

# Khôlles de Mathématiques - Semaine 18

Hugo Vangilluwen, Kylian Boyet

20 Février 2024

## 1 L'ensemble des nombres premiers est infini

*Démonstration.* Notons l'ensemble des nombres premiers  $\mathcal{P} = \{n \in \mathbb{N} \mid |\mathcal{D}(n) \cup \mathbb{N}| = 2\}$ . Par l'absurde, supposons que  $\mathcal{P}$  est fini.

Posons  $m = 1 + \prod_{p \in \mathcal{P}} p \in \mathbb{N}$ .

Comme  $2 \in \mathcal{P}$ ,  $m \geq 2$ . Donc  $m$  admet un diviseur premier,  $\exists q \in \mathcal{P} : q \mid m$ . Donc  $q \wedge m = q$ .

Par ailleurs,  $m = 1 + q \left( \prod_{\substack{p \in \mathcal{P} \\ p \neq q}} p \right)$ . Donc  $m - q \left( \prod_{\substack{p \in \mathcal{P} \\ p \neq q}} p \right) = 1$ . D'après le théorème de Bézout,

$q \wedge m = 1$ .

Donc  $q = 1$  ce qui est une contradiction avec  $q \in \mathcal{P}$ .  $\square$

## 2 Caractérisation de la valuation $p$ -adique

Soit  $n \in \mathbb{N}^*$ ,  $p \in \mathcal{P}$ ,  $k_0 \in \mathbb{N}$ .

$$\nu_p(n) = k_0 \iff \exists m \in \mathbb{Z} : \begin{cases} n = p^{k_0} \\ m \wedge p = 1 \end{cases} \quad (1)$$

*Démonstration.*  $\implies$  Supposons que  $\nu_p(n) = k_0$ .

Par définition de la valuation  $p$ -adique,  $p^{\nu_p(n)} \mid n$  donc  $p^{k_0} \mid n$ . Notons  $m \in \mathbb{Z}$  le quotient de la division euclidienne de  $n$  par  $p^{k_0}$ . Nous avons  $n = p^{k_0}m$ .

Comme  $m \wedge p \in \mathcal{D}(p) \cap \mathbb{N}$ ,  $m \wedge p \in \{1, p\}$ . Par l'absurde, supposons que  $m \wedge p = p$ .

$$\begin{aligned} p \mid m &\implies \exists m' \in \mathbb{Z} : m = pm' \\ &\implies \exists m' \in \mathbb{Z} : n = pp^{k_0}m' = p^{k_0+1}m' \\ &\implies k_0 + 1 \in \{k \in \mathbb{N} \mid p^k \mid n\} \\ &\implies k_0 + 1 \leq \max \{k \in \mathbb{N} \mid p^k \mid n\} = \nu_p(n) = k_0 \end{aligned}$$

Ce qui est une contradiction donc  $m \wedge p = 1$ .

$$\iff \text{Supposons } \exists m \in \mathbb{Z} : \begin{cases} n = p^{k_0} \\ m \wedge p = 1 \end{cases}$$

Par définition de la valuation  $p$ -adique,  $p^{\nu_p(n)} \mid n$  donc  $p^{\nu_p(n)} \mid p^{k_0}m$ . Or  $m \wedge p = 1$  donc  $m \wedge p^{\nu_p(n)} = 1$ . D'après le théorème de Gauss,  $p_{\nu_p(n)} \mid p^{k_0}$ . Donc  $\exists \alpha \in \mathbb{Z} : \alpha p_{\nu_p(n)} = p^{k_0}$

$$\begin{aligned} \alpha p_{\nu_p(n)} = p^{k_0} &\implies p^{k_0} - \alpha p_{\nu_p(n)} = 0 \\ &\implies p^{k_0} (1 - \alpha p^{\nu_p(n)-k_0}) = 0 \text{ car } k_0 \leq \nu_p(n) \\ &\implies \alpha p^{\nu_p(n)-k_0} = 1 \text{ car } \mathbb{Z} \text{ est int\`egre} \\ &\implies p^{\nu_p(n)-k_0} \in \mathcal{D}(1) \cap \mathbb{N} \\ &\implies p^{\nu_p(n)-k_0} = 1 \\ &\implies \nu_p(n) - k_0 = 0 \\ &\implies \nu_p(n) = k_0 \end{aligned}$$

$\square$

### 3 Caractérisation de $a|b$ par les valuations $p$ -adiques et preuve de leur propriété de morphisme.

*Démonstration.* Montrons que :  $a|b \iff \forall p \in \mathcal{P}, \nu_p(a) \leq \nu_p(b)$ .

Premièrement, montrons que la valuation  $p$ -adique est un morphisme de  $(\mathbb{Z}^*, \times)$  dans  $(\mathbb{N}, +)$ .

Soient de tels entiers relatifs  $a, b$ .

$$\exists m, n \in (\mathbb{Z}^*)^2 : ((a = p^{\nu_p(a)}m) \wedge (m \wedge p = 1)) \wedge ((b = p^{\nu_p(b)}n) \wedge (n \wedge p = 1)),$$

donc  $ab = p^{\nu_p(a)+\nu_p(b)}mn$  et  $mn \wedge p = 1$ , par la réciproque de la caractérisation des valuations  $p$ -adiques :

$$\nu_p(ab) = \nu_p(a) + \nu_p(b).$$

Prouvons le sens réciproque de la susdite caractérisation. Supposons le membre de droite.

D'après le théorème de décomposition en facteurs premiers,

$$|b| = \prod_{p \in \mathcal{P}} p^{\nu_p(b)} = \prod_{p \in \mathcal{P}} p^{\nu_p(a)} (p^{\nu_p(b)-\nu_p(a)}) = \prod_{p \in \mathcal{P}} p^{\nu_p(a)} \prod_{p \in \mathcal{P}} p^{\nu_p(b)-\nu_p(a)} = |a| \prod_{p \in \mathcal{P}} p^{\nu_p(b)-\nu_p(a)},$$

la première manipulation se justifie par hypothèse et la seconde peut se justifier par le calcul.

Ainsi,  $|a||b|$  donc  $a|b$ .

Prouvons le sens direct. Supposons le membre de gauche.

Soit  $p \in \mathcal{P}$ . Il existe  $k \in \mathbb{Z}$  tel que  $ak = b$  car  $a|b$ . Ainsi,

$$\nu_p(b) = \nu_p(ak) = \nu_p(a) + \nu_p(k) \geq \nu_p(a).$$

Ce qui suffit. □

### 4 Expression du pgcd et du ppcm à partir des décomposition en facteurs premiers de $a$ et $b$ .

Le pgcd comme produit des  $p$  à la puissance du minimum des  $\nu_p$  et le ppcm comme le produit des  $p$  à la puissance du maximum des  $\nu_p$ .

*Démonstration.* Prouvons la formule du pgcd et déduisons-en la formule du ppcm.

Soient  $(a, b) \in (\mathbb{Z}^*)^2$ . Soit  $p \in \mathcal{P}$ . Il faut et il suffit de montrer que  $\nu_p(a \wedge b) = \min(\nu_p(a), \nu_p(b))$  pour obtenir le résultat. On a  $a \wedge b|a$  et  $a \wedge b|b$  donc d'après la caractérisation de la divisibilité par les valuations  $p$ -adiques,  $\nu_p(a \wedge b) \leq \nu_p(a)$  et  $\nu_p(a \wedge b) \leq \nu_p(b)$  donc  $\nu_p(a \wedge b) \leq \min(\nu_p(a), \nu_p(b))$ . Posons  $m = \min(\nu_p(a), \nu_p(b))$ . On a

$$|a| = \prod_{q \in \mathcal{P}} q^{\nu_q(a)} = p^m \left( (p^{\nu_p(a)-m}) \prod_{q \in \mathcal{P} \setminus \{p\}} q^{\nu_q(a)} \right),$$

car par définition,  $m \leq \nu_p(a)$ , donc  $p^m|a$ , on montrerait de même que  $p^m|b$ , donc par définition,  $p^m|a \wedge b$ , donc une nouvelle fois en appliquant la caractérisation de la divisibilité par les valuations  $p$ -adiques,  $m \leq \nu_p(a \wedge b)$ . Finalement,  $\nu_p(a \wedge b) = m$ .

On en déduit la formule du ppcm :

$$|a||b| = (a \wedge b)(a \vee b) \implies a \vee b = \prod_{p \in \mathcal{P}} p^{\nu_p(a)+\nu_p(b)-\min(\nu_p(a), \nu_p(b))} = \prod_{p \in \mathcal{P}} p^{\nu_p \max(\nu_p(a), \nu_p(b))}$$

□

### 5 Pour $p$ premier, $(a+b)^p \equiv a^p + b^p \pmod{p}$ , en déduire le petit Th. de Fermat (2 versions), expression du résultat dans $\mathbb{Z}/p\mathbb{Z}$ .

Petit Th. de Fermat :

- (i)  $\forall a \in \mathbb{Z}, a^p \equiv a \pmod{p}$   
 $\forall x \in \mathbb{Z}/p\mathbb{Z}, x^p = x$
- (ii)  $\forall a \in \mathbb{Z}, p \nmid a, \implies a^{p-1} \equiv 1 \pmod{p}$   
 $\forall x \in \mathbb{Z}/p\mathbb{Z}, x^{p-1} = 1$

*Démonstration.* Soient  $a, b$  de tels entiers relatifs et soit  $p$  un nombre premier. Calculons,

$$(a+b)^p = \sum_{k=0}^p \binom{p}{k} a^{p-k} b^k = a^p + b^p + \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k} b^k \equiv a^p + b^p \pmod{p},$$

car  $\forall k \in \llbracket 1, p-1 \rrbracket$ ,  $p \mid \binom{p}{k}$  (élémentaire), d'où le résultat.

Dans  $\mathbb{Z}/p\mathbb{Z}$ , ce résultat s'énonce comme suit :

$$\forall (x, y) \in \mathbb{Z}/p\mathbb{Z}^2, (x+y)^p = x^p + y^p.$$

En guise d'application, démontrons le petit Th. de Fermat énoncé plus haut.

Démonstration du (i). Considérons le prédicat  $\mathcal{P}(\cdot)$  défini sur  $\mathbb{N}$  par :

$$\mathcal{P}(a) : "a^p \equiv a \pmod{p}."$$

Initialisation : Pour  $a = 0$ , rien à faire, donc  $\mathcal{P}(0)$  est vrai.

Hérédité : Soit  $a \in \mathbb{N}$  tel que  $\mathcal{P}(a)$ . Calculons,

$$(a+1)^p \equiv a^p + 1 \pmod{p} \stackrel{\mathcal{P}(a)}{\equiv} a + 1 \pmod{p},$$

donc  $\mathcal{P}(a+1)$  vrai.

Par Th. de récurrence sur  $\mathbb{N}$ ,  $\mathcal{P}(a)$  est vrai pour tout  $a \in \mathbb{N}$ .

Il faut maintenant étendre le résultat à  $\mathbb{Z}$ . Soit  $p \in \mathcal{P} \setminus \{2\}$ , ainsi  $p$  est impair. Soit  $a \in \mathbb{Z} \setminus \mathbb{N}$ . Calculons,

$$a^p \equiv (-|a|)^p \pmod{p} \equiv -|a|^p \pmod{p} \stackrel{\text{Th. de Fermat pour } a \leftarrow |a|}{\equiv} -|a| \pmod{p} \equiv a \pmod{p}.$$

Si  $p = 2$ ,  $a^2 \equiv |a|^2 \pmod{2} \equiv |a| \pmod{2} \equiv -|a| \pmod{2} \equiv a \pmod{2}$ .

Le (ii), soit  $a \in \mathbb{Z}$  tel que  $p \nmid a$ .

$$(p \nmid a) \wedge (p \in \mathcal{P}) \implies p \wedge a = 1,$$

d'après le (i),  $p \mid a^p - a \implies p \mid a(a^{p-1} - 1) \stackrel{\text{Th. de Gauss}}{\implies} p \mid a^{p-1} - 1 \implies a^{p-1} \equiv 1 \pmod{p}$ .

Les écritures dans  $\mathbb{Z}/p\mathbb{Z}$  ne posent pas de problème.s, ce qui conclut.  $\square$

## 6 $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si $n$ est premier.

*Démonstration.* Montrons le sens réciproque, supposons  $n \in \mathcal{P}$ .

Soit  $x \in \mathbb{Z}/n\mathbb{Z}$  tel que  $x \neq \bar{0}$ .

$\exists a \in \llbracket 0, p-1 \rrbracket : c = \bar{a}, I = \llbracket 0, p-1 \rrbracket$  étant un système de représentant des classes.

Comme  $a \in I$ ,  $n \nmid a$ , or  $n \in \mathcal{P}$ , donc  $n \wedge a = 1$ . Par Bezout, il existe  $u, v \in \mathbb{Z}$  tels que  $au + nv = 1$ , donc  $u$  est l'inverse de  $a$  modulo  $n$  donc  $a \in \mathbb{Z}/n\mathbb{Z}^\times$ , dès lors, tout élément non nul de  $\mathbb{Z}/n\mathbb{Z}$  est inversible, or c'est un anneau commutatif, donc c'est un corps.

Montrons le sens direct en raisonnant par contraposition, supposons  $n \notin \mathcal{P}$ .

Comme  $n$  n'est pas premier et est plus grand que 2, il admet un diviseur,  $d$ , dans  $I \setminus \{0, 1\} = J$ . Notons  $d'$  le quotient de la division euclidienne de  $n$  par  $d$ , on a alors  $a = dd'$  et  $d' \in J$ . Donc  $\bar{d}\bar{d}' = \bar{0}$  et comme  $d, d' \in J$ , on a  $d, d' \neq 0$ , donc  $\bar{d}$  est un diviseur de zéro de  $\mathbb{Z}/n\mathbb{Z}$ , donc  $\bar{d}$  est un élément non nul de  $\mathbb{Z}/n\mathbb{Z}$  non inversible, donc  $\mathbb{Z}/n\mathbb{Z}$  n'est pas un corps. En contraposant ce que nous venons de démontrer on a le résultat. Ce qui conclut.  $\square$

## 7 Les éléments inversibles d'un anneau $A$ forment un groupe multiplicatif noté $(A^\times, \times)$

*Démonstration.* Soit  $(A, +, \times)$  un anneau.

Un élément inversible (ou unité) est un élément de  $A$  symétrisable pour la loi  $\times$ . Posons l'ensemble des éléments inversibles  $A^\times = \{a \in A \mid \exists b \in A : a \times b = b \times a = 1_A\}$ .

- ★ Montrons que la LCI  $\times$  se restreint bien à  $A^\times$  en un LCI  $\times_{A^\times}$ .  
Soient  $(a_1, a_2) \in A^{\times 2}$ . Par définition de  $A^\times$ ,  $\exists (b_1, b_2) \in A^2 : a_1 \times b_1 = b_1 \times a_1 = 1_A$  et  $a_2 \times b_2 = b_2 \times a_2 = 1_A$ .

$$\begin{aligned} (a_1 \times a_2) \times (b_2 \times b_1) & \underbrace{=}_{\text{loi associative}} a_1 \times \underbrace{a_2 \times b_2}_{= 1_A} \times b_1 = a_1 \times b_1 = 1_A \\ (b_2 \times b_1) \times (a_1 \times a_2) & \underbrace{=}_{\text{loi associative}} b_2 \times \underbrace{b_1 \times a_1}_{= 1_A} \times a_2 = b_2 \times a_2 = 1_A \end{aligned}$$

Donc  $(a_1 \times a_2) \in A^\times$ .

- ★ La loi  $\times$  est associative donc la loi  $\times_{A^\times}$  l'est aussi.
- ★  $1_A$  vérifie  $1_A \times 1_A = 1_A$  donc  $1_A \in A^\times$ .  
De plus,  $\forall a \in A^\times, 1_A \times_{A^\times} a = a \times_{A^\times} 1_A = a$  donc  $\times_{A^\times}$  admet  $1_A$  comme élément neutre.
- ★ Soit  $a \in A^\times$ . Par définition de  $A^\times$ ,  $\exists b \in A : a \times b = b \times a = 1_A$ .  
D'où  $b \in A^\times$ . En pensant les égalités ci-dessus dans  $A^\times$ ,

$$a \times_{A^\times} b = b \times_{A^\times} a = 1_A$$

Donc  $a$  est inversible dans  $A^\times$ .

Ainsi,  $(A^\times, \times_{A^\times})$  est un groupe. □

## 8 L'image directe par un morphisme d'anneau d'un sous-anneau de l'anneau de départ est un sous anneau de l'anneau d'arrivée. De même pour l'image réciproque.

*Démonstration.* Soient  $(A, +, \times)$  et  $(B, +, \times)$  deux anneaux et  $f : A \rightarrow B$  un morphisme d'anneau. Soit  $A'$  un sous-anneau de  $A$ . Montrons que  $f(A')$  est un sous-anneau de  $B$ .

- ★ Par définition de  $f$ ,  $f(A') \subset B$  et  $(B, +, \times)$  est un anneau.
- ★ Soient  $(u, v) \in f(A')^2$ . Alors  $\exists (a, b) \in A'^2 : f(a) = u$  et  $f(b) = v$ .  $f$  est un morphisme d'anneau donc un morphisme de groupe de  $(A, +)$  dans  $(B, +)$  donc

$$u - v = f(a) - f(b) = f(a - b)$$

Comme  $A'$  est un sous-anneau,  $a - b \in A'$ . Donc  $u - v \in f(A')$ .

De même,  $f$  est un morphisme d'anneau donc un morphisme de monoïde de  $(A, \times)$  dans  $(B, \times)$  donc

$$u \times v = f(a) \times f(b) = f(a \times b)$$

Comme  $A'$  est un sous-anneau,  $a \times b \in A'$ . Donc  $u \times v \in f(A')$ .

- ★  $f$  est un morphisme d'anneau donc  $1_B = f(1_A)$ . Or  $A'$  est un sous-anneau donc  $1_A \in A'$ . D'où  $1_B \in f(A')$ .

Soit  $B'$  un sous-anneau de  $B$ . Montrons que  $f^{-1}(B')$  est un sous-anneau de  $A$ .

- ★ Par définition de  $f$ ,  $f^{-1}(B') \subset A$  et  $(A, +, \times)$  est un anneau.
- ★ Soient  $(a, b) \in f^{-1}(B')^2$ .  $f$  est un morphisme d'anneau donc un morphisme de groupe de  $(A, +)$  dans  $(B, +)$  donc

$$f(a - b) = \underbrace{f(a)}_{\in B'} - \underbrace{f(b)}_{\in B'} \in B'$$

Donc  $a - b \in f^{-1}(B')$ .

De même,  $f$  est un morphisme d'anneau donc un morphisme de monoïde de  $(A, \times)$  dans  $(B, \times)$  donc

$$f(ab) = \underbrace{f(a)}_{\in B'} \underbrace{f(b)}_{\in B'} \in B'$$

Donc  $ab \in f^{-1}(B')$ .

- ★  $f$  est un morphisme d'anneau donc  $1_B = f(1_A)$ . Or  $B'$  est un sous-anneau donc  $1_B \in B'$ . D'où  $1_A \in f^{-1}(B')$ .

□