# ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ
## ΤΜΗΜΑ Α (ΠΕΡΙΤΤΟΙ)
## Ασκήσεις # 3

1) Να βρεθούν ακέραιοι $x, y$ ώστε $x\,5390 + y\,700 = (5390, 700)$
Βρείτε $[5390, 700]$ με δύο τρόπους.

2) Βρείτε ακεραίους $a, b, c$ και $d$ ώστε
$(a, 700) = 1$ $(b, 700) = 5$ $[c, 700] = 7700$
$(d, 700) = 5$ και $[d, 700] = 23100$

3) Αν $x \in \mathbb{Z}$, τότε $(2x+1, 9x+4) = 1$

4) Βρείτε ακεραίους $a, b, c$ ώστε
$(112, 96, 24) = 112x + 96y + 24z$

5) Αν $a = 2^k(2\ell+1)$ και $b = 2^n(2q+1)$ με $k < n$, τότε
$(a, b) = 2^k(\ell - q, 2q+1)$

6) Να βρεθούν οι ακέραιοι $a$ και $b$ με $a(b-1) = b+1$

7) Βρείτε το μικρότερο σύνθετο με μορφή $p_1 p_2 \cdots p_n + 1$ όπου $p_i$ πρώτος, $p_1 = 2$ και $p_1, \ldots, p_n$ διαδοχικοί πρώτοι

8) Να βρεθεί ο μικρότερος $n$ και πρώτος $p$ ώστε οι αριθμοί του Fermat $F_n$ και Mersenne $M_p$ να μην είναι πρώτοι

9) Να δείξετε ότι υπάρχουν άπειροι πρώτοι μορφής $4k+1$ με $k \in \mathbb{N}$.

14/11/2016

**Άσκηση**: Να βρεθούν ακέραιοι $x, y$ ώστε $x5390 + y7\text{Τ}00 = (5390, 7\text{Τ}00)$

Βρείτε $[5390, 7\text{Τ}00]$ με 2 τρόπους.

Λύση

$x5390 + y7\text{Τ}00 = (5390, 7\text{Τ}00)$

$5390 = \text{Τ} \cdot 7\text{Τ}00 + 490$

$7\text{Τ}00 = 1 \cdot 490 + 210$

$210 = 3 \cdot \text{Τ}0 + 0$

Οπότε $(5390, 7\text{Τ}00) = (7\text{Τ}00, 490) = (490, 210) = (210, \text{Τ}0) = \text{Τ}0$

οπότε $x = 3$ και $y = -23$

$[5390, 7\text{Τ}00]$

**Α τρόπος**

$5390 = 2 \cdot 5 \cdot \text{Τ}^2 \cdot 11$

$\text{Τ}00 = 2^2 \cdot 5^2 \cdot \text{Τ}$

άρα $[5390, 7\text{Τ}00] = 2^2 \cdot 5^2 \cdot \text{Τ}^2 \cdot 11$

**Β τρόπος**

Είναι $[5390, 7\text{Τ}00] = \dfrac{5390 \cdot 7\text{Τ}00}{\text{Τ}0}$

Άσκηση: Βρείτε ακέραιους $a, b, c$ και $d$ ώστε
$(a, 700) = 1$ $(b, 700) = 5$ $[c, 700] = 7700$
$(d, 700) = 5$ και $[d, 700] = 23100$

## Λύση

$(a, 700) = 1$ $a = 3$

| | |
|---|---|
| 700 | 2 |
| 350 | 2 |
| 175 | 5 |
| 35 | 5 |
| 7 | 7 |

$700 = 2^2 \cdot 5^2 \cdot 7$

$(b, 700) = 5$
$b = 5k$ $k \nmid 2, 5, 7$

$[c, 700] = 7700 = 700 \cdot 11$

Αν $(c, 700) = 1$ τότε $c = 11$
Αν $(c, 700) = 2$
$2 | 700$ τότε $c = \frac{7700}{2 \cdot 700}$

$(d, 700) = 5$ και $[d, 700] = 23100$

$(d, 700) \cdot [d, 700] = d \cdot 700$
$5 \cdot 23100 = d \cdot 700 \Rightarrow d = \frac{5 \cdot 23100}{700} = 165$

Άσκηση 6 : Να βρεθούν οι ακέραιοι a και b με
$a(b-1) = b+1$

Λύση

$a(b-1) = b+1$ •

• $ab - a = b+1$

$b-1 \mid b+1$

$b-1 \mid b-1 \Rightarrow b-1 \mid b+1-(b-1)$

$b-1 \mid 2 \Rightarrow b-1 = |1| \text{ ή } b-1 = |2|$

$b-1 = -1 \Rightarrow b = 0$

$b-1 = 1 \Rightarrow b = 2$

$b-1 = 2 \Rightarrow b = 3$

$b-1 = -2 \Rightarrow b = -1.$

Αντικαθιστώντας βρίσκουμε

Για $b=0$: $a(0-1) = 0+1 \Rightarrow -a = 1 \Rightarrow \boxed{a = -1}$

Για $b=2$

Για $b=3$

Για $b=-1$.

**Άσκηση 3 :** Αν $x \in \mathbb{Z}$, τότε $(2k+1, 9k+4) = 1$

**Λύση**

Αν $x \in \mathbb{Z}$ $(2k+1, 9k+4) = 1$

$(2k+1, 9k+4) = (9k+4, 2k+1)$

$(9k+4-4(2k+1), 2k+1) =$

- $(9k+4-8k-4, 2k+1) =$
- $(k, 2k+1) = (2k+1, k) =$
- $(2k+1-2k, k) = (1, k) = 1$

**Άσκηση 5 :** Αν $a = 2^k(2l+1)$ και $b = 2^m(2q+1)$ με $k < m$, τότε $(a, b) = 2^k(l-q, 2q+1)$

**Λύση**

$k < m \Rightarrow 2^k < 2^m$

$(a, b) = (2^k(2l+1), 2^m(2q+1)) = 2^k(2l+1, 2^{m-k}(2q+1)) =$

$= 2^k(2l+1, 2q+1) =$

$= 2^k(2l+1-(2q+1), 2q+1) = 2^k(2(l-q), 2q+1) =$

$= 2^k(l-q, 2q+1)$

# Σχέση ισοδυναμίας

14/11/2016

Α σύνολο και $\Sigma \subseteq A \times A$
$\Sigma$ είναι σχέση ισοδυναμίας

1) Ανακλαστική: $\forall a \in A \quad (a,a) \in \Sigma$ ή $a \Sigma a$

2) Συμμετρική: Αν $(a,b) \in \Sigma \Rightarrow (b,a) \in \Sigma$
$a \Sigma b \Rightarrow b \Sigma a$

3) Μεταβατική: Αν $(a,b) \in \Sigma$ και $(b,c) \in \Sigma \Rightarrow (a,c) \in \Sigma$
$a \Sigma b$ και $b \Sigma c \Rightarrow a \Sigma c$.

Σε μια σχέση ισοδυναμίας μας ενδιαφέρει να βρούμε τα στοιχεία που είναι ισοδύναμα μεταξύ τους και να τα βάλουμε σε ένα σύνολο το οποίο καλείται κλάση ισοδυναμίας.

$\bar{a}$ ή $[a] = \{b \mid b \in A$ και $a \Sigma b$ ή $(a,b) \in \Sigma\}$

$[a] \cap [b] = \emptyset$ ή $[a] = [b]$

Το Α χωρίζεται σε ξένα υποσύνολα τα οποία ονομαζόμαστε από τις κλάσεις ισοδυναμίας

# Ισοτιμίες

**Ορισμός**

Έστω $m \geq 1$ φυσικός. Δύο ακέραιοι $a$ και $b$ καλούνται ισοδύναμοι ή ίσοι ή ισοϋπόλοιποι modulo $m$, αν $a-b=km$ για κάποιον ακέραιο $k$.

Γράφουμε $a \equiv b \bmod m$

**Παράδειγμα**

$m=7 \quad a=13 \quad b=-36$

$a \equiv b \bmod m$

$a-b=13-(-36)=49=7 \cdot 7$

άρα $7 \mid a-b \Rightarrow a \equiv b \bmod 7$

**Πρόταση**

Η σχέση modulo στους ακεραίους είναι σχέση ισοδυναμίας.

**Απόδειξη**

Η σχέση ορίζεται με το modulo. Δηλαδή

$a \mathcal{R} b \Leftrightarrow a-b=km$

1) Ανακλαστική: $\forall a \in \mathbb{Z} \Rightarrow a \mathcal{R} a \Leftrightarrow a-a=km$

$0=0m$

2) Συμμετρική: Αν $a \mathcal{R} b \Rightarrow b \mathcal{R} a$

$a \mathcal{R} b \Leftrightarrow a-b=km$ θέλουμε $b-a=k'm$

$a-b=km \Rightarrow b-a=(-k)m$ ισχύει.

3) Μεταβατική: Αν $a \mid b$ και $b \mid c \Rightarrow a \mid c$

Έχουμε $a-b=km$ και $b-c=k'm \Rightarrow$

$a-b+b-c=km+k'm \Rightarrow a-c=(k+k')m$ Ισχύει.

Πρέπει να βρούμε τις λύσεις ισοδυναμίας.

Παράδειγμα

Βρείτε τις λύσεις ισοδυναμίας modulo 5

$0 \mid a \Leftrightarrow 0-a=k\cdot 5=5k \Leftrightarrow 5 \mid a$

$0 \mid 5\lambda \quad [0]_5 = \{5\lambda \mid \lambda \in \mathbb{Z}\}$ ← το modulo

$1 \notin [0]_5 \qquad [1]_5 = \{5k+1 \mid k \in \mathbb{Z}\}$

$1 \mid a \Leftrightarrow 1-a$ ή $a-1=5k \Leftrightarrow$

$a=5\lambda+1$ Όταν ο $a$ διαιρεθεί με το 5 αφήνει υπόλοιπο 1.

$2 \in [0]_5 \cup [1]_5$

$[2]_5 = \{5\mu+2 \mid \mu \in \mathbb{Z}\}$

$[3]_5 = \{5\nu+3 \mid \nu \in \mathbb{Z}\}$

$[4]_5 = \{5\rho+4 \mid \rho \in \mathbb{Z}\}$

$\mathbb{Z} = [0]_5 \cup [1]_5 \cup [2]_5 \cup [3]_5 \cup [4]_5$

Έστω $m$ τυχαίος ακέραιος

Ευκλείδης $m = 5n + u \iff m - u = 5n \iff m \equiv u$

$0 \le u \le 4$ $\quad m \in [u]_5$

άρα $m \in [0]_5 \cup [1]_5 \cup [2]_5 \cup [3]_5 \cup [4]_5$

Ορίζουμε $\mathbb{Z}_5 = \{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\}$

Πρόταση

Έστω $m \ge 1$ φυσικός. Οι υπλάσεις ισοδυναμίας modulo $m$ θα καθορίζονται από τα υπόλοιπα ως προς διαίρεση με το $m$. Δηλαδή $0, 1, 2, \ldots, m-1$

$[0]_m, [1]_m, \ldots, [m-1]_m$ υπλάσεις

$\mathbb{Z} = [0]_m \cup [1]_m \cup \ldots \cup [m-1]_m$

όπου $[0]_m = \{k_0 \cdot m \mid k_0 \in \mathbb{Z}\}$

$[1]_m = \{k_1 m + 1 \mid k_1 \in \mathbb{Z}\}$

$\vdots$

$[m-1]_m = \{k_{m-1} \cdot m + m - 1 \mid k_{m-1} \in \mathbb{Z}\}$

$\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\}$

Προσοχή!

$[i]_m$ $\quad 0 \le i \le m-1$ $\quad \{km+i \mid k \in \mathbb{Z}\}$

$=$

$[m+i]_m$

Πρόταση

Αν $a \in \mathbb{Z}$ τυχαίο, τότε $\mathbb{Z}_m = \{[a]_m, [a+1]_m, [a+2]_m, \ldots [a+m-1]_m\}$

---

- Δηλαδή $\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\} = \{[a]_m, [a+1]_m, [a+2]_m \ldots [a+m-1]_m$

$a = 5m+1$

$[a]_m = [0]_m$

Παράδειγμα

$b \quad m \quad a$

$12 \bmod 24 \equiv 36$ $\quad 36-12 = 24 \mid 24$ ✓

$24 = 4 \cdot 6$

$= 2^3 \cdot 3$

$36 \equiv 12 \bmod 24 \Rightarrow \quad 36 \equiv 12 \bmod 4$

$36 \equiv 12 \bmod 6$

$\Rightarrow \quad 36 \equiv 12 \bmod 8 \iff 4 \equiv 4 \bmod 8$

$36 \equiv 12 \bmod 3 \quad 0 \equiv 0 \bmod 3$