Compléments sur les anneaux et les idéaux, arithmétique

Lundi 19 janvier 2026

Table des matières

Table des matières

1. Compléments sur les produits d'anneaux

1.1. Théorème chinois

1.1. Théorème chinois

Exercice 1

Si on distribue équitablement n bonbons à 4 enfants, il en reste 3, mais si on les distribue équitablement aux 3 enfants les plus sages, il en reste 1. Combien y a t-il de bonbons ?

Theoreme 1

(des restes chinois) Soient $m, n \in \mathbb{N}$ tels que $m \wedge n = 1$. Alors on a un isomorphisme d'anneaux $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Remarques :

- . . .

Méthode :

. . .

Exercice 2

Résoudre le système de congruence : $\begin{cases} x \equiv 2\ [3] \\ x \equiv 3\ [5] \end{cases}$.

Remarques :

- ...

Exercice 3

(Sun Zi 450) Soit des objets dont on ignore le nombre. En les comptant 3 par 3 il en reste 2, en les comptant 5 par 5, il en reste 3 et en les comptant 7 par 7, il en reste 2. Combien y a-t-il d'objets ?

1.2. Indicatrice et théorème d'Euler

1.2. Indicatrice et théorème d'Euler

Rappel :

...

Definition 1

On appelle *indicatrice d'Euler* l'application $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ qui à tout n associe le nombre d'entiers de $[\![0, n-1]\!]$ premiers avec n.

Proposition 1

$\varphi(1) = 1$ et pour tout $n \geqslant 2$: $\varphi(n) = \mathrm{card}\left((\mathbb{Z}/n\mathbb{Z})^\times\right)$.

Exercice 4

Déterminer les valeurs de $\varphi(n)$ pour $n \in [\![1, 12]\!]$.

1.2. Indicatrice et théorème d'Euler

Lemme

Si m et n sont premiers entre eux, les groupes multiplicatifs $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$ et $(\mathbb{Z}/mn\mathbb{Z})^\times$ sont isomorphes.

Proposition 2

- Si m et n sont premiers entre eux, $\varphi(mn) = \varphi(m)\varphi(n)$.
- Si p est un nombre premier, $\varphi(p^k) = p^{k-1}(p-1)$ pour tout $k \in \mathbb{N}^*$.

Proposition 3

Soit $n \geqslant 2$ avec $n = p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k}$ sa décomposition en produit de facteurs premiers (les p_i deux à deux distincts et $\alpha_i > 0$). Alors

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\cdots\left(1 - \frac{1}{p_k}\right)$$

Remarques :

- ...

Exercice 5

Calculer $\varphi(120)$.

1.2. Indicatrice et théorème d'Euler

Theoreme 2

(d'Euler) Soit $n \geqslant 2$ un entier naturel et soit $a \in \mathbb{Z}$ premier avec n. Alors $a^{\varphi(n)} \equiv 1\ [n]$.

Remarque :

$\ldots$

Theoreme 3

(de Fermat) Soit p premier et soit $a \in \mathbb{Z}$ non divisible par p. Alors $a^{p-1} \equiv 1\ [p]$.

Corollaire 1

(de Fermat bis) Si p est premier et $a \in \mathbb{Z}$, $a^p \equiv a\ [p]$.

Exercice 6

Déterminer les élements inversibles de l'algèbre $\mathcal{M}_2(\mathbb{F}_2)$ et montrer que $GL_2(\mathbb{F}_2) \simeq S_3$.

Table des matières

2. Opérations sur les idéaux

2.0.

Proposition 4

Toute intersection d'idéaux de A est un idéal de A.

Definition 2

Soit P une partie de A. On appelle *idéal engendré* par P l'intersection de tous les idéaux de A contenant P. On le note (P).

Definition 3

Soient I et J deux idéaux de A. On appelle *somme* de I et J l'ensemble :

$$I + J = \{a + b, (a, b) \in I \times J\}$$

Proposition 5

$I + J$ est l'idéal engendré par $I \cup J$.

Remarques :

- On a $I + J = J + I$.
- On montre facilement $(I + J) + K = I + (J + K)$, ce qu'on note $I + J + K$.
- Plus généralement, $I_1 + \cdots + I_n = \left(\bigcup_{k=1}^{n} I_k\right)$

Definition 4

Soit $a \in A$. on appelle *idéal engendré* par a l'idéal engendré par $\{a\}$. On le note (a).
Un idéal engendré ainsi par un seul élément est appelé un idéal *principal*.

Proposition 6

Soit $a \in A$. L'idéal (a) est l'ensemble

$$aA = \{ax,\ x \in A\}$$

On peut aussi le noter Aa.

Remarque :

Plus généralement :

$$(\{a_1, \ldots, a_n\}) = (a_1) + \cdots + (a_n) = \{a_1 x_1 + \cdots + a_n x_n,\ (x_1, \ldots, x_n) \in A^n\}$$

2.0.

Definition 5

On dit que l'anneau commutatif A est *principal* lorsque :

- A est intègre
- Tout idéal de A est principal, c'est-à-dire engendré par un seul élément.

Theoreme 4

- L'anneau $\mathbb{Z}$ est principal.
- L'anneau $\mathbb{K}[X]$ est principal.

Remarque :

Unicité des générateurs ?

Table des matières

3. Compléments d'arithmétique dans $\mathbb{Z}$ et $\mathbb{K}[X]$

3.1. PGCD et PPCM dans les anneaux principaux

3.1. PGCD et PPCM dans les anneaux principaux

Definition 6

Soit A un anneau principal et $a_1, \dots, a_n \in A$, avec $n \geqslant 2$.

- On appelle pgcd de $a_1, \dots, a_n$ tout générateur de l'idéal $(a_1) + \cdots + (a_n)$.
- On appelle ppcm de $a_1, \dots, a_n$ tout générateur de l'idéal $(a_1) \cap \cdots \cap (a_n)$.

Remarque :

Identité de Bézout ?

Exercice 7

a) Montrer que a est un pgcd de $a_1, \ldots, a_n$ **ssi**

- $\forall k \in [\![1, n]\!],\ a | a_k$
- $\forall b \in a,\ (\forall k \in [\![1, n]\!],\ b | a_k) \Rightarrow b | a$

b) Énoncer et démontrer un énoncé similaire pour le ppcm.

Remarque :

Borne inférieure et supérieure ?

Exemple :

Interprétation d'un pgcd et d'un ppcm et 4 et 6 ?

3.2. Éléments premiers entre eux et théorème de Bézout

3.2. Éléments premiers entre eux et théorème de Bézout

Definition 7

A étant un anneau principal, on dit que $a_1, \dots, a_n \in A$ sont *premiers entre eux* lorsque 1_A est un pgcd de $a_1, \dots, a_n$.

Proposition 7

[Théorème de Bézout] $a_1, \dots, a_n$ sont premiers entre eux **ssi** il existe $x_1, \dots, x_n \in A$ tels que :

$$1_A = a_1 x_1 + \cdots + a_n x_n$$

3.3. Cas des anneaux $\mathbb{Z}$ et $\mathbb{K}[X]$

3.3. Cas des anneaux $\mathbb{Z}$ et $\mathbb{K}[X]$

Definition 8

Soient $a_1, \dots, a_n \in \mathbb{Z}$, avec $n \geqslant 2$.

- Si les a_i sont <u>non tous nuls</u>, on appelle PGCD de $a_1, \dots, a_n$ l'unique générateur strictement positif de l'idéal $(a_1) + \cdots + (a_n)$. On le note $a_1 \wedge \cdots \wedge a_n$, ou $\mathrm{PGCD}(a_1, \dots, a_n)$.
- Si les a_i sont <u>tous non nuls</u>, on appelle PPCM de $a_1, \dots, a_n$ l'unique générateur strictement positif de $a_1\mathbb{Z} \cap \cdots \cap a_n\mathbb{Z}$. On le note $a_1 \vee \cdots \vee a_n$, ou $\mathrm{PPCM}(a_1, \dots, a_n)$.

Remarque :

Restriction de $|$ à $\mathbb{N}^*$?

Definition 9

Soient $P_1, \dots, P_n \in \mathbb{K}[X]$, avec $n \geqslant 2$.

- Si les P_i sont non tous nuls, on appelle PGCD de $P_1, \dots, P_n$ l'unique générateur unitaire de l'idéal $(P_1) + \cdots + (P_n)$. On le note $P_1 \wedge \cdots \wedge P_n$ ou $\text{PGCD}(P_1, \dots, P_n)$.
- Si les P_i sont tous non nuls, on appelle PPCM de $P_1, \dots, P_n$ l'unique générateur unitaire de l'idéal $(P_1) \cap \cdots \cap (P_n)$. On le note $P_1 \vee \cdots \vee P_n$ ou $\text{PPCM}(P_1, \dots, P_n)$.

Remarque :

Restriction à l'ensemble des polynômes unitaires non nuls ?