## Introduction :

La théorie des nombres consiste à étudier l'ensemble des entiers relatifs :

$$\mathbb{Z} = \{ \cdots -3, -2, -1, 0, 1, 2, 3 \cdots \}$$

et de son sous ensemble

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$$

appelé l'ensemble des entiers naturels.

Par exemple, considérons la suite suivante d'entiers

$$1 = 0^2 + 1^2$$
$$2 = 1^2 + 1^2$$
$$4 = 0^2 + 2^2$$
$$5 = 1^2 + 2^2$$
$$9 = 0^2 + 3^2$$
$$13 = 2^2 + 3^2$$
$$\vdots$$

Une question naturelle est de se demander quels sont les nombres qui s'écrivent comme somme de deux carrés.
Fermat a trouvé la solution à cette question. Il a démontré par exemple qu'un entier impair $n$ est somme de deux carrés si et seulement si $n-1$ est divisible par 4.

## 1. Principe de récurrence :

On va utiliser la propriété importante de l'ensemble des entiers naturels :

" Toute partie non-vide de $\mathbb{N}$ admet un plus petit élément "

Soit $f(n)$ une propriété dépendante de $n \in \mathbb{N}$.

**Théorème** : S'il existe un entier $n_0$ tels que $f(n_0)$ est vraie si et seulement si pour tout entier $n$, $n \geq n_0$ ; $f(n)$ entraîne $f(n+1)$ alors pour tout entier $n$, $n \geq n_0$ , $f(n)$ est vraie

**Preuve** :

On va effectuer un raisonnement par l'absurde :

notons $A = \{ n \geq n_0 : f(n) \text{ est faux} \}$

et supposons $A$ est non-vide.

Alors $A$ admet un plus petit élément que nous notons $n_1$.

Donc $n_1 - 1 \notin A$ et de plus $n_1 > n_0$ car $f(n_0)$ est vraie

Donc $n_1 - 1 \geq n_0$. Mais $n_1 - 1 \notin A$ signifie que $f(n_1 - 1)$ est vraie. Donc par hypothèse sur $f$, $f(n_1)$ est vraie

d'où la contradiction avec le fait que $n_1 \in A$.

Donc $A$ est vide ∎

Exemple :

On va montrer que

$$\forall n \in \mathbb{N}^*, \quad \sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

On note

$$f(n) : \sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

Pour $n=1$, $\frac{1(1+1)(2+1)}{6} = 1 = 1^2$ d'où $f(1)$ est vraie

Supposons $f(n)$ est vrai. Alors

$$\sum_{i=1}^{n+1} i^2 = \sum_{i=1}^{n} i^2 + (n+1)^2 = \frac{n(n+1)(2n+1)}{6} + (n+1)^2$$

$$= \frac{n+1}{6}\left( n(2n+1) + 6(n+1) \right)$$

$$= \frac{n+1}{6}\left( 2n^2 + 6n + 7 \right)$$

$$= \frac{(n+1)(n+1+1)(2(n+1)+1)}{6}$$

D'où $f(n) \Rightarrow f(n+1)$. D'après le principe de récurrence $f(n)$ est vrai $\forall n \geq 1$.

## 2. Les nombres rationnels :

On note $\mathbb{Q}$ l'ensemble des nombres rationnels. Ils s'écrivent sous la forme $r = \frac{p}{q}$ avec $p \in \mathbb{Z}$ et $q \in \mathbb{N} - \{0\}$.

On a la règle $\frac{a}{b} = \frac{a'}{b'}$ si et seulement si $ab' = ba'$, et on identifie un entier relatif $n$ avec la fraction $\frac{n}{1}$.

L'addition et la multiplication sont définis par :

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \quad \text{et} \quad \frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}$$

## 3. Divisibilité :

**Définition** : Soient $a$ et $b$ deux entiers, on dit que $a$ divise $b$, ou que $b$ est divisible par $a$ s'il existe un entier $q$ tel que $b = aq$.

On dit que $a$ est un diviseur de $b$ ou que $b$ est un multiple de $a$.

On le note $a|b$

**Propriété** :

① Si $a$ et $b$ sont deux entiers avec $b \neq 0$, $b$ divise $a$ si et seulement si la fraction $\frac{a}{b}$ est un entier

② Tous les entiers divisent 0.

③ Un entier $n$ est toujours divisible par $1, -1, n$ et $-n$.

④ Si $a|b$ et $b|c$ alors $a|c$.

⑤ Si $a|b_1, \ldots, a|b_n$, alors $a|b_1 \cdot c_1 + \cdots + b_n c_n$ quels que soient les entiers $c_1, \ldots, c_n$.

⑥ Si $a|b$ et $b \neq 0$, alors $|a| \leq |b|$

⑦ Si $a|b$ et $b|a$ alors $|a| \leq |b|$.

## 4. La division euclidienne :

**Théorème :** Soient $a \in \mathbb{Z}$, $b \in \mathbb{Z} \setminus \{0\}$. Alors il existe un unique couple $(q,r) \in \mathbb{Z} \times \mathbb{N}$ tel que

$$a = bq + r \quad \text{où} \quad 0 \leq r \leq |b| - 1$$

$q$ s'appelle le quotient de la division euclidienne de $a$ par $b$,
$r$ s'appelle le reste de la division euclidienne de $a$ par $b$
Cette opération s'appelle

**Preuve :**
Nous montrons d'abord l'existence du couple $(q,r)$.

- Supposons $b \geq 1$ et définissons $A := \{a - bk, k \in \mathbb{Z}\} \cap \mathbb{N}$,
alors $A \neq \emptyset$ (on peut prendre par exemple $k = -|a|$)
On note $r := \min A$ et $q$ tel que $a - bq = r$.
Montrons que $r < b$.
Raisonnons par l'absurde : Si $r \geq b$, alors

$$0 \leq r - b = a - bq - b = a - (q+1)b$$

donc $(r-b) \in A$ et $r - b < r$ : contradiction avec la minimalité de $r$.
On a par ailleurs $r \geq 0$ par hypothèse car $A \subseteq \mathbb{N}$.

- Si $b \leq -1$, nous appliquons le résultat précédent à $a$ et $|b|$ :

$$a = |b|q + r \quad \text{donc} \quad a = b(-q) + r$$

Pour l'unicité, supposons que $a = bq + r = bq' + r'$
et $0 \leq r, r' \leq |b| - 1$. Alors $b(q - q') = r - r'$.
Donc $|b|\,|q - q'| = |r - r'|$. Or $|r' - r| \leq |b| - 1$, donc $q - q' = 0$
donc $q = q'$ et $r = r'$. ∎