Arithmétique : Amyot 0

VANDERBROUCK @u-pair.fr

" b est multiple de a "

$\exists k_1 \in \mathbb{Z} \mid b = k_1 a$ ①

" c est multiple de a "

$\exists k_2 \in \mathbb{Z} \mid c = k_2 a$ ②

Donc $b + c = k_1 a + k_2 a$

$b + c = a(k_1 + k_2)$

Donc $\exists k \in \mathbb{Z} \mid k = (k_1 + k_2)$

or $b + c = ak$ donc $a \mid b + c$

Concept fondamental : La division euclidienne

Soit $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$, $\exists ! (q, r) \in \mathbb{Z} \times \mathbb{N}^*$

$$\begin{cases} a = bq + r \\ 0 \leq r < q \end{cases}$$

Démo :

600	124
-496	4
104	

Alors $600 = 4 \times 124 + 104$

Démo :

-600	124
-646	-5
+46	

Donc $-600 = -5 \times 124 + 96$

$16 \geq 0$ et $16 < 124$: ✓

$2 \equiv 2 \ [10]$

$8 \equiv 8 \ [10]$

-8	10
-10	0
2	

$x \bmod y$

$x \to$ unique

$-x \bmod y$

$\iff x \bmod y$

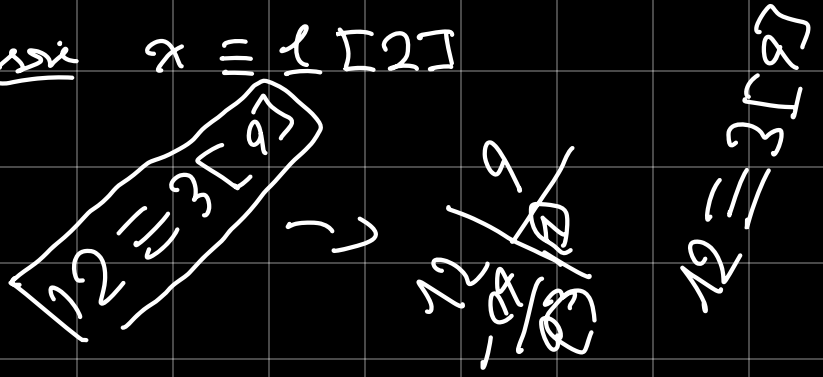
Concepts fondamentaux : Les congruences

Définition : Soit $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$

On dit que $a \equiv b \ [n]$ (a "congrue" "modulo" n) si le reste de la division euclidienne de a par n est b.

On peut "partionné" $\mathbb{Z}$ avec cette notion :

Les pairs : $\forall x \in \mathbb{Z}$ ssi $x \equiv 0 \ [2]$
Les impairs : $\forall x \in \mathbb{Z}$ ssi $x \equiv 1 \ [2]$



Propriétés :

* Si $a \equiv b \ [n]$ alors $b \equiv a \ [n]$ ← réflexivité
* Si $a \equiv b \ [n]$ et $b \equiv c \ [n]$ alors $a \equiv c \ [n]$
  ↳ transitivité

* Compatibilité avec les opérations :

* La somme : Si : $\left\{\begin{array}{l} a \equiv c\ [m] \\ b \equiv d\ [m] \end{array}\right\} \rightarrow a+b \equiv c+d\ [m]$

↳ preuve : $a - c = k_1 m$ et $b - d = k_2 m$

donc $a + b - (c+d)$

$\Rightarrow a + b - c - d$

$\Rightarrow (a-c) + (b-d)$

$\Rightarrow k_1 m + k_2 m \Rightarrow m(k_1 + k_2)$

Donc $a - b \equiv c+d\ [m]$ (QFD)

* Le produit : Si : $\left\{\begin{array}{l} a \equiv c\ [m] \\ b \equiv d\ [m] \end{array}\right\} \Rightarrow ab \equiv cd\ [m]$

↳ preuve (en utilisant l'autre caractérisation)

Soit q_1 et r_1 | $a = q_1 m + r_1$

Soit $q_{1'}$ | $c = q_{1'} m + r_1$

Soit q_2 et r_2 | $b = q_2 m + r_2$

Soit $q_{2'}$ | $d = q_{2'} m + r_2$

Alors $ab = (q_1 n + r_1) \times (q_2 n + r_2)$

$= n^2 q_1 q_2 + q_1 n r_2 + q_2 n r_1 + r_1 r_2$

$= n(q_1 q_2 + q_1 r_2 + q_2 r_1) + r_1 r_2$

Donc $\exists K_1 = (q_1 q_2 + q_1 r_2 + q_2 r_1)$
tel que $ab = Kn + r_1 r_2 \Rightarrow ab \equiv r_1 r_2 [n]$

De la même façon, $cd \equiv r_1 r_2 [n]$
Donc $ab \equiv cd [n]$

Application immédiate : les critères de divisibilité :

$123456 \equiv ? [9]$

$123456 \equiv \underbrace{1}_{1} \times 10^5 + \underbrace{2}_{2} \times 10^4 + \underbrace{3}_{3} \times 10^3 + \underbrace{4}_{4} \times 10^2 + \underbrace{5}_{5} \times 10^1 + 6$

$123456 \equiv 1 + 2 + 3 + 4 + 5 + 6$

$123456 \equiv 21 [9] \Leftrightarrow 123456 \equiv 3 [9]$

Concept fondamental : Le PGCD

PGCD (95991, 13083) = ?

Lemme : Si $a, b \in \mathbb{Z}$, et $a = bq + r$,
alors PGCD(a, b) = PGCD(b, r)

Sa preuve : L'ensemble des diviseurs de a et b
et le même que celui de b et r

car $a = bq + r$ ...
$a - bq = r$

Algorithme d'Euclide :

95991	13083
- 91518	7
4473	

13083	4410
- 8820	2
4263	

4410	4263
− 4263	1
147	

4263	147
− 4263	29
0	

Donc PGCD (95991, 13083) = 147

Théorème de Bezout :

Si a et b $\in \mathbb{Z}$, si PGCD(a, b) = d, alors $\exists (u, v) \in \mathbb{Z}^2$ tel que $d = au + bv$

Ici d'après le théorème de Bézout :
$\exists (u, v) \mid 147 = ua + vb$

$$147 = 4410 - 4263 \times 1$$

$4263 = 13083 - 2 \times 4410$

$$147 = -13083 + 3 \times 4410$$

$4410 = a - 7b$

$$147 = 3a - 22b$$

1ère division :

$95991 = 7 \times 13083 + 4410$, $a = 95991, b = 13083,$

$\Leftrightarrow 4410 = 95991 - 7 \times 13083$

$4410 = a - 7 \times b$

2ème division :

$13083 = 2 \times 4410 + 4263$

$4263 = 13083 - 2 \times 4410$

$\Leftrightarrow 4263 = a - 7b$

3ème divisia :

$4410 = 1 \times 4263 + 147$

$147 = 4410 - 4263$

$a - 7b$ $\quad -2a + 15b$

$147 = 3a - 22b.$

$95991 = 1a + 0b$

$13083 = 0a + 1b$

$4410 = 1a - 7b$

$4263 = -2a + 15b$

$147 = 3a - 22b$

* **Propriété :** Soit $a, b \in \mathbb{Z}$, a et b sont premiers entre eux ssi $\exists (u,v) \in \mathbb{Z}^2 \mid au + bv = 1$.

↳ preuve : d'après le Théorème de Bézout avec $d = 1$, $\Leftarrow$ réciproque : On suppose qu'il existe $(u,v) \in \mathbb{Z}^2 \mid au + bv = 1$.

Si $d \mid a$ et $d \mid b$ alors $d \mid au + bv$ donc $d \mid 1$

Donc $d = 1$. CQFD

Théorème de Gauss :

Soit $a, b \in \mathbb{Z}^*$, si $a \mid bc$ et $PGCD(a,b) = 1$ alors $a \mid c$

↳ preuve : (comme $PGCD(a,b) = 1$, $\exists (u,v) \in \mathbb{Z}^2$ tel que $au + bv = 1$

On multiplie par c, $cau + cbv = c$

On a : $a \mid acu$ car $a \mid a \Rightarrow a \mid acu$

On a : $a \mid bcv$ car $a \mid bc \Rightarrow a \mid bcv$

Donc $a \mid c$. (QFD

Lien PGCD et PPCM :

Soit $a, b \in \mathbb{Z}$

Soit $d = PGCD(a, b)$

On note $\tilde{a}$ Tel que $a = \tilde{a} d$

et $\tilde{b}$ Tel que $b = \tilde{b} d$

On note $m = \tilde{a} \tilde{b} d$, alors dans ce cas on dit que m est le PPCM de a et b

$a = 18, b = 24, d = 6.$

$\tilde{a} = 3, \tilde{b} = 4$

$m = \tilde{a} \tilde{b} d = 4 \times 3 \times 6 = 72$

La preuve : Soit $m = \tilde{a} \tilde{b} d$

1) m est un multiple de a et b

car $\begin{cases} m = \tilde{a} b \leftarrow \hat{a} b \Leftrightarrow \tilde{a} \tilde{b} d \Leftrightarrow m \\ m = \tilde{b} a \leftarrow \tilde{b} a \Leftrightarrow \tilde{b} \hat{a} d \Leftrightarrow m \end{cases}$

2) Si m' est un autre multiple de a et b :

$\exists\, k_1 \in \mathbb{Z} \mid m' = k_1 a = k_1 \tilde{a} d$ ①

$\exists\, k_2 \in \mathbb{Z} \mid m' = k_2 b = k_2 \tilde{b} d$ ②

or $m' =$ ① et $m' =$ ②, donc ① = ②

$\Rightarrow \tilde{a} d k_1 = \tilde{b} d k_2$, donc $\tilde{a} \mid \tilde{b} d k_2$

mais $\tilde{a}$ est premier avec $\tilde{b}$ donc $\tilde{a} \mid k_2$

Or $\exists\, k_3 \in \mathbb{Z} \mid k_2 = k_3 \tilde{a}$

Donc $m' = \tilde{b} d k_2 \Leftrightarrow m' = \underbrace{\tilde{b} d \tilde{a}}_{m} k_3$

Or $\tilde{b} d \tilde{a} = m$, donc $m' = m k_3 \Rightarrow m \mid m'$

Donc $m < m'$, donc m est le PPCM. CQFD.