

Nombres premiers

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

Déf: Un entier $p \geq 2$ est dit premier si ses seuls diviseurs positifs sont 1 et p .

Un entier $n \geq 2$ qui n'est pas premier est dit composé.

Attention: 0 et 1 ne sont pas de nombres premiers, ni des nombres composés.

Remarque: Si $n \geq 2$ n'est pas un nombre premier, alors il existe $a \in \mathbb{Z}, 1 < a < n$ tel que $a|n$.

En TD nous avons montré les propositions suivantes. Pour compléter le cours, nous les redémontrons ci-dessous.

Proposition 1 (Lemme de Gauss)

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

Dém

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

$$au + bv = 1$$



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

$$\text{" } \Downarrow \text{"}$$
$$acu + bcv$$

$a|bc$



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

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

Proposition 2: Soit p un nombre premier et soient $a, b \in \mathbb{Z}$.
Si $p|ab \Rightarrow p|a$ ou $p|b$.

Dém

- Si $p|a$ alors l'énoncé est vrai.
 - Si $p \nmid a$, alors $\text{pgcd}(p, a) = 1$ (car les seuls diviseurs de p sont 1 et p).
- Donc $p|ab$ et $\text{pgcd}(p, a) = 1 \xrightarrow{\text{Lemme de Gauss}} p|b$.

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.

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 : puisqu'un produit vide est égal à 1, 1 est produit de zéro nombres premiers ($k=0$).

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 $\exists a, b \in \mathbb{Z}, 1 < a, b < n$ 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 soit que

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

On remarque que $p_1 \mid p_1 \cdots p_s$ et $p_1 \cdots p_s = q_1 \cdots q_t$
 $\Rightarrow p_1 \mid q_1 \cdots q_t \Rightarrow \exists 1 \leq j \leq t$ 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 :

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

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 : Relations 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 : $A = \{ \text{étudiants en L3MI} \}$

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

Def. Soit $\sim$ une relation d'équivalence sur un ensemble A
 $\forall x \in A$, la classe d'équivalence de x
 modulo $\sim$ est le sous-ensemble de A

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

Chaque élément de $[x]$ est appelé un représentant de $[x]$.

L'ensemble

ensemble de sous-ensemble de A

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

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

Exemple : $A = \{ \text{étudiants en L3M1} \}$

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

$$[Em.]_{\sim} = \{ Em., Eug., Alp., \dots \} = [Eug.]_{\sim}$$

$$[Cel.]_{\sim} = \{ Cel., Cle., \dots \} = [Cle.]_{\sim}$$

$$A/\sim = \{ [Em.]_{\sim}, [Cel.]_{\sim} \} = \{ \text{groupe 1, groupe 2} \}$$

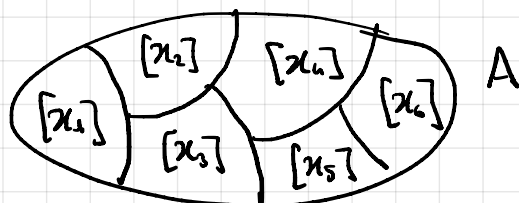
Remarque : Si $\sim$ est une relation d'équivalence sur
 un ensemble non vide A , alors

$A/\sim = \{ A_i \}_{i \in I}$ est une partition de A , c'est-à-dire :

$$1) A_i \neq \emptyset, \forall i \in I$$

$$2) \bigcup_{i \in I} A_i = A$$

$$3) \forall i \neq j, A_i \cap A_j = \emptyset.$$



$$A_i = [x_i]$$

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

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

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

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

On dit que a est congruent à b mod n
et on écrit

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

si $n \mid a-b$.

Le nombre n est appelé le modulo de la congruence.

Exemples

1) $\boxed{n=1}$. On note $\sim_1$ la relation de congruence modulo 1.

$$a \sim_1 b \iff a \equiv b \pmod{1} \iff 1 \mid (a-b).$$

$$\begin{aligned} [0]_{\sim_1} &= \{a \in \mathbb{Z} : a \equiv 0 \pmod{1}\} = \\ &= \{a \in \mathbb{Z} : 1 \mid a\} = \mathbb{Z} \end{aligned}$$

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

$$\mathbb{Z}/\sim_1 = \{[0]_{\sim_1}\} = \{[2026]_{\sim_1}\}$$

2) $\boxed{n=2}$. On note $\sim_2$ la relation de congruence modulo 2.

$$a \sim_2 b \iff a \equiv b \pmod{2} \iff 2 \mid a-b$$

$$\begin{aligned} [0]_{\sim_2} &= \{a \in \mathbb{Z} : a \equiv 0 \pmod{2}\} = \\ &= \{a \in \mathbb{Z} : 2 \mid a\} = \{\text{entiers pairs}\} \end{aligned}$$

$$\begin{aligned}
[1]_{\mathbb{N}_2} &= \{a \in \mathbb{Z} : a \equiv 1 \pmod{2}\} = \\
&= \{a \in \mathbb{Z} : 2 \mid a-1\} = \\
&= \{a \in \mathbb{Z} : \exists k \in \mathbb{Z} \text{ t.q. } a-1 = 2k\} \\
&= \{a \in \mathbb{Z} : \exists k \in \mathbb{Z} \text{ t.q. } a = 2k+1\} \\
&= \{\text{entiers impairs}\}
\end{aligned}$$

$$\mathbb{Z}/\mathbb{N}_2 = \{[0]_{\mathbb{N}_2}, [1]_{\mathbb{N}_2}\} = \{\text{pairs}\}, \{\text{impairs}\}$$