

$$1) \ x5390 + y700 = (5390, 700)$$

$$\begin{array}{r} 5390 \cancel{0} \mid \cancel{700} \\ 49 \mid 7 \end{array} \quad x539 + y70$$

$$\begin{array}{r|l} 70 & 49 \\ \hline 21 & 1 \end{array} \quad \begin{array}{r|l} 49 & 21 \\ \hline 7 & 2 \end{array} \quad \begin{array}{r|l} 21 & 7 \\ \hline 0 & 3 \end{array}$$

$$x539 + y70 = 7$$

$$7 = 49 - 21 \cdot 2 = 3 \cdot 49 - (70 - 49) \cdot 2 = 3(539 - 7 \cdot 70) + 0 = 3 \cdot 539 - 22 \cdot 70 \Rightarrow$$

$$21 = 70 - 49$$

$$49 = 539 - 7 \cdot 70$$

$$\Rightarrow 7 = 3 \cdot 539 - 22 \cdot 70$$

$$\Rightarrow 70 = 3 \cdot 5390 - 22 \cdot 700$$

$$b) = [5390, 700] = \frac{5390 \cdot 700}{(5390, 700)} = \frac{5390 \cdot 700}{70} = 53900$$

δίνεται και με πρωτογενή ανάλυση.

$$2) \ a, b, c, d \in \mathbb{Z}$$

$$(a, 700) = 1$$

$$(1, 700) = 1 = (11, 700) = 700 = 2^3 \cdot 5^2 \cdot 7$$

Άρα το a δεν πρέπει να διαιρείται από τα: $2, 5, 7$.

$$a = p_1^{u_1} \cdots p_l^{u_l}, \quad p_1, \dots, p_l \neq 2, 5, 7$$

$$(b, 700) = 5.$$

$$(b, 2^2 \cdot 5^2 \cdot 7) = 5.$$

$$b = 5 \cdot p_1^{\alpha_1} \dots p_k^{\alpha_k} \text{ где } p_1 \dots p_k \neq 2, 5, 7 \Rightarrow b = 5a$$

$$[c, 700]$$

$$[c, 2^2 \cdot 5^2 \cdot 7] = 11 \cdot 700 = 11 \cdot 2^2 \cdot 5^2 \cdot 7.$$

$$c = 11$$

$$c = 11 \cdot 2$$

$$c = 11 \cdot 2^2$$

$$c = 11 \cdot 5$$

...

$$c = 11 \cdot 2^k \cdot 5^l \cdot 7^m$$

$$k = 0, 1, 2$$

$$l = 0, 1, 2$$

$$m = 0, 1$$

$$(d, 700) = 5.$$

$$(d, 700) = 23100$$

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

$$\frac{d \cdot 700}{5} = 23100 \Rightarrow$$

$$d = \frac{5 \cdot 231}{7} = 5 \cdot 33 = 5 \cdot 3 \cdot 11 = 3 \cdot 5 \cdot 11.$$

$$3) (2k+1, 9k+4) = 1$$

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

$$= (2k+1, k) = (2k+1 - 2k, k) = (1, k) = 1.$$

$$4) a, b, c \in \mathbb{Z}.$$

$$(112, 96, 24) = 112x + 96y + 24z.$$

$$(112, 96) = 16 = 112 - 96 \quad (1)$$

$$\begin{array}{r|l} 112 & 96 \\ 16 & \end{array} \quad \begin{array}{r|l} 96 & 16 \\ 0 & 6 \end{array}$$

$$(16, 24) = 8 = 24 - 16 \quad (1)$$

$$\begin{array}{r|l} 24 & 16 \\ 8 & 1 \end{array} \quad \begin{array}{r|l} 16 & 8 \\ 0 & 2 \end{array}$$

$$(112, 96, 24) = 8 = 24 - 112 + 96 = -112 + 96 + 24$$

$$x = -1 \quad y = 1 \quad z = 1.$$

$$5) a = 2^k(2l+1)$$

$$b = 2^m(2q+1)$$

$$k < m$$

$$N_{\Delta 0}(a, b) = 2^k(l-q, 2q+1)$$

$$(2^k(2l+1), 2^m(2q+1)) = 2^k(\underbrace{2l+1}_{\times 2}, 2^{m-k}(2q+1)) =$$

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

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

$$= 2^k(2-(l-q), 2q+1) = 2^k(\cancel{2}(l-q), 2q+1)$$

$$6) a, b \in \mathbb{Z}$$

$$a(b-1) = b+1$$

$$a(b-1) = b+1 = b-1+2$$

$$a(b-1) - (b-1) = 2 \Rightarrow$$

$$(a-1)(b-1) = 2$$

$a-1 = -1$	$a-1 = 1$	$a-1 = -2$	$a-1 = 2$
$b-1 = -2$	$b-1 = 2$	$b-1 = -1$	$b-1 = 1$

9) $4k+3$ πρώτος, $m \in \mathbb{N}$ $m = 4n+1$
 $m = 4n+3$

Έστω ότι είναι γενεαγενείς.

$p_1 = 3, p_2, \dots, p_m$

όσοι είναι πρώτοι της μορφής $4k+3$, και δεν υπάρχει άλλος
πρώτος με αυτή τη μορφή.

~~$4p_1 p_2 \dots p_m + 3 = \text{γινόμενο, άρτιος} = q_1 q_2 \dots q_l$~~

~~$4p_2 \dots p_m + 3$~~

Όσο q_1, q_l δε μπορεί να είναι πρώτοι, της μορφής $4k+3$. Αν κάποιος
είναι τέταρτος πρώτος, τότε θα είναι κάποιος από τους $p_2 \dots p_m$.

Αν είναι ο p_i , θα έχουμε ότι:

$$\begin{array}{l} p_1 / q_1 q_2 \dots q_l \\ p_1 / 4 p_2 p_3 \dots p_m \end{array} \nmid p_1 / 3 \text{ Αδύνατο.}$$

Από οι $q_1, \dots, q_l$ είναι πρώτοι μορφής $4m+1$. Τους γράφουμε:

$$q_1 = 4k+1, \dots, q_l = 4\ell+1 \Rightarrow q_1 \dots q_l = 4A+1$$

Από έχουμε:

$$4B+3 = 4A+1 \Rightarrow$$

$$4B+2 = 4A \Rightarrow$$

$$4/2 \text{ Αδύνατο.}$$

Προβλή: Δύο ακεραίοι a και b , κατανίται ισοδύναμοι ή ισοδύναμοι ή ισοτίμοι modulo m , αν $m \mid a-b$.
Γράφουμε $a \equiv b \pmod{m}$

$a \equiv b \pmod{m} \Leftrightarrow a-b$ διαίρεται από τον m
($\Rightarrow$) a και b έχουν το ίδιο υπόλοιπο δια m

Τα υπόλοιπα του m είναι $0, 1, 2, 3, \dots, m-1$.
Αυτές θα είναι και οι κλάσεις modulo m .

Υπάρχουν άπειροι ακεραίοι με το ίδιο υπόλοιπο.
Όλους αυτούς που αφήνουν το ίδιο υπόλοιπο u , τους θα βρούμε σε
ένα σύνολο, το οποίο συμβολίζουμε: $[u]_m = \{m \cdot k + u \mid k \in \mathbb{Z}\}$
και καταίμε κλάση του u ως προς το m .

π.χ. $m=4$ κλάσεις του 4;

$$[0]_4 = \{4k \mid k \in \mathbb{Z}\} = \{0, \pm 4, \pm 8, \dots\}$$

$$[1]_4 = \{4k+1 \mid k \in \mathbb{Z}\} = \{1, 5, 9, \dots\} \cup \{-3, -7, \dots\}$$

$$[2]_4 = \{4k+2 \mid k \in \mathbb{Z}\}$$

$$[3]_4 = \{4k+3 \mid k \in \mathbb{Z}\}$$

$$[1]_4 = [5]_4 = [9]_4$$

$$\mathbb{Z} = [0]_4 \cup [1]_4 \cup [2]_4 \cup [3]_4 \quad \text{Διαμέριση}$$

Πρόταση: Η σχέση modulo αποτελεί σχέση ισοδυναμίας στο $\mathbb{Z}$.

Πρόταση: Έστω $m > 1$ πρώτος, τότε $\mathbb{Z} = [0]_m \cup [1]_m \cup \dots \cup [m-1]_m$
Ισχύει ότι $[a]_m \cap [b]_m = \emptyset$ ή ταυτίζονται.

Πείραξη: Με το σύνολο $\mathbb{Z}_m$ θα απεικονίσουμε το σύνολο των κλάσεων ως προς m .

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

Ορίσουμε πράξεις:

$$\text{Πρόσθεση: } [a]_m \oplus [b]_m = [a+b]_m$$

$$\text{ex. } m=5 : [3]_m \oplus [12]_m = [15]_m = [15]_5 = [0]_5.$$

$$[12]_5 = 2$$

$$\text{Εφόσον } [3]_5 \oplus [2]_5 = [0]_5, \text{ τότε οι κλάσεις}$$

$[3]_5$ και $[2]_5$ είναι αντίθετες.

Στο $\mathbb{Z}$ ο αντίθετος του 3 είναι ο -3.

$$[-3]_5 = [-3+5]_5 = [2]_5.$$

Παρατήρηση: Η αντίθετη κλάση του $[a]_m$ είναι $[m-a]_m$

$$[a]_m \oplus [m-a]_m = [m]_m = [0]_m$$

$$n \times [a]_m = [a + km]_m$$

$$[b]_m = [b + lm]_m$$

$$[a]_m \oplus [b]_m = [a + b]_m$$

$$[a + b + km + lm]_m$$

// Η πράξη είναι καλά ορισμένη.

Πρόταση: Η πράξη της πρόσθεσης είναι προσεταιριστική, έχει ουδέτερο στοιχείο, κάθε στοιχείο έχει αντίθετο και είναι και αντιμεταθετική.

$$1) ([a]_m \oplus [b]_m) \oplus [c]_m = [a]_m \oplus ([b]_m \oplus [c]_m)$$

$$2) [a]_m \oplus [0]_m = [a]_m$$

$$3) \text{Αντίθετος του } [a]_m \text{ είναι } [m-a]_m$$

$$4) [a]_m \oplus [b]_m = [b]_m \oplus [a]_m$$

$\oplus$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[0]_6$	$[0]$	$[1]$	$[2]$			
$\mathbb{Z}_6 : [1]_6$						
$[2]_6$			(4)		(0)	$[1]$
$[3]_6$						
$[4]_6$						
$[5]_6$						

Ορισμός: Στο σύνολο $\mathbb{Z}_m$ ορίζεται πράξη πολλαπλασιασμού.
 $[a]_m \odot [b]_m = [a \cdot b]_m$

π.χ. $m=6$: $[2]_6 \odot [2]_6 = [4]_6$

$$[2]_6 \odot [3]_6 = [0]_6 \quad \Rightarrow \quad [2]_6 = [0]_6$$
$$[3]_6 = [0]_6.$$

Καίνω τον αντίστοιχο πίνακα για τον πολλαπλασιασμό.