MATIN cours du 16.11.2020

lundi, 16 novembre 2020 08:19

Bachet - Bézout : pour toute paire $a, b \in \mathbb{Z}^*$

il existe une sol. **Entière** $(x, y \in \mathbb{Z})$

tels que $a \cdot x + b \cdot y = PGCD(a, b)$

Remarque: On dit que a divise b si: $b \bmod a = 0$

ou si: $b = \alpha \cdot a$

α multiplicateur $\in \mathbb{N}$

autrement dit a est un diviseur de b.

Il n'existe AUCUN diviseur de $b > b$!

A noter que les coeff de Bézout sont en nombre infinité !

Rappel: Si a et b sont premiers entre eux, alors on a

$PGCD(a, b) = 1$ et l'équation $a \cdot x + b \cdot y = 1$ a des sol. entières !

Arithmétique Modulaire: (Modulo) - Gauss (1801)

Soient $a, b, n \in \mathbb{Z}$, on dit que $a \bmod n = b$

si: $a = k \cdot n + b$ où $k \in \mathbb{Z}$ et $b \in \mathbb{Z}$,

mais $b \in [0, a-1]$.

Notations alternatives:

$a \,\%\, n = b$

$a \equiv_n b$

↑ égalité au modulo près $a \bmod n = b \bmod n$

$a \equiv_n b$ cela s'appelle la CONGRUENCE

a est congruent à b modulo n !

Cela s'applique aussi si $b \notin [0, n-1]$

Exemples:

$108 \bmod 32 = ? \ 12$

$= 3 \cdot 32 + 12$

108	32
- 96	3
12	

$108 \bmod 54 = 0 = 2 \cdot 54 + 0$

108	54
- 108	2
0	

$108 \bmod n \in [0, 1, 2, \dots, 107]$

$108 \bmod \underbrace{X}_{110} = 108$? est-ce possible OUI

c'est possible si $X > 108$

108	110
- 0	0
108	

$a \bmod n = a$ possible si (et seulement) $a < n$.

En revanche:

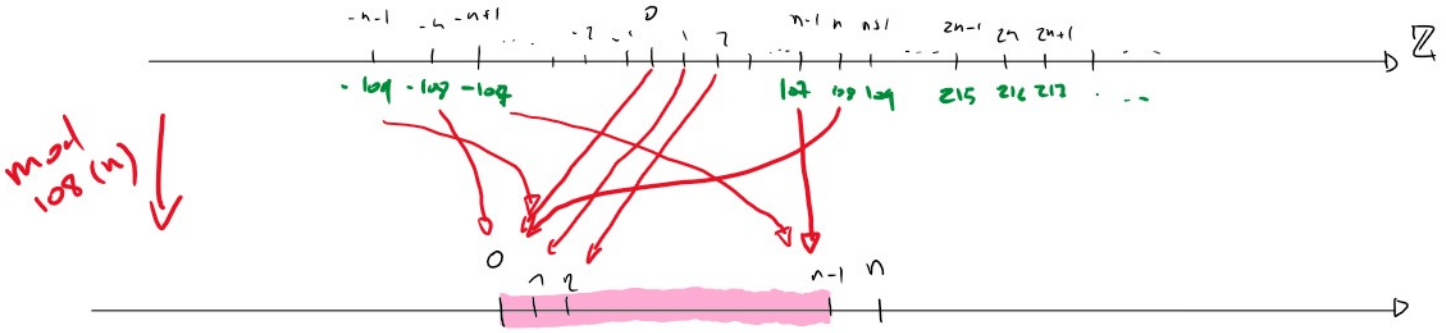
$a \bmod \underbrace{108}_{0} = \underbrace{108}_{1}$? est-ce possible NON

↳ $a \bmod 108 = k \cdot 108 + 108 = (k+1) \cdot 108 + 0$

$= \log$? Non car si

$a \bmod 108 = \log = k \cdot 108 + 109 = (k+1) \cdot 108 + 1$

$a \bmod N \in [0, \dots, n-1]$



$a \bmod 108 \longrightarrow [0, 107]$

$-1273 \bmod 108 = 23 \quad \in [0,107]$

$-1273 = (-11) \cdot (108 - 85$

$-1273 = -12 \cdot 108 - 85 + 108$

$= -12 \cdot 108 + 23$

-1273	108
$-(-11) \cdot 108$	-11
$+1188$	
-85	

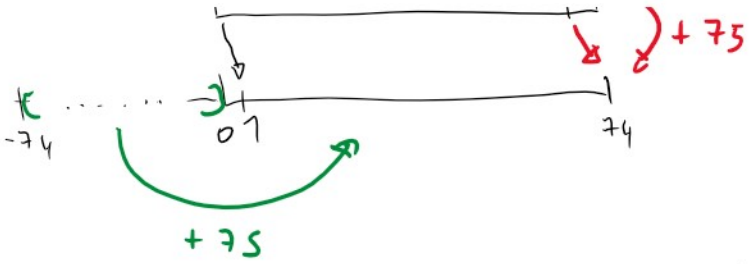
Exercices:

1) $3048 \bmod 75 = ?$ 48 car $3048 = 40,64 \cdot 75 = 40 \cdot 75 + 0,64 \cdot 75 = 40 \cdot 75 + 48$

2) $-3048 \bmod 75 = ?$ 27 $(-40,64 \cdot 75) = -40 \cdot 75 - 48$

3) $705 \bmod 5 = ?$ 0 $\Rightarrow$ car $705 = 121 \cdot 5 + 0$

4) $705 \bmod 23 = ?$ 15



Si $x < 0$

$\epsilon [-N-1, \dots, 0]$

alors $x \bmod N = -k \cdot N - y$

$= -(k+1) \cdot N + (N-y)$

$\epsilon [0, \dots, N-1]$

Preuve: $a \bmod n = a$ (A) si et seulement si $a < n$ (B)

(A) → (B) $a \bmod n = a$ par déf. du modulo on sait

$a \bmod n \in [0, n-1] \Rightarrow a \in [0, n-1] \Rightarrow a < n$ (donc) prouve (A) → (B)

(B) → (A) Si $a < n \Rightarrow a = 0 \cdot n + a \in [0, n-1]$ car $a < n$

$\Rightarrow a \bmod n = a$ (par déf. du modulo) $\Rightarrow$ prouve (B) → (A)

CQFD !

CONGRUENCE: a est congruent à b modulo N $(a, b \in \mathbb{Z},\ N \in \mathbb{N})$

Si $a \bmod N = b \bmod N$

On l'écrit $\boxed{a \equiv_N b}$

$a = k \cdot N + x = k \cdot N + x = b$

$$a = k_1 \cdot N + X = k_2 \cdot N + X = b$$

Exemples:

103 et 70 sont congrus modulo 33 !

$103 \bmod 33 = 4 \qquad (33 \cdot 3 + 4)$

$70 \bmod 33 = 4 \qquad (2 \cdot 33 + 4)$

$$103 \equiv_{33} 70$$

Exercice: trouver les éléments congruents à 173 mod 31 !

$173 \bmod 31 = 18$

$X \equiv_{31} 18 \quad$ si $\quad X = k \cdot 31 + 18$, $k \in \mathbb{Z}$

$k = \ldots -2 \; -1 \; 0 \; 1 \; 2 \; 3 \ldots$

$X \in [\ldots, -44, -13, 18, 49, 80, 111, \ldots]$

⚠ il y a une INFINITÉ de nombres congruents à 173 mod 31 !

-44
-13
111

Question: Si $\equiv_N$ définit un ensemble de nombres congruents, combien de ces ensembles différents y a-t-il ? Il y en a N

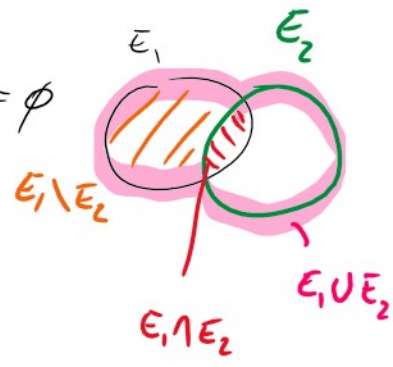
$E_0 = \{ x \text{ où } x \equiv_N 0 \}$

$E_1 = \{ x \text{ où } x \equiv_N 1 \}$

$\vdots$

$E_{N-1} = \{ x \text{ où } x \equiv_N N-1 \}$

que vaut $E_1 \cap E_2 = \emptyset$



Grâce à la congruence on DIVISE $\mathbb{Z}$ en N sous-ensembles DISJOINTS

$$\mathbb{Z} = E_0 \cup E_1 \cup E_2 \cup \dots \cup E_{N-1}$$

$$E_i \cap E_j = \underset{\text{ensemble vide}}{\emptyset} \quad \text{si } i \neq j$$

Prouvons que c'est VRAI :

2 choses à prouver

a) tout $x \in \mathbb{Z}$ fait partie de au moins un ensemble E_i

b) x ne peut pas faire partie de 2 ensembles différents.