

12/02/15 (Βασικό Βιβλίο "Δ. ΠΟΥΛΑΚΗ : Μαθηματικά Θεωρ. Αα")

- Εισαγωγή

Κεφ. 1 : Διαμερώσιμα Ακέραια

Κεφ. 2 : Αριθμητικές Συναρτήσεις.

Κεφ. 3 : Ισοτιμίες κ' Συναρτήσεις Γραμμικών Ισοτιμιών.

Κεφ. 4 : Αρχικές Ρίζες κ' Δείκτες

Κεφ. 5 : Τετραγωνικά Υπόλοιπα

Κεφ. 6 : Εφαρμογές Φυσικών Αριθμών στην Κρυπτογραφία.



Είναι η Θ. Αριθμών;

- Η μελέτη του συνόλου των φυσικών αριθμών κ' κάποιων εφαρμογών του.

$$\mathbb{N} = \{1, 2, 3, 4, \dots\}$$

$$\mathbb{N}_0 = \{0, 1, 2, \dots\} = \mathbb{N} \cup \{0\}$$

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\} = \mathbb{N} \cup \{0\} \cup (-\mathbb{N})$$

$$\mathbb{Z}^+ = \mathbb{N}$$

$$\mathbb{Q} = \left\{ \frac{a}{b}, a, b \in \mathbb{Z}, b \neq 0 \right\}$$

$\mathbb{R}$ = πραγματικοί αριθμοί

$\mathbb{C}$ = μιγαδικοί αριθμοί

Είναι: $\mathbb{N} \subseteq \mathbb{N}_0 \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

↗ μελέτη με βάση τη διαμερώσιμη ακέραιων.

ΚΛΑΔΟΙ ΘΕΩΡΙΑΣ ΑΡΙΘΜΩΝ

1) Στοιχειώδης Θεωρία Αριθμών (Μαθηματικά)

2) Αναλυτική Θεωρία Αριθμών

3) Αλγεβρική Θ.Α.

4) Διοφαντική Ανάλυση

5) Αριθμητική Μηθεωρητική Γεωμετρία

6) Υπολογιστική Θ.Α.

7) Προβλεπτική Θ.Α.

8) Πιθανοθεωρητική Θ.Α.



Μελέτη του συνόλου $N = \{1, 2, \dots\}$

Κατηγορίες αριθμών:

- Περικτικοί : $1, 3, 5, 7, 9, 11, \dots : 2k+1, k \in \mathbb{N}_0$

- Άρτιοι : $2, 4, 6, 8, 10, \dots : 2k, k \in \mathbb{N}$

- Τετραγωνικοί : $1, 4, 9, 16, 25, \dots : k^2, k \in \mathbb{N}$

- Κυβικοί Αριθμοί : $1, 8, 27, 64, \dots : k^3, k \in \mathbb{N}$

- Τριγωνικοί Αριθμοί:
 $\begin{matrix} & & \circ & & \circ \circ & & \circ \circ \circ & & \circ \circ \circ \circ & & \circ \circ \circ \circ \circ \\ & 1 & & 3 & & 6 & & 10 & & 15 & \dots \end{matrix}$

Ο k -τριγωνικός αριθμός $1 + 2 + \dots + k = \frac{k(k+1)}{2}$

❗ - Πρώτοι αριθμοί: οι μόνοι διαιρέτες τους είναι το 1 κ'ο εαυτός τους!! ΔΕΝ ΥΠΑΡΧΕΙ ΤΥΠΟΣ ΠΟΥ ΝΑ ΠΕΡΙΓΡΑΦΕΙ ΟΛΟΤΕ ΤΟΥΣ ΠΡΩΤΟΥΣ

(2, 3, 5, 7, 11, 13, 17, 19, 23, 29, ...) ΑΡΙΘΜΟΥΣ!

- Σύνθετοι αριθμοί: Οι αριθμοί που δεν είναι πρώτοι: ~~4, 6, 8, 9, ...~~
 $4, 6, 8, 9, \dots$

- Τέλειοι αριθμοί: 6, 28, 496, ... (όλοι οι γνωστοί τέλειοι αριθμοί είναι άρτιοι κ'είναι (ήπειρα) σε πλήθος, δεν είναι

66 έχουμε $\frac{1}{2}$ τους πρώτους γνωστό αν υπάρχει περριός τέλειος αριθμός, αν υπάρχει αριθμούς Mersenne θα πρέπει να είναι $> 10^{1500}$).

• μεγαλύτερος άρτιος έχει περίπου 34.000.000 ψηφία.

- Αριθμοί Fibonacci : 1, 1, 2, 3, 5, 8, 13, 21, ...

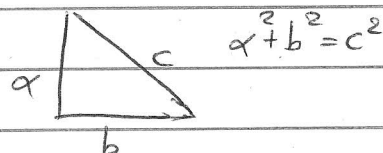
Αν f_n ο n -οστός αριθμός Fibonacci, τότε:

$$f_n = f_{n-1} + f_{n-2}, n > 3.$$

ΤΥΠΙΚΑ ΠΡΟΒΛΗΜΑΤΑ Θ.Α.

∃ θετικοί ακέραιοι a, b, c : $a^2 + b^2 = c^2$.

(Βαβυλώνιοι ~ 1600 π.χ.).



Αν υπάρχουν τέτοιοι αριθμοί

τότε καλούνται πυθαγόρειες τριάδες

π.χ.

$$(3, 4, 5) : 3^2 + 4^2 = 5^2$$

$$(5, 12, 13) : 5^2 + 12^2 = 13^2$$

$$(8, 15, 17) : 8^2 + 15^2 = 17^2$$

∴ (υπάρχουν άπειρα πυθ. τριάδες)

Είναι το πλήθος των πυθ. τριάδων άπειρο;

- αν (a, b, c) : πυθαγόρεια τριάδα, τότε $\forall d \in \mathbb{N}$:

(da, db, dc) : πυθαγόρεια τριάδα

διότι

$$\rightarrow a^2 + b^2 = c^2 \text{ τότε } (da)^2 + (db)^2 = d^2 a^2 + d^2 b^2 = d^2 (a^2 + b^2) = d^2 c^2 = (dc)^2 \Rightarrow (da, db, dc) : \text{πυθ. τριάδα}$$

βι επιπλέον d αυθαίρετο $\Rightarrow$ ∃ άπειρες πυθ. τριάδες!

- Υπάρχουν 3άδες θετ. ακέραιων (a, b, c) : $a^3 + b^3 = c^3$;

- // - // - // - : $a^4 + b^4 = c^4$;

- // - // - // - // - : $a^n + b^n = c^n$; , $n \geq 3$.

- ΕΙΚΑΣΙΑ FERMAT : OXI

• 1637 (Fermat) : $n=4$

• 18⁵³-19⁰³ αλ. : Gauss-Euler : $n=3$.

~~Dirichlet~~ Dirichlet - Legendre : $n=5$.

• 1823 Sophie Germain : OXI, όταν το n έχει τις ακοτ. ιδιοτ. :
 n & $n+1$ πρώτοι αριθμοί και $n \nmid a \cdot b \cdot c$ ("διαίρει")

• 1994 Wiles (Taylor) : OXI, $\forall n \geq 3$

(ΑΝΟΙΧΤΑ) ΠΡΟΒΛΗΜΑΤΑ Θ.Α.

• Υπάρχουν άπειροι πρώτοι αριθμοί; ΝΑΙ! (Ευκλείδης)

$$\begin{array}{rcl} -1/- & -1/- & \text{ως κορυφής: } 4k+1 \\ & & 4k+3 \\ & & 6k+1 \\ & & 6k+5 \\ & & \vdots \end{array} \left. \vphantom{\begin{array}{rcl} -1/- & -1/- & \text{ως κορυφής: } 4k+1 \\ & & 4k+3 \\ & & 6k+1 \\ & & 6k+5 \\ & & \vdots \end{array}} \right\} \text{ΝΑΙ!}$$

Ποιοι αριθμοί είναι άθροισμα δύο τετραγώνων αριθμών;

3	$5 = 2^2 + 1^2$	7	11	$17 = 4^2 + 1^2$
↑	↑	↑	↑	↑
ΟΧΙ	ΝΑΙ	ΟΧΙ	ΟΧΙ	ΝΑΙ

$$\begin{array}{l} \textcircled{*} \textcircled{*} \textcircled{0} \text{ πρώτος αριθμός } P = a^2 + b^2 \Leftrightarrow P = 4k+1 \\ -1/- \quad P \neq a^2 + b^2 \Leftrightarrow P = 4k+3 \end{array} \left. \vphantom{\begin{array}{l} \textcircled{*} \textcircled{*} \textcircled{0} \text{ πρώτος αριθμός } P = a^2 + b^2 \Leftrightarrow P = 4k+1 \\ -1/- \quad P \neq a^2 + b^2 \Leftrightarrow P = 4k+3 \end{array}} \right\} k \in \mathbb{N}$$

$\textcircled{*}$ Θεώρημα του Lagrange: Κάθε φυσικός αριθμός $n \in \mathbb{N}$ είναι άθροισμα τεσσάρων τετραγώνων.

Εικασία του Goldbach: Κάθε άρτιος αριθμός > 2 είναι άθροισμα 2 πρώτων αριθμών.

Αβθενής εικασία Goldbach: Κάθε περιττός αριθμός > 5 είναι άθροισμα 3 πρώτων αριθμών.

Ανάνυση: ΝΑΙ (Helfgott) ~ 2013 .

Δύο πρώτοι αριθμοί p, q καλούνται δίδυμοι πρώτοι $\Leftrightarrow$

$$\Leftrightarrow |p - q| = 2 \quad ((3, 5), (5, 7), (11, 13), \dots, \text{~~29, 31~~}, \dots)$$

ΑΝΟΙΧΤΟ ΠΡΟΒΛΗΜΑ: Είναι το πλήθος των δίδυμων πρώτων αριθμών άπειρο;

ΓΕΝΙΚΟ ΠΡΟΒΛΗΜΑ: Υπάρχουν άπειροι πρώτοι αριθμοί p, q έτσι ώστε $|p - q| = k$, όπου $k \geq 2$;

- Zhang (2013) : $\exists k \in \mathbb{N}$, έδειξε το ΓΕΝΙΚΟ ΠΡΟΒΛΗΜΑ να
να έχει θετική απάντηση για $k \leq \pm 5.000.000$

- ~~Gu~~ Tao, Mainard 2014 : $k \leq 3.578$, $k \leq 600$.

• Πρόβλημα : Υπάρχουν άπειροι πρώτοι της μορφής $n^2 + 1$;
(Ανοιχτό πρόβλημα)

Dirichlet : αν $\text{ΜΚΔ}(n, m) = 1$, τότε υπάρχουν άπειροι πρώτοι
της μορφής : $nk + m$

$AD \equiv K \equiv H \vee X \Gamma N \vee \Delta \leadsto \text{ΚΡΥΠΤΟΓΡΑΦΙΑ}$

1. Βασικές ιδιότητες Ακεραίων

Βασικές ιδιότητες του $\mathbb{Z}$:

- | | |
|---|---|
| • $(a+b)+c = a+(b+c)$ | • $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ |
| • $a+b = b+a$ | • $ab = b \cdot a$ |
| • $a \cdot (b+c) = a \cdot b + a \cdot c$ | • $a \cdot 1 = a = 1 \cdot a$ |
| • $(a+b) \cdot c = a \cdot c + b \cdot c$ | |

• $\mathbb{N}_0$: $a+0 = a = 0+a$.

• $\mathbb{Z}$: $\forall a \in \mathbb{Z} : a+(-a) = 0 = (-a)+a$.

Σύμβαση : $\forall a, b \in \mathbb{Z} : a-b = a+(-b)$

$a > b \Leftrightarrow a-b > 0$ δηλ αν $(a-b) \in \mathbb{N}$

$\mathbb{Z} = (-\mathbb{N}) \cup \{0\} \cup \mathbb{N}$.

$a \geq b \Leftrightarrow \begin{cases} a=b \\ a > b \end{cases}$

• $a \cdot b = 0 \Leftrightarrow a=0$ ή $b=0$

• $a < b \Rightarrow a+c < b+c \quad \forall c \in \mathbb{Z}$

• $a < b \Rightarrow a \cdot d < b \cdot d, \quad \forall d \in \mathbb{N}$