ΜΑΘΗΜΑ 2

ΑΚΕΡΑΙΟΙ - ΡΗΤΟΙ

Υπενθυμίζουμε ότι στο $\mathbb{N}$ ορίζεται μια πράξη (: πρόσθεση) για την οποία ισχύει ο νόμος της διαγραφής:

$$m, n, p \in \mathbb{N} \text{ και } m+p = n+p \Rightarrow m = n.$$

Ωστόσο, η εξίσωση

$$m = x + n$$

δεν λύνεται πάντα (: δεν έχει λύση μέσα στο $\mathbb{N}$). Αν λύνεται, η λύση είναι μοναδική. Επιπλέον είναι λύση και όλων των εξισώσεων

$$(*) \qquad (m+k) = x + (n+k), \quad k \in \mathbb{N}.$$

Δηλ. η λύση όλων των εξισώσεων $(*)$ είναι μία, και προσδιορίζεται πλήρως από το ζεύγος $(m, n) \in \mathbb{N}$.

Πότε αυτή η λύση υπάρχει και πότε δεν υπάρχει; Από τον τρόπο που ορίστηκε η διάταξη $\leq$ των φυσικών, ισχύουν οι ισοδυναμίες

$$\exists\, x \in \mathbb{N} : m = x + n \Leftrightarrow m > n,$$

και

$$\nexists\, x \in \mathbb{N} : m = x + n \Leftrightarrow m \leq n.$$

Επειδή κάθε υπαρκτή λύση $x \in \mathbb{N}$ της $m = n + x$ προσδιορίζεται πλήρως από το ζεύγος (m, n) (ή οποιοδήποτε άλλο $(m+k, n+k)$) με $m > n$, θα προσεγγίσουμε τις λύσεις που δεν υπάρχουν $\in \mathbb{N}$ (: αρνητικοί αριθμοί) μέσω ζευγών (m, n) με $m \leq n$.

Υπενθύμιση.

Υπενθυμίζουμε ότι μια σχέση ισοδυναμίας R σε ένα σύνολο A είναι μια διμελής σχέση $R \subseteq A \times A$ που είναι:

(i) ανακλαστική, δηλ. $\forall x \in A: (x,x) \in R$.

(ii) συμμετρική, δηλ. $(x,y) \in R \Rightarrow (y,x) \in R$.

(iii) μεταβατική, δηλ. $(x,y) \in R \wedge (y,z) \in R \Rightarrow (x,z) \in R$.

Κάθε σχέση ισοδυναμίας διαμερίζει το σύνολο A σε κλάσεις ισοδυναμίας:

$\forall x \in A$, η κλάση ισοδυναμίας του x είναι το σύνολο

$$[x] = \{a \in A : (x,a) \in R\}.$$

Οι κλάσεις ισοδυναμίας έχουν τις παρακάτω ιδιότητες:

(i) κάθε $[x] \neq \emptyset$, αφού $x \in [x]$.

(ii) για δύο κλάσεις $[x]$, $[y]$ ισχύει $[x] = [y]$ ή $[x] \cap [y] = \emptyset$.

(iii) κάθε στοιχείο $a \in A$ ανήκει σε κάποια κλάση (στην $[a]$), άρα $\bigcup_{a \in A} [a] = A$.

Ορίζουμε στο σύνολο $\mathbb{N} \times \mathbb{N}$ την

$$R \subseteq (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N}):$$

ως εξής:

$$((m,n),(p,q)) \in R \iff m+q = n+p.$$

Για ευκολία γράφουμε

$$(m,n) R (p,q), \text{ αντί } ((m,n),(p,q)) \in R$$

Η σχέση R έχει τις ιδιότητες:

(i) ανακλαστική: $(m,n) R (m,n) \iff m+n = n+m$, ισχύει.

(ii) συμμετρική: $(m,n) R (p,q) \Rightarrow m+q = n+p \Rightarrow$

$$\Rightarrow p+n = q+m \Rightarrow (p,q) R (m,n), \text{ ισχύει.}$$

(iii) μεταβατική: $(m,n) R (p,q)$ και $(p,q) R (x,y) \Rightarrow$

$$\Rightarrow m+q = n+p \text{ και } p+y = q+x \overset{(+)}{\Rightarrow}$$

$$\Rightarrow m+q+p+y = n+p+q+x \Rightarrow \text{(νόμος διαγραφής)}$$

$$\Rightarrow m+y = n+x \Rightarrow (m,n) R (x,y), \text{ ισχύει.}$$

Άρα η R είναι σχέση ισοδυναμίας στο $\mathbb{N}\times\mathbb{N}$.

Παρατηρούμε ότι $\forall n \in \mathbb{N}$:

$[(n+1,1)] = [(n+2,2)] = \dots = [(n+k,k)]$, $\forall k \in \mathbb{N}$,

(και, αν ξέραμε τί είναι η αφαίρεση,

$[(n+1,1)] = [(x,y)] \Leftrightarrow (n+1,1)\,R\,(x,y) \Leftrightarrow$

$\Leftrightarrow n+1+y = x+1 \Leftrightarrow$

$\Leftrightarrow x-y = n.$)

Ομοίως, $\forall n \in \mathbb{N}$:

$[(1,n+1)] = [(2,n+2)] = \dots = [(k,n+k)]$, $\forall k \in \mathbb{N}$

(και, αν ξέραμε και τους αρνητικούς αριθμούς,

$[(1,n+1)] = [(x,y)] \Leftrightarrow (1,n+1)\,R\,(x,y) \Leftrightarrow$

$\Leftrightarrow 1+y = x+n+1 \Leftrightarrow$

$\Leftrightarrow -n = x-y$).

$\boxed{\text{ΟΡΣ}}$ Ονομάζουμε σύνολο των ακεραίων αριθμών και συμβολίζουμε με $\mathbb{Z}$ το σύνολο των κλάσεων ισοδυναμίας $[(x,y)]$ ως προς την σχέση R στο $\mathbb{N}\times\mathbb{N}$.

Στο $\mathbb{Z}$ ορίζουμε πρόσθεση και πολ/σμό:

$[(m,n)] + [(p,q)] = [(m+p, n+q)]$.

$[(m,n)]\cdot[(p,q)] = [(mp+nq, mq+np)]$.

Και οι δύο πράξεις είναι καλά ορισμένες, δηλ. δεν εξαρτώνται από τους αντιπροσώπους των θεωρούμενων κλάσεων.

$\boxed{\text{Πρόταση}}$ Η απεικόνιση $f: \mathbb{N} \to \mathbb{Z}: f(n) = [(n+1,1)]$. είναι 1-1.

Απόδ. $f(n) = f(m) \Rightarrow [(n+1,1)] = [(m+1,1)] \Rightarrow$

$\Rightarrow (n+1,1)\,R\,(m+1,1) \Rightarrow (m+1)+1 = (n+1)+1 \Rightarrow$

$\Rightarrow m+2 = n+2 \Rightarrow m = n.$

Η f μας επιτρέπει να ταυτίζουμε το $\mathbb{N}$ με την εικόνα του, δηλ. να θεωρούμε ότι $\mathbb{N} \equiv f(\mathbb{N}) \subseteq \mathbb{Z}$, άρα ταυτίζουμε $n \equiv [(n+1, 1)]$, $\forall n \in \mathbb{N}$.

Θέτουμε

$$-n := [(1, n+1)], \quad \forall n \in \mathbb{N}.$$

$$0 := [(n,n)], \quad n \in \mathbb{N}.$$

Οπότε $\mathbb{Z} = \mathbb{N} \cup \{0\} \cup \{-n : n \in \mathbb{N}\}$.

Οι πράξεις που ορίσαμε στο $\mathbb{Z}$ έχουν τις ιδιότητες που περιγράφονται στην επόμενη

ΠΡΟΤΑΣΗ

Η πρόσθεση του $\mathbb{Z}$ έχει τις ιδιότητες:

(i) Είναι μεταθετική:

$$a+b = b+a, \quad \forall a,b \in \mathbb{Z}.$$

(ii) Είναι προσεταιριστική:

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

(iii) Έχει ουδέτερο στοιχείο, το $0 = [(n,n)]$, $n \in \mathbb{N}$:

$$0+a = a+0 = a, \quad \forall a \in \mathbb{Z}$$

(iv) κάθε $a \in \mathbb{Z}$ έχει αντίθετο, δηλ. υπάρχει ένα στοιχείο που συμβολίζεται με $-a$ και έχει τις ιδιότητες:

$$a+(-a) = (-a)+a = 0.$$

Ο πολλ/σμός του $\mathbb{Z}$ έχει τις ιδιότητες:

(i) Είναι μεταθετικός:

$$a \cdot b = b \cdot a, \quad \forall a,b \in \mathbb{Z}.$$

(ii) Είναι προσεταιριστικός:

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

(iii) Έχει ουδέτερο στοιχείο, το $1 \equiv [(2,1)] = [(n+1, n)]$, $n \in \mathbb{N}$:

$$1 \cdot a = a \cdot 1 = a, \quad \forall a \in \mathbb{Z}.$$

Τέλος, οι δύο πράξεις συνδέονται με την επιμεριστική ιδιότητα:

$$a \cdot (b+c) = ab + ac, \quad \forall a,b,c \in \mathbb{Z}.$$

Σύμφωνα με την αλγεβρική ορολογία $(\mathbb{Z},+)$ είναι (αβελιανή) ομάδα και $(\mathbb{Z},+,\cdot)$ είναι (μοναδιαίος, μεταθετικός) δακτύλιος.

Εκτός των πράξεων, ορίζουμε και διάταξη στο $\mathbb{Z}$.

$\boxed{\text{ΟΡΣ}}$ Ένα $a \in \mathbb{Z}$ λέγεται <u>μη αρνητικό</u>, αν $a = [(m,n)]$ με $m \geq n$. Συμβολίζουμε με $\mathbb{Z}^+$ τους μη αρνητικούς ακέραιους.

Παρατηρούμε ότι η ισότητα $\mathbb{Z} \equiv \mathbb{N} \cup \{0\} \cup \{-n : n \in \mathbb{N}\}$ μας δίνει $\mathbb{Z}^+ \equiv \mathbb{N} \cup \{0\} = \mathbb{N}_0$

$\boxed{\text{ΠΡΟΤΑΣΗ}}$ Το $\mathbb{Z}^+$ έχει τις ακόλουθες ιδιότητες:

(i) $a, b \in \mathbb{Z}^+ \Rightarrow a+b \in \mathbb{Z}$.

(ii) $a, b \in \mathbb{Z}^+ \Rightarrow ab \in \mathbb{Z}$.

(iii) $\forall a \in \mathbb{Z} : a \in \mathbb{Z}^+$ ή $-a \in \mathbb{Z}^+$.

(iv) $a \in \mathbb{Z}^+$ και $-a \in \mathbb{Z}^+ \Rightarrow a = 0$.

Επίσης, όπως γίνεται και στο $(\mathbb{N}, \leq)$, ορίζεται η διάταξη των ακεραίων μέσω της σχέσης:

$$a \leq b \iff \exists\, c \in \mathbb{Z}^+ : a + c = b$$

Αποδεικνύεται ότι η ανωτέρω σχέση είναι <u>ολική διάταξη</u>.

Η διάταξη του $\mathbb{Z}$, όπως και αυτή του $(\mathbb{N}, \leq)$, "σέβεται τις πράξεις":

$\boxed{\text{ΠΡΟΤΑΣΗ}}$

Για την διάταξη $(\mathbb{Z}, \leq)$ ισχύουν:

(1) $a \leq b \Rightarrow a + c \leq b + c \quad \forall\, c \in \mathbb{Z}$.

(2) $0 \leq a \leq b$ και $0 \leq c \leq d \Rightarrow ac \leq bd$.

Όπως στους φυσικούς δεν λύνεται πάντα η εξίσωση $n + x = m$, έτσι και στους ακεραίους, δεν λύνεται πάντα η εξίσωση $ax = b$

Για $a = 0 \Rightarrow ax = 0 \quad \forall x \in \mathbb{Z}$ (για $a \neq 0$, $b = 0$ η $ax = 0 \Rightarrow x = 0$).

ΤΑΥΤΟΤΗΤΑ ΤΗΣ ΔΙΑΙΡΕΣΗΣ

ΟΡΣ $b\in\mathbb{Z}$, $a\in\mathbb{N}$. Λέμε ότι ο a διαιρεί τον b $(a|b)$ αν $\exists\, q\in\mathbb{Z}: b=aq$

ΘΕΩΡΗΜΑ (Ταυτότητα της διαίρεσης)
$\forall b\in\mathbb{Z}, \forall a\in\mathbb{N}, \quad \exists! (q,r)\in\mathbb{Z}\times\mathbb{N}_0:$
$b=aq+r$ με $0\leq r<a$.

Απόδ. Παρατηρώ ότι $\forall s\in\mathbb{Z}: b-as\in\mathbb{Z}$. Παίρνω
$A:=\{b-sa : s\in\mathbb{Z}\}\cap\mathbb{N}\subseteq\mathbb{N}$
Τότε $A\neq\emptyset$: αν $b\geq 0$ για $s=0\Rightarrow b-sa=b-0=b\geq 0$

αν $b<0$ για $s=b\Rightarrow b-ba=\underset{<0}{b}\underbrace{(1-a)}_{\leq 0}\geq 0$.

Άρα το A έχει ελάχιστο r.

Θδο $0\leq r<a$. Είναι $r\geq 0$ από ορσ. του A.
Άρα πρέπει νδο $r<a$. Αν $r\geq a\Rightarrow$

$r=b-aq\geq a\Rightarrow r-a=b-aq-a\geq 0\Rightarrow$

$$\left.\begin{array}{l}\Rightarrow \underbrace{r-a}_{\geq 0}=b-(q+1)a\in A, \quad \text{και} \\ \qquad\qquad r-a<r\end{array}\right\}\Rightarrow r=\text{όχι ελάχιστο, άτοπο.}$$

Το ζεύγος είναι μοναδικό: αν $(q_1,r_1)\neq(q_2,r_2)$ τέτοια ζεύγη, τότε

$q_1>q_2 \iff aq_1>aq_2 \iff b-aq_1<b-aq_2 \iff r_1<r_2$.

όμως:

$$\left.\begin{array}{l}a>r_1\geq 0 \\ a>r_2\geq 0\end{array}\right\}\Rightarrow \left.\begin{array}{l}0\geq -r_1>-a \\ a>r_2\geq 0\end{array}\right\}\overset{(+)}{\Rightarrow} r_2-r_1<a$$

$a>r_2-r_1=b-aq_2-b+aq_1=a\underbrace{(q_1-q_2)}_{\geq 1}\geq a$, άτοπο.

Λέμε ότι ο $a \in \mathbb{Z} \setminus \{0\}$ διαιρεί τον $b \in \mathbb{Z}$, αν $\exists x \in \mathbb{Z}$:

$$ax = b \quad (*)$$

δηλ. αν λύνεται η ανωτέρω εξίσωση.
Όπως και η εξίσωση

$$m + x = n$$

δεν λύνεται πάντα στο $\mathbb{N}$, έτσι και η (*) δεν λύνεται πάντα στο $\mathbb{Z}$: αν στην ταυτότητα της διαίρεσης

$$b = aq + r$$

είναι $r = 0$, τότε η (*) λύνεται, με $x = q$; αν $r \neq 0$, η (*) δεν λύνεται στο $\mathbb{Z}$.

Για να φτιάξουμε ένα αριθμοσύνολο, όπου όλες οι εξισώσεις της μορφής (*), με $a \neq 0$, να έχουν λύση, εργαζόμαστε όπως στην κατασκευή του $\mathbb{Z}$ από το $\mathbb{N}$:

Στο σύνολο $\mathbb{Z} \times \mathbb{N}$ ορίζουμε την σχέση

$$Q \subseteq (\mathbb{Z} \times \mathbb{N}) \times (\mathbb{Z} \times \mathbb{N})$$

ως εξής:

$$((a,m),(b,n)) \in P \overset{\text{συμβ.}}{\iff} (a,m)\,Q\,(b,n) \iff$$

$$\iff an = bm$$

(Παρατηρείστε ότι, για όποιον ήδη γνωρίζει τί είναι τα κλάσματα, η τελευταία ισότητα σημαίνει $a/m = b/n$).

Αποδεικνύεται ότι η Q είναι σχέση ισοδυναμίας.
Για κάθε κλάση ισοδυναμίας $[(a,m)]$ χρησιμοποιούμε το σύμβολο

$$\frac{a}{m} := [(a,m)]$$

Ονομάζουμε σύνολο των ρητών αριθμών το σύνολο

$$\mathbb{Q} = \left\{ \frac{a}{m} = [(a,m)] : a \in \mathbb{Z},\ m \in \mathbb{N} \right\}$$

των ανωτέρω κλάσεων ισοδυναμίας.

Στο σύνολο $\mathbb{Q}$ ορίζονται οι πράξεις

$$[(a,m)] + [(b,n)] = [(an+bm,\ mn)]$$

και

$$[(a,m)]\cdot[(b,n)] = [(ab,\ mn)]$$

(που αντιστοιχούν στις ιδιότητες

$$\frac{a}{m}+\frac{b}{n} = \frac{an+bm}{mn} \quad \text{και} \quad \frac{a}{m}\cdot\frac{b}{n} = \frac{ab}{mn}).$$

Οι ιδιότητες των πράξεων περιγράφονται στην επόμενη

$\boxed{\text{ΠΡΟΤΑΣΗ}}$ Η πρόσθεση του $\mathbb{Q}$ έχει τις ιδιότητες:

(A1) Είναι μεταθετική, δηλ.

$$p+q = q+p, \quad \forall\, p,q \in \mathbb{Q}.$$

(A2) Είναι προσεταιριστική, δηλ.

$$(p+q)+r = p+(q+r), \quad \forall\, p,q,r \in \mathbb{Q}.$$

(A3) Έχει ουδέτερο στοιχείο, το $0 = 0/1 = [(0,1)] \in \mathbb{Q}$:

$$\forall\, q \in \mathbb{Q}:\ q+0 = 0+q = q.$$

(A4) Κάθε $q \in \mathbb{Q}$ έχει αντίθετο, δηλ. υπάρχει $-q \in \mathbb{Q}$:

$$q+(-q) = (-q)+q = 0.$$

Ο πολ/σμός του $\mathbb{Q}$ έχει τις ιδιότητες:

(M1) Είναι μεταθετικός, δηλ.

$$p\cdot q = q\cdot p, \quad \forall\, p,q \in \mathbb{Q}.$$

(M2) Είναι προσεταιριστικός, δηλ.

$$p\cdot(q\cdot r) = (p\cdot q)\cdot r, \quad \forall\, p,q,r \in \mathbb{Q}.$$

(M3) Έχει ουδέτερο στοιχείο, το $1 = 1/1 = [(1,1)] \in \mathbb{Q}$:

$$1\cdot q = q\cdot 1 = q, \quad \forall\, q \in \mathbb{Q}.$$

(M4) Κάθε μη-μηδενικό $q \in \mathbb{Q}\setminus\{0\}$ έχει αντίστροφο:

$$\exists\, q^{-1} \in \mathbb{Q}:\ q\cdot q^{-1} = q^{-1}\cdot q = 1.$$

Οι δύο πράξεις συνδέονται με την επιμεριστική ιδιότητα:

(E) $p(q+r) = pq+pr, \quad \forall\, p,q,r \in \mathbb{Q}.$

Σύμφωνα με την αλγεβρική ορολογία οι ιδιότητες (A1-4), (M1-4) και (E) κάνουν το $(\mathbb{Q},+,\cdot)$ <u>σώμα</u>.

Το σώμα των ρητών διατάσσεται ολικά μέσω της σχέσης

$$[(a,m)] \geq [(b,n)] \iff an-bm \geq 0$$

(που αντιστοιχεί στην γνωστή μας σχέση

$$\frac{a}{m} \geq \frac{b}{n} \iff \frac{a}{m}-\frac{b}{n} = \frac{an-bm}{m\cdot n} \geq 0.)$$

ΠΡΟΤΑΣΗ. Η ολική διάταξη του $\mathbb{Q}$ έχει τις επόμενες ιδιότητες:

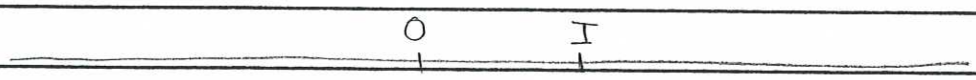
(i) Είναι τριχοτομία, δηλ. $\forall\, p,q \in \mathbb{Q}$ ισχύει ακριβώς μία από τις
$p<q$ ή $p=q$ ή $p>q$.

(ii) $p \leq q \Rightarrow p+r \leq q+r$, $\quad p,q,r \in \mathbb{Q}$.

(iii) $p \leq q$ και $r>0 \Rightarrow pr \leq qr$, $\quad p,q,r \in \mathbb{Q}$.

(iv) $1>0$.

Παράσταση των ρητών σε ευθεία: Επιλέγουμε τυχαία μία ευθεία ε, και δύο σημεία της ε, τα $O \neq I$. Χρησιμοποιώντας σαν



μονάδα μέτρησης το μήκος του ευθυγράμμου τμήματος OI, αντιστοιχίζουμε κάθε $q \in \mathbb{Q}$ σε ένα μονοσήμαντα ορισμένο σημείο της ευθείας: $p<q \Rightarrow P$ βρίσκεται αριστερά του Q.

Αξίζει ακόμη να παρατηρήσουμε ότι, όπως μπορούμε να θεωρούμε $\mathbb{N} \subseteq \mathbb{Z}$, έτσι μπορούμε να θεωρούμε $\mathbb{Z} \subseteq \mathbb{Q}$:

ΠΡΟΤΑΣΗ. Η απεικόνιση

$$g: \mathbb{Z} \to \mathbb{Q} : a \mapsto g(a) := [(a,1)] = a/1.$$

είναι 1-1 και διατηρεί τις πράξεις και την διάταξη του $\mathbb{Z}$, δηλ: $\forall\, a,b \in \mathbb{Z}$:

(i) $g(a+b) = g(a)+g(b)$

(ii) $g(ab) = g(a)\cdot g(b)$

(iii) $a \leq b \Rightarrow g(a) \leq g(b)$.

Με την κατασκευή του $\mathbb{Q}$ έχουμε ένα ολικά διατεταγμένο σώμα, στο οποίο (επομένως) λύνονται όλες οι εξισώσεις

$$p+x=q,$$
$$px=q, \quad \text{για } p\neq 0.$$

ΟΜΩΣ: (1) Στην αναπαράσταση των ρητών σε ευθεία (ε), κάθε ρητός αντιστοιχεί σε σημείο της ευθείας, αλλά όχι το αντίστροφο.

(2) Δεν λύνονται όλες οι εξισώσεις της μορφής

$$x^2=q, \quad q\in\mathbb{Q}$$

Το (1) απορρέει από το (2). Θδ το (2):

Λήμμα Κάθε $q\in\mathbb{Q}$ γράφεται με ανάγωγη μορφή, δηλ. $\exists\, (b,n)\in[(a,m)]=q$: ο μόνος κοινός φυσικός διαιρέτης των b και n είναι το 1.

Αποδ. Έστω $q\in\mathbb{Q}$. Θεωρούμε το σύνολο

$$E(q)=\{n\in\mathbb{N} : \exists\, b\in\mathbb{Z} \text{ με } b/n=[(b,n)]=q\}.$$

Τότε: $E(q)\subseteq\mathbb{N}$. Επίσης $E(q)\neq\emptyset$,

$$q=[(a,m)] \Rightarrow m\in E(q).$$

Από την Αρχή Ελαχίστου, $\exists$ ελάχιστο $n_0\in E(q)$, που συμμετέχει σε ένα $(b,n_0)\in[(a,m)]=q$.

Αν $\exists$ φυσικός $p>1$ με $p|b$ και $p|n_0$, τότε
$\exists\, b_1, n_1\in\mathbb{Z}$: $b=pb_1$, $n_0=pn_1 \Rightarrow$
$\Rightarrow [(b,n_0)]=[(pb_1,pn_1)]=[(b_1,n_1)]=q \Rightarrow$

$$\left(q=\frac{a}{m}=\frac{b}{n_0}=\frac{pb_1}{pn_1}=\frac{b_1}{n_1}\right)$$

$\Rightarrow n_1\in E(q)$ με $n_1<n_0$, άτοπο. ∎

ΘΕΩΡ. $\nexists\, q\in\mathbb{Q}$: $q^2=2$.

Αποδ. Έστω $q \in \mathbb{Q}$ με $q^2 = 2$. Επειδή $q^2 = (-q)^2$, μπορούμε να θεωρούμε $q > 0$. Γράφουμε το q σε ανάγωγη μορφή $q = \frac{m}{n}$ με $m, n \in \mathbb{N}$. Τότε

$$q^2 = 2 \Rightarrow \frac{m^2}{n^2} = 2 \Rightarrow m^2 \overset{(*)}{=} 2n^2 \Rightarrow$$

$$\Rightarrow 2 \mid 2n^2 = m^2$$

Ισχυριζόμαστε ότι $2 \mid m^2 \Rightarrow 2 \mid m$.

Πράγματι, από την ταυτότητα της διαίρεσης, $m = 2p + r$ με $r = 0$ ή $r = 1$. Για $r = 1 \Rightarrow m = 2p + 1 \Rightarrow$ $\Rightarrow m^2 = 4p^2 + 4p + 1 = 2(2p^2 + 2p) + 1$ <u>δεν</u> διαιρείται με τον 2, άτοπο. Άρα $r = 0$ και $m = 2p$. Οπότε η $(*)$ γίνεται

$$(2p)^2 = 2n^2 \Rightarrow 2p^2 = n^2$$

και επαναλαμβάνοντας τους ίδιους συλλογισμούς, παίρνουμε $n = 2s$, $s \in \mathbb{N}$. Άρα το κλάσμα

$$\frac{m}{n} = \frac{2p}{2s}$$

δεν είναι ανάγωγο, άτοπο. ■

ΑΣΚΗΣΕΙΣ

(1) Νδο στο $(\mathbb{N},+)$ ισχύει ο νόμος της διαγραφής:
$$m+n=m+p \Rightarrow n=p.$$

(2) Θεωρείστε την σχέση ισοδυναμίας R στο $\mathbb{N}\times\mathbb{N}$:
$$(m,n)\,R\,(p,q) \Leftrightarrow m+q=n+p$$
Να βρείτε τα στοιχεία των κλάσεων $[(3,1)]$, $[(2,2)]$ και $[(1,4)]$.

(3) Νδο η πρόσθεση που ορίζεται στο $\mathbb{Z}$ μέσω της
$$[(m,n)]+[(p,q)]=[(m+p,\,n+q)]$$
είναι καλά ορισμένη. Δηλ. νδο αν $[(m,n)]=[(m',n')]$ και $[(p,q)]=[(p',q')]$, τότε
$$[(m+p,\,n+q)]=[(m'+p',\,n'+q')].$$
Ομοίως για τον πολ/σμό
$$[(m,n)]\cdot[(p,q)]=[(mp+nq,\,mq+np)].$$

(4) Νδο η κλάση $[(n,n)]\in\mathbb{Z}$, $n\in\mathbb{N}$, είναι ουδέτερο στοιχείο (μηδεν) της πρόσθεσης του $\mathbb{Z}$, και ότι κάθε $[(m,n)]\in\mathbb{Z}$ έχει αντίθετο την κλάση $[(n,m)]$.

(5) Νδο ο πολ/σμός του $\mathbb{Z}$ έχει ουδέτερο στοιχείο το $[(n+1,n)]$, $n\in\mathbb{N}$, και ότι οι κλάσεις $[(n,n)]$ και $[(n+2,n)]$, $n\in\mathbb{N}$, δεν έχουν αντίστροφο.

(6) Νδο η πρόσθεση και ο πολ/σμός του $\mathbb{Z}$ ικανοποιούν την επιμεριστική ιδιότητα.