10. Φυσικοί αριθμοί (συνέχεια)

Χρησιμοποιώντας τα τρία αξιώματα του Peano με τα οποία ορίζεται το σύνολο $\mathbb{N}_0$ των φυσικών αριθμών, αποδείξαμε ότι:

$$\mathbb{N}_0 = \{0\} \cup \{\varepsilon(m) : m \in \mathbb{N}_0\} \text{ και } \varepsilon(m) \neq 0 \ \forall m \in \mathbb{N}_0$$

Ορίζουμε $\mathbb{N} = \mathbb{N}_0 \setminus \{0\}$ και $1 = \varepsilon(0) \neq 0, 1 \in \mathbb{N}$.

Στη συνέχεια αποδείξαμε το Θεώρημα (αναδρομής) σύμφωνα με το οποίο αν $f: X \to X$ είναι μια συνάρτηση από το σύνολο X στο X και $c \in X$ ορίζεται μια μοναδική συνάρτηση $\varphi: \mathbb{N}_0 \to X$ με ώστε: $\varphi(0) = c$ και $\varphi(\varepsilon(n)) = f(\varphi(n)) \ \forall n \in \mathbb{N}_0$.

Με την χρήση του Θεωρήματος αναδρομής ορίζεται η πράξη της πρόσθεσης και η πράξη του πολλαπλασιασμού στο σύνολο $\mathbb{N}_0$:

Ορισμός Πρόσθεσης στο $\mathbb{N}_0$

Έστω $\boxed{m \in \mathbb{N}_0}$. Για κάθε $n \in \mathbb{N}_0$ ορίζουμε:

$$m + n = \varphi_m(n)$$

όπου $\varphi_m: \mathbb{N}_0 \to \mathbb{N}_0$ συνάρτηση ώστε:

$$\varphi_m(0) = m \text{ και}$$
$$\varphi_m(\varepsilon(n)) = \varepsilon(\varphi_m(n)) \ \forall n \in \mathbb{N}_0.$$

Ορισμός Πολλαπλασιασμού στο $\mathbb{N}_0$

Επίσης για κάθε $n \in \mathbb{N}_0$ ορίζουμε:

$$m \cdot n = \mu_m(n)$$

όπου $\mu_m: \mathbb{N}_0 \to \mathbb{N}_0$ συνάρτηση ώστε:

$$\mu_m(0) = 0 \text{ και}$$
$$\mu_m(\varepsilon(n)) = \mu_m(n) + m.$$

Εφαρμόζοντας το Θεώρημα αναδρομής οι συναρτήσεις φ_m, μ_m είναι μοναδικές, για $m \in \mathbb{N}$.

Θέτοντας $\varepsilon(0)=1$ έχουμε για κάθε $m\in\mathbb{N}_0$

$$m+1 = m+\varepsilon(0) = \varphi_m(\varepsilon(0)) = \varepsilon(\varphi_m(0)) = \varepsilon(m)$$

Άρα, $m+1=\varepsilon(m)$ $\forall\ m\in\mathbb{N}_0$

Επίσης, $m\cdot 0 = 0$ $\forall\ m\in\mathbb{N}_0$ και

$$m\cdot 1 = \mu_m(1) = \mu_m(\varepsilon(0)) = \mu_m(0)+m = 0+m = m \quad \forall\ m\in\mathbb{N}_0.$$

Χρησιμοποιώντας την αρχή επαγωγής (Φ_3) αποδεικνύονται για κάθε $m\in\mathbb{N}$:

$0+m=m$, $1+m=\varepsilon(m)$, $1\cdot m=m$, $0\cdot m=0$

Για παράδειγμα:

$\forall m\in\mathbb{N}_0$ $0+m=m$, διότι $S=\{m\in\mathbb{N}_0 : 0+m=m\}=\mathbb{N}_0$

συμφωνα με την αρχή επαγωγής (Φ_3):

$0\in S$, διότι $0+0=\varphi_0(0)=0$.

Αν $m\in S$ έχουμε $0+m=m$. Άρα, $m+1\in S$, διότι

$$0+(m+1) = 0+\varepsilon(m) = \varphi_0(\varepsilon(m)) = \varepsilon(\varphi_0(m)) = \varepsilon(0+m) = \varepsilon(m) = m+1$$

Άρα, $0+m=m$ $\forall\ m\in\mathbb{N}_0$.

Επίσης για κάθε $m,n,\rho\in\mathbb{N}_0$ ισχύουν:

1. $(m+n)+\rho = m+(n+\rho)$
2. $m+n = n+m$ (Έστω $m\in\mathbb{N}$. Τότε $m+n=n+m$ $\forall n\in\mathbb{N}$)
3. $(m\cdot n)\cdot\rho = m\cdot(n\cdot\rho)$
4. $m\cdot n = n\cdot m$
5. $m\cdot(n+\rho) = m\cdot n + m\rho$. ν

Ακολούθως τα αξιώματα του Peano έχουν την μορφή:

(Φ_1) $n+1\neq 0$ για κάθε $n\in\mathbb{N}$.

(Φ_2) $m+1=n+1 \Longrightarrow m=n$ $\forall\ n,m\in\mathbb{N}$

(Φ_3) Αν $S\subseteq\mathbb{N}$ και ισχύουν οι (i) και (ii)

(i) $0\in\mathbb{N}$, (ii) $n\in S \Longrightarrow n+1\in S$,

τότε $S=\mathbb{N}_0$ (αρχή επαγωγής)

Πρόταση 2.5 (ιδιότητες διαγραφής)
Έστω $m, n, q \in \mathbb{N}_0$. Τότε ισχύουν:

(i) $m+q = n+q \iff m = n$

(ii) $m \cdot q = n \cdot q$, $q \neq 0 \iff m = n$

Απόδειξη Έστω $m, n \in \mathbb{N}_0$.

(i) ($\Rightarrow$) Έστω το σύνολο:

$$S = \{q \in \mathbb{N}_0 \mid m+q = n+q \Rightarrow m = n\}$$

$0 \in S$, διότι $m+0 = n+0 \Rightarrow m = n$.

Έστω $q \in S$, Άρα,

(*) $m+q = n+q \Rightarrow m = n$.

Τότε $q+1 \in S$. Πράγματι:

αν $m+(q+1) = n+(q+1)$ θα έχουμε

$(m+q)+1 = (n+q)+1$ (Ιδιότητα (1).)

Επομένως

από το (Φ_2) αξίωμα έχουμε:

$$m+q = n+q.$$

Άρα απο την υπόθεση $q \in S$ έχουμε:

$$m = n.$$

Συνεπώς $q+1 \in S$.

Απο την αρχή της επαγωγής $S = \mathbb{N}_0$

δηλαδή ισχύει η συνεπαγωγή (i).

($\Leftarrow$) Αν $m = n$, προφανώς $m+q = n+q$.

(ii) ($\Rightarrow$) Έστω το σύνολο

$$P = \{m \in \mathbb{N}_0 \mid m \cdot q = n \cdot q \Rightarrow m = n \ \forall n \in \mathbb{N}_0, q \in \mathbb{N}\}$$

$(0 \in P)$ διότι αν $0 \cdot q = n \cdot q$ για $n \in \mathbb{N}_0$, $q \in \mathbb{N} = \mathbb{N}_0 - \{0\}$, τότε έχουμε $n \cdot q = 0$ και $q \neq 0$. Τότε $n = 0$.

Πράγματι, αν $n \neq 0$, τότε $n = r+1$ για $r \in \mathbb{N}_0$.
Επομένως, $n.q = (r+1).(p+1) = r.(p+1) + (p+1) =$
$(r.p + r) + (p+1) = ((rp+r)+p) + 1 \neq 0$, Άτοπο.
Άρα, $n = 0$ και επομένως $\boxed{0 \in P}$

Έστω $m \in P$, δηλαδή $m \in \mathbb{N}_0$ και $m.q = n.q \Rightarrow m = n$ για κάθε $n \in \mathbb{N}_0$ και $q \in \mathbb{N}$.
Τότε $m+1 \in P$.

Πράγματι, έστω $(m+1).q = n.q$ για $n \in \mathbb{N}_0$, $q \in \mathbb{N}$.
Έχουμε $q \neq 0$ και $m+1 \neq 0$, άρα, σύμφωνα με τα παραπάνω $(m+1).q \neq 0$. Άρα
$n.q \neq 0$ και ακολούθως $n \neq 0$.
Έστω $n = r+1$ για $r \in \mathbb{N}_0$. Τότε:
$(m+1).q = (r+1)q \iff m.q = r.q \iff m = r.$
από την επαγωγική υπόθεση.
Συνεπώς, $m+1 = r+1 = n$ και άρα
$m+1 \in P$.
Από την αρχή επαγωγής έχουμε $P = \mathbb{N}$.

Επομένως, αν $m.q = n.q$ για $m, n, q \in \mathbb{N}_0$ και $q \neq 0$, τότε $m = n$.

Αφαίρεση – Διάταξη φυσικών αριθμών

Για κάθε $m, n \in \mathbb{N}_0$ ορίζουμε:
$m \geq n$ αν και μόνο αν $m = r + n$ για $r \in \mathbb{N}_0$.

Για κάθε $m, n \in \mathbb{N}_0$ όπου $m \geq n \iff m = n + r$, $r \in \mathbb{N}_0$ ορίζουμε την διαφορά $m - n$ ως ακολούθως:

$$m - n = r \iff m = n + r.$$

Η διαφορά είναι καλά ορισμένη καθώς $m = n + r$ για μοναδικό $r \in \mathbb{N}_0$
$(n + r_1 = n + r_2 \implies r_1 = r_2)$

Ιδιότητες αφαίρεσης – διάταξης

(α) Αν $m, n, r \in \mathbb{N}$ και $m \geq n \geq r$, τότε
$m - (n - r) = (m - n) + r$.

Απόδειξη

$m - (n-r) = (m-n) + r \overset{\text{ορισμός}}{\iff} m = ((m-n)+r) + (n-r))$
$\iff m = (m-n) + (r + (n-r))$ (από προσεταιριστική ιδιότητα)
$\iff m = (m-n) + r$ (από ορισμό διαφοράς)
ισχύει.

(β) Αν $n \geq r$ τότε $m + (n-r) = (m+n) - r$

Απόδειξη

$m + (n-r) = (m+n) - r \overset{\text{ορισμός}}{\iff}$
$[m + (n-r)] + r = m + n \iff$ (προσεταιριστική)
$m + n = m + [(n-r) + r] \iff$ ορισμός
$m + n = m + n$ ισχύει.

(γ) Αν $n \geq r$, τότε $m \cdot (n-r) = m \cdot n - m \cdot r$
(απόδειξη σημειώσεις μαθήματος

Ορισμός

Ορίσαμε για δύο φυσικούς αριθμούς $m, n \in \mathbb{N}_0$

$$m \geq n \iff m = r + n \text{ για } r \in \mathbb{N}_0$$

Έπίσης μπορούμε να ορίσουμε

$$m \leq n \iff n \geq m$$

$$m > n \iff m \geq n \text{ και } m \neq n$$

$$m < n \iff n > m$$

Προτάσεις 2.6 & 2.7

Η σχέση $\geq$ στο $\mathbb{N}_0 \times \mathbb{N}_0$ είναι σχέση διάταξης.

Απόδειξη

(1) $m \geq m$ $\forall$ $m \in \mathbb{N}_0$, διότι $m = 0 + m$ (ανακλαστική)

(2) Αν $m \geq n$ και $n \geq m$, τότε $m = n$. (αντισυμμετρική)

[$m \geq n$, άρα $m = r + n$ για $r \in \mathbb{N}_0$ και

$n \geq m$, άρα $n = t + m$ για $t \in \mathbb{N}_0$. Επομένως

$0 + n = n = t + (r + n) = (t + r) + n$.

Άρα, $t + r = 0$.

Αν $t \neq 0$, τότε $t = q + 1$ για κάποιο $q \in \mathbb{N}_0$,

άρα $0 = (q + 1) + r = q + (1 + r) = q + (r + 1) = (q + r) + 1$.

Άτοπο, από το αξίωμα (Φ_4)

Συνεπώς $t = 0$ και άρα $m = n$]

(3) Αν $m \geq n$ και $n \geq p$, τότε $m \geq p$. (μεταβατική)

[Πραγματι, αν $m = r + n$ και $n = s + p$ για $r, s \in \mathbb{N}_0$,

τότε $m = r + (s + p) = (r + s) + p$, $r + s \in \mathbb{N}_0$.

Άρα, $m \geq p$]

Πρόταση 2.8 $m, n, p, q \in \mathbb{N}_0$.

Αν $m \geq n$ και $p \geq q$, τότε $m + p \geq n + q$, $m \cdot p \geq n q$.

[$m = r + n$ και $p = s + q$ για $r, s \in \mathbb{N}_0$. Οπότε

$m + p = (r + n) + (s + q) \geq n + q$.

$m \cdot p = (r + n)(s + q) = n \cdot q + (r \cdot s + r \cdot q + n \cdot s)$

Άρα, $m \cdot p \geq n \cdot q$.]

Πρόταση 2.9
Αν $m \in \mathbb{N}_0$, τότε $m \geq 0$.
Απόδειξη
$m = m + 0 \geq 0 + 0 = 0$

Πρόταση 2.10
Αν $m \in \mathbb{N}_0$ και $m > 0$, τότε $m \geq 1$.
[$m \neq 0$, άρα $m = q+1$ για $q \in \mathbb{N}_0$. Επομένως $m \geq 1$.

Πρόταση 2.11
Αν $m, n \in \mathbb{N}_0$ και $m > n$, τότε $m \geq n+1$.
[$m > n$, άρα $m = r+n$ για $r \in \mathbb{N}_0$ και $r \neq 0$.
Συνεπώς $r = q+1$ για $q \in \mathbb{N}_0$.
Επομένως $m = (q+1)+n = q+(n+1)$. Άρα $m \geq n+1$.

Πρόταση 2.12
Η σχέση $\geq$ στο $\mathbb{N}_0$ είναι ολική διάταξη.
Απόδειξη
Η $\geq$ είναι σχέση διάταξης και είναι ολική διάταξη.
Πράγματι, έστω $m, n \in \mathbb{N}_0$. Θέτουμε
$$S(m) = \{n \in \mathbb{N}_0 : m \geq n \text{ ή } n \geq m\}$$
Ισχύει $S(m) = \mathbb{N}_0$:
(1) $0 \in S(m)$, διότι $0 \leq m$.
(2) Έστω $n \in S(m)$. Τότε $m \geq n$ ή $n \geq m$.
Αν $m \geq n$, τότε είτε $\boxed{m = n}$, οπότε $n+1 \geq m$ και $n+1 \in S(m)$, είτε $\boxed{m > n}$, οπότε $m > n > n+1$, και $n+1 \in S(m)$
Σε κάθε περίπτωση $n+1 \in S(m)$
Από την αρχή επαγωγής έχουμε ότι $S(m) = \mathbb{N}_0$.

Πρόταση
Η σχέση $>$ είναι αυστηρή διάταξη. και για κάθε $m, n \in \mathbb{N}_0$ ισχύει:

Πρόταση 2.13 (διαγραφής)
Για κάθε $m, n, q \in \mathbb{N}_0$ ισχύουν:
1. $m+q > n+q \Rightarrow m > n$
2. Αν $q \neq 0$ και $m \cdot q > n \cdot q$, τότε $m > n$.

Απόδειξη
1. Αν δεν ισχύει $m > n$, τότε $m \leq n$. Από την Πρόταση 8 $m+q \leq n+q$ για κάθε $q \in \mathbb{N}_0$ Άτοπο, από την υπόθεση. Άρα, $m > n$.
2. Έστω $q \neq 0$ και $m \cdot q > n \cdot q$. Αν δεν ισχύει $m > n$, τότε $m \leq n$. Από την Πρόταση 8 τότε έχουμε $m \cdot q \leq nq$. Άτοπο, άρα $m > n$

Παραλλαγές της επαγωγής
(i) Έστω $m \in \mathbb{N}_0$ και $S \subseteq \mathbb{N}_0$ με τις εξής ιδιότητες:
(α) $m \in S$, και
(β) Για κάθε $n \in S$ με $n \geq m$ ισχύει ότι $n+1 \in S$
Τότε $\{n \in \mathbb{N}_0 : n \geq m\} \subseteq S$

Απόδειξη
Έστω $A = \{n \in \mathbb{N}_0 : m+n \in S\}$
Τότε $0 \in A$ διότι $m+0 = m \in S$ (α)
Αν $n \in A$, έχουμε $m+n \in S$ και $m+n \geq m$, άρα $(m+n)+1 \in S$ (β). Τότε $m+(n+1) = (m+n)+1 \in S$, και τελικά $n+1 \in A$.
Από αρχή επαγωγής έχουμε $A = \mathbb{N}_0$ και άρα για κάθε $n \in \mathbb{N}_0$ ισχύει $m+n \in S$.
Δηλαδή $\{n \in \mathbb{N}_0 : n \geq m\} \subseteq S$

Πόρισμα Έστω $S \subseteq \mathbb{N}_0$ με τις ιδιότητες:
($\mathcal{H}_1$) (α) $m \in S$, και
(β) Αν $m, m+1, \ldots, n \in S$, τότε $n+1 \in S$
Τότε $\{n \in \mathbb{N}_0 : n \geq m\} \subseteq S$.
Αναλογη απόδειξη με χρήση της ισχυρής

(ii) Ισχυρή μορφή επαγωγής

Έστω $S \subseteq \mathbb{N}_0$ με τις ακόλουθες ιδιότητες:

(α) $0 \in S$ και

(β) Αν $0, 1, \ldots, n \in S$, τότε $n+1 \in S$

Τότε $S = \mathbb{N}_0$

Απόδειξη

Έστω $T = \{n \in \mathbb{N}_0 : 0 \in S, 1 \in S, \ldots, n \in S\} \subseteq \mathbb{N}_0$

Τότε: $0 \in T$, διότι $0 \in S$ (α) και

αν $n \in T$, δηλαδή $0 \in S, 1 \in S, \ldots, n \in S$, (β)

τότε $n+1 \in S$, οπότε $0 \in S, \ldots, n \in S, n+1 \in S$,

και οπότε $n+1 \in T$.

Από την αρχή της επαγωγής $T = \mathbb{N}_0$ και

άρα $m \in S$ για κάθε $n \in \mathbb{N}_0$, δηλαδή $S = \mathbb{N}_0$.

Το παρακάτω Βασικό Θεώρημα έπεται απο την αρχή της επαγωγής και μάλιστα είναι ισοδύναμο.

Θεώρημα 14 (Αρχή ελαχίστου)

Κάθε μη κενό υποσύνολο M του $\mathbb{N}_0$, έχει ελάχιστο στοιχείο, δηλαδή υπάρχει $m_0 \in M$, που είναι μικρότερο ή ίσο απο κάθε στοιχείο του M, ($m_0 \leq m \ \forall \ m \in M$)

Απόδειξη

Έστω $M \subseteq \mathbb{N}$ και $M \neq \phi$.

Υποθέτουμε ότι το M δεν έχει ελάχιστο στοιχείο, και Θέτουμε:

$$T = \{n \in \mathbb{N}_0 : n \notin M\} = \mathbb{N}_0 \setminus M.$$

Τότε $0 \in T$, διότι αν $0 \notin T$ θα είχαμε $0 \in M$, και άρα το M θα είχε ελάχιστο στοιχείο.

Έστω $0, 1, \ldots, n \in T$. Τότε $0, 1, \ldots, n \notin M$

Τότε $n+1 \notin M$, διότι αν $n+1 \in M$ το M θα είχε το $n+1$ ελάχιστο στοιχείο.

Άρα, $n+1 \in T$. Οπότε $T = \mathbb{N}_0$. (ισχυρή επαγωγή)

Άτοπο! διότι τότε $M = \phi$. Άρα, το M

Διαίρεση φυσικών αριθμών

Έστω $a, b \in \mathbb{N}_0$.

Ο a διαιρεί τον b αν υπάρχει $n \in \mathbb{N}_0$ ώστε:

$$b = n.a$$

Τότε γράφουμε $a|b$, και λέμε ότι ο a είναι διαιρέτης του b ή ο b είναι πολλαπλάσιο του a. Συνέπειες του ορισμού είναι:

(1) $a|a \ \forall \ a \in \mathbb{N}_0 \quad (a = 1.a)$

(2) $a|0 \ \forall \ a \in \mathbb{N}_0 \quad (0 = 0.a)$

(3) $1|a \ \forall \ a \in \mathbb{N}_0 \quad (a = 1.a)$

(4) $0|a \Leftrightarrow a = 0 \quad (a = 0.a = 0)$

(5) $a|b$ και $b|\gamma \Rightarrow a|\gamma$ (από τον ορισμό)

(6) $a|b$ και $a|\gamma \Rightarrow a|\kappa.b + \lambda\gamma \ \forall \ \kappa, \lambda \in \mathbb{N}_0$ (άσκηση)

Θεώρημα

Έστω $a \in \mathbb{N} = \mathbb{N}_0 - \{0\}$ και $b \in \mathbb{N}_0$. Υπάρχουν μοναδικοί $q, r \in \mathbb{N}_0$ ώστε:

$$b = qa + r \quad \text{όπου} \quad 0 \leq r < a.$$

Απόδειξη

Έστω το σύνολο:

$$S = \{x \in \mathbb{N}_0 : x = b - qa \text{ για } q \in \mathbb{N}_0\} \subseteq \mathbb{N}_0.$$

$S \neq \phi$, διότι $b = b - 0.a \in S$

Από την αρχή ελαχίστου το S έχει ελάχιστο στοιχείο, έστω το $r = b - qa \in \mathbb{N}_0$ για $q \in \mathbb{N}_0$.

Τότε $\boxed{b = q.a + r}$.

Θα αποδείξουμε ότι $0 \leq r < a$.

Αφού $r \in \mathbb{N}_0$, έχουμε ότι $0 \leq r$.

Επίσης, $r < a$, διότι αν $r \geq a$, τότε $\boxed{r = a + s}$ για $s \in \mathbb{N}_0$, και ακολούθως $\boxed{s < r}$. $(a > 0)$

Άρα, $b = (q+1)a + s$ όπου $s \in \mathbb{N}_0$, $s < r$.

Επομένως $\boxed{s = b - (q+1)a} \in \mathbb{N}_0$, $s < r$.

Άρα, $s \in S$ και $s < r$. Άτοπο. Άρα $r < a$.

Επομένως, $b = q.a + r$ και $0 \leq r < a$.

Θεώρημα Έστω $a, \beta \in \mathbb{N}$. Υπάρχει ο μέγιστος κοινός διαιρέτης $\gamma = ΜΚΔ(a,\beta) \in \mathbb{N}$ των a, β, δηλαδή υπάρχει μοναδικός αριθμός $\gamma \in \mathbb{N}$ ώστε:

(i) $\gamma | a$ και $\gamma | \beta$, και

(ii) αν $\kappa \in \mathbb{N}$ και $\kappa | a$, $\kappa | \beta$, τότε $\kappa \leq \gamma$.

Απόδειξη.

Αν $a = \beta$, τότε $a = \beta = ΜΚΔ(a,\beta) = \gamma$

Έστω $a < \beta$. Τότε, από το προηγούμενο θεώρημα

$\beta = \kappa_1 a + \gamma_1$ με $\gamma_1 < a$, $\gamma_1 \in \mathbb{N}$, $\kappa_1 \in \mathbb{N}$

$a = \kappa_2 \gamma_1 + \gamma_2$ με $\gamma_2 < \gamma_1$, $\gamma_2 \in \mathbb{N}$, $\kappa_2 \in \mathbb{N}$

$\gamma_1 = \kappa_3 \gamma_2 + \gamma_3$ με $\gamma_3 < \gamma_2$, $\gamma_3 \in \mathbb{N}$, $\kappa_3 \in \mathbb{N}$

. . . .

$\gamma_{\nu-2} = \kappa_\nu \gamma_{\nu-1} + \gamma_\nu$ με $\gamma_\nu < \gamma_{\nu-1}$, $\gamma_\nu \in \mathbb{N}$, $\kappa_\nu \in \mathbb{N}$

$\gamma_{\nu-1} = \kappa_{\nu+1} \cdot \gamma_\nu$, με $\kappa_{\nu+1} \in \mathbb{N}$.

Η ακολουθία $\beta > a > \gamma_1 > \gamma_2 > \gamma_3 > \cdots > \gamma_{\nu-1} > \gamma_\nu$ των ανθυφαιρετικών υπολοίπων είναι γνήσια φθίνουσα ακολουθία φυσικών αριθμών άρα δεν μπορεί παρά να είναι πεπερασμένη σύμφωνα με την **αρχή ελαχίστου**.

(i) Με μια πεπερασμένη επαγωγή προς τα άνω αποδεικνύεται ότι ο γ_ν είναι κοινός διαιρέτης των a, β [ο γ_ν διαιρεί τον $\gamma_{\nu-1}$, άρα τον $\gamma_{\nu-2}$, ..., άρα τον γ_1, άρα τον a, άρα τον β]

(ii) Με μια πεπερασμένη επαγωγή προς τα κάτω αποδεικνύεται ότι κάθε κοινός διαιρέτης των a, β είναι και διαιρέτης του γ_ν.

Άρα, $\gamma = \gamma_\nu$ είναι ο μέγιστος κοινός διαιρέτης των a, β. $\gamma = \gamma_\nu = ΜΚΔ(a,\beta)$. και είναι μοναδικός.

Η προηγούμενη διαδικασία για την εύρεση του μέγιστου κοινού διαιρέτη δύο αριθμών είναι γνωστή ως Ευκλείδιος αλγόριθμος, διότι το Θεώρημα αυτό και η απόδειξή του είναι ακριβώς η Πρόταση 7.2 του Εβδόμου Βιβλίου των "Στοιχείων" του Ευκλείδη.

Σύμφωνα με την Ιστορία των Αρχαίων Ελληνικών Μαθηματικών η ανακάλυψη της διαδικασίας αυτής οφείλεται στους Πυθαγόριους.

Παράδειγμα 3.3.13 (Σημειώσεις μαθήματος)
ΜΚΔ(391, 2533) = 17 ΜΚΔ(365, 13) = 1 (365 = 13.28 + 1, 13 = 13.1)

Λήμματα διαιρετότητας

Λήμμα 1
Αν $a, b \in \mathbb{N}$ και $\delta = ΜΚΔ(a, b)$, τότε $a = \gamma.\delta$, $b = \varepsilon.\delta$ και $ΜΚΔ(\gamma, \varepsilon) = 1$, δηλαδή γ, ε είναι πρώτοι μεταξύ τους.

Απόδειξη
Έστω $ΜΚΔ(\gamma, \varepsilon) = \rho > 1$. Τότε $\varepsilon = \zeta.\rho$, $\gamma = \eta.\rho$.
Τότε $a = \gamma.\delta = (\eta.\rho).\delta = \eta.(\rho.\delta)$ και
$b = \varepsilon.\delta = (\zeta.\rho).\delta = \zeta(\rho.\delta)$
Επομένως ο αριθμός $\rho.\delta$ είναι κοινός διαιρέτης των a, b και $\rho.\delta > \delta$. Άτοπο διότι ο δ είναι ο μέγιστος κοινός διαιρέτης των a, b.

Λήμμα 2

Αν $\alpha, \beta \in \mathbb{N}$ και $ΜΚΔ(\alpha,\beta)=1$, τότε αν ο α διαιρεί το $\beta.\gamma$, για $\gamma \in \mathbb{N}$, τότε ο α διαιρεί τον γ.

Απόδειξη

Έστω ο α διαιρεί το $\beta.\gamma$. Τότε υπάρχει αριθμός δ ώστε $\alpha.\delta = \beta.\gamma$. Τότε $\frac{\alpha}{\beta} = \frac{\gamma}{\delta}$. Άρα $\gamma = κ.\alpha$ και $\delta = κ.\beta$ Άρα ο α διαιρεί τον γ.

Παράδειγμα:

Αν 8 διαιρεί το $3m$, τότε 8 διαιρεί τον m.

Λήμμα 3

Έστω $\alpha, \beta, \gamma \in \mathbb{N}$ με $ΜΚΔ(\alpha,\beta)=1$. Αν ο γ διαιρεί τα $\alpha.\beta$, τότε υπάρχουν μοναδικοί φυσικοί αριθμοί σ, τ ώστε ο σ να διαιρεί τον α, ο τ να διαιρεί τον β και $\gamma = \tau.\sigma$, $ΜΚΔ(\sigma,\tau)=1$.

Απόδειξη

Έστω $\boxed{\sigma = ΜΚΔ(\alpha,\gamma)}$ Από το Λήμμα 1, $\alpha = κ.\sigma$, $\gamma = \tau.\sigma$ και $ΜΚΔ(κ,\tau)=1$. Έχουμε ότι $\gamma = \tau.\sigma$ διαιρεί το $\alpha.\beta = κ.\sigma.\beta$. Άρα, ο τ διαιρεί το $κ.\beta$. Εφ' όσον $ΜΚΔ(κ,\tau)=1$, από το Λήμμα (2) ο τ διαιρεί το β. Θα αποδείξουμε ότι $ΜΚΔ(\sigma,\tau)=1$. Πράγματι, ο $ΜΚΔ(\sigma,\tau)$ διαιρεί τον σ, άρα διαιρεί και τον $\alpha = κ.\sigma$. Επίσης ο $ΜΚΔ(\sigma,\tau)$ διαιρεί τον τ, άρα διαιρεί και τον β. Άρα ο $ΜΚΔ(\sigma,\tau)$ διαιρεί και τον $ΜΚΔ(\alpha,\beta)=1$, οπότε $ΜΚΔ(\sigma,\tau)=1$.

5. Ανάλυση αριθμών σε γινόμενο πρώτων αριθμών

Σύμφωνα με και με τους ορισμούς που δίδονται στο Έβδομο Βιβλίο των Στοιχείων του Ευκλείδη αριθμός είναι πλήθος μονάδων (άρα η μονάδα δεν είναι αριθμός), [Ορισμός 7.2] και ένας αριθμός π είναι **πρώτος** αν γράφεται ως γινόμενο αριθμών μονο με την μορφή $\pi = \pi \cdot 1 \ (= 1 \cdot \pi)$ [Ορισμός 7.12]
Δηλαδή ένας φυσικός αριθμός $a > 1$ είναι **πρώτος** άν οι μόνοι φυσικοί αριθμοί που τον διαιρούν είναι ο 1 και ο π.
Αν ο $a > 1$ δεν είναι πρώτος τότε είναι **σύνθετος** [Ορισμός 7.14]

Θεώρημα Έστω $a, \beta \in \mathbb{N}$ και $\rho \in \mathbb{N}$ πρώτος αριθμός. Αν ο ρ διαιρεί το $a \cdot \beta$, τότε είτε ρ διαιρεί τον α είτε ρ διαιρεί τον β. [Πρόταση 7.30, Στοιχείων]

Απόδειξη
Έστω ότι ο $\rho \nmid$ δεν διαιρεί τον α. Αφού ο ρ είναι πρώτος οι μόνοι διαιρέτες του είναι οι 1 και ρ, άρα $ΜΚΔ(\rho, a) = 1$. Αφού ο ρ διαιρεί το $a \cdot \beta$, τότε ο ρ διαιρεί τον β (Λημμα 2).

Επαγωγικά μπορούμε να αποδείξουμε:

Θεώρημα Έστω $a_1, a_2, \ldots, a_n \in \mathbb{N}$ και $\rho \in \mathbb{N}$ πρώτος αριθμός. Αν ο ρ διαιρεί το γινόμενο $a_1 \cdot a_2 \ldots a_n$, τότε ο ρ διαιρεί τουλάχιστον ένα απο τούς $a_1, \ldots, a_n$.

Θεμελιώδες Θεώρημα της Αριθμητικής

Κάθε φυσικός αριθμός $n > 1$ είναι ίσος με γινόμενο πρώτων αριθμών κατά τρόπο μοναδικό (αν αγνοήσουμε την διάταξη).

Απόδειξη

Έστω ένας φυσικός αριθμός $n \geq 2$.

Θα αποδείξουμε με τη χρήση της Ισχυρής μορφής επαγωγής ότι κάθε φυσικός αριθμός $n \geq 2$ γράφεται ως γινόμενο πρώτων αριθμών. (Πόρισμα $(ii)_1$).

Έστω $S = \{n \in \mathbb{N}_0 : n \geq 2$ και n είναι γινόμενο πρώτων αριθμών$\}$

Τότε $2 \in S$ διότι το 2 είναι πρώτος αριθμός

Έστω $\{2, 3, \ldots, n\} \subseteq S$.

Τότε αν ο $n+1$ είναι πρώτος προφανώς $n+1 \in S$.

Αν ο $n+1$ δεν είναι πρώτος τότε $n+1 = n_1 \cdot n_2$, όπου $2 \leq n_1, n_2 \leq n$

Από την επαγωγική υπόθεση οι αριθμοί n_1, n_2 μπορούν να γραφούν ως γινόμενο πρώτων αριθμών, επομένως και ο $n+1$ θα γράφεται ως γινόμενο πρώτων αριθμών και άρα $n+1 \in S$.

Σύμφωνα με το Πόρισμα $(ii)_1$ της Ισχυρής μορφής της επαγωγής έχουμε ότι $S = \{n \in \mathbb{N}_0 : n \geq 2\}$.

Πόρισμα

Κάθε φυσικός αριθμός $n > 1$ γράφεται μοναδικά στη μορφή: $n = p_1^{k_1} \cdots p_r^{k_r}$, όπου $p_1 < \ldots < p_r$ πρώτοι αριθμοί και $k_1, \ldots, k_r \in \mathbb{N}$.

Απειρία πρώτων αριθμών

(Πρόταση 9.20 των Στοιχείων του Ευκλείδ
Οι πρώτοι αριθμοί είναι περισσότεροι από κάθε πεπερασμένο πλήθος.
Σε σύγχρονη ορολογία: Το σύνολο των πρώτων αριθμών είναι άπειρο.

Απόδειξη

Έστω ότι οι πρώτοι αριθμοί είναι πλήθους n, δηλαδή είναι οι $\pi_1, \pi_2, \ldots, \pi_\nu$, που είναι διαφορετικοί μεταξύ τους. Έστω

$$\pi = \pi_1 \cdot \pi_2 \ldots \pi_\nu + 1$$

Ο π είναι μεγαλύτερος από όλους τους αριθμούς $\pi_1, \pi_2, \ldots, \pi_\nu$, άρα διαφορετικός.

Αν ο π δεν είναι πρώτος, από το θεμελιώδες θεώρημα ο π θα διαιρείται από ένα πρώτο αριθμό $2 \leq \theta < \pi$.

Ο πρώτος αριθμός θ είναι διαφορετικός από κάθε $\pi_1, \ldots, \pi_\nu$. Πράγματι αν $\theta = \pi_\kappa$ για $1 \leq \kappa \leq \nu$, τότε ο θ διαιρεί το γινόμενο $\pi_1 \ldots \pi_\nu$ και αφού διαιρεί τον π θα διαιρεί και το 1.

Αυτό είναι άτοπο, διότι $2 \leq \theta$.

Άρα ο π είναι πρώτος και διαφορετικός από τους $\pi_1, \ldots, \pi_\nu$

Άτοπο!

Άρα, οι πρώτοι αριθμοί έχουν άπειρο πλήθος.

Εκτοτε δόθηκαν και διάφορες σύγχρονες και πολύ πρόσφορες αποδείξεις του θεμελιώδους θεωρήματος, όμως η απόδειξη που υπάρχει στα Στοιχεία του Ευκλείδη είναι η πιό σύντομη και ευρηματική.

Θεώρημα Έστω $m \in \mathbb{N}$, $m \geq 2$. Κάθε $n \in \mathbb{N}_0$, γράφεται κατά μοναδικό τρόπο στη μορφή:

$$n = a_0 + a_1 m + a_2 m^2 + \dots + a_k m^k$$

όπου $k \in \mathbb{N}_0$, ώστε $m^k \leq n < m^{k+1}$ και $a_0, a_1, \dots, a_k \in \mathbb{N}_0$ ώστε $0 \leq a_0, a_1, \dots, a_k \leq m-1$ και $a_k \neq 0$, αν $k \neq 0$.

Απόδειξη

Θα χρησιμοποιήσουμε την ισχυρή μορφή της επαγωγής:

(α) Για $n = 0$ έχουμε $n = a_0$, όπου $a_0 = 0$, άρα ισχύει το θεώρημα.

(β) Έστω ότι ισχύει το θεώρημα για $0, 1, \dots, n$. Τότε ισχύει και για $n+1$.

Πράγματι, αν $\boxed{n+1 < m}$ τότε:

$$n+1 = a_0,$$ και ισχύει το θεώρημα

Αν $\boxed{n+1 \geq m}$ τότε:

$$n+1 = q \cdot m + r \quad \text{όπου } q \in \mathbb{N}_0,\ 0 \leq r < m.$$

Επομένως, αφού $n+1 \geq m$, ισχύει ότι:

$$0 < q < q \cdot m \leq n+1 \Rightarrow 0 < q \leq n.$$

και από την επαγωγική υπόθεση

$$q = a_1 + a_2 m + \dots + a_k m^{k-1}$$

για μοναδικούς αριθμούς $a_1, \dots, a_k \in \mathbb{N}_0$ ώστε $0 \leq a_1, \dots, a_k \leq m+1$ και $a_k \neq 0$

Θέτοντας $a_0 = r$ έχουμε:

$$n+1 = a_0 + q \cdot m = a_0 + a_1 m + \dots + a_k m^k.$$

Η αναπαράσταση του $n+1$ είναι μοναδική.

Έστω $n+1 = b_0 + b_1 m + \dots + b_\lambda m^\lambda$, $b_\lambda \neq 0$, $0 \leq b_i \leq m-1$ $i = 1, \dots, \lambda$

Τότε $n+1 = r_1 + m \cdot q_1$ για $\boxed{r_1 = b_0}$ και

$$q_1 = b_1 + \dots + b_\lambda m^{\lambda-1} \in \mathbb{N}_0.$$

Από την μοναδικότητα της διαίρεσης του $n+1$ με το m έχουμε ότι $r_1 = r$, $q_1 = q$.

Άρα, $b_0 = r_1 = r = a_0$ και

αφού $q_1 = q$, από την επαγωγική υπόθεση $k = \lambda$ και $a_i = b_i$ για $i = 1, \dots, k$.