Algèbre et Arithmétique Effectives – 23/09/25 Cours 3

Nombres premiers

Rappel : $\forall n \in \mathbb{Z}$, $1 \mid n$ et $n \mid n$.

Déf : Un **nombre premier** est un entier naturel (≥ 0) qui possède exactement deux diviseurs entiers distincts et positifs : 1 et lui même.

Un entier $n > 1$ qui n'est pas premier est dit **composé**.

Attention : 0 et 1 ne sont pas des nombres premiers (ni des nombres composés).

Théorème fondamental de l'arithmétique

Soit $n \in \mathbb{Z}$, $n \neq 0$.

Alors n peut s'écrire sous la forme

$$n = \pm p_1^{e_1} \cdots p_k^{e_k} = \pm \prod_{i=1}^{k} p_i^{e_i}$$

où $p_1, \dots, p_k$ sont des nombres premiers distincts et $e_1, \dots, e_k$ sont des entiers strictement positifs.

De plus, cette écriture est unique, à l'ordre des facteurs près.

Remarque : Si $n = \pm 1 \Rightarrow k = 0$ (remarquer que un produit vide est égal à 1).

Proposition (Lemme de Gauss)

Soient $a, b, c \in \mathbb{Z}$ tels que $a \mid bc$ et $\text{pgcd}(a, b) = 1$. Alors $a \mid c$.

Dém

Puisque $\text{pgcd}(a,b)=1$, alors $\exists\, u,v \in \mathbb{Z}$ tels que

$$au+bv = 1$$

$$\Downarrow$$

$$c\cdot(au+bv) = c\cdot 1$$

$$acu + bcv$$

$a \mid bc$

On remarque que $a \mid acu$ et $a \mid bcv \Rightarrow$

$\Rightarrow a \mid acu+bcv = c \Rightarrow a \mid c$.

Proposition : Soit p un nombre premier et soient $a,b \in \mathbb{Z}$.
Si $p \mid ab \Rightarrow p \mid a$ ou $p \mid b$.

Dém

Si $p \mid a$ alors l'énoncé est vrai.

Si $p \nmid a$, alors $\text{pgcd}(p,a)=1 \Rightarrow p \mid b$.

$p \mid ab$

Lemme de Gauss

Démonstration du théorème

Sans perte de généralité on peut supposer $n>0$

(si $n<0$, alors $n = -\underbrace{(-n)}_{>0}$)

- **Existence de la factorisation**

On procède par récurrence forte.

Si $n=1$, l'énoncé est vrai (1 est produit de zéro nombres premiers)

Soit $n>1$. On suppose que chaque entier $0<m<n$ peut s'écrire comme produit de nombres premiers.

Si n est premier, alors l'énoncé est vrai.

Si n n'est pas premier, alors n est composé, donc $\exists\ a,b \in \mathbb{Z}$, $0 < a,b < n$ tels que

$$n = ab.$$

Par hypothèse de récurrence, a et b s'écrivent comme produit de puissances de nombres premiers, donc cela vaut aussi pour n.

- **Unicité de la factorisation**

On veut montrer que si

$$n = p_1 \cdots p_s = q_1 \cdots q_t$$

où p_i, q_j sont des nombres premiers pas forcément distincts, alors $s = t$ et $(p_1, \dots, p_s)$ est une permutation de $(q_1, \dots, q_t)$.

On procède par récurrence sur s.

Si $s = 0 \Rightarrow n = 1 \Rightarrow t = 0$ et l'énoncé est vrai

Supposons que l'énoncé est vrai pour $s-1$.
On montre qu'il est vrai pour s aussi.

On sait que

$$n = p_1 \cdots p_s = q_1 \cdots q_t \qquad (*)$$

On remarque que $p_1 \mid p_1 \cdots p_s$ et $p_1 \cdots p_s = q_1 \cdots q_t$

$\Rightarrow p_1 \mid q_1 \cdots q_t \Rightarrow \exists\ 1 \le j \le t$ tel que

↑ Proposition précédente

$p_1 \mid q_j \Rightarrow p_1 = q_j$.

↑ p_1, q_j nombres premiers

Donc, en divisant $(*)$ à gauche par p_1 et à

droite par q_j, on obtient :

$$\underbrace{p_2 \cdots p_s}_{s-1 \text{ termes}} = q_1 \cdots q_{j-1}\, q_{j+1} \cdots q_t$$

Par hypothèse de récurrence $s-1 = t-1$ et $(p_2, \dots, p_s)$ est une permutation de $(q_1, \dots, q_{j-1}, q_{j+1}, \dots q_t)$

Donc $s=t$ et $(p_1, \dots, p_s)$ est une permutation de $(q_1, \dots, q_t)$.

Entiers modulo n

Dans les applications en cryptographie et théorie des codes on travaille souvent avec des sous-ensembles finis de $\mathbb{Z}$.

Rappels : Relation d'équivalence

Def : Soit A un ensemble.
Une relation binaire $\sim_R$ sur A est un sous-ensemble R de $A \times A$.

Si $(a,b) \in R$, on note $a \sim_R b$

Une relation binaire $\sim$ sur A est une relation d'équivalence si :

1) $\sim$ est réflexive : $a \sim a$, $\forall\ a \in A$

2) $\sim$ est symétrique : $\forall\ a,b \in A$, si $a \sim b$ alors $b \sim a$

3) $\sim$ est transitive : $\forall\ a,b,c \in A$, si $a \sim b$ et $b \sim c$, alors $a \sim c$.

Exemple : $A = \{$étudiants en L3HI$\}$

$\forall\ x,y \in A$, $x \sim y \iff$ x et y sont dans le même groupe de TD.

Déf : Soit $\sim$ une relation d'équivalence sur un ensemble A. $\forall\, x \in A$, la <u>classe d'équivalence</u> de x modulo $\sim$ est le sous-ensemble de A

$$\overline{x} = [x]_\sim = \{ y \in A : x \sim y \} \subseteq A$$

Chaque élément de $[x]$ est appelé un <u>représentant</u> de $[x]$.

L'ensemble

$$A/\sim \;=\; \{ [x] : x \in A \} \neq A$$

des classes d'équivalence de A modulo $\sim$ est dit <u>ensemble quotient</u> de A par $\sim$.

Exemple : $A = \{$étudiants en L3MI$\}$

$\forall\, x, y \in A$, $\quad x \sim y \iff x$ et y sont dans le même groupe de TD.

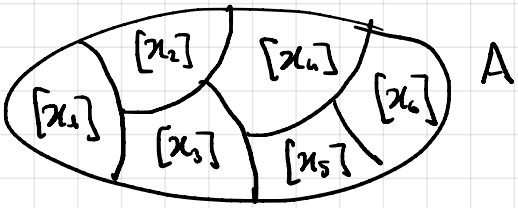
$$A/\sim \;=\; \{ \text{groupe 1}, \text{groupe 2} \}$$

$$[\text{Mel.}] = \text{groupe 1}$$

$$[\text{Gas.}] = \text{groupe 2},$$

Remarque : Si $\sim$ est une relation d'équivalence sur un ensemble non vide A, alors

$A/\sim$ est une partition de A.



En TD vous allez montrer que la relation suivante est une relation d'équivalence :

Soit $n \in \mathbb{Z}_{>0}$. Soient $a, b \in \mathbb{Z}$

$$a \sim_n b \iff n \mid a-b.$$

Def : Soit $n \in \mathbb{Z}_{>0}$
Soient $a, b \in \mathbb{Z}$

On dit que <u>a est congruent à b mod n</u>
et on écrit

$$a \equiv b \pmod{n}$$

si $n \mid a-b$.

Le nombre n est appelé le <u>module</u> de la congruence.

<u>Exemples</u>

1) $n = 1$. On note $\sim_1$ la relation de congruence modulo 1.
$3 \equiv 5 \mod 1$? Oui car $1 \mid 3-5$.

$$[0]_{\sim_1} = \{a \in \mathbb{Z} : a \equiv 0 \mod 1\} = \{a \in \mathbb{Z} : 1 \mid a\} = \mathbb{Z}$$

$\uparrow$ $\forall a \in \mathbb{Z},\ 1 \mid a$

$$\mathbb{Z}/_{\sim_1} = \{[0]_{\sim_1}\} = \{[2025]_{\sim_1}\}$$

2) $n = 2$. On note $\sim_2$ la relation de congruence modulo 2.
$a \equiv b \mod 2 \iff 2 \mid a-b$

$$[0]_{\sim_2} = \{a \in \mathbb{Z} : a \equiv 0 \mod 2\} = \{a \in \mathbb{Z} : 2 \mid a\} = \{\text{entiers pairs}\}$$

$$[1]_{\sim_2} = \{a \in \mathbb{Z} : a \equiv 1 \mod 2\} = \{a \in \mathbb{Z} : 2 \mid a-1\} =$$

$$= \{a \in \mathbb{Z} : \exists\, k \in \mathbb{Z} \text{ t.q. } a-1 = 2k\}$$
$$= \{a \in \mathbb{Z} : \exists\, k \in \mathbb{Z} \text{ t.q. } a = 2k+1\}$$
$$= \{\text{entiers impairs}\}$$

$$\mathbb{Z}/_{\sim_2} = \{[0]_{\sim_2}, [1]_{\sim_2}\}$$

Def : L'ensemble des classes d'équivalence pour la relation de congruence modulo n est noté

$$\mathbb{Z}/_{n\mathbb{Z}} := \mathbb{Z}/_{\sim_n}$$

Notation : $n\mathbb{Z} := \{nk,\ k \in \mathbb{Z}\}$.