ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ

Τα Μαθηματικά σαν επιστήμη ξεκίνησαν όταν κάποιοι (κατά πιθανότατα αρχαίοι Έλληνες) απέδειξαν προτάσεις οι οποίες αναφέρονται χωρίς να χρησιμοποιούν τα αντικείμενα. (πχ 1+1=2, οχι Μαθ. αλλά υπάρχουν άπειροι πρωτοι αριθμοι, ναι Μαθ.)

ΟΡΙΣΜΟΣ (ΠΡΟΤΑΣΗΣ)

Δήλωση είναι μια γραμματική πρόταση για την οποία γνωρίζαμε εαν αποκλειστικά είναι αληθής ή ψευδής.

πχ

$2+2=4$ ΝΑΙ

Τι ωραία μέρα ΟΧΙ

Αυτός είναι φοιτητής (εξαρτάται από τη μεταβλητή).

ΟΡΙΣΜΟΣ (ΜΑΘΗΜΑΤΙΚΗΣ ΠΡΟΤΑΣΗΣ)

Μια μαθηματική πρόταση είναι μια γραμματική πρόταση η οποία εξαρτάται από ένα πεπερασμένο σύνολο μεταβλητών και η αλήθεια εξαρτάται από τις ακριβείς τιμές των μεταβλητών.

πχ.

$D=\{1,2,3\}$ και $x^2 \geq x$, $x \in D$ ΑΛΗΘΗΣ

και

$D'=\{\frac{1}{2},1,2,3\}$ και $x^2 \geq x$, $x \in D'$ ΨΕΥΔΗΣ

Συχνά λάθη (ΑΠΟΔΕΙΞΕΩΝ)

Ενεργήσαμε το θεώρημα ή τη μαθηματική πρόταση που θέλαμε να δείξουμε όσο το δυνατόν πιο κατανοητά, δίχως ασάφειες.

1) Εαν έχουμε μεταβλητές στην πρόταση θα τις καθορίσουμε από την αρχή μαζί με τα σύνολα που λαμβάνουν τιμές

(2)

π.χ

ο m είναι ακέραιος

2) Αν μια μεταβλητή έχει ή απειτωσε (κατά τη διάρκεια της απόδειξης) επιπλέον ιδιότητες, αυτές θα τις δηλώσουμε.

π.χ

ο m είναι άρτιος : $m = 2k$, $k \in \mathbb{Z}$

3) Χρησιμοποιούμε παραδείγματα για να καταναόσουμε τις εννοιες μου όχι για απόδειξη. Πιθανόν τα παραδείγματα να μας βοηθούσαν στην αντίληψη μου των ιδέα της απόδειξης.

4) Δεν χρησιμοποιούμε το ίδιο γράμμα για διαφορετικές έννοιες ή μεταβλητές

π.χ

Έστω m & n περιττοί:

$m = 2k+1 \neq n = 2\lambda + 1$ (και όχι $n = 2k+1$ διοτι προκύπτει ισότητα μεταξύ των n & m)

5) Δεν παιδάμε λογικά βήματα κατά τη διάρκεια της απόδειξης

Παράδειγμα

Το γινόμενο περιττών είναι περιττός:

Λύση

Έστω m και n περιττοί

$m = 2k+1$ και $n = 2\lambda + 1$, $k, \lambda \in \mathbb{Z}$

Θέλουμε $m \cdot n$ περιττός $\Leftrightarrow m \cdot n = 2v + 1$ $v \in \mathbb{Z}$

$m \cdot n = (2k+1)(2\lambda+1) = 2 \cdot (2k\lambda + k + \lambda) + 1 = 2 \cdot v + 1$

όπου $v = 2k\lambda + k + \lambda$, $v \in \mathbb{Z}$ ΑΛΗΘΗΣ.

ΠΡΟΣΟΧΗ με το "εαν" Να μην το μπερδεύουμε με το "επειδή" ή το "διοτι"

π.χ

Έστω m πρώτος. Αν m πρώτος τότε... (όχι επειδή λάθος)

ΑΝΤΙΠΑΡΑΔΕΙΓΜΑ:

Το αντιπαράδειγμα το χρησιμοποιούμε όταν θέλουμε να αποδείξουμε ότι μια πρόταση είναι ψευδής

Παρατήρηση: Η απόδειξη που θα πιάσουμε, θα πρέπει να στηρίζεται σε μαθηματικές προτάσεις οι οποίες δεν θα αφήνουν καμία αοριστία

Ικανή συνθήκη ή Συνεπαγωγή ($\Rightarrow$):

Π.χ

1) Αν το 12 διαιρείται από το 6, τότε διαιρείται και από το 3.

ΛΥΣΗ

Εφόσον 12 διαιρείται από το 6 τότε $12 = 2 \cdot 6$

Άλλα,

$12 = 2 \cdot 6 = 2 \cdot 2 \cdot 3 = 4 \cdot 3 \Rightarrow$ Το 12 διαιρείται από το 3.

2) Ο Αλέξης έχει μεγάλη βαλίτσα $\not\Rightarrow$ έχει πολλά ρούχα

3) i) Αν σήμερα είναι Πάσχα, τότε αύριο είναι Δευτέρα (Έτσι μέσω της αντιθετοαντιστροφής)

Εαν σήμερα **όχι** Δευτέρα τότε χθες δεν ήταν Πάσχα και ο συμβολισμός είναι ως εξής:

$(p \Rightarrow q) \Leftrightarrow (\sim p \Rightarrow \sim q)$.

ii) (Ο Αλέξης δεν χρειάζεται μικρή βαλίτσα $\Rightarrow$ ο Αλέξης δεν έχει λίγα ρούχα) $\Leftrightarrow$ (ο Αλέξης έχει λίγα ρούχα $\Rightarrow$ $\Rightarrow$ ο Αλέξης χρειάζεται μικρή βαλίτσα)

ΟΡΙΣΜΟΣ ΣΥΝΟΛΩΝ:

$\mathbb{N} = \{0, 1, 2, \ldots\}$ φυσικοί αριθμοί

$\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$ Ακέραιοι αριθμοί

$\mathbb{Q} = \left\{ \frac{p}{q} : p, q \in \mathbb{Z} \text{ και } q \neq 0 \right\}$ ρητοί αριθμοί

- Η πρόσθεση και ο πολ/μος είναι καλά ορισμένες πράξεις στο $\mathbb{N}$. Δηλ. άθροισμα φυσικών (ή γινόμενο φυσικών) δίνει πάντα φυσικό
- Η αφαίρεση δεν είναι καλά ορισμένη στο $\mathbb{N}$ διότι $1-2=-1 \notin \mathbb{N}$
- Η διαίρεση δεν είναι καλά ορισμένη στο $\mathbb{N}$ διότι $1:2 = \frac{1}{2} \notin \mathbb{N}$.

Εάν, θέλαμε την πράξη της αφαίρεσης στο $\mathbb{N}$, θα πρέπει να επεκτείναμε το $\mathbb{N}$ (προσθέτοντας στοιχεία) οπότε καταλήγουμε στο $\mathbb{Z}$

Εάν, θέλουμε την πράξη της διαίρεσης στο $\mathbb{N}$ και κατά συνέπεια στο $\mathbb{Z}$, πρέπει να επεκτείνουμε το $\mathbb{Z}$ οπότε καταλήγουμε στο $\mathbb{Q}$

Ταυτότητες που θα χρησιμοποιούμε κατά κόρον

$$a^n - \beta^n = (a-\beta)\cdot(a^{n-1} + a^{n-2}\cdot\beta + \ldots + a\cdot\beta^{n-2} + \beta^{n-1})$$

$$a^n + \beta^n = (a+\beta)\cdot(a^{n-1} - a^{n-2}\cdot\beta + \ldots + (-1)^i\cdot a^{n-1-i}\cdot\beta^i + \ldots$$

$$\ldots + (-1)^{n-1}\cdot \cancel{a^{n-1-(n-1)}}_{1}\cdot\beta^{n-1}$$

• ΔΙΑΙΡΕΤΟΤΗΤΑ •

ΙΔΙΟΤΗΤΕΣ:

1) Αν n και d είναι ακέραιοι με $d \neq 0$, τότε ο n διαιρείται από τον $d \Leftrightarrow n = k \cdot d$ $(\forall k \in \mathbb{Z})$.
Γράφουμε ότι $d \mid n$ (d διαιρεί τον n)
[και γράφουμε $d \nmid n$ (d δεν διαιρεί τον n)]

2) Ο n διαιρείται από το $d \Leftrightarrow$ ο n είναι πολ/σιο του $d \Leftrightarrow$
$\Leftrightarrow$ ο d διαιρεί τον n

Πχ

1) Κάθε μη μηδενικός ακέραιος διαιρεί το 0
2) Διαιρέτες του 1 : ± 1
3) Αν $a \mid b \Rightarrow |a| \leq |b|$
4) $d \nmid n \Rightarrow \frac{n}{d} \notin \mathbb{Z}$

ΟΡΙΣΜΟΣ: Ο $n > 1$ καλείται πρώτος αν-ν οι μόνοι φυσικοί διαιρέτες του είναι το 1 και ο εαυτός του.

Πχ

2, 3, 5, 7, 11, 13, 17, 19, 23

ΟΡΙΣΜΟΣ:

Ο n καλείται σύνθετος, αν υπάρχουν ακέραιοι και m διαφορετικοί από 0 και ± 1, ώστε $n = k \cdot m$

Πχ

$6 = 2 \cdot 3$ & $12 = 3 \cdot 4$

ΘΕΩΡΗΜΑ

Κάθε αριθμός φυσικός $n>1$ διαιρείται από έναν πρώτο

ΙΔΙΟΤΗΤΕΣ

1) Αν $a|b$ και $b|a$, τότε $|a|=|b|$
2) Αν $n=4k+1$, τότε $8|n^2-1$
   Αν $n=4k+3$, τότε $8|n^2-1$
3) Αν $a|b$ και $a|c$, τότε $a|b\pm c$
4) Αν $a|b$, τότε $a|b\cdot c$
5) Αν $a|b \not\Rightarrow a\cdot c|b$ ($6|12 \not\Rightarrow 6\cdot 3|12$)
6) Αν $a|b+c \not\Rightarrow a|b$ και $a|c$ ($5|2+3$ αλλά $5\nmid 2$ και $5\nmid 3$)
7) Αν $a|b\cdot c \not\Rightarrow a|b$ ή $a|c$ ($6|2\cdot 3 \not\Rightarrow 6|2$ ή $6|3$)

Πότε ισχύει το (7);

Ισχύει εάν $a=$ πρώτος, τότε $a|bc \Rightarrow a|b$ ή $a|c$

8) Αν $a|b \Rightarrow a^2|b^2$

ΑΠΟΔΕΙΞΗ

1) $$\left.\begin{array}{l} \text{Εαν } a|b \iff (\exists k\in\mathbb{Z}): b=a\cdot k \\ \text{Εαν } b|a \iff (\exists \lambda\in\mathbb{Z}): a=b\cdot\lambda \end{array}\right\} \Rightarrow$$

$$\Rightarrow a=b\cdot\lambda=a k\lambda \Rightarrow a-ak\lambda=0 \Rightarrow a=0 \text{ ή } k\lambda=1$$

(Αδύνατον αφού $b|a$)

Αφού, $k,\lambda\in\mathbb{Z}$ τότε $k=\lambda=1$ ή $k=\lambda=-1$

Αλλά, τότε $a=b$ ή $|a|=|b|$

2) Αν $n=4k+1 \Rightarrow 8|n^2-1$

Αλλά, $8|n^2-1 \iff (\exists\lambda\in\mathbb{N}): n^2-1=8\lambda \Rightarrow$

$$\Rightarrow (4k+1)^2-1=(4k+2)\cdot 4k=16k^2+8k=$$
$$=8\underbrace{(2k+1)\cdot k}_{\lambda\in\mathbb{N}}$$

3) Αν $a|b$ και $a|c \Rightarrow a|b \pm c$

$a|b \Rightarrow (\exists k): b = ak$

$a|c \Rightarrow (\exists \lambda): c = a\lambda$

$a|b \pm c$ $\begin{cases} \rightarrow (\exists \mu): b+c = a\cdot\mu \\ \rightarrow (\exists \nu): b-c = a\cdot\nu \end{cases}$

Άρα, $b = ak \Rightarrow b \pm c = ak \pm a\lambda \Rightarrow b \pm c = a(k \pm \lambda)$

- Ισχυρισμοί (Conjectures)

Ισχυρισμός είναι μια πρόταση για την οποία έχουμε πληροφορίες ότι είναι αληθής αλλά δεν μπορούμε να την αποδείξουμε.

Πχ

$2 = 1+1$, $4 = 1+3$, $6 = 1+5$, $8 = 1+7$, $10 = 3+7$, $12 = 5+7$.

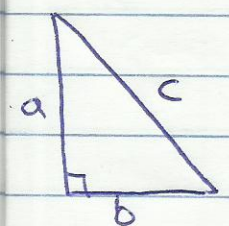
Το παράδειγμα αυτό το παρατήρησε ο Goldbach (1690-1764)

Δηλαδή, κάθε άρτιος μπορεί να γραφεί ως άθροισμα πρώτων και 2. (Έχουν εξεταστεί όλες οι περιπτώσεις που να μπορούσες χπο 1.000.000.000.000.000.000).

- Η ΕΙΚΑΣΙΑ ΤΟΥ FERMAT (1650)

(Αποδείχθηκε το 2000).

ΠΥΘΑΓΟΡΕΙΟ ΘΕΩΡΗΜΑ



$c^2 = a^2 + b^2$ $\left(c^2 = 1^2 + 1^2 \right.$ $\left. 5^2 = 4^2 + 3^2\right)$, $c^3 = a^3 + b^3$ υπάρχουν φυσικοί αριθμοί c, a, b ώστε να ισχύει;

Και γενικότερα: $c^k = a^k + b^k$, $k \in \mathbb{N}$, $k \geq 2$

ΘΕΩΡΗΜΑ FERMAT

Αν ο n φυσικός και >2, $\nexists$ φυσικοί a,b,c ώστε $a^n+b^n=c^n$.

Για $n=2$ είναι το Π.Θ

(Πριν την απόδειξη εξετάστηκαν $n<200.000$).

ΑΣΚΗΣΗ

Είναι ο αριθμός 2^9-1 πρώτος για ρ πρώτος;

ΕΦΑΡΜΟΓΗ

Ένας φυσικός n διαιρείται από το $3(\nmid 9)$, εάν το αθροίσμα των ψηφίων του διαιρείται από το $3(\nmid 9)$.

Έστω ότι n γράφεται

$n=a_k\cdot a_{k-1}\dots a_1\cdot a_0$, $1\le a_k\le 9$ και $0\le a_i\le 9$, $i=0,\dots,k-1$

Πχ

- $n=10397050$
- $n=111=1\cdot10^2+1\cdot10^1+1\cdot10^0$

$n=a_k\cdot a_{k-1}\dots a_1\cdot a_0=a_k\cdot10^k+a_{k-1}\cdot10^{k-1}+\dots+a_1\cdot10^1+a_0\cdot10^0$

Γνωρίζουμε $a_k+a_{k-1}+\dots+a_0$ διαιρείται από το 3

Αν ο n διαιρείται από το 3 και το $a_k+\dots+a_0$ διαιρείται από το 3 $\Rightarrow$ Τότε $3-(a_k+a_{k-1}+\dots+a_0)=$

$=a_k\cdot10^k+a_{k-1}\cdot10^{k-1}+\dots+a_1\cdot10+a_0-a_k-a_{k-1}-\dots-a_1-a_0$

όπου

$a_k\cdot10^k-a_k=a_k(10^k-1)=a_k(10^k-1^k)=$

$=a_k\cdot(10-1)(10^{k-1}+10^{k-2}\cdot1+\dots+10^1\cdot1^{k-2}+10^0\cdot1^{k-1})=$

$=a_k\cdot9\cdot(10^{k-1}+10^{k-2}+\dots+10+1)=\dots$