρχει $1 \in \mathbb{Z}$ ώστε $1 \neq 0$, $1 \cdot a = a \quad \forall a \in \mathbb{Z}$

(v) Για κάθε $a,b,\gamma \in \mathbb{Z}$ ισχύει
$$a \cdot (b+\gamma) = a \cdot b + a\gamma.$$

Απόδειξη

Έστω $a = \langle m, n \rangle$, $b = \langle p, q \rangle$ και $\gamma = \langle \tau, \xi \rangle \in \mathbb{Z}$

(i) $a+b = \langle m+p, n+q \rangle = \langle p+m, q+n \rangle = b+a$.

(ii) $a+(b+\gamma) = \langle m,n \rangle + (\langle p,q \rangle + \langle \tau, \xi \rangle) = \langle m+(p+\tau), n+(q+\xi) \rangle \overset{\text{επιμ. στο } \mathbb{N}_0}{=}$
$\langle (m+p)+\tau), (n+q)+\xi \rangle = \langle m+p, n+q \rangle + \langle \tau, \xi \rangle = (a+b)+\gamma$.

(iii) Θέτουμε $0 = \langle 0,0 \rangle$. Τότε
$0+a = 0+\langle m,n \rangle = \langle 0,0 \rangle + \langle m,n \rangle = \langle m+0, n+0 \rangle = \langle m,n \rangle = a$

(iv) Έστω $a = \langle m,n \rangle \in \mathbb{Z}$
Θέτουμε $-a = \langle n,m \rangle \in \mathbb{Z}$. Τότε $a+(-a) = 0$,
διότι $a+(-a) = \langle m,n \rangle + \langle n,m \rangle = \langle m+n, m+n \rangle \overset{\text{ορισμός}}{=} \langle 0,0 \rangle = 0$

(i') $a \cdot b = \langle m,n \rangle \cdot \langle p,q \rangle = \langle mp+nq, mq+np \rangle =$
$= \langle pm+qn, qm+pn \rangle$ (αντιμεταθετικότης στο $\mathbb{N}_0$)
$= \langle p,q \rangle \cdot \langle m,n \rangle = b \cdot a$.

(ii') $a \cdot (b \cdot \gamma) = (a \cdot b) \cdot \gamma$
$a \cdot (b \cdot \gamma) = \langle m,n \rangle \cdot (\langle p,q \rangle \cdot \langle \tau, \xi \rangle) = \langle m,n \rangle \cdot \langle p\tau+q\xi, p\xi+q\tau \rangle$
$= \langle m \cdot (p\tau+q\xi)+n(p\xi+q\tau), m(p\xi+q\tau)+n(p\tau+q\xi) \rangle$
$= \ldots = (a \cdot b) \cdot \gamma$.

(iii') Υπάρχει $1 \in \mathbb{Z}$ ώστε $1 \neq 0$ και $1 \cdot a = a$ $\forall a \in \mathbb{Z}$
Θέτουμε $1 = \langle 1, 0 \rangle \in \mathbb{Z}$. Τότε
$\langle 1, 0 \rangle \neq \langle 0, 0 \rangle$ διότι $1+0 = 1 \neq 0+0 = 0$,
και για $a = \langle m,n \rangle \in \mathbb{Z}$
$\langle 1,0 \rangle \cdot \langle m,n \rangle = \langle 1 \cdot m + 0 \cdot n, 1 \cdot n + 0 \rangle = \langle m,n \rangle$.

(v) Για κάθε $a, b, \gamma \in \mathbb{Z}$ ισχύει
$a \cdot (b+\gamma) = a \cdot b + a \cdot \gamma$ (επιμεριστική ιδιότητα).

(v) $a \cdot (b+\gamma) = \langle m,n \rangle \cdot \langle p+\tau, q+\xi \rangle =$
$= \langle m(p+\tau)+n(q+\xi), m(q+\xi)+n(p+\tau) \rangle =$
$= \langle (m \cdot p + m \cdot \tau)+(nq+n \cdot \xi), (mq+m\xi)+(np+n\tau) \rangle =$
$= \langle (mp+nq)+(m\tau+n\xi), (mq+np)+(m\xi+n\tau) \rangle =$
$= \langle mp+nq, mq+np \rangle + \langle m\tau+n\xi, m\xi+n\tau \rangle =$
$= \langle m,n \rangle \cdot \langle p,q \rangle + \langle m,n \rangle \cdot \langle \tau, \xi \rangle =$
$= a \cdot b + a \cdot \gamma$.

Διάταξη στο $\mathbb{Z}$

Αρχικά ορίζουμε:

$$\mathbb{Z}^+ = \{ \langle m,n \rangle \in \mathbb{Z} : m \geq n \ (\text{στο } \mathbb{N}_0) \}$$

Το σύνολο $\mathbb{Z}^+$ υποσύνολο του $\mathbb{Z}$ έχει τις ιδιότητες

(Σ1) Αν $\alpha, \beta \in \mathbb{Z}^+$, τότε $\alpha+\beta \in \mathbb{Z}^+$

(Αν $\alpha, \beta \in \mathbb{Z}^+$, τότε $\alpha = \langle m,n \rangle$, $m \geq n$ και $\beta = \langle \kappa, \lambda \rangle$, $\kappa \geq \lambda$, για $m,n,\kappa,\lambda \in \mathbb{N}_0$.
Τότε $\alpha+\beta = \langle m+\kappa, n+\lambda \rangle \in \mathbb{Z}^+$, διότι $m+\kappa \geq n+\lambda$, αφού $m \geq n$ και $\kappa \geq \lambda$.)

(Σ2) Για $\alpha \in \mathbb{Z}$ έχουμε είτε $\alpha \in \mathbb{Z}^+$ είτε $-\alpha \in \mathbb{Z}^+$

(αν $\alpha = \langle m,n \rangle \in \mathbb{Z}$ και $\langle m,n \rangle \notin \mathbb{Z}^+$, τότε $m < n$ και άρα $-\alpha = \langle n,m \rangle \in \mathbb{Z}^+$.

(Σ3) Αν $\alpha \in \mathbb{Z}^+$ και $-\alpha \in \mathbb{Z}^+$, τότε $\alpha = 0$

(Αν $\alpha \in \mathbb{Z}^+$, $\alpha = \langle m,n \rangle \in \mathbb{Z}$ και $m \geq n$, και αν $-\alpha \in \mathbb{Z}^+$, τότε $-\alpha = \langle n,m \rangle \in \mathbb{Z}$ και $n \geq m$.
Άρα αν $\alpha \in \mathbb{Z}^+$ και $-\alpha \in \mathbb{Z}^+$, τότε $n = m$, δηλαδή $\alpha = \langle n,n \rangle = \langle 0,0 \rangle = 0 \in \mathbb{Z}$).

Ορισμός

Για $\langle m,n \rangle, \langle p,q \rangle \in \mathbb{Z}$ ορίζουμε:

$\langle m,n \rangle \geq \langle p,q \rangle$ αν και μόνο αν υπάρχει $\langle r,s \rangle \in \mathbb{Z}^+$ ώστε:

$$\langle m,n \rangle = \langle p,q \rangle + \langle r,s \rangle.$$

Η σχέση $\geq$ στο $\mathbb{Z}$ είναι σχέση διάταξης και μάλιστα είναι **ολική** διάταξη, σύμφωνα με την παρακάτω Πρόταση:

Πρόταση

Η σχέση $\geq$ στο $\mathbb{Z}$ έχει τις ακόλουθες ιδιότητες:

(Δ1) Έστω $\alpha, \beta, \gamma \in \mathbb{Z}$. Αν $\alpha \geq \beta$ και $\beta \geq \gamma$, τότε $\alpha \geq \gamma$

[Απόδειξη Αν $\alpha \geq \beta$, τότε $\alpha = \beta + \varepsilon_1$ όπου $\varepsilon_1 \in \mathbb{Z}^+$ και αν $\beta \geq \gamma$, τότε $\beta = \gamma + \varepsilon_2$ όπου $\varepsilon_2 \in \mathbb{Z}^+$.

Επομένως $\alpha = (\gamma + \varepsilon_2) + \varepsilon_1 \overset{(ii)}{=} \gamma + (\varepsilon_2 + \varepsilon_1)$ όπου $\varepsilon_2 + \varepsilon_1 \in \mathbb{Z}^+$ (Σ.1). Άρα $\alpha \geq \gamma$.

(Δ3) Έστω $\alpha, \beta \in \mathbb{Z}$. Αν $\alpha \geq \beta$ και $\beta \geq \alpha$, τότε $\alpha = \beta$

[Αν $\alpha \geq \beta$, τότε $\alpha = \beta + \varepsilon_1$ με $\varepsilon_1 \in \mathbb{Z}^+$ και αν $\beta \geq \alpha$, τότε $\beta = \alpha + \varepsilon_2$ με $\varepsilon_2 \in \mathbb{Z}^+$.

Άρα, $\alpha = (\alpha + \varepsilon_2) + \varepsilon_1 = \alpha + (\varepsilon_1 + \varepsilon_2)$ με $\varepsilon_1 + \varepsilon_2 \in \mathbb{Z}^+$

Επομένως $\varepsilon_1 + \varepsilon_2 = 0$ και άρα $\varepsilon_1 = \varepsilon_2 = 0$ οπότε $\alpha = \beta$]

Άρα η σχέση $\geq$ στο $\mathbb{Z}$ είναι **σχέση διάταξης** ($\alpha \geq \alpha$ ισχύει προφανώς)

Μάλιστα είναι **ολική** διάταξη διότι:

(Δ2) Για κάθε $\alpha, \beta \in \mathbb{Z}$ είτε $\alpha \geq \beta$ είτε $\beta \geq \alpha$.

[Έστω $\alpha = \langle m, n \rangle$ $\beta = \langle p, q \rangle$. $m, n, p, q \in \mathbb{N}_0$

Τότε είτε $m + q \geq n + p$

είτε $m + q \leq n + p$

Άρα, είτε $\alpha \geq \beta$ είτε $\beta \geq \alpha$.

(Δ4) Έστω $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$. Αν $\alpha \geq \beta$ και $\gamma \geq \delta$, τότε $\alpha + \gamma \geq \beta + \delta$.

(Δ5) Έστω $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$. Αν $\alpha \geq \beta \geq 0$ και $\gamma \geq \delta \geq 0$, τότε $\alpha \cdot \gamma \geq \beta \cdot \delta$.

(Άσκηση)

Ορίζουμε στη συνέχεια για $\alpha, \beta \in \mathbb{Z}$:
$\alpha > \beta \Leftrightarrow \alpha \geqslant \beta$ και $\alpha \neq \beta$
$\alpha \leqslant \beta \Leftrightarrow \beta \geqslant \alpha$
$\alpha < \beta \Leftrightarrow \beta > \alpha$
Τότε για κάθε $\alpha, \beta \in \mathbb{Z}$ ισχύει η τριχοτομία:
Ισχύει ακριβώς μία από τις:
$$\alpha > \beta,\ \alpha = \beta,\ \beta > \alpha$$
Συμβολισμός των ακεραίων αριθμών

Ορίσαμε
$$\mathbb{Z}^+ = \{\langle m, n\rangle \in \mathbb{Z} : m \geqslant n\} = \{\langle m-n, 0\rangle : m-n \geqslant 0\} = \{\langle r, 0\rangle : r \in \mathbb{N}_0\} \equiv \mathbb{N}_0$$

Επίσης από την Πρόταση (Σ_2) έχουμε ότι:
για κάθε $\alpha \in \mathbb{Z}$, είτε $\alpha \in \mathbb{Z}^+ \Leftrightarrow \alpha = \langle r, 0\rangle$, $r \in \mathbb{N}_0$,
είτε $-\alpha \in \mathbb{Z}^+ \Leftrightarrow -\alpha = -\langle r, 0\rangle = \langle 0, r\rangle$ για $r \in \mathbb{N}_0$.

<u>Πρόταση</u>

Η συνάρτηση $f : \mathbb{N}_0 \to \mathbb{Z}^+$ με $f(n) = \langle n, 0\rangle$ είναι 1-1 και επί. Επίσης $f(m+n) = f(m) + f(n)$, $f(m \cdot n) = f(m) \cdot f(n)$, $m \geqslant n \Leftrightarrow f(m) \geqslant f(n)$.
(άσκηση)

Με βάση την Πρόταση αυτή μπορούμε να ταυτίσουμε το $\boxed{\mathbb{N}_0 \text{ με το } \mathbb{Z}^+}$, ταυτίζοντας το $n \in \mathbb{N}_0$ με το $\langle n, 0\rangle \in \mathbb{Z}^+$.
Οπότε το $\mathbb{N}_0$ μπορεί να θεωρηθεί υποσύνολο του $\mathbb{Z}$ ($\langle n, 0\rangle \equiv n$) και επίσης ταυτίζοντας το $-n$, για $n \in \mathbb{N}_0$, με το $\langle 0, n\rangle \in \mathbb{Z}$, έχουμε ότι $\boxed{\langle 0, n\rangle = -n}$ για $n \in \mathbb{N}_0$.
Οπότε κάθε ακέραιος αριθμός
είτε ανήκει στο $\mathbb{N}_0$
είτε είναι αντίθετος κάποιου στοιχείου του $\mathbb{N}_0$.

Διαίρεση στο $\mathbb{Z}$

Για $a, b \in \mathbb{Z}$ λέμε ότι ο a διαιρεί τον β και γράφουμε $a|\beta$ αν υπάρχει $x \in \mathbb{Z}$ ώστε:

$$\beta = a.x$$

Ισχύουν οι ιδιότητες:

(1) $a|a \quad \forall a \in \mathbb{Z}$

(2) $a|0 \quad \forall a \in \mathbb{Z}$

(3) $1|a$ και $-1|a \quad \forall a \in \mathbb{Z}$

(4) $0|\alpha \Leftrightarrow a=0$

(5) $a|b$ και $b|\gamma \Rightarrow a|\gamma$

(6) $a|b$ και $a|\gamma \Rightarrow a|bx+\gamma y \quad \forall x,y \in \mathbb{Z}$

(7) $a|\pm 1 \Leftrightarrow a = \pm 1$.
(άσκηση)

(8) Για $a \in \mathbb{N}$ και $b \in \mathbb{Z}$ υπάρχουν μοναδικοί $q \in \mathbb{Z}$, $r \in \mathbb{N}_0$ ώστε:

$$b = qa + r \quad 0 \leq r < a.$$

Απόδειξη (ανάλογη με την απόδειξη για $b, q \in \mathbb{N}_0$).

Έστω $S = \{x \in \mathbb{N}_0 : x = b - q.a \text{ για } q \in \mathbb{Z}\}$
$S \neq \phi$, διότι $x = b - 0.a = b \in S$ αν $b \in \mathbb{N}_0 = \mathbb{Z}^+$ και $x = b - ab = b(1-a) \in S$ αν $b < 0 \Leftrightarrow b \notin \mathbb{Z}^+$
Από την αρχή ελαχίστου το S έχει ελάχιστο στοιχείο έστω το $r = b - qa \in \mathbb{N}_0$ για $q \in \mathbb{Z}$, οπότε $b = q.a + r$. Έχουμε $0 \leq r$ και $r < a$, διότι αν $r \geq a$, τότε $b - (q+1)a = b - aq - a = r - a \geq 0$, επομένως $b - (q+1)a \in S$, άτοπο διότι το $r = b - qa$ είναι ελάχιστο στοιχείο του S.
Άρα, $b = qa + r$ για $q \in \mathbb{Z}$ και $0 < r \leq a$.
Έστω $b = q_1 a + r_1 = q_2 a + r_2$, $0 \leq r_1 < r_2 < a$, $q_1 \neq q_2$
Τότε $r_2 - r_1 = (q_1 - q_2).a$. Άτοπο, διότι $0 < r_2 - r_1 < a$, ενώ $(q_1 - q_2)a \geq a$.

Άρα σύμφωνα με την προηγούμενη απόδειξη κάθε ακέραιος αριθμός b γράφεται κατά μοναδικό τρόπο, για δεδομένο αριθμό $a \in \mathbb{N}$, ως
$$b = q \cdot a + r \quad \text{όπου } q \in \mathbb{Z} \text{ και } 0 \leq r < a$$

Όπως αποδείξαμε στο προηγούμενο μάθημα για δεδομένους αριθμούς $a, b \in \mathbb{N}$ υπάρχει ο μέγιστος κοινός διαιρέτης $\gamma \in \mathbb{N}$, ο οποίος υπολογίζεται με τον λεγόμενο Ευκλείδιο αλγόριθμο, μια ανακάλυψη των Πυθαγορείων.
Στη συνέχεια θα αποδείξουμε ότι ο $ΜΚΔ(a, b) = \gamma$ είναι ο ελάχιστος θετικός ακέραιος γραμμικός συνδυασμός των a, b, δηλαδή:
$$ΜΚΔ(a,b) = \min\{ax + by : x, y \in \mathbb{Z}\} \cap \mathbb{N}.$$

Θεώρημα

Έστω $a, b \in \mathbb{N}$. Αν $\gamma = ΜΚΔ(a, b) \in \mathbb{N}$ είναι ο μέγιστος κοινός διαιρέτης των a, b, τότε
$$\gamma = ΜΚΔ(a,b) = \min\{ax + by : x, y \in \mathbb{Z}\} \cap \mathbb{N} = \delta.$$

Απόδειξη

Έστω $I = \{ax + by : x, y \in \mathbb{Z}\} \cap \mathbb{N}$.

1. $I \neq \emptyset$ διότι $a = a \cdot 1 + b \cdot 0 \in I$
2. Από την αρχή ελαχίστου το I έχει ελάχιστο στοιχείο, έστω το $\delta = ax + by \in \mathbb{N}$, $x, y \in \mathbb{Z}$.
3. Το δ διαιρεί κάθε στοιχείο του I.

Πράγματι, αν $z = ax_1 + by_1 \in I$, όπου $x_1, y_1 \in \mathbb{Z}$.
Από το προηγούμενο Θεώρημα υπάρχουν μοναδικοί $q \in \mathbb{Z}$, $r \in \mathbb{N}_0$ ώστε:
$$z = q \cdot \delta + r, \quad \text{με } 0 \leq r < \delta$$
Τότε
$$r = z - q\delta = ax_1 + by_1 - q \cdot (ax + by) = a(x_1 - qx) + b(y_1 - qy).$$
Αν $r > 0$, τότε $r \in I$ και $r < \delta$, άτοπο.
Άρα $r = 0$, και επομένως ο δ διαιρεί το z.

Επομένως ο $\delta \in \mathbb{N}$ είναι κοινός διαιρέτης των στοιχείων του I.
Αφού ο $\delta \in \mathbb{N}$ διαιρεί κάθε στοιχείο του I, θα διαιρεί και τους α, β.
Έστω τώρα $\kappa \in \mathbb{N}$ που διαιρεί τους α, β.
Τότε ο κ θα διαιρεί και τον $\delta = \alpha x + \beta y$, άρα $\kappa \geq \delta$.
Επομένως ο δ είναι ισος με τον μέγιστο κοινο διαιρέτη $\gamma = \text{ΜΚΔ}(\alpha, \beta)$, δηλαδή

$$\gamma = \text{ΜΚΔ}(\alpha, \beta) = \delta = \min\{\alpha x + \beta y : x, y \in \mathbb{Z}\} \cap \mathbb{N}.$$

<u>Λήμμα 2</u> (σημειώσεων για τους φυσικούς αριθμούς)
Αν $\alpha, \beta \in \mathbb{N}$ και $\text{ΜΚΔ}(\alpha, \beta) = 1$, τότε αν ο α διαιρεί το γινόμενο $\beta \cdot \gamma$, όπου $\gamma \in \mathbb{N}$, τότε ο α διαιρεί τον γ.

<u>Απόδειξη</u>
Αφου $\text{Μ.ΚΔ}(\alpha, \beta) = 1$, από το προηγούμενο Θεώρημα,

$$1 = \alpha x + \beta y \quad \text{για } x, y \in \mathbb{Z}$$

Άρα,

$$\gamma = \alpha \cdot \gamma \cdot x + \beta \cdot \gamma \cdot y$$

Αφού ο α διαιρει το $\beta \cdot \gamma$, ο α θα διαιρεί το $\alpha \cdot \gamma \cdot x$ και το $\beta \cdot \gamma \cdot y$, άρα θα διαιρεί και το $\gamma = \alpha \gamma x + \beta \cdot \gamma y$.

<u>Λήμμα 4</u> Έστω $\alpha, \beta \in \mathbb{N}$ και $\text{ΜΚΔ}(\alpha, \beta) = 1$. Αν ο α διαιρεί τον $m \in \mathbb{N}$ και ο β διαιρεί τον $m \in \mathbb{N}$, τότε και ο $\alpha \cdot \beta$ διαιρεί τον m.

<u>Απόδειξη</u>
Αφού $\text{ΜΚΔ}(\alpha, \beta) = 1$, υπάρχουν απο το προηγούμενο Θεώρημα $x, y \in \mathbb{Z}$ ώστε:

$$1 = \alpha \cdot x + \beta y, \text{ και άρα } m = \alpha \cdot m \cdot x + \beta \cdot m \cdot y.$$

Αφού ο β διαιρει τον m ο $\alpha \cdot \beta$ διαιρει τον $\alpha \cdot m \cdot x$, και αφού ο α διαιρει τον m ο $\alpha \cdot \beta$ διαιρεί τον $\beta \cdot m \cdot y$
Άρα, ο $\alpha \cdot \beta$ διαιρει τον m.

Για παράδειγμα αν 4 διαιρεί τον $m \in \mathbb{N}$ και 5 διαιρεί τον m. Τότε το 20 διαιρεί τον m

Λήμμα 5

Έστω $\alpha, \beta, \gamma \in \mathbb{N}$ και $\text{ΜΚΔ}(\alpha, \beta) = 1$.
Αν ο γ διαιρεί το γινόμενο $\alpha \cdot \beta$ τότε υπάρχουν μοναδικοί αριθμοί $x, y \in \mathbb{N}_0$, ώστε

$\gamma = x \cdot y$ όπου x διαιρεί το α και y διαιρεί το β και επιπλέον $\text{ΜΚΔ}(x, y) = 1$

Απόδειξη

Έστω $x = \text{ΜΚΔ}(\gamma, \alpha)$. Απο Λήμμα 1, $\gamma = x \cdot y$, $\alpha = x \cdot y'$ και $\text{ΜΚΔ}(y, y') = 1$. για $y, y' \in \mathbb{N}_0$.
Έχουμε ότι ο $\gamma = x \cdot y$ διαιρεί το $\alpha \cdot \beta = x \cdot y' \cdot \beta$ άρα ο y διαιρεί το $y' \cdot \beta$ και αφού $\text{ΜΚΔ}(y, y') = 1$, από το Λήμμα 2, ο y διαιρεί τον β.

. Θα δείξουμε τώρα ότι $\text{ΜΚΔ}(x, y) = 1$.
Πράγματι, έστω $\mu = \text{ΜΚΔ}(x, y)$. Ο μ διαιρεί τον x, άρα διαιρεί τον $\alpha = x \cdot y'$. Επίσης ο μ διαιρεί τον y, άρα διαιρεί τον β (αφού ο y διαιρεί τον β
Επομένως ο $\text{ΜΚΔ}(x, y)$ διαιρεί τον $\text{ΜΚΔ}(\alpha, \beta) = 1$.
Άρα, $\text{ΜΚΔ}(x, y) = 1$.

Για την μοναδικότητα των $x, y \in \mathbb{N}_0$, ας υποθέσουμε ότι $\gamma = x_1 \cdot y_1$, όπου $\text{ΜΚΔ}(x_1, y_1) = 1$, και ότι ο x_1 διαιρεί τον α και ο y_1 διαιρεί τον β.
Τότε ο x_1 διαιρεί τον α και τον γ άρα ο x_1 διαιρεί τον $x = \text{ΜΚΔ}(\alpha, \gamma)$. Επίσης, αφού ο x διαιρεί τον α, ο y_1 διαιρεί τον β και $\text{ΜΚΔ}(\alpha, \beta) = 1$ συμπεραίνουμε ότι $\text{ΜΚΔ}(x, y_1) = 1$.

Επομένως, αφού έχουμε ότι ο $x = \text{ΜΚΔ}(\gamma, \alpha)$ διαιρεί τον $\gamma = x_1 y_1$ και $\text{ΜΚΔ}(x, y_1) = 1$, από το Λήμμα 2 έχουμε ότι ο x διαιρεί τον x_1.
Άρα, $x = x_1$ και τελικά και $y = y_1$.