Chapitre 1 : Divisibilité et congruences dans $\mathbb{Z}$

1. Propriétés de $\mathbb{N}$:

Axiome : « Toute partie de $\mathbb{N}$ non vide admet un plus petit élément ».

Conséquence : Toute partie majorée de $\mathbb{N}$ admet un plus grand élément.

2. Divisibilité dans $\mathbb{Z}$:

2.1. Diviseur et multiple :

Soient a et b deux entiers relatifs.

On dit que **a est un multiple de b** (ou que **b est un diviseur de a**) s'il existe un entier relatif k tel que $\boldsymbol{a = kb}$, on note $b|a$.

On dit encore que **a est divisible par b** ou que **b divise a**.

Propriétés immédiates :

- Tout entier relatif divise 0 mais 0 ne divise aucun entier.
- Tout entier a admet des diviseurs parmi lesquels $-1, 1, -a, a$.
- Les multiples de a sont $\ldots -3a, -2a, -a, 0, a, 2a, 3a, \ldots$, nous ne résisterons pas à la tentation de le noter $a\mathbb{Z}$.
- Tout entier admet un nombre fini de diviseurs (en effet ils sont tous compris entre $-|a|$ et $|a|$, il y en a donc au plus $2|a|$).

2.2. Propriétés de la divisibilité dans $\mathbb{Z}$: (démonstrations à connaître).

Soient a, b et c des entiers relatifs.

- Si a divise b et $b \neq 0$, alors $1 \leq |a| \leq |b|$.
- Si a divise b et b divise c alors a divise c : **transitivité** de la divisibilité.
- Si a divise b, alors pour tout entier relatif k, ka divise kb.
- Si c divise a et b alors c divise $a + b, a - b$, et plus généralement toute **combinaison linéaire** $au + bv$ (u, v dans $\mathbb{Z}$) de a et b.

2.3. Division euclidienne : (démonstration à connaître).

> Soit a un entier relatif et b un entier naturel non nul.
> Il existe un unique couple $(q; r)$ d'entiers relatifs tels que $a = bq + r$ et $0 \leq r < b$.
>
> On nomme **division euclidienne** l'opération qui au couple $(a; b)$ associe le couple $(q; r)$. q est le **quotient** et r le **reste**.

3. PGCD :

3.1. Définition : Soient a et b deux entiers relatifs non nuls. L'ensemble des diviseurs communs à a et b admet un plus grand élément δ, appelé PGCD de a et b. On le note $\boldsymbol{PGCD(a,b)}$ ou $\boldsymbol{PGCD(b,a)}$.

Remarques importantes :

- $b|a$ si et seulement si $PGCD(a,b) = b$. (*démonstration à connaître*).
- Pour démontrer que $PGCD(a,b) = PGCD(m,n)$, on peut par exemple démontrer que l'ensemble des diviseurs communs à a et b est le même que celui de m et n.
- A la calculatrice, on utilise la touche « gcd ».

3.2. Algorithme d'Euclide, calcul du PGCD :

Soient a et b deux entiers naturels non nuls. La suite des divisions euclidiennes :

- de a par b : $a = bq_0 + r_0$;
- de b par r_0 (si $r_0 \neq 0$) : $b = r_0q_1 + r_1$;
- de r_0 par r_1(si $r_1 \neq 0$) : $r_0 = r_1q_2 + r_2$;
- ….
- de r_{n-1} par r_n (si $r_n \neq 0$) : $r_{n-1} = r_nq_{n+1} + r_{n+1}$.

finit par s'arrêter, l'un des restes r_i étant nul.

Le dernier reste non nul est alors le PGCD de a et b.

Démonstration :

Lemme : Soient a, b, q, r des entiers relatifs non nuls tels que $a = bq + r$.
Alors $PGCD(a,b) = PGCD(b,r)$.

Démonstration du lemme : on va montrer que les ensembles de diviseurs des deux couples sont les mêmes.

- Soit d un diviseur commun à a et b. Alors d divise toute combinaison linéaire de a et b, et en particulier $a - bq$. Donc $d|r$. d est donc un diviseur commun à b *et* r.
- Réciproquement, soit d' un diviseur commun à b *et* r. Alors d' divise $a = bq + r$, comme combinaison linéaire de b et r. Donc d' est un diviseur commun à b *et* a.
- Les ensembles des diviseurs communs aux deux couples étant les mêmes, ces deux couples ont le même PGCD.

Démonstration du théorème : Les propriétés liées à la division euclidienne imposent que $b > r_0 > r_1 > \cdots > r_i > \cdots \geq 0$. La suite (r_i) est donc une suite d'entiers strictement décroissante d'entiers naturels, elle est donc finie. Elle possède donc un plus petit élément strictement positif (le dernier reste non nul), notons-le r_n.

D'après le lemme, on a : $PGCD(a,b) = PGCD(b,r_0) = PGCD(r_0,r_1) = \cdots = PGCD(r_{n-2},r_{n-1}) = PGCD(r_{n-1},r_n)$

Or $r_{n-2} = r_{n-1}q_n + r_n$ et $r_{n-1} = r_nq_{n+1}$ (car r_n est le dernier reste non nul). Donc $r_n|r_{n-1}$ et $PGCD(r_{n-1},r_n) = r_n$.

D'où $PGCD(a,b) = r_n$.

3.3. Propriétés du PGCD, nombres premiers entre eux : (DAC)

- L'ensemble des **diviseurs communs à a et b** est l'ensemble des **diviseurs de leur PGCD.**
- Pour tous entiers naturels a, b et k non nuls, on a $\boxed{PGCD(ka, kb) = kPGCD(a, b)}$.

Csq : Pour tous entiers naturels a, b et k non nuls, avec k diviseur de a et b on a $PGCD\left(\frac{a}{k}, \frac{b}{k}\right) = \frac{1}{k}PGCD(a, b)$.

- Les deux entiers relatifs non nuls a et b sont dits **premiers entre eux** ou **étrangers**, lorsque leur PGCD est 1.

> Soit $(a, b) \in \mathbb{Z}^* \times \mathbb{Z}^*$. Si $d = PGCD(a, b)$ alors il existe deux entiers relatifs a'et b' premiers entre eux tels que $a = d \times a'$et $d = d \times b'$.

4. Congruences dans $\mathbb{Z}$:

4.1. Entiers congrus modulo n :

- *Définition :* Soient n un entier naturel supérieur ou égal à 2, a et b deux entiers relatifs. On dit que a et b sont **congrus modulo n** lorsque a et b ont le **même reste** dans la division euclidienne par n.
  On note alors $\boldsymbol{a \equiv b \ (modulo\ n)}$ ou $\boldsymbol{a \equiv b \ (n)}$.

On a par exemple $2012 \equiv 2\ (10)$, $65 \equiv 1\ (8)$, $-9 \equiv 5\ (7)$.

- *De façon immédiate :*
  $a \equiv a\ (n)$ Si $a \equiv b\ (n)$ alors $b \equiv a\ (n)$ Si $a \equiv b\ (n)$ et $b \equiv c\ (n)$ alors $a \equiv c\ (n)$

Cette dernière propriété nous permet d'écrire des « congruences en chaîne » : $21 \equiv 15 \equiv 9 \equiv 3 \equiv -3\ (6)$.

Théorème :

> Soient n un entier naturel supérieur ou égal à 2, a et b deux entiers relatifs.
> Alors $\boldsymbol{a \equiv b\ (n)}$ si et seulement si $\boldsymbol{a - b}$ **est un multiple de** $\boldsymbol{n}$, ie $a - b \equiv 0\ (n)$.

4.2. Propriétés des congruences : compatibilité de la relation de congruence avec l'addition et la multiplication dans $\mathbb{Z}$:

Théorème : R💙C

> Soient n un entier naturel supérieur ou égal à 2, a, b, a' et b' des entiers relatifs tels que :
>
> $$\boldsymbol{a \equiv b\ (n)} \text{ et } \boldsymbol{a' \equiv b'\ (n)}.$$
>
> Alors :
>
> $$\boldsymbol{a + a' \equiv b + b'(n)} \quad \boldsymbol{a\,a' \equiv b\,b'(n)} \text{ et pour tout } k \in \mathbb{N} : \boldsymbol{a^k \equiv b^k(n)}.$$

Exemples :

1- Déterminer les restes successifs dans la division euclidienne par 7 des nombres :
$50^{100}; 100\ ;\ 100^3\ ;\ 50^{100} + 100^{100}$
2- Montrer que pour tout entier naturel n $5^{2n} - 4^n$ est divisible par 7.
3- Démontrer qu'un entier a le même reste dans la division par 9 (ou par 3), que la somme de ses chiffres.