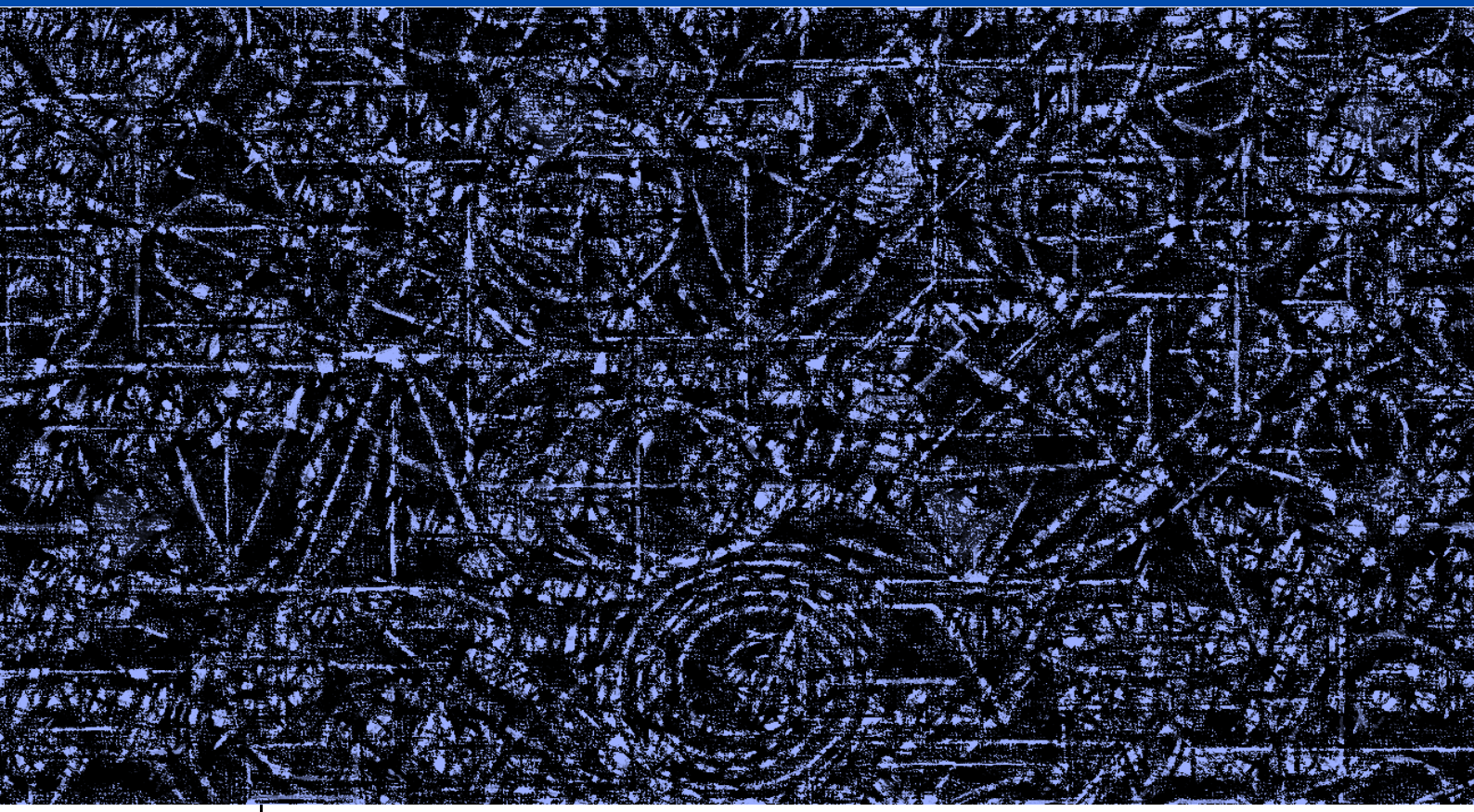
Arithmétique dans $\mathbb{Z}$: PGCD et PPCM

10



Introduction

Quand on fait de l'arithmétique (et pas forcément dans $\mathbb{Z}$), il y a deux notions fondamentales : le PGCD et le PPCM. Ces deux objets mathématiques sont très techniques à construire dans le cadre des entiers relatifs et l'est encore plus avec les polynômes (**chapitre 15**).
Nous étudierons d'abord le PGCD et le PPCM de deux entiers relatifs avant de traiter le cas général avec un nombre fini d'entiers relatifs.

Nous utiliserons la notion d'*idéal* (fondamentale en arithmétique) pour construire le PGCD et le PPCM de deux polynômes.
Autrefois, en terminale C c'est de la même façon qu'on construisait ces deux notions avec les entiers relatifs (qui sera d'ailleurs reprise en licence 2).

Prérequis

- Arithmétique dans $\mathbb{Z}$: divisibilité et congruences (**chapitre 9**)

Objectifs du chapitre

- Démontrer les propriétés liées à l'ensemble des diviseurs d'un entier relatif
- Définir le **PGCD** d'entiers relatifs
- Démontrer les propriétés du PGCD
- Mise en place de l'**algorithme d'Euclide**
- Introduire la notion de nombres premiers entre eux (dans leur ensemble et deux à deux)
- Démontrer le **théorème de Bézout** (**algorithme d'Euclide étendu**)
- Démontrer le **théorème de Gauss**
- Démontrer un critère de divisibilité par 7
- Etudier les éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ $(n \geqslant 1)$
- Définir le **PPCM** d'entiers relatifs
- Démontrer les propriétés du PPCM
- Démontrer la **relation PGCD-PPCM**

Le cours du chapitre 10

1 PGCD de deux entiers relatifs

A Diviseurs d'un entier relatif

Quel que soit l'entier relatif n, on note $\mathcal{D}_n$ l'ensemble des diviseurs de n et $\mathcal{D}_n^+$ l'ensemble des diviseurs positifs de n.

Il est alors clair que pour tout entier relatif n :

$$\mathcal{D}_n = \{k \in \mathbb{Z}, k \mid n\} \text{ et } \mathcal{D}_n^+ = \mathcal{D}_n \cap \mathbb{N}\,.$$

Compte tenu du **théorème 4** du **chapitre 9**, l'ensemble des diviseurs d'un entier relatif est un ensemble fini.

Par exemple, $\mathcal{D}_6 = \{-6,-1,-2,-3,1,2,3,6\}$ et $\mathcal{D}_6^+ = \{1,2,3,6\}$.

Théorème 1

Soient a et b deux entiers relatifs.

1) $\mathcal{D}_a \cap \mathcal{D}_0 = \mathcal{D}_a$ 2) $\mathcal{D}_a \cap \mathcal{D}_1 = \{-1,1\}$ 3) $\mathcal{D}_a = \mathcal{D}_{|a|}$ 4) $b \mid a \Rightarrow \mathcal{D}_a \cap \mathcal{D}_b = \mathcal{D}_b$.

Preuve

On rappelle que tous les entiers relatifs divise 0.

1) $\mathcal{D}_a \cap \mathcal{D}_0 = \mathcal{D}_a \cap \mathbb{Z} = \mathcal{D}_a$ (car $\mathcal{D}_a \subset \mathbb{Z}$).

2) Il est clair que $\mathcal{D}_1 = \{-1,1\}$ et que $\mathcal{D}_1 \subset \mathcal{D}_a$, d'où $\mathcal{D}_a \cap \mathcal{D}_1 = \{-1,1\}$.

3) C'est une conséquence directe du **théorème 2** du **chapitre 9**.

En effet, quand a est négatif on a :
$\mathcal{D}_a = \{k \in \mathbb{Z}, k \mid a\} = \{k \in \mathbb{Z}, k \mid -a\}$
$= \mathcal{D}_{-a}$.

4) Supposons que $b \mid a$.

Alors $\mathcal{D}_b \subset \mathcal{D}_a$, en effet, si d désigne un élément de $\mathcal{D}_b$, alors $d \mid b$. Comme par hypothèse $b \mid a$, il vient que $d \mid a$.

Par suite, $\mathcal{D}_a \cap \mathcal{D}_b = \mathcal{D}_b$. □

Théorème 2

$$\forall (a,b) \in \mathbb{Z}^2, \forall k \in \mathbb{Z}, \mathcal{D}_a \cap \mathcal{D}_b = \mathcal{D}_{a-kb} \cap \mathcal{D}_b\,.$$

Preuve

Preuve par double-inclusion.

- Soit d un élément de $\mathcal{D}_a \cap \mathcal{D}_b$.

Alors d est un diviseur à la fois de a et de b.
Il vient (**théorème 7** du **chapitre 2**), que d divise $a - kb$ et donc $d \in \mathcal{D}_{a-kb}$.

Ainsi, comme $d \in \mathcal{D}_b$, $\mathcal{D}_a \cap \mathcal{D}_b \subset \mathcal{D}_{a-kb} \cap \mathcal{D}_b$.

- Soit d un élément de $\mathcal{D}_{a-kb} \cap \mathcal{D}_b$.

Alors d est un diviseur à la fois de $a - kb$ et de b.
Il vient (**théorème 7** du **chapitre 2**), que d divise $(a-kb)+kb$, c'est-à-dire a, et donc $d \in \mathcal{D}_a$.

Ainsi, comme $d \in \mathcal{D}_b$, $\mathcal{D}_{a-kb} \cap \mathcal{D}_b \subset \mathcal{D}_a \cap \mathcal{D}_b$.

Finalement, $\mathcal{D}_a \cap \mathcal{D}_b = \mathcal{D}_{a-kb} \cap \mathcal{D}_b$. □

Remarque

En choisissant $k = 1$ dans le **théorème 2**, on a en particulier $\mathcal{D}_a \cap \mathcal{D}_b = \mathcal{D}_{a-b} \cap \mathcal{D}_b$.

Théorème 3

Soient a et b deux entiers relatifs avec b non nul.
En désignant par r le reste de la division euclidienne de a par b, on a $\mathcal{D}_a \cap \mathcal{D}_b = \mathcal{D}_r \cap \mathcal{D}_b$.

Le **théorème 3** est une conséquence du **théorème 2**.

Preuve

Attention, dans ce cas on a nécessairement $r < |b|$.

Comme r est le reste de la division euclidienne de a par b, il existe un entier relatif q tel que $a = bq + r$.

Donc $r = a - bq$ et alors $\mathcal{D}_r \cap \mathcal{D}_b = \mathcal{D}_{a-bq} \cap \mathcal{D}_b$.

D'après le **théorème 2**, il vient que $\mathcal{D}_r \cap \mathcal{D}_b = \mathcal{D}_a \cap \mathcal{D}_b$. □

B PGCD de deux entiers relatifs

La notion de PGCD est connue du lecteur depuis la classe de troisième. Mais ni son existence, ni son unicité n'ont été justifiées. C'est ce que nous allons faire dans ce paragraphe.

Le cours du chapitre 10

Le **théorème 4** est très important.

Théorème 4

Soient a et b deux entiers relatifs non simultanément nuls.
L'ensemble $\mathcal{D}_a \cap \mathcal{D}_b$ admet un plus grand élément.

Preuve

- L'ensemble $\mathcal{D}_a \cap \mathcal{D}_b$ est par définition une partie de $\mathbb{Z}$.

En effet, on sait que 1 (et -1) divise tous les entiers relatifs.

- L'ensemble $\mathcal{D}_a \cap \mathcal{D}_b$ n'est pas vide car il contient 1 (on peut aussi dire -1).

- Il reste à montrer que cet ensemble est majoré.

Soit d un élément de $\mathcal{D}_a \cap \mathcal{D}_b$.

Supposons que a est nul.

L'entier b n'est pas nul car a et b ne doivent pas être nul en même temps.

Alors b n'est pas nul et donc $\mathcal{D}_a \cap \mathcal{D}_b = \mathcal{D}_0 \cap \mathcal{D}_b = \mathcal{D}_b$.

Le lecteur sera ravi de montrer que quel que soit l'entier relatif d : $d \leqslant |d|$.

Ainsi, d est un diviseur de b et donc (via le **théorème 4** du **chapitre 9**) $d \leqslant |b|$.

Supposons que b est nul.

Alors a n'est pas nul et donc $\mathcal{D}_a \cap \mathcal{D}_b = \mathcal{D}_a \cap \mathcal{D}_0 = \mathcal{D}_a$.

Ainsi, d est un diviseur de a et donc $d \leqslant |a|$.

En résumé $d \leqslant \max(|a|, |b|)$.

Supposons enfin que a et b sont non nuls.

Comme $d \in \mathcal{D}_a \cap \mathcal{D}_b$, on a $d \leqslant |a|$ et $d \leqslant |b|$, d'où $d \leqslant \min(|a|, |b|)$.

Dans tous les cas, l'ensemble $\mathcal{D}_a \cap \mathcal{D}_b$ est majoré.

Finalement, l'ensemble $\mathcal{D}_a \cap \mathcal{D}_b$ est une partie non vide de $\mathbb{Z}$ et majoré : il admet un plus grand élément. □

Définition 1

Soient a et b deux entiers relatifs non simultanément nuls.
Le plus grand élément de l'ensemble $\mathcal{D}_a \cap \mathcal{D}_b$ est appelé **le plus grand diviseur commun** de a et b.

Soyons très précis, il s'agit du plus grand diviseur commun au sens de la relation d'ordre usuelle dans $\mathbb{Z}$.
Nous verrons que ce plus grand élément coïncide avec la relation d'ordre « divise » dans $\mathbb{Z}$.

Remarque

1. Le plus grand diviseur commun de a et b est noté $\text{PGCD}(a, b)$ mais il est parfois commode de le noter $a \wedge b$.

Selon la **définition 1**, le PGCD de 0 et de 0 désignerait le plus grand élément de $\mathbb{Z}$. Un tel élément n'existant pas, nous convenons à la convention ci-contre.

2. On se permet d'étendre la **définition 1** en posant $\text{PGCD}(0, 0) = 0$.

3. Il est clair que $\text{PGCD}(a, b) \geqslant 1$.

4. Par définition, en notant $\delta = a \wedge b$, il est clair que :

$$\forall k \in \mathbb{Z}, \begin{cases} k \mid a \\ k \mid b \end{cases} \Rightarrow k \leqslant \delta .$$

Autrement dit, un diviseur commun de a et b est inférieur ou égal au PGCD de a et b.

5. En vertu du **théorème 1-3**, il est aussi clair que $\text{PGCD}(a, b) = \text{PGCD}(|a|, |b|)$.

Si bien que nous pouvons toujours nous ramener à des entiers naturels pour la détermination du PGCD.

Exemple

Déterminons le PGCD des nombres 12 et 30.

On a $\mathcal{D}_{12}^+ = \{1, 2, 3, 4, 6, 12\}$ et $\mathcal{D}_{30}^+ = \{1, 2, 3, 5, 6, 10, 15, 30\}$.

Il est inutile de considérer les diviseurs négatifs (voir la troisième remarque précédente).

Donc $\mathcal{D}_{12}^+ \cap \mathcal{D}_{30}^+ = \{1, 2, 3, 6\}$ et alors $\text{PGCD}(12, 30) = 6$.

C Propriétés du PGCD

Les propriétés du PGCD sont nombreuses. C'est le théorème suivant qui va les justifier.
On rappelle que si a désigne un entier relatif, alors $a\mathbb{Z}$ désigne l'ensemble de ses multiples.

Le **théorème 5** est très important pour toute la suite du cours.

Théorème 5 **Relation fondamentale du PGCD de deux entiers relatifs**

Soient a et b deux entiers relatifs et δ leur PGCD.

$$a\mathbb{Z} + b\mathbb{Z} = \delta\mathbb{Z} .$$

Rappel de notation :
$a\mathbb{Z} + b\mathbb{Z} = \{x \in \mathbb{Z}, \exists (u, v) \in \mathbb{Z}^2, x = au + bv\}$.
Ainsi, si a et b sont nuls, la relation ci-contre devient claire.

Preuve

Soit x un élément de $a\mathbb{Z} + b\mathbb{Z}$.

Par définition, il existe un couple $(u, v) \in \mathbb{Z}^2$ tel que $x = au + bv$.

Utilisation du **théorème 7** du **chapitre 9**.

Comme δ est un diviseur commun des entiers a et b ($\delta \in \mathcal{D}_a \cap \mathcal{D}_b$), on a $\delta \mid au + bv$, c'est à dire $\delta \mid x$.

Il vient alors que $x \in \delta\mathbb{Z}$ d'où $a\mathbb{Z}+b\mathbb{Z} \subset \delta\mathbb{Z}$.

Cette partie de la démonstration est très délicate.

Pour démontrer l'inclusion réciproque, il nous faut passer par autre chose.

On va montrer que l'ensemble $(a\mathbb{Z}+b\mathbb{Z})\cap\mathbb{N}^*$ admet un plus petit élément.

- C'est évidemment par construction une partie de $\mathbb{N}$.

Le cas où a et b sont nuls est exclu (la relation devient évidente). On est par conséquent sûr que l'un des entiers a ou b n'est pas nul. Ici, on a choisi a et il n'y a pas perte de généralité.

- Il n'est pas vide car si a est strictement positif, alors clairement $a \in (a\mathbb{Z}+b\mathbb{Z})\cap\mathbb{N}^*$ (prendre $u=1$ et $v=0$) et si a est strictement négatif, alors comme $-a \in a\mathbb{Z}+b\mathbb{Z}$ (prendre $u=-1$ et $v=0$) $|a| \in (a\mathbb{Z}+b\mathbb{Z})\cap\mathbb{N}^*$.

L'ensemble $(a\mathbb{Z}+b\mathbb{Z})\cap\mathbb{N}^*$ admet ainsi un plus petit élément qu'on notera d.

N'oubliez pas : $d \in \mathbb{N}^*$.

Comme $d \in a\mathbb{Z}+b\mathbb{Z}$, on a $d\mathbb{Z} \subset a\mathbb{Z}+b\mathbb{Z}$.

En effet, considérons $y \in d\mathbb{Z}$.

Alors $d \mid y$ et il existe un entier relatif e tel que $y=de$.

Par ailleurs, comme $d \in a\mathbb{Z}+b\mathbb{Z}$, il existe un couple $(u,v) \in \mathbb{Z}^2$ tel que $d=au+bv$.

Par conséquent, $y=de=a(eu)+b(ev)$ et donc $y \in a\mathbb{Z}+b\mathbb{Z}$: c'est l'inclusion recherchée.

On va montrer que $a\mathbb{Z}+b\mathbb{Z} \subset d\mathbb{Z}$.

Effectuons la division euclidienne de x par d.

Il existe un couple $(q,r) \in \mathbb{Z}^2$ tel que $x=dq+r$ et $0 \leqslant r < d$.

Faire l'**exercice 2** pour montrer que l'ensemble $a\mathbb{Z}+b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.

Comme x et d sont dans $a\mathbb{Z}+b\mathbb{Z}$, on a $dq \in a\mathbb{Z}+b\mathbb{Z}$ (puisque $d\mathbb{Z} \subset a\mathbb{Z}+b\mathbb{Z}$) et alors $x-dq \in a\mathbb{Z}+b\mathbb{Z}$, soit $r \in a\mathbb{Z}+b\mathbb{Z}$.

Raisonnement par l'absurde.

Si $r \neq 0$, alors $r \in (a\mathbb{Z}+b\mathbb{Z})\cap\mathbb{N}^*$, ce qui est absurde puisque $r < d = \min((a\mathbb{Z}+b\mathbb{Z})\cap\mathbb{N}^*)$.

Donc r est nul et alors $x=dq$, d'où $x \in d\mathbb{Z}$.

Ainsi, on a montré que $a\mathbb{Z}+b\mathbb{Z} \subset d\mathbb{Z}$ et donc $a\mathbb{Z}+b\mathbb{Z}=d\mathbb{Z}$.

Voir l'**exercice 1**.

Enfin, comme $d\mathbb{Z} \subset \delta\mathbb{Z}$ (puisque $a\mathbb{Z}+b\mathbb{Z} \subset \delta\mathbb{Z}$), δ divise d donc $\delta \leqslant d$.

Comme d divise a et b (car $a\mathbb{Z}+b\mathbb{Z}=d\mathbb{Z}$ et $a,b \in a\mathbb{Z}+b\mathbb{Z}$), on a par définition de δ, $d \leqslant \delta$, d'où $d=\delta$.

Bilan : $d\mathbb{Z}=\delta\mathbb{Z}$ et donc $a\mathbb{Z}+b\mathbb{Z}=\delta\mathbb{Z}$. □

Nous sommes maintenant amenés à démontrer les propriétés du PGCD.

Théorème 6

Soient a et b deux entiers relatifs.

1) $\mathrm{PGCD}(a,b)=\mathrm{PGCD}(b,a)$ 2) $\mathrm{PGCD}(a,0)=|a|$ 3) $\mathrm{PGCD}(a,1)=1$ 4) $a \mid b \Rightarrow \mathrm{PGCD}(a,b)=|a|$.

L'égalité 1) traduit la commutativité du PGCD.

Preuve

Pour finir les preuves, le lecteur pourra prouver à titre d'exercice :

$\forall (a,b) \in \mathbb{Z}^2, a\mathbb{Z}=b\mathbb{Z} \Leftrightarrow |a|=|b|$.

On pourra aussi voir l'**exercice 3**.

1) On a : $(a\wedge b)\mathbb{Z}=a\mathbb{Z}+b\mathbb{Z}=b\mathbb{Z}+a\mathbb{Z}=(b\wedge a)\mathbb{Z}$, ce qui permet de conclure.

2) On a : $a\mathbb{Z}=a\mathbb{Z}+0\mathbb{Z}=(a\wedge 0)\mathbb{Z}$, ce qui permet de conclure.

3) Il est clair que $a\mathbb{Z}+\mathbb{Z}=\mathbb{Z}$, donc $\mathbb{Z}=(a\wedge 1)\mathbb{Z}$.

4) Supposons que $a \mid b$.

On utilise le fait que $a\mathbb{Z}+a\mathbb{Z}=a\mathbb{Z}$ qui est immédiat justifier.

Alors $b\mathbb{Z} \subset a\mathbb{Z}$ et donc (en vertu de l'**exercice 9** du **chapitre 4**) $b\mathbb{Z}+a\mathbb{Z} \subset a\mathbb{Z}$.

De plus, l'inclusion $a\mathbb{Z} \subset b\mathbb{Z}+a\mathbb{Z}$ étant claire, on obtient $a\mathbb{Z}+b\mathbb{Z}=a\mathbb{Z}$ d'où $(a\wedge b)\mathbb{Z}=b\mathbb{Z}$. □

Théorème 7 Homogénéité du PGCD

$$\forall (a,b) \in \mathbb{Z}^2, \forall k \in \mathbb{Z}, \mathrm{PGCD}(\lambda a,\lambda b)=|\lambda|\,\mathrm{PGCD}(a,b).$$

Le **théorème 7** traduit l'homogénéité du PGCD.

Attention à ne pas oublier la valeur absolue au second membre de l'égalité.

Preuve

On a immédiatement : $\lambda a\mathbb{Z}+\lambda b\mathbb{Z}=\lambda(a\mathbb{Z}+b\mathbb{Z})=\lambda(\delta\mathbb{Z})=(\lambda\delta)\mathbb{Z}$.

Bien entendu, δ désigne de PGCD de a et b.

Ainsi $\mathrm{PGCD}(\lambda a,\lambda b)=|\lambda\delta|=|\lambda|\delta$. □

Théorème 8

Soient a et b deux entiers relatifs et δ leur PGCD.

$$\forall k \in \mathbb{Z}, \begin{cases} k \mid a \\ k \mid b \end{cases} \Leftrightarrow k \mid \delta.$$

Le **théorème 8** explique que le PGCD des entiers a et b est le plus grand diviseur de a et b au sens de la relation « divise » (qui jusqu'ici était au sens de la relation d'ordre usuelle).

Preuve

On dispose des équivalences suivantes : $\begin{cases} k \mid a \\ k \mid b \end{cases} \Leftrightarrow \begin{cases} a\mathbb{Z} \subset k\mathbb{Z} \\ b\mathbb{Z} \subset k\mathbb{Z} \end{cases} \Leftrightarrow a\mathbb{Z}+b\mathbb{Z} \subset k\mathbb{Z} \Leftrightarrow \delta\mathbb{Z} \subset k\mathbb{Z} \Leftrightarrow k \mid \delta$. □

Utilisation de l'**exercice 9** du **chapitre 4**.

Remarque

Une conséquence immédiate du **théorème 8** et que les diviseurs du PGCD de a et b sont exactement les diviseurs commun de a et b et ainsi :

$$\mathcal{D}_a \cap \mathcal{D}_b = \mathcal{D}_\delta .$$

Le **théorème 9** traduit l'associativité du PGCD.
Il est plus commode de citer le théorème avec la notation « $\wedge$ ».

Théorème 9 **Associativité du PGCD**

$$\forall (a,b,c) \in \mathbb{Z}^3,\ a \wedge (b \wedge c) = (a \wedge b) \wedge c .$$

Preuve

En utilisant l'associativité de l'addition dans $\mathcal{P}(\mathbb{Z})$, on a : $a\mathbb{Z} + (b\mathbb{Z} + c\mathbb{Z}) = (a\mathbb{Z} + b\mathbb{Z}) + c\mathbb{Z}$. □

Remarques

1. D'après le **théorème 9** on pourra écrire $a \wedge b \wedge c$ au lieu de $a \wedge (b \wedge c)$ (ou $(a \wedge b) \wedge c$).
2. Le couple $(\mathbb{Z}, \wedge)$ est un demi-groupe commutatif.

Euclide d'Alexandrie (~300 av JC) était un mathématicien grec.

D Algorithme d'Euclide

Jusqu'ici, pour déterminer le PGCD de deux entiers relatifs on dressait la liste de leurs diviseurs positifs commun et on prenait le plus grand de cette liste.
Cette méthode a bien sûr ses limites. L'**algorithme d'Euclide** permet de déterminer rapidement le PGCD de deux entiers relatifs.
Limitons-nous aux entiers naturels et choisissons deux entiers naturels a et b avec $0 < b \leqslant a$.

- Si b divise a, on sait déjà que $a \wedge b = b$.
- Supposons alors que b ne divise par a.

Effectuons la division euclidienne de a par b.

Il existe un couple $(q_0, r_0) \in \mathbb{N}^2$ tel que $a = bq_0 + r_0$ et $0 \leqslant r_0 < b$.

C'est une conséquence immédiate du **théorème 3**.

Il est clair que $a \wedge b = b \wedge r_0$. Deux cas sont alors à traiter :

- ou bien $r_0 = 0$ et dans ce cas $a \wedge b = b \wedge 0 = b$;
- ou bien $r_0 \neq 0$ et on effectue à nouveau la division euclidienne de b par r_0.

On obtient alors un couple $(q_1, r_1) \in \mathbb{N}^2$ tel que $b = r_0 q_1 + r_1$ avec $0 \leqslant r_1 < r_0$.

Il est alors clair que $a \wedge b = b \wedge r_0 = r_0 \wedge r_1$. Deux cas sont alors à traiter :

On remarque alors que le PGCD de a et b est le dernier reste non nul dans les divisions euclidiennes.

- ou bien $r_1 = 0$ et dans ce cas $a \wedge b = b \wedge r_0 = r_0 \wedge 0 = r_0$;
- ou bien $r_1 \neq 0$ et on effectue à nouveau la division euclidienne de r_0 par r_1.

On construit alors des couples (q_0, r_0), (q_1, r_1) ... tels que :

$$\begin{cases} a = bq_0 + r_0 \\ 0 \leqslant r_0 < b \end{cases}, \begin{cases} b = r_0 q_1 + r_1 \\ 0 \leqslant r_1 < r_0 \end{cases} \ldots$$

Considérons la suite r des restes définis sur $\mathbb{N}$. Que peut-on dire de cette suite ?
Supposons qu'aucun des termes de cette suite s'annule. On aurait alors une suite strictement décroissante d'entiers naturels. Comme vous le savez, une telle suite n'existe pas. Mais une suite décroissante d'entiers naturels est stationnaire (**théorème 36** du **chapitre 7**).

On a : $r_0 < r_1 < r_2 < \ldots$.

Une suite décroissante d'entiers naturels ne « stationne pas » nécessairement en 0.

Ainsi, puisque qu'il existe au moins un terme nul de cette suite, cette dernière finit par « stationner en 0 », autrement dit, l'**algorithme d'Euclide** prend fin à partir d'un moment.
Il existe alors un entier naturel N tel que :

$$\begin{cases} a = bq_0 + r_0 \\ 0 \leqslant r_0 < b \end{cases}, \begin{cases} b = r_0 q_1 + r_1 \\ 0 \leqslant r_1 < r_0 \end{cases} \ldots \begin{cases} r_{N-2} = r_{N-1} q_N + r_N \\ 0 \leqslant r_N < r_{N-1} \end{cases}, \ r_N \neq 0 \text{ et } r_{N+1} = 0 .$$

Donc $a \wedge b = b \wedge r_0 = r_1 \wedge r_2 = \ldots = r_{N-1} \wedge r_N = r_N \wedge r_{N+1} = r_N$ qui correspond au dernier reste non nul.

Exemple

Déterminons le PGCD des entiers 455 et 312.

$455 = 312 \times 1 + 143$
$312 = 143 \times 2 + 26$
$143 = 26 \times 5 + 13$
$26 = 2 \times 13 + 0$.

Le dernier reste non nul étant 13, on a $\text{PGCD}(455, 312) = 13$.

Remarque

En 1844, le mathématicien **Gabriel Lamé** (1795-1870) montre que le nombre d'étapes dans l'algorithme d'Euclide est majoré par cinq fois le nombre de chiffres du plus grand des deux entiers choisis.

Pour l'exemple ci-dessus, le nombre d'étapes est majoré par 15 mais il est en pratique inférieur à la moitié, soit 7 étapes (ici 4 étapes ont suffi).

2 Nombres premiers entre eux

Attention à ne pas confondre avec la notion de *nombre premier* (étudiée dans le **chapitre 13**).

A Généralités

Définition 2

Soient a et b deux entiers relatifs.

Dire que les entiers a et b sont **premiers entre eux** signifie que leur PGCD est égal à 1.

Une méthode pour montrer que deux entiers relatifs a et b sont premiers entre eux consiste à montrer que tout diviseur commun à a et à b vaut nécessairement -1 ou 1.
Cette méthode est mise en œuvre dans la démonstration du **théorème 11**.

Exemples

1. Les entiers 3 et 7 sont premiers entre eux.
2. Les entiers 10 et 14 ne sont pas premiers entre eux car 2 est un diviseur commun de ces entiers.

Théorème 10

$$\forall (a,b) \in \mathbb{Z}^2, \exists (a',b') \in \mathbb{Z}^2, \begin{cases} a = \delta a', b = \delta b' \\ a' \wedge b' = 1 \end{cases}.$$

Pour plus de souplesse dans les théorèmes qui suivent, nous avons noté δ le PGCD de a et b.

Preuve

Toute paire d'entiers relatifs premiers entre eux convient.

Si a et b sont nuls, le résultat est évident. On suppose désormais que $(a,b) \neq (0,0)$.

L'existence d'entiers relatifs a' et b' tels que $a = \delta a'$ et $b = \delta b'$ est évidente puisque δ est un diviseur de a et b. Il faut en revanche vérifier la dernière condition.

On se sert du fait que le PGCD est homogène.

On a : $\delta = \text{PGCD}(a,b) = \text{PGCD}(\delta a', \delta b') = \delta \, \text{PGCD}(a',b')$.

Par régularité de la multiplication dans $\mathbb{N}$ (vu que $\delta \geqslant 1$), il vient que $a' \wedge b' = 1$. □

Théorème 11

$$\forall (a,b,c) \in \mathbb{Z}^3, \begin{cases} a \wedge b = 1 \\ c \mid b \end{cases} \Rightarrow a \wedge c = 1.$$

Autrement dit, si a et b sont premiers entre eux, alors a est premier avec tout diviseur de b.

Preuve

Supposons que $a \wedge b = 1$ et $c \mid b$.

Considérons un diviseur positif d de a et c.

Par définition de d, on a $d \mid a$ et $d \mid c$.

Comme par hypothèse $c \mid b$, on a $d \mid b$, et donc $d = 1$ (puisque a et b sont premiers entre eux).

Ainsi, les entiers a et c sont premiers entre eux. □

Exemple

17 et 15 sont premiers entre eux. Donc 17 est premier avec tout diviseur de 15 comme 5.

Remarque

La réciproque du **théorème 11** est évidemment fausse.

B Théorème de Bézout

Claude-Gaspard Bachet de **Méziriac** (1581-1638) était un mathématicien français.

Théorème 12 Théorème de Bézout

$$\forall (a,b) \in \mathbb{Z}^2, a \wedge b = 1 \Leftrightarrow \exists (u,v) \in \mathbb{Z}^2, au + bv = 1.$$

Le **théorème 12** est le plus important de ce chapitre. Il fournit une caractéristique de la **définition 2**.
De nombreux résultat vont se déduire de ce théorème.

Preuve

($\Rightarrow$) Supposons que les entiers a et b soient premiers entre eux.

On a alors $a\mathbb{Z}+b\mathbb{Z}=\mathbb{Z}$.

Mais $1\in\mathbb{Z}$ et donc il existe un couple $(u,v)\in\mathbb{Z}^2$ tel que $au+bv=1$.

($\Leftarrow$) Supposons qu'il existe un couple $(u,v)\in\mathbb{Z}^2$ tel que $au+bv=1$.

On rappelle que δ désigne le PGCD de a et b.

On sait que $a\mathbb{Z}+b\mathbb{Z}=\delta\mathbb{Z}$. Puis, comme $1\in a\mathbb{Z}+b\mathbb{Z}$, $1\in\delta\mathbb{Z}$, donc δ divise 1 et alors $\delta=1$. □

Remarque

Si a et b désignent des nombres relatifs non nuls, l'équation d'inconnue (x,y) : $ax+by=1$ admet des solutions dans $\mathbb{Z}^2$ si et seulement si $a\wedge b=1$.

Théorème 13

$$\forall (a,b)\in(\mathbb{Z}^*)^2,\ a\wedge b=1\Rightarrow\exists(u,v)\in\mathbb{Z}^2,\begin{cases}au+bv=1\\|u|<|b|,|v|\leqslant|a|\end{cases}.$$

Le **théorème 13** permet d'obtenir des coefficients u et v « assez petits ».

Attention ! La deuxième inégalité est large contrairement à la première. Il est tout de même possible de la rendre strict mais c'est plus délicat à justifier.

Preuve

Supposons que $a\wedge b=1$.

Compte tenu de ce qu'on doit obtenir, il est raisonnable de supposer $b>0$ (pour la division euclidienne par b).

D'après le **théorème de Bézout**, il existe un couple $(u',v')\in\mathbb{Z}^2$ tel que $au'+bv'=1$.

Le couple (a,b) peut être remplacé par le couple $(-a,-b)$ pour que b soit positif puisque :
$au+bv=(-a)(-u)+(-b)(-v)$.

En effectuant la division euclidienne de u' par b, il existe un couple $(q,u)\in\mathbb{Z}^2$ tel que $u'=bq+u$ et $0\leqslant u<b$.

La condition $|u|<|b|$ est alors remplie.

Puis, en notant $v=aq+v'$, on a $au+bv=a(u'-bq)+b(aq+v')=au'-abq+abq+bv'=au'+bv'=1$.

De plus, comme $au+bv=1$, $|bv|=|1-au|\leqslant 1+|a|u<1+|a|b$ et donc $|v|b\leqslant|a|b$, soit $|v|\leqslant|a|$. □

Remarque

La réciproque du **théorème 13** est évidemment vraie : *qui peut le plus peu le moins* !

C Algorithme d'Euclide étendu

Soient un couple $(a,b)\in\mathbb{Z}^*\times\mathbb{N}^*$ tel que $a\wedge b=1$.

On va élaborer un algorithme, appelé **algorithme d'Euclide étendu** permettant de déterminer un couple d'entiers relatifs (u,v) tel que $au+bv=1$.

D'après l'**algorithme d'Euclide**, il existe un entier naturel N et des entiers $q_0,r_0,...,q_N,r_N,q_{N+1},r_{N+1}$ tels que :

$$\begin{cases}a=bq_0+r_0\\0\leqslant r_0<b\end{cases},\ \begin{cases}b=r_0q_1+r_1\\0\leqslant r_1<r_0\end{cases}\ \ldots\ \begin{cases}r_{N-2}=r_{N-1}q_N+r_N\\0\leqslant r_N<r_{N-1}\end{cases},\ r_N\neq 0,\ r_{N+1}=0.$$

Donc, puisque $r_N=1$, $r_{N-2}-r_{N-1}q_N=1$.

Puis, $r_{N-3}=r_{N-2}q_{N-1}+r_{N-1}$, donc $r_{N-1}=r_{N-3}-r_{N-2}q_{N-1}$, d'où $r_{N-2}-(r_{N-3}-r_{N-2}q_{N-1})q_N=1$.

On remonte ainsi les divisions euclidiennes jusqu'à atteindre les entiers a et b.

Exemple

Cherchons un couple $(u,v)\in\mathbb{Z}^2$ tel que $412u+11v=1$.

- On prend le réflexe de regarder si 412 et 11 sont bien premiers entre eux : c'est bien le cas car 11 n'est pas un diviseur de 412 et que $\mathcal{D}_{11}=\{-11,-1,1,11\}$.

- On applique l'**algorithme d'Euclide** au couple (412,11) :
$412=11\times37+5$; $11=5\times2+1$ et $2=1\times2+0$.

- On forme un couple d'entier relatif (u,v) tel que $412u+11v=1$:
$1=11-5\times2=11-(412-11\times37)\times2=11-(412\times2-11\times74)=412\times(-2)+11\times75$.

Ainsi le couple $(-2,75)$ convient.

D Théorème de Gauss

Johann Carl Friedrich Gauss (1777-1855) était un mathématicien allemand.

Le **théorème de Gauss** est très important pour la suite du cours.

Théorème 14 Théorème de Gauss

$$\forall(a,b,c)\in\mathbb{Z}^3,\begin{cases}a\mid bc\\a\wedge b=1\end{cases}\Rightarrow a\mid c.$$

Preuve

On laisse le soin au lecteur de vérifier que si l'un des trois entiers a, b et c est nul, l'implication reste toujours vraie.

Supposons que $a \mid bc$ et $a \wedge b = 1$.

D'après le **théorème de Bézout**, il existe un couple $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$.

Utilisation du **théorème 7** du **chapitre 9**.

Donc $acu + bcv = c$. Puis, comme a divise bc et lui-même, il divise $acu + bcv$, c'est-à-dire c. □

E Conséquences du théorème de Bézout et de Gauss

Les conséquences de ces deux théorèmes sont nombreuses et très pratiques. Vous devez les connaître.

Théorème 15

$$\forall (a,b,c) \in \mathbb{Z}^3, \begin{cases} a \wedge b = 1 \\ a \wedge c = 1 \end{cases} \Leftrightarrow a \wedge (bc).$$

Autrement dit, un entier est premier avec un produit si et seulement s'il est premier avec chacun des facteurs du produit.

Preuve

Naturellement, on écarte les cas où l'un des entiers a, b et c est nul.

$(\Rightarrow)$ Supposons que $a \wedge b = 1$ et $a \wedge c = 1$.

Il existe alors des entiers relatifs u, v, u', v' tels que $au + bv = 1$ et $au' + cv' = 1$.

Multiplication membre à membre.

Donc $(au + bv)(au' + cv') = 1$, soit $a^2uu' + acuv' + abu'v + bcvv' = 1$, soit $a(auu' + cuv' + bu'v) + (bc)(vv') = 1$.

Puisque $auu' + cuv' + bu'v \in \mathbb{Z}$ et $vv' \in \mathbb{Z}$, on conclut que $a \wedge (bc) = 1$.

$(\Leftarrow)$ Réciproquement, supposons que $a \wedge (bc)$.

Comme $b \mid bc$ et $c \mid bc$, il vient que (**théorème 11**) $a \wedge b$ et $a \wedge c = 1$. □

Théorème 16

$$\forall (a,b,c) \in \mathbb{Z}^3, \begin{cases} a \wedge b = 1 \\ a \mid c, b \mid c \end{cases} \Rightarrow ab \mid c.$$

Le **théorème 16** est très utile en pratique.

Attention à ne pas oublier que a et b doivent être premiers entre eux !

Preuve

Naturellement, on écarte les cas où l'un des entiers a, b et c est nul.

Supposons à présent que $a \wedge b = 1$, $a \mid c$ et $b \mid c$.

Comme $a \mid c$, il existe un entier relatif k tel que $c = ak$.

Donc $b \mid ak$ et comme $a \wedge b = 1$, on d'après le **théorème de Gauss**, $b \mid k$.

Il existe donc à nouveau un entier relatif l tel que $k = bl$.

Ainsi, $c = a(bl) = (ab)l$ et alors $ab \mid c$. □

Remarque

La réciproque du **théorème 16** est fausse mais si la condition « $a \wedge b = 1$ » est supprimée, elle devient vraie.

F Application des théorèmes de Bézout et de Gauss

Application 1 : critère de divisibilité

Nous avons démontré dans le chapitre précédent les critères de divisibilité de 2, 3, 4, 5, 8, 9, 10 et 11. Nous allons à présent démontrer un critère de divisibilité par 7.

Rappelons le **théorème des systèmes de numération** appliquer à la base 10 :

$$\forall a \in \mathbb{N}^*, \exists n \in \mathbb{N}, \exists !(a_0, ..., a_n) \in \mathbb{N}^{n+1}, \begin{cases} a = a_0 + a_1 \times 10 + a_2 \times 10^2 + ... + a_n \times 10^n \\ 0 \leqslant a_0, ..., a_n < n \\ a_n \neq 0 \end{cases}.$$

Pour toute la suite, on notera $N = \sum_{k=0}^{n} a_k 10^k$. L'entier N s'écrit alors $\overline{a_n ... a_1 a_0}$ où nous avons omis la base 10 car il n'y aura pas d'ambiguïté.

Théorème 17 **Critère de divisibilité par 7**

L'entier N est divisible par 7 si et seulement si $7 \mid \overline{a_n ... a_1} - 2a_0$.

Autrement dit, N est divisible par 7 si et seulement si la différence entre son nombre de dizaines et le double du chiffre des unités est divisible par 7.

($\Rightarrow$) Supposons que N est divisible par 7.

Comme $7 \mid 21$, alors (**théorème 7** du **chapitre 9**) $7 \mid \sum_{k=0}^{n} a_k 10^k - 21a_0$.

Or, $\sum_{k=0}^{n} a_k 10^k - 21a_0 = \sum_{k=1}^{n} a_k 10^k + a_0 - 21a_0 = \sum_{k=1}^{n} a_k 10^k - 20a_0 = 10\left(\sum_{k=1}^{n} a_k 10^{k-1} - 2a_0\right)$.

Donc $7 \mid 10\left(\sum_{k=1}^{n} a_k 10^{k-1} - 2a_0\right)$.

Remarquez que $7 \times (-7) + 10 \times 5 = 1$.

L'entier 7 étant premier avec 10, on a d'après le **théorème de Gauss** $7 \mid \sum_{k=1}^{n} a_k 10^{k-1} - 2a_0$.

Ainsi, $7 \mid \overline{a_n \dots a_1} - 2a_0$.

($\Leftarrow$) Supposons que $7 \mid \overline{a_n \dots a_1} - 2a_0$.

Utilisation du **théorème 5** du **chapitre 9**.

Alors $7 \mid 10(\overline{a_n \dots a_1} - 2a_0)$ soit $7 \mid 10\left(\sum_{k=1}^{n} a_k 10^{k-1} - 2a_0\right)$, soit encore $7 \mid \sum_{k=1}^{n} a_k 10^k - 20a_0$.

Mais 7 divise 21, d'où 7 divise $21a_0$ et alors $7 \mid \sum_{k=1}^{n} a_k 10^k - 20a_0 + 21a_0$, soit $7 \mid \sum_{k=1}^{n} a_k 10^k + a_0$, soit $7 \mid \sum_{k=0}^{n} a_k 10^k$.

Ainsi N est divisible par 7. □

Exemple

Le nombre 868 est-il divisible par 7 ?

On a : $86 - 2 \times 8 = 86 - 16 = 70 = 7 \times 10$.

Réponse : oui.

Application 2 : éléments inversibles dans Z/nZ

Le théorème suivant est très important :

Théorème 18

Soit n un entier naturel non nul.

Les éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ sont ceux dont les représentants sont premiers avec n.

Autrement dit, les éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ sont les éléments $\overline{x}$ tel que $x \wedge n = 1$.

Preuve

On considère l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$.

On va montrer que tout représentant de x est premier avec n.

- Soit x un élément inversible de $\mathbb{Z}/n\mathbb{Z}$ (il existe alors un entier relatif a tel que $x = \overline{a}$).

Il existe alors un élément y (il existe aussi un entier relatif b tel que $y = \overline{b}$) de $\mathbb{Z}/n\mathbb{Z}$ tel que $xy = \overline{1}$.

L'égalité $xy = \overline{1}$ est équivalente à l'égalité $\overline{a} \times \overline{b} = \overline{ab} = \overline{1}$, c'est-à-dire $ab \equiv 1\ [n]$, soit $n \mid ab - 1$.

Il existe donc un entier relatif k tel que $ab - 1 = nk$ et alors $ab + n \times (-k) = 1$.

D'après le **théorème de Bézout**, a et n sont premiers entre eux.

- Réciproquement, soit x un élément de $\mathbb{Z}/n\mathbb{Z}$ (il existe alors un entier relatif a tel que $x = \overline{a}$).

Supposons que a et n sont premiers entre eux.

D'après le **théorème de Bézout**, il existe deux entiers relatifs u et v tels que $au + nv = 1$.

Dans $\mathbb{Z}/n\mathbb{Z}$, $\overline{n} = \overline{0}$.

Donc $\overline{au + nv} = \overline{au} + \overline{nv} = \overline{a} \times \overline{u} + \overline{n} \times \overline{v} = x \times \overline{u} = \overline{1}$.

Ce qui prouve que x est inversible dans $\mathbb{Z}/n\mathbb{Z}$. □

Exemple

On rappelle que pour un anneau A, la notation $A^\times$ désigne l'ensemble des éléments inversibles de A.

$(\mathbb{Z}/8\mathbb{Z})^\times = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$.

3 PGCD de plusieurs entiers relatifs

Nous allons généraliser la théorie du PGCD avec un nombre fini d'entiers relatifs. Les preuves seront plus succinctes. Reportez-vous aux cas avec deux entiers relatifs si certaines preuves vous semblent difficiles à comprendre.

Le cours du chapitre 10

A Définition

Commençons par une constatation :

Théorème 19

Soient $n \in \mathbb{N}^*$ et $(x_1, ..., x_n) \in \mathbb{Z}^n \setminus \{(0, ..., 0)\}$.

L'ensemble des diviseurs communs à $x_1, ..., x_n$ admet un plus grand élément.

Les entiers $x_1,...,x_n$ ne doivent pas être tous nuls.

Preuve

Notons $\mathcal{D}$ l'ensemble des diviseurs communs à $x_1, ..., x_n$.

- L'ensemble $\mathcal{D}$ est une partie de $\mathbb{Z}$.
- L'ensemble $\mathcal{D}$ n'est pas vide puisqu'il contient 1.
- L'ensemble $\mathcal{D}$ est majoré par :

$\max(|x_1|, ..., |x_n|)$ si l'un au moins des entiers est nul ;

sinon il est majoré par $\min(|x_1|, ..., |x_n|)$ si aucun des entiers est nul.

En réalité, seul le premier cas suffit puisqu'il est clair que : $\min(|x_1|, ..., |x_n|) \leqslant \max(|x_1|, ..., |x_n|)$.

Ainsi l'ensemble $\mathcal{D}$ admet un plus grand élément. □

Définition 3

Soient $n \in \mathbb{N}^*$ et $(x_1, ..., x_n) \in \mathbb{Z}^n \setminus \{(0, ..., 0)\}$.

Le plus grand élément de l'ensemble des diviseurs communs à $x_1, ..., x_n$ est appelé le **plus grand diviseur commun** de $x_1, ..., x_n$.

Il s'agit du plus grand diviseur commun pour l'ordre usuel.

Remarque

1. Le plus grand diviseur commun de $x_1, ..., x_n$ est noté $\text{PGCD}(x_1, ..., x_n)$ où encore $\text{PGCD}((x_i)_{1 \leqslant i \leqslant n})$.

Parfois, on pourra pour plus de commodité employer la notation $\bigwedge_{i=1}^{n}$ pour le PGCD de $x_1, ..., x_n$.

2. On se permet d'étendre la **définition 3** en posant $\text{PGCD}(0, ..., 0) = 0$.

3. Il est clair que $\text{PGCD}(x_1, ..., x_n) \geqslant 1$ (quand les entiers $x_1, ..., x_n$ ne sont pas tous nuls).

4. Par définition, en notant $\delta = \text{PGCD}(x_1, ..., x_n)$, il est clair que :

$$\forall k \in \mathbb{Z}, (\forall i \in \{1, ..., n\}, k \mid x_i) \Rightarrow k \leqslant \delta .$$

5. En vertu du **théorème 1-3**, il est clair que $\text{PGCD}(x_1, ..., x_n) = \text{PGCD}(|x_1|, ..., |x_n|)$.

Exemple

$\text{PGCD}(10, 16, 20) = 2$.

B Propriétés du PGCD

Théorème 20 **Relation fondamentale du PGCD de plusieurs entiers relatifs**

Soient n un entier naturel non nul, $x_1, ..., x_n$ des entiers relatifs et δ leur PGCD.

$$\sum_{i=1}^{n} x_i\mathbb{Z} = \delta\mathbb{Z} .$$

Le **théorème 20** est très important pour toute la suite du cours.

Preuve

Soit x un élément de $\sum_{i=1}^{n} x_i\mathbb{Z}$.

Il existe alors un n-uplet $(u_1, ..., u_n) \in \mathbb{Z}^n$ tel que $x = \sum_{i=1}^{n} x_i u_i$.

Comme pour tout i de $\{1, ..., n\}$ on a $\delta \mid x_i$, il vient que $\delta \mid x$ et alors $x \in \delta\mathbb{Z}$.

On obtient l'inclusion $\sum_{i=1}^{n} x_i\mathbb{Z} \subset \delta\mathbb{Z}$.

Il reste à établir l'inclusion réciproque qui n'est pas simple.

L'ensemble $\left(\sum_{i=1}^{n} x_i\mathbb{Z}\right) \cap \mathbb{N}^*$ est une partie de $\mathbb{N}$ et non vide (il contient $|x_1|$) : il contient un plus petit élément qu'on notera d.

Puisque $d \in \sum_{i=1}^{n} x_i\mathbb{Z}$, on a $d\mathbb{Z} \subset \sum_{i=1}^{n} x_i\mathbb{Z}$.

Effectuons la division euclidienne de x par d.

Il existe un couple $(q, r) \in \mathbb{Z}^2$ tel que $x = dq + r$ et $0 \leqslant r < d$.

L'ensemble $\sum_{i=1}^{n} x_i\mathbb{Z}$ étant un sous-groupe de $\mathbb{Z}$ avec $x \in \sum_{i=1}^{n} x_i\mathbb{Z}$ et $d \in \sum_{i=1}^{n} x_i\mathbb{Z}$, on a $r \in \sum_{i=1}^{n} x_i\mathbb{Z}$.

Raisonnement par l'absurde.

Supposons que $r > 0$.

Alors $r \in \left(\sum_{i=1}^{n} x_i\mathbb{Z}\right) \cap \mathbb{N}^*$, ce qui est absurde puisque $r < d = \min\left(\left(\sum_{i=1}^{n} x_i\mathbb{Z}\right) \cap \mathbb{N}^*\right)$.

Donc r est nul et alors $x = dq \in d\mathbb{Z}$.

L'inclusion $\sum_{i=1}^{n} x_i\mathbb{Z} \subset d\mathbb{Z}$ est donc établie.

Ainsi $\sum_{i=1}^{n} x_i\mathbb{Z} = d\mathbb{Z}$ (et donc $d\mathbb{Z} \subset \delta\mathbb{Z}$).

La dernière inclusion entraîne que $\delta \mid d$, soit $\delta \leqslant d$.

Puis, comme d divise chacun des entiers $x_1, ..., x_n$, il vient que $d \leqslant \delta$, d'où $d = \delta$.

Finalement, $\sum_{i=1}^{n} x_i\mathbb{Z} = \delta\mathbb{Z}$. □

Le **théorème 21** traduit l'homogénéité du PGCD.
Attention à ne pas oublier la valeur absolue au second membre de l'égalité.

Théorème 21 **Homogénéité du PGCD**

$$\forall n \in \mathbb{N}^*, \forall (x_1, ..., x_n) \in \mathbb{Z}^n, \forall k \in \mathbb{Z}, \text{PGCD}(kx_1, ..., kx_n) = |k|\text{PGCD}(x_1, ..., x_n)$$

Preuve

En notant $\delta = \text{PGCD}(x_1, ..., x_n)$, on a $\sum_{i=1}^{n} (kx_i)\mathbb{Z} = k\sum_{i=1}^{n} x_i\mathbb{Z} = k(\delta\mathbb{Z}) = (k\delta)\mathbb{Z}$.

Donc $\text{PGCD}(kx_1, ..., kx_n) = |k\delta| = |k|\delta$. □

Ainsi, le PGCD des entiers $x_1,...,x_n$ correspond au plus grand élément (au sens de la relation « divise ») des diviseurs communs de ces entiers.

Théorème 22

Soient n un entier naturel non nul, $x_1, ..., x_n$ des entiers relatifs et δ leur PGCD.

$$\forall k \in \mathbb{Z}, (\forall i \in \{1, ..., n\}, k \mid x_i) \Leftrightarrow k \mid \delta.$$

Preuve

On dispose des équivalences suivantes : $\forall i \in \{1, ..., n\}, k \mid x_i \Leftrightarrow \forall i \in \{1, ..., n\}, x_i\mathbb{Z} \subset k\mathbb{Z} \Leftrightarrow \sum_{i=1}^{n} x_i\mathbb{Z} \subset k\mathbb{Z} \Leftrightarrow \delta\mathbb{Z} \subset k\mathbb{Z}$

$\Leftrightarrow k \mid \delta$. □

4 Nombres premiers entre eux : cas général

A Généralités

Avec trois entiers ou plus, une subtilité existe avec la notion de nombres premiers entre eux.

Comparer la **définition 4** avec la **définition 5**.

Définition 4

Soient $n \in \mathbb{N}^*$ et $(x_1, ..., x_n) \in \mathbb{Z}^n$.

Dire que les entiers $x_1, ..., x_n$ sont **premiers entre eux dans leur ensemble** signifie que $\text{PGCD}(x_1, ..., x_n) = 1$.

Exemples

1. Les entiers 2, 3 et 4 sont premiers entre eux dans leur ensemble.
2. Les entiers 4, 6 et 20 ne sont pas premiers entre eux dans leur ensemble.

Puisque 2 est un diviseur commun des trois entiers.

Définition 5

Soient $n \in \mathbb{N}^*$ et $(x_1, ..., x_n) \in \mathbb{Z}^n$.

Dire que les entiers $x_1, ..., x_n$ sont **premiers entre eux deux à deux** signifie que :

$$\forall (i, j) \in \{1, ..., n\}^2, i \neq j \Rightarrow x_i \wedge x_j = 1.$$

Exemples

1. Les entiers 2, 3 et 4 ne sont pas premiers entre eux deux à deux (il y a 2 et 4).
2. Les entiers 3, 4 et 5 sont premiers entre eux deux à deux.

Remarques

1. Selon le principe de *qui peut le plus, peut le moins*, des nombres premiers entre eux deux à deux sont premiers entre eux dans leur ensemble.
2. Attention, ce n'est pas parce que des entiers sont premiers entre eux dans leur ensemble qui sont premiers entre eux deux à deux.

En effet, par exemple, les entiers 10, 13 et 14 sont premiers entre eux dans leur ensemble mais 10 et 14 ont 2 comme diviseur commun (donc un PGCD différent de 1).

3. Deux entiers relatifs sont premiers entre eux si et seulement s'ils sont premiers entre eux dans leurs ensembles.
4. Deux entiers relatifs sont premiers entre eux si et seulement s'ils sont premiers entre eux deux à deux.

En réalité, ce n'est pas si simple à justifier rigoureusement. Il nous faudrait pour cela énoncer l'associativité du PGCD dans le cadre général mais ce théorème est admis (il a été simplement vu dans le cas de trois entiers).

Utilisation de la négation :

$$\exists (i, j) \in \{1, ..., n\}^2, \begin{cases} i \neq j \\ x_i \wedge x_j \neq 1 \end{cases}.$$

Théorème 23

$$\forall n \in \mathbb{N}^*, \forall (x_1, ..., x_n) \in \mathbb{Z}^n, \exists ({x_1}', ..., {x_n}') \in \mathbb{Z}^n, \begin{cases} \forall i \in \{1, ..., n\}, x_i = \delta {x_i}' \\ {x_1}' \wedge ... \wedge {x_n}' = 1 \end{cases}.$$

Ici, δ désigne de PGCD de $x_1,...,x_n$.

Preuve

Si tous les entiers $x_1, ..., x_n$ sont nuls, le résultat est évident.

Supposons que $(x_1, ..., x_n) \neq (0, ..., 0)$.

Puisque δ est un diviseur de chacun des entiers $x_1, ..., x_n$, il existe un n-uplet $({x_1}', ..., {x_n}')$ tel que pour tout i de l'ensemble $\{1, ..., n\}$, $x_i = \delta {x_i}'$.

Puis, $\delta = \text{PGCD}(x_1, ..., x_n) = \text{PGCD}(\delta {x_1}', ..., \delta {x_n}') = \delta \, \text{PGCD}({x_1}', ..., {x_n}')$.

Ainsi, $\text{PGCD}({x_1}', ..., {x_n}') = 1$. □

B Théorème de Bézout : cas général

Théorème 24 Théorème de Bézout (version 2)

Soient $n \in \mathbb{N}^*$ et $(x_1, ..., x_n) \in \mathbb{Z}^n$.

Les entiers $x_1, ..., x_n$ sont premiers entre eux dans leur ensemble si et seulement s'il existe un u-uplet $(u_1, ..., u_n)$ d'entiers relatifs tel que :

$$\sum_{i=1}^{n} x_i u_i = 1.$$

Preuve

($\Rightarrow$) Supposons que les entiers $x_1, ..., x_n$ sont premiers entre eux dans leur ensemble.

Alors $\sum_{i=1}^{n} x_i \mathbb{Z} = \mathbb{Z}$, puis comme $1 \in \mathbb{Z}$, il existe un u-uplet $(u_1, ..., u_n) \in \mathbb{Z}^n$ tel que $\sum_{i=1}^{n} x_i u_i = 1$.

($\Leftarrow$) Supposons qu'il existe un u-uplet $(u_1, ..., u_n) \in \mathbb{Z}^n$ tel que $\sum_{i=1}^{n} x_i u_i = 1$.

Comme $\sum_{i=1}^{n} x_i\mathbb{Z} = \delta\mathbb{Z}$ et que $1 \in \sum_{i=1}^{n} x_i\mathbb{Z}$, il vient que $1 \in \delta\mathbb{Z}$, soit $\delta = 1$.

Ainsi, $\text{PGCD}(x_1, ..., x_n) = 1$ et les entiers $x_1, ..., x_n$ sont premiers entre eux (dans leur ensemble). □

C Conséquences du théorème de Bézout et de Gauss

Voici une généralisation du **théorème 15** :

Théorème 25

Soient $n \in \mathbb{N}^*$, $(x_1, ..., x_n) \in \mathbb{Z}^n$ et $a \in \mathbb{Z}$.

$$(\forall i \in \{1, ..., n\}, a \wedge x_i = 1) \Leftrightarrow a \wedge \prod_{i=1}^{n} x_i = 1.$$

Autrement dit, un entier est premier avec plusieurs entiers si et seulement s'il est premier avec leur produit.

Preuve

$(\Rightarrow)$ Effectuons une récurrence sur n.

Il est clair que l'implication est vraie quand $n = 1$ (puisque, en particulier $a \wedge x_1 = 1$).

Soit $n \in \mathbb{N}^*$ et supposons que pour des entiers $x_1, ..., x_{n+1}$ donnés, on ait :

$$(\forall i \in \{1, ..., n\}, a \wedge x_i = 1) \Rightarrow a \wedge \prod_{i=1}^{n} x_i = 1.$$

Admettons aussi que :

$$\forall i \in \{1, ..., n+1\}, k \wedge x_i = 1.$$

On a $k \wedge \prod_{i=1}^{n+1} x_i = k \wedge \left(\left(\prod_{i=1}^{n} x_i \right) x_{n+1} \right)$.

Ainsi, comme $k \wedge \prod_{i=1}^{n} x_i$ et $k \wedge x_{n+1}$, on a $k \wedge \prod_{i=1}^{n+1} x_i = 1$.

$(\Leftarrow)$ Supposons que $k \wedge \prod_{i=1}^{n} x_i = 1$.

Alors d'après le **théorème 11**, on a immédiatement : $\forall i \in \{1, ..., n\}, k \wedge x_i = 1$. □

Le théorème précédent permet d'énoncer le théorème qui suit :

Théorème 26

$$\forall (a, b) \in \mathbb{Z}, \forall (n, m) \in (\mathbb{N}^*)^2, a \wedge b = 1 \Leftrightarrow a^n \wedge b^m = 1.$$

Autrement dit, deux entiers sont premiers entre eux si et seulement si leurs puissances sont premiers entre eux.

Preuve

$(\Rightarrow)$ Supposons que a et b sont premiers entre eux.

D'après le **théorème 25**, pour tout entier naturel n non nul on a $a \wedge \prod_{i=1}^{n} b = 1$, soit $a \wedge b^n = 1$.

En appliquant encore le **théorème 25**, on a pour tout couple $(n, m) \in (\mathbb{N}^*)^2$, $b^n \wedge \prod_{i=1}^{m} a = 1$, soit $a^m \wedge b^n = 1$.

$(\Leftarrow)$ Supposons que tout couple $(n, m) \in (\mathbb{N}^*)^2$, $a^n \wedge b^m = 1$.

Alors d'après le **théorème 25**, pour tout entier naturel n non nul $a^n \wedge b = 1$.

Puis, toujours d'après le même théorème, $a \wedge b = 1$. □

Exemple

Déterminons le PGCD de 46^{123} et 7^{1914}.

Les entiers 7 et 46 sont premiers entre eux, donc (**théorème 26**) les entiers 46^{123} et 7^{1914} sont premiers entre eux.

Le théorème suivant est une conséquence immédiate du **théorème 26** :

Le cours du chapitre 10

Théorème 27

$$\forall (a,b)\in\mathbb{Z},\forall n\in\mathbb{N}^*,(a\wedge b)^n=a^n\wedge b^n\,.$$

Preuve

Notons $\delta=a\wedge b$.

On sait qu'il existe deux entiers relatifs a' et b' tels que $a=\delta a'$, $b=\delta b'$ et $a'\wedge b'=1$.

Utilisation du **théorème 26**.

Donc pour tout entier naturel n non nul, $a^n\wedge b^n=(\delta a')^n\wedge(\delta b')^n=\delta^n a'^n\wedge\delta^n b'^n=\delta^n(a'^n\wedge b'^n)=\delta^n(a'\wedge b')^n=\delta^n$.

Ainsi, pour tout entier naturel n non nul, $(a\wedge b)^n=a^n\wedge b^n$. □

Théorème 28

Soient $n\in\mathbb{N}^*$, $x_1,\dots,x_n$ des entiers relatifs deux à deux premiers entre eux et a un entier relatif.

$$\forall i\in\{1,\dots,n\},x_i\mid a\Rightarrow\prod_{i=1}^{n}x_i\mid a\,.$$

Attention, on demande à ce que les entiers soient premiers entre eux deux à deux (et non dans leur ensemble).

Autrement dit, si plusieurs entiers (qui sont premiers entre eux deux à deux) divisent un même entier, alors leur produit divise cet entier.

Preuve

Récurrence sur n.

L'implication est claire quand $n=1$.

Soit $n\in\mathbb{N}^*$ et supposons que pour les entiers $x_1,\dots,x_{n+1}$ deux à deux premiers entre eux, on ait :

$$\forall i\in\{1,\dots,n\},x_i\mid a\Rightarrow\prod_{i=1}^{n}x_i\mid a\,.$$

Supposons aussi que :

$$\forall i\in\{1,\dots,n+1\},x_i\mid a\,.$$

Pour tout i de $\{1,\dots,n\}$ on a $x_{n+1}\wedge x_i=1$, d'où (**théorème 25**) $x_{n+1}\wedge\prod_{i=1}^{n}x_i=1$.

Puis, comme $\prod_{i=1}^{n}x_i\mid a$ et $x_{n+1}\mid a$, il vient que $\left(\prod_{i=1}^{n}x_i\right)x_{n+1}$ divise a, c'est-à-dire $\prod_{i=1}^{n+1}x_i$ divise a. □

5 PPCM de deux entiers relatifs

A Généralités

Théorème 29

Soient a et b deux entiers relatifs non nuls.

L'ensemble $(a\mathbb{Z}\cap b\mathbb{Z})\cap\mathbb{N}^*$ admet un plus petit élément.

Le **théorème 29** est fondamentale.

La notation $(a\mathbb{Z}\cap b\mathbb{Z})\cap\mathbb{N}^*$, lourde, désigne l'ensemble des multiples commun strictement positifs de a et b.

Preuve

L'ensemble $(a\mathbb{Z}\cap b\mathbb{Z})\cap\mathbb{N}^*$ est une partie de $\mathbb{N}$ qui n'est pas vide car il contient $|ab|$.

Cet ensemble admet donc un plus petit élément. □

Définition 6

Soient a et b deux entiers relatifs non nuls.

Le plus petit élément de l'ensemble $(a\mathbb{Z}\cap b\mathbb{Z})\cap\mathbb{N}^*$ est appelé le **plus petit multiple commun** de a et b.

Il s'agit du plus petit multiple commun pour l'ordre usuel.

Remarque

1. Le plus petit multiple commun de a et b est noté $\mathrm{PPCM}(a,b)$ mais il est parfois commode de le noter $a\vee b$.
2. On se permet d'étendre la **définition 6**, en posant $\mathrm{PPCM}(a,b)=0$ dès lors où l'un des entiers a et b est nul.
3. Il est clair que $\mathrm{PPCM}(a,b)\geqslant 1$ quand a et b sont non nuls.
4. Par définition, en notant $\mu=a\vee b$, il est clair que :

$$\forall k\in\mathbb{N}^*,\begin{cases}a\mid k\\ b\mid k\end{cases}\Rightarrow\mu\leqslant k\,.$$

En particulier, $\mathrm{PPCM}(0,0)=0$.

Autrement dit, tout multiple strictement positif de a et de b est supérieur ou égal au PPCM de a et b.

5. Puisque pour tout entier relatif a on a $a\mathbb{Z}=-a\mathbb{Z}$, on a $\mathrm{PPCM}(a,b)=\mathrm{PPCM}(|a|,|b|)$.

Exemple

Déterminons le PPCM des nombres 6 et 15.

Les premiers multiples strictement positifs de 6 sont : 6, 12, 18, 24, 30...

Les premiers multiples strictement positifs de 15 sont : 15, 30, 45, 60, 75...

Donc $\text{PPCM}(6,15)=30$.

Cette méthode ne semble pas efficace. D'autres méthodes comme pour le PGCD seront travaillées.

B Propriétés du PPCM

Comme pour le PGCD, il existe une relation fondamentale pour le PPCM. Nous pourrons ensuite déduire de cette dernière toutes les propriétés du PPCM.

Théorème 30 Relation fondamentale du PPCM de deux entiers relatifs

Soient a et b deux entiers relatifs et μ leur PPCM.

$$a\mathbb{Z}\cap b\mathbb{Z}=\mu\mathbb{Z}\,.$$

Le **théorème 30** est fondamental pour toute la suite du cours.

Preuve

On peut supposer que a et b sont non nuls pour la suite.

Puisque $a\mid\mu$ et $b\mid\mu$, on a $\mu\mathbb{Z}\subset a\mathbb{Z}$ et $\mu\mathbb{Z}\subset b\mathbb{Z}$.

Donc $\mu\mathbb{Z}\subset a\mathbb{Z}\cap b\mathbb{Z}$.

Mais (**théorème 23** du **chapitre 4**) l'ensemble $a\mathbb{Z}\cap b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$, donc (**théorème 25** du **chapitre 4**) il existe un entier naturel m tel que $a\mathbb{Z}\cap b\mathbb{Z}=m\mathbb{Z}$.

De l'inclusion $\mu\mathbb{Z}\subset a\mathbb{Z}\cap b\mathbb{Z}$, on en tire que $\mu\mathbb{Z}\subset m\mathbb{Z}$ et donc $m\leqslant\mu$ (ils sont positifs et non nuls).

Puis, comme μ et m sont des multiples de a et b, on a $\mu\leqslant m$ (**remarque n°4** de la **définition 6**).

Ainsi, $m=\mu$ et $a\mathbb{Z}\cap b\mathbb{Z}=\mu\mathbb{Z}$. □

Dans le cas contraire, la relation devient triviale.

L'entier m ne peut pas être nul puisque a et b ne le sont pas.

Théorème 31

Soient a et b deux entiers relatifs.

1) $\text{PPCM}(a,b)=\text{PPCM}(b,a)$ 2) $\text{PPCM}(a,0)=0$ 3) $\text{PPCM}(a,1)=|a|$ 4) $a\mid b\Rightarrow\text{PPCM}(a,b)=|b|$.

L'égalité 1) traduit la commutativité du PPCM.
L'implication 4) dit en particulier que $\text{PPCM}(a,a)=|a|$ (puisque $a\mid a$).

Preuve

1) On a : $(a\vee b)\mathbb{Z}=a\mathbb{Z}\cap b\mathbb{Z}=b\mathbb{Z}\cap a\mathbb{Z}=(b\vee a)\mathbb{Z}$, ce qui permet de conclure.

2) Immédiat compte tenu de la définition étendue du PPCM.

3) On a : $(a\vee 1)\mathbb{Z}=a\mathbb{Z}\cap\mathbb{Z}=a\mathbb{Z}$, ce qui permet de conclure.

4) Supposons que $a\mid b$.

Alors $b\mathbb{Z}\subset a\mathbb{Z}$ et alors $a\mathbb{Z}\cap b\mathbb{Z}=b\mathbb{Z}$, ce qui permet de conclure puisque $a\mathbb{Z}\cap b\mathbb{Z}=\mu\mathbb{Z}$. □

Théorème 32 Homogénéité du PPCM

$$\forall(a,b)\in\mathbb{Z}^2,\forall k\in\mathbb{Z},\text{PPCM}(ka,kb)=|k|\,\text{PPCM}(a,b)\,.$$

Le **théorème 32** traduit l'homogénéité du PPCM.

Preuve

On a : $ka\mathbb{Z}\cap kb\mathbb{Z}=k(a\mathbb{Z}\cap b\mathbb{Z})=k(\mu\mathbb{Z})=(k\mu)\mathbb{Z}$.

Ainsi, $\text{PPCM}(ka,kb)=|k\mu|=|k|\,\mu$. □

Bien entendu, μ désigne de PPCM de a et b.

Théorème 33

Soient a et b deux entiers relatifs et μ leur PPCM.

$$\forall k\in\mathbb{Z},\begin{cases}a\mid k\\ b\mid k\end{cases}\Leftrightarrow\mu\mid k\,.$$

Le **théorème 33** explique que le PPCM des entiers a et b est le plus petit multiple commun strictement positif de a et b au sens de la relation « divise » (qui jusqu'ici était au sens de la relation d'ordre usuelle).

Preuve

On dispose des équivalences suivantes : $\begin{cases}a\mid k\\ b\mid k\end{cases}\Leftrightarrow\begin{cases}k\mathbb{Z}\subset a\mathbb{Z}\\ k\mathbb{Z}\subset b\mathbb{Z}\end{cases}\Leftrightarrow k\mathbb{Z}\subset a\mathbb{Z}\cap b\mathbb{Z}\Leftrightarrow k\mathbb{Z}\subset\mu\mathbb{Z}\Leftrightarrow\mu\mid k$. □

L'associativité déjà rencontrée avec le PPCM de deux entiers reste encore valable avec le PPCM :

Le cours du chapitre 10

Le **théorème 34** traduit l'associativité du PPCM.

Théorème 34 **Associativité du PPCM**

$$\forall (a,b,c)\in\mathbb{Z}^3,\ a\vee(b\vee c)=(a\vee b)\vee c\,.$$

Preuve

En utilisant l'associativité de l'intersection dans $\mathcal{P}(\mathbb{Z})$, on a : $a\mathbb{Z}\cap(b\mathbb{Z}\cap c\mathbb{Z})=(a\mathbb{Z}\cap b\mathbb{Z})\cap c\mathbb{Z}$. □

Remarques

1. D'après le **théorème 34** on pourra écrire $a\vee b\vee c$ au lieu de $a\vee(b\vee c)$ (ou $(a\vee b)\vee c$).
2. Le couple $(\mathbb{Z},\vee)$ est un demi-groupe commutatif.

Le **théorème 35** donne un moyen pratique de calculer le PPCM de deux entiers. Mais attention, on demande aux deux entiers d'être premiers entre eux.

Théorème 35

Soient a et b deux entiers relatifs premiers entre eux.

$$\mathrm{PPCM}(a,b)=|ab|\,.$$

Preuve

On écarte le cas où l'un des entiers a et b est nul (sinon l'égalité devient triviale).

On note $\mu=a\vee b$.

Il est clair que ab est un multiple commun de a et b.

On parle ici du plus petit au sens de la relation divise !

Le PPCM étant le plus petit multiple commun strictement positif de a et b, on a (**théorème 33**) $\mu\,|\,ab$.

Puis, comme $a\,|\,\mu$ et $b\,|\,\mu$, alors (**théorème 16**) $ab\,|\,\mu$.

Ainsi, $\mu=|ab|$. □

Remarque

A titre d'exercice, le lecteur pourra démontrer le **théorème 35** sans utiliser le **théorème 33** (et donc en utilisant la relation d'ordre usuelle).

Le **théorème 36** permet de calculer le PPCM de deux entiers à partir du PGCD de ces mêmes entiers.

Théorème 36 **Relation PGCD-PPCM**

$$\forall (a,b)\in\mathbb{Z}^2,(a\vee b)(a\wedge b)=|ab|\,.$$

Preuve

On écarte le cas où l'un des entiers a et b est nul (sinon l'égalité devient triviale).

Notons $\delta=a\wedge b$ et $\mu=a\vee b$.

D'après le **théorème 10**, il existe deux entiers relatifs a' et b' tels que $a=\delta a'$ et $b=\delta b'$ et $a'\wedge b'=1$.

Utilisation de l'homogénéité du PPCM et du **théorème 35**.

Donc, $\mu=a\vee b=(\delta a')\vee(\delta b')=\delta(a'\vee b')=\delta\,|a'b'|$.

Ainsi, $\delta\mu=\delta^2\,|a'b'|=|(\delta a')(\delta b')|=|ab|$. □

Exemple

Déterminons le PPCM des entiers 315 et 196.

Grâce à l'algorithme d'Euclide on a :

$315=196\times1+119$; $196=119\times1+77$; $119=77\times1+42$; $77=42\times1+35$; $42=35\times1+7$; et $35=7\times5+0$.

Donc $\mathrm{PGCD}(315,196)=7$.

Puis, en utilisant le **théorème 36**, il vient que $\mathrm{PPCM}(315,196)=\dfrac{315\times196}{7}=45\times196=8820$.

Remarque

Le **théorème 36** ne se généralise pas !

Considérons les entiers 2, 4 et 5.

On a $\mathrm{PGCD}(2,4,5)=1$ et $\mathrm{PPCM}(2,4,5)=\mathrm{PPCM}(1,2)=2$.

Il est alors clair que $\mathrm{PGCD}(2,4,5)\times\mathrm{PPCM}(2,4,5)\neq2\times4\times5$.

6 PPCM de plusieurs entiers relatifs

Nous allons généraliser la théorie du PPCM avec un nombre fini d'entiers relatifs. Les preuves seront plus succinctes. Reportez-vous aux cas avec deux entiers relatifs si certaines preuves vous semblent difficiles à comprendre.

Le cours du chapitre 10

A Définition

Commençons par une constatation :

Théorème 37

Soient $n \in \mathbb{N}^*$ et $(x_1, ..., x_n) \in (\mathbb{Z}^*)^n$.

L'ensemble des multiples communs strictement positifs de $x_1, ..., x_n$ admet un plus petit élément.

Preuve

L'ensemble des multiples communs strictement positifs à $x_1, ..., x_n$ est une partie de $\mathbb{N}$ et contient $\left|\prod_{i=1}^{n} x_i\right|$.

Cet ensemble admet donc un plus petit élément. □

Définition 7

Soient $n \in \mathbb{N}^*$ et $(x_1, ..., x_n) \in (\mathbb{Z}^*)^n$.

Le plus petit élément de l'ensemble des multiples communs strictement positifs de $x_1, ..., x_n$ est appelé le **plus petit multiple commun** de $x_1, ..., x_n$.

Il s'agit du plus petit multiple commun pour l'ordre usuel.

Remarque

1. Le plus petit élément de l'ensemble des multiples communs strictement positifs de $x_1, ..., x_n$ est noté $\text{PPCM}(x_1, ..., x_n)$ où encore $\text{PPCM}((x_i)_{1 \leqslant i \leqslant n})$.

Parfois, on pourra pour plus de commodité employer la notation $\bigvee_{i=1}^{n}$ pour le PPCM de $x_1, ..., x_n$.

2. On se permet d'étendre la **définition 7** en posant $\text{PGCD}(x_1, ..., x_n) = 0$ dès lors où l'un des entiers $x_1, ..., x_n$ est nul.

3. Il est clair que $\text{PPCM}(x_1, ..., x_n) \geqslant 1$ quand les entiers $x_1, ..., x_n$ sont tous non nuls.

4. Par définition, en notant $\mu = \text{PPCM}(x_1, ..., x_n)$, il est clair que :

$$\forall k \in \mathbb{N}^*, (\forall i \in \{1, ..., n\}, x_i \mid k) \Rightarrow \mu \leqslant k .$$

5. Il est clair que $\text{PPCM}(x_1, ..., x_n) = \text{PPCM}(|x_1|, ..., |x_n|)$.

B Propriété du PPCM

Théorème 38 **Relation fondamentale du PPCM de plusieurs entiers relatifs**

Le **théorème 38** est très important pour toute la suite du cours.

Soient n un entier naturel non nul, $x_1, ..., x_n$ des entiers relatifs non nuls et μ leur PPCM.

$$\bigcap_{i=1}^{n} x_i\mathbb{Z} = \mu\mathbb{Z} .$$

Preuve

On va supposer que tous les entiers $x_1, ..., x_n$ sont non nuls (sinon la relation devient évidente).

Pour tout i de $\{1, ..., n\}$ on a $x_i \mid \mu$, donc pour i de $\{1, ..., n\}$ on a $\mu\mathbb{Z} \subset x_i\mathbb{Z}$ et donc $\mu\mathbb{Z} \subset \bigcap_{i=1}^{n} x_i\mathbb{Z}$.

Puisque (**théorème 23** du **chapitre 4**) l'ensemble $\bigcap_{i=1}^{n} x_i\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$, il existe un entier naturel m non nul tel que $\bigcap_{i=1}^{n} x_i\mathbb{Z} = m\mathbb{Z}$ (**théorème 25** du **chapitre 4**).

On a alors $\mu\mathbb{Z} \subset m\mathbb{Z}$, d'où $m \leqslant \mu$.

Pour tout i de $\{1, ..., n\}$, comme μ et m sont des multiples communs de $x_1, ..., x_n$, on a $\mu \leqslant m$ et ainsi $m = \mu$.

On conclut donc que $\bigcap_{i=1}^{n} x_i\mathbb{Z} = m\mathbb{Z} = \mu\mathbb{Z}$. □

Le cours du chapitre 10

Le **théorème 39** traduit l'homogénéité du PGCD.
Attention à ne pas oublier la valeur absolue au second membre de l'égalité.

Théorème 39 **Homogénéité du PPCM**

$$\forall n \in \mathbb{N}^*, \forall (x_1, ..., x_n) \in \mathbb{Z}^n, \forall k \in \mathbb{Z}, \text{PPCM}(kx_1, ..., kx_n) = |k| \text{PPCM}(x_1, ..., x_n) .$$

Preuve

En notant $\mu = \text{PPCM}(x_1, ..., x_n)$, on a $\bigcap_{i=1}^{n} kx_i\mathbb{Z} = k\bigcap_{i=1}^{n} x_i\mathbb{Z} = k(\mu\mathbb{Z}) = (k\mu)\mathbb{Z}$.

Donc $\text{PPCM}(kx_1, ..., kx_n) = |k\mu| = |k|\,\mu$. □

Théorème 40

Soient n un entier naturel non nul, $x_1, ..., x_n$ des entiers relatifs et μ leur PPCM.

$$\forall k \in \mathbb{Z}, (\forall i \in \{1, ..., n\}, x_i \mid k) \Leftrightarrow \mu \mid k .$$

Ainsi, le PPCM des entiers $x_1,...,x_n$ correspond au plus petit élément (au sens de la relation « divise ») des multiples communs strictement positifs de ces entiers.

Preuve

On dispose des équivalences suivantes : $\forall i \in \{1, ..., n\}, x_i \mid k \Leftrightarrow \forall i \in \{1, ..., n\}, k\mathbb{Z} \subset x_i\mathbb{Z} \Leftrightarrow k\mathbb{Z} \subset \bigcap_{i=1}^{n} x_i\mathbb{Z} \Leftrightarrow k\mathbb{Z} \subset \mu\mathbb{Z}$

$\Leftrightarrow \mu \mid k$. □

Terminons ce chapitre par une généralisation du **théorème 35** :

Le **théorème 41** donne un moyen de calculer le PPCM de plusieurs entiers. Mais attention, ces entiers doivent être premiers entre eux.

Théorème 41

Soient n un entier naturel non nul, $x_1, ..., x_n$ des entiers relatifs deux à deux premiers entre eux.

$$\text{PPCM}(x_1, ..., x_n) = \left| \prod_{i=1}^{n} x_i \right| .$$

Preuve

On écarte le cas où tous les entiers $x_1, ..., x_n$ est nuls (le résultat devient trivial sinon).

Notons $\mu = \text{PPCM}(x_1, ..., x_n)$.

Il est clair que $\prod_{i=1}^{n} x_i$ est un multiple commun des entiers $x_1, ..., x_n$.

Le PPCM étant le plus petit multiple commun strictement positif de $x_1, ..., x_n$, on a (**théorème 40**) $\mu \mid \prod_{i=1}^{n} x_i$.

Enfin, pour tout i de $\{1, ..., n\}$, comme $x_i \mid \mu$, on a (**théorème 28**) pour tout i de $\{1, ..., n\}$, $\prod_{i=1}^{n} x_i \mid \mu$.

Ainsi, $\mu = \left| \prod_{i=1}^{n} x_i \right|$. □

Les exercices du chapitre 10

1 **Démonstrations supplémentaires de cours** 🖫

Montrer que : $\forall (a,b) \in \mathbb{Z}^2, a \mid b \Leftrightarrow b\mathbb{Z} \subset a\mathbb{Z}$.

2 **Démonstrations supplémentaires de cours** 🖫

Soient a et b deux entiers relatifs.

Montrer que l'ensemble $a\mathbb{Z} + b\mathbb{Z}$ est un sous-groupe additif de $\mathbb{Z}$.

3 **Démonstrations supplémentaires de cours** 🖫

Montrer que : $(a,b,c) \in \mathbb{Z}^3, a \wedge b \Rightarrow a \wedge (bc) = a \wedge b$.

4 **Démonstrations supplémentaires de cours** 🖫

Montrer que deux entiers relatifs consécutifs sont nécessairement premiers entre eux.

5 **Démonstrations supplémentaires de cours** 🖫

Montrer que : $\forall (a,b) \in \mathbb{Z}^2, \forall n \in \mathbb{N}^*, (a \vee b)^n = a^n \vee b^n$.

6 **Démonstrations supplémentaires de cours** 🖫

1) Montrer que :

$$\forall (a,b) \in (\mathbb{N} - \{0,1\})^2, \sup(a,b) = a \vee b\,.$$

2) Montrer que :

$$\forall (a,b) \in (\mathbb{N} - \{0,1\})^2, \inf(a,b) = a \wedge b\,.$$

7 **Nombres premiers entre eux**

Montrer que pour tout entier naturel n non nul :

1) $(n^2 \wedge n) \wedge (2n+1) = 1$ 2) $(n^3 + 2n) \wedge (n^4 + 3n^2 + 1) = 1$

3) $(n^2+1) \wedge ((n+1)^2 + 1) \in \{1,5\}$.

8 **Divisibilité**

Déterminer tous les entiers relatifs n tel que :

$$77 \mid 3n^2 - 5\,.$$

9 **Congruences**

Soit n un entier relatif impair tel que 3 ne divise pas n.

Montrer que :

$$n^2 \equiv 1\,[24]\,.$$

10 **Système d'équations diophantiennes**

Résoudre dans $\mathbb{N}^2$ le système d'équations d'inconnu (x,y) :

$$\begin{cases} x \wedge y = 18 \\ x \vee y = 540 \end{cases}.$$

11 **Système d'équations diophantiennes**

Résoudre dans $\mathbb{N}^2$ le système d'équations d'inconnu (x,y) :

$$\begin{cases} x + y = 1008 \\ x \wedge y = 24 \end{cases}.$$

12 **Système d'équations diophantiennes**

Résoudre dans $\mathbb{N}^2$ le système d'équations d'inconnu (x,y) :

$$\begin{cases} (x \vee y) - (x \wedge y) = 534 \\ (x \vee y) - 5(x \wedge y) = 510 \end{cases}.$$

13 **Equation diophantienne**

Résoudre dans $\mathbb{N}^2$ l'équation d'inconnue (x,y) :

$$(x \vee y) - 3(x \wedge y) = 135\,.$$

14 **Système d'équations diophantiennes**

Résoudre dans $\mathbb{N}^2$ le système d'équations d'inconnu (x,y) :

$$\begin{cases} x^2 + y^2 = 19\,476 \\ x \vee y = 1260 \end{cases}.$$

15 **Equation diophantienne**

Résoudre dans $\mathbb{N}^2$ l'équation d'inconnue (x,y) :

$$(x \wedge y) + (x \vee y) = y + 9\,.$$

16 **Equation diophantienne**

1) Montrer que 442 et 495 sont premiers entre eux.

2) Trouver tous les couples d'entiers relatifs (u,v) tels que :

$$442u + 495v = 1\,.$$

3) Résoudre dans $\mathbb{Z}/495\mathbb{Z}$ l'équation d'inconnue x :

$$\overline{442}x = \overline{314}\,.$$

17 ★ **Démonstrations supplémentaires de cours** 🖫

Théorie

Soit $(a,b,c) \in \mathbb{Z}^* \times \mathbb{Z}^* \times \mathbb{Z}$.

1) Résoudre dans $\mathbb{Z}^2$ l'équation d'inconnue (x,y) :

$$ax + by = c\,.$$

Application

2) Résoudre dans $\mathbb{Z}^2$ l'équation d'inconnue (x,y) :

a) $9x + 15y = 11$ b) $9x + 15y = 18$.

18 **Système d'équations diophantiennes**

Résoudre dans $\mathbb{N}^4$ le système d'équations d'inconnu (x,y,z,t) :

$$\begin{cases} xyz = 840 \\ xyt = 900 \\ yzt = 2100 \end{cases}.$$

19 **Divisibilité**

Montrer que : $\forall n \in \mathbb{Z}, 360 \mid n^2(n^2-1)(n^2-4)$.

20 **Equation diophantienne**

Montrer que : $\forall (x,y,z,t) \in \mathbb{Z}^4, \begin{cases} x^2 + 10y^2 = z^2 \\ 10x^2 + y^2 = t^2 \end{cases} \Leftrightarrow x = y = z = t = 0$.

21 ★ **Divisibilité**

Montrer que : $\forall (a,b,c) \in (\mathbb{Z}^*)^3, c \mid ab \Rightarrow c \mid (a \wedge c)(b \wedge c)$.

22 ★ **Nombres premiers entre eux**

Soient n un entier supérieur ou égal à 1, $a_1, ..., a_n$ des entiers relatifs non nuls premiers entre eux deux à deux.

Pour tout i de $\{1, ..., n\}$, on note :

$$A_i = \prod_{\substack{1 \leqslant k \leqslant n \\ k \neq i}}^{n} a_k\,.$$

Montrer que $A_1, ..., A_n$ sont premiers entre eux dans leur ensemble.

23 ★★ **Congruences**

Trouver tous les triplets d'entiers naturels (x,y,z) tels que :

$$2 \leqslant x \leqslant y \leqslant z\,,\ xy \equiv 1\,[z]\,,\ xz \equiv 1\,[y] \text{ et } yz \equiv 1\,[x]\,.$$

Les exercices du chapitre 10

24 ★ **Diviseurs de zéro de l'anneau Z/nZ** 🖫

Soit n un entier naturel non nul.

Déterminer les diviseurs de zéro de l'anneau $(\mathbb{Z}/n\mathbb{Z}\,,+,\times)$.

25 **PGCD**

1) Etablir que pour tout entier relatif n :

$$(5n^3-n)\wedge(n+2)=(n+2)\wedge 38\,.$$

2) Déterminer les entiers naturels d tels que :

$$(5n^3-n)\wedge(n+2)=19\,.$$

26 **Système d'équations diophantiennes**

Résoudre dans $\mathbb{Z}$ le système d'équations d'inconnu x :

$$\begin{cases}5x\equiv 7\ [11]\\ 7x\equiv 11\ [5]\\ 11x\equiv 5\ [7]\end{cases}.$$

27 **Système d'équations diophantiennes**

Résoudre dans $\mathbb{Z}$ le système d'équations d'inconnu x :

$$\begin{cases}x\equiv 1\ [6]\\ x\equiv 3\ [10]\\ x\equiv 7\ [15]\end{cases}.$$

28 **Système d'équations diophantiennes**

Déterminer le plus petit entier naturel x tel que :

$$x\equiv 6\ [23]\ \text{ et }\ x^2\equiv 13\ [23^2]\,.$$

29 ★ **Système d'équations diophantiennes** 🖫

Soient a et b deux entiers naturels non nuls.

Théorie

1) Résoudre dans $\mathbb{N}^2$ le système d'équations d'inconnu (x,y) :

$$\begin{cases}x\wedge y=a\\ x\vee y=b\end{cases}.$$

Application

2) Résoudre dans $\mathbb{N}^2$ le système d'équations d'inconnu (x,y) :

a) $\begin{cases}x\wedge y=10\\ x\vee y=22\end{cases}$ b) $\begin{cases}x\wedge y=8\\ x\vee y=80\end{cases}$.

30 ★★ **Equation fonctionnelle**

Démontrer qu'il n'existe pas d'application $f:\mathbb{Z}\longrightarrow\mathbb{Z}$ telle que :

$$\forall x\in\mathbb{Z},\ f(f(x))=x+1\,.$$

31 **Système d'équations diophantiennes**

Résoudre dans $\mathbb{N}^2$ le système d'équations d'inconnu (x,y) :

$$\begin{cases}x\wedge y=10\\ x\vee y=100\end{cases}.$$

32 **Equation diophantienne**

Résoudre dans $(\mathbb{N}^*)^2$ l'équation d'inconnue (x,y) :

$$(x\wedge y)+(x\vee y)=x+y\,.$$

33 **PGCD**

Soit n un entier naturel.

Montrer que le PGCD des entiers $2n+4$ et $3n+3$ ne peut être que 1, 2, 3 ou 6.

34 **PGCD**

Montrer que : $\forall n\in\mathbb{N},(2n+4)\wedge(3n+3)\,|\,6$.

35 **Nombres premiers entre eux** 🖫

Montrer que : $\forall(a,b)\in\mathbb{Z}^2,\ a\wedge b=1\Leftrightarrow(ab)\wedge(a+b)=1$.

36 **Divisibilité**

Montrer que : $\forall(x,y)\in\mathbb{Z}^2,\ 41\,|\,25x+3y\Leftrightarrow 41\,|\,31x+7y$.

37 ★ **PGCD** 🖫

Soient a un entier naturel et b un entier naturel non nul.

1) Montrer que si r est le reste de la division euclidienne de a par b, alors 2^r-1 est le reste de la division euclidienne de 2^a-1 par 2^b-1.

2) Montrer que :

$$(2^a-1)\wedge(2^b-1)=2^{a\wedge b}-1\,.$$

38 **Système d'équations diophantiennes**

Résoudre dans $\mathbb{N}^2$ le système d'équations d'inconnu (x,y) :

$$\begin{cases}192x+39y=192\wedge 39\\ 2520x-3960y=6480\end{cases}.$$

39 ★★ **Divisibilité**

Soient a un entier naturel supérieur ou égal à 2, b et c deux entiers naturels non nuls premiers entre eux.

Montrer que :

$$(a^b-1)(a^c-1)\,|\,(a-1)(a^{bc}-1)\,.$$

40 **Equation diophantienne**

Résoudre les équations d'inconnues x dans les ensembles indiqués.

1) $\overline{3}x=\overline{1}$ (dans $\mathbb{Z}/7\mathbb{Z}$).

2) $\overline{3}x=\overline{1}$ (dans $\mathbb{Z}/12\mathbb{Z}$).

3) $x^2+\overline{7}x+\overline{1}=\overline{0}$ (dans $\mathbb{Z}/9\mathbb{Z}$).

41 **Système d'équations diophantiennes**

Résoudre dans $(\mathbb{Z}/9\mathbb{Z})^2$ puis sur $(\mathbb{Z}/8\mathbb{Z})^2$ le système d'équations d'inconnu (x,y) :

$$\begin{cases}\overline{7}x+\overline{5}y=\overline{2}\\ \overline{5}x+\overline{4}y=\overline{7}\end{cases}.$$

42 **Equation diophantienne**

Résoudre les équations d'inconnues x dans les ensembles indiqués.

1) $x^2-\overline{2}x-\overline{2}=\overline{0}$ (dans $\mathbb{Z}/5\mathbb{Z}$).

2) $x^2-\overline{2}x+\overline{2}=\overline{0}$ (dans $\mathbb{Z}/5\mathbb{Z}$).

3) $x^2-x-\overline{1}=\overline{0}$ (dans $\mathbb{Z}/5\mathbb{Z}$).

4) $2x^2-3x-2\equiv 0\ [7]$ (dans $\mathbb{Z}$).

5) $x^2=\overline{1}$ (dans $\mathbb{Z}/18\mathbb{Z}$).

6) $x^3-\overline{3}x^2+\overline{2}x=\overline{0}$ (dans $\mathbb{Z}/24\mathbb{Z}$).

7) $x^2-\overline{4}x+\overline{3}=\overline{0}$ (dans $\mathbb{Z}/143\mathbb{Z}$).

43 **Système d'équations diophantiennes**

Résoudre dans $(\mathbb{Z}/20\mathbb{Z})^2$ le système d'équations d'inconnu (x,y) :

$$\begin{cases}\overline{5}x+\overline{2}y=\overline{3}\\ \overline{2}x+\overline{4}y=\overline{6}\end{cases}.$$

Les exercices du chapitre 10

44 **PGCD** 🖫

Soient m, n, a, b, c et d des entiers relatifs tels que $ad-bc=1$.

Montrer que :

$$(am+bn)\wedge(cm+dn)=m\wedge n\,.$$

45 **PGCD**

Montrer que : $\forall n\in\mathbb{Z},(21n+4)\wedge(14n+3)=1$.

46 **PPCM**

Montrer que :

$$\forall n\in\mathbb{N}^*,\text{PPCM}(1,2,...,2n)=\text{PPCM}(n+1,n+2,...,2n)\,.$$

47 **PGCD**

Montrer que : $\forall(a,b)\in\mathbb{Z}^2,(a^2+b^2)\wedge(ab)=(a\wedge b)^2$.

48 **PGCD et PPCM** 🖫

Montrer que : $\forall(a,b)\in\mathbb{Z}^2,(a+b)\wedge(a\vee b)=a\wedge b$.

49 **PGCD**

Montrer que : $\forall(a,b)\in\mathbb{Z}^2,a^2\wedge(ab)\wedge b^2=(a\wedge b)^2$.

50 **PGCD**

Montrer que :

$$\forall(a,b)\in\mathbb{N}^2,a\wedge b=1\Rightarrow(a^2-ab+b^2)\wedge(a+b)\leqslant 3\,.$$

On utilisera l'exercice 46.

51 **Démonstrations supplémentaires de cours** 🖫

Soient n et p deux entiers naturels non nuls.

Montrer que :

$$\forall(x_1,...,x_n)\in\mathbb{Z}^n,\forall(y_1,...,y_p)\in\mathbb{Z}^p,\left(\bigwedge_{i=1}^{n}x_i\right)\left(\bigwedge_{j=1}^{p}y_j\right)=\bigwedge_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant p}}x_iy_j\,.$$

52 **PGCD** 🖫

Montrer que :

$$\forall(a,b,c,d)\in\mathbb{Z}^4,a\wedge b=c\wedge d=1\Rightarrow(ac)\wedge(bd)=(a\wedge d)(b\wedge c)\,.$$

53 **Démonstrations supplémentaires de cours** 🖫

Montrer que : $\forall(a,b)\in\mathbb{N}^*\times\mathbb{N}^*,\mathcal{D}^+_{ab}=\mathcal{D}^+_a\mathcal{D}^+_b$.

54 **Nombres premiers entre eux** 🖫

Soient a, b et c des entiers relatifs.

Montrer que si a, b et c sont premiers entre eux deux à deux, alors les entiers $ab+bc+ca$ et abc sont premiers entre eux.

55 **PGCD**

Trouver tous les entiers naturels n tels que :

$$(2n+8)\wedge(3n+15)=6\,.$$

56 **Système d'équations diophantiennes**

Résoudre dans $\mathbb{N}^2$ le système d'équations d'inconnu (x,y) :

$$\begin{cases}x+y=56\\x\vee y=105\end{cases}.$$

57 **Equation diophantienne**

Résoudre dans $\mathbb{N}^2$ l'équation d'inconnue (x,y) :

$$(x\vee y)-(x\wedge y)=243\,.$$

58 **Système d'équations diophantiennes**

Résoudre dans $\mathbb{N}^2$ le système d'équations d'inconnu (x,y) :

$$\begin{cases}(2x+y)(5x+2y)=1620\\xy=3(x\vee y)\end{cases}.$$

59 **Système d'équations diophantiennes**

Résoudre dans $\mathbb{N}^2$ le système d'équations d'inconnu (x,y) :

$$\begin{cases}x\wedge y=12\\x\vee y=420\\20<y<x\end{cases}.$$

60 **Système d'équations diophantiennes**

Résoudre dans $\mathbb{N}^2$ le système d'équations d'inconnu (x,y) :

$$\begin{cases}x\wedge y=x-y\\x\vee y=72\end{cases}.$$

61 **Système d'équations diophantiennes**

Résoudre dans $\mathbb{N}^2$ le système d'équations d'inconnu (x,y) :

$$\begin{cases}x+y=84\\x\vee y=(x\wedge y)^2\end{cases}.$$

62 **Divisibilité**

Soient a et b deux entiers naturels non nuls tel que $a\wedge b=1$.

Trouver les entiers naturels x non nuls tels que :

$$a\,|\,bx\ \text{ et }\ b\,|\,xa\ \text{ et }\ x\,|\,ab\,.$$

63 **Egalité de Bézout**

1) Vérifier que 429 et 700 sont premiers entre eux.

2) Déterminer tous les couples d'entiers relatifs (u,v) tels que :

$$700u+429v=1\,.$$

3) Quel est l'inverse de $\overline{429}$ dans $\mathbb{Z}/700\mathbb{Z}$?

64 **Egalité de Bézout**

Montrer que : $\forall n\in\mathbb{Z},\exists(a,b,c)\in\mathbb{Z}^3,n=1914a+1915b+1916c$.

65 **PGCD**

Montrer que : $\forall n\in\mathbb{N},(2^n+3^n)\wedge(2^{n+1}+3^{n+1})=1$.

66 **PGCD**

Pour tout entier naturel n non nul, on note :

$$u_n=2^n+3^n+5^n\,.$$

Montrer que :

$$\forall n\in\mathbb{N}^*,\text{PGCD}(u_n,u_{n+1},u_{n+2})=2\,.$$

67 **Equation fonctionnelle**

Trouver toutes les applications $f:\mathbb{N}^*\times\mathbb{N}^*\longrightarrow\mathbb{N}^*$ telles que :

$$\begin{vmatrix}\forall a\in\mathbb{N}^*,f(a,a)=a\\\forall(a,b)\in\mathbb{N}^*\times\mathbb{N}^*,f(a,b)=f(b,a)\\\forall(a,b)\in\mathbb{N}^*\times\mathbb{N}^*,f(a,b)=f(a,a+b)\end{vmatrix}.$$

68 **Equation diophantienne**

Résoudre dans $\mathbb{Z}^2$ l'équation d'inconnue (x,y) :

$$(x-27)(y+12)=xy\,.$$

Les exercices du chapitre 10

69 **Divisibilité**

1) Montrer que :

$$\forall n \in \mathbb{Z}, 12 \mid n^4 - 4n^3 + 5n^2 - 2n\,.$$

2) Montrer que :

$$\forall (m,n) \in \mathbb{Z}^2, 30 \mid mn(m^4 - n^4)\,.$$

3) Montrer que :

$$\forall n \in \mathbb{N}, 3804 \mid (n^3 - n)(5^{8n+4} + 3^{4n+2})\,.$$

70 ★★ **Equation fonctionnelle**

Soit $f : \mathbb{N}^* \longrightarrow \mathbb{N}^*$ une application telle que :

- f est strictement croissante ;
- $f(2) = 2$;
- $\forall (m,n) \in (\mathbb{N}^*)^2, m \wedge n = 1 \Rightarrow f(mn) = f(m)f(n)$.

Montrer que :

$$\forall n \in \mathbb{N}^*, f(n) = n\,.$$

71 **PGCD**

Soient a, b, c et n des entiers naturels non nuls tels que :

$$a \wedge b = 1 \text{ et } ab = c^n\,.$$

Montrer qu'il existe un couple (α, β) de $(\mathbb{N}^*)^2$ tel que :

$$a = \alpha^n \text{ et } b = \beta^n\,.$$

72 **Nombres premiers entre eux** 🖫

Montrer que : $\forall n \in \mathbb{N}^*, n\,! \wedge (n\,! + 1) = 1$.

73 **PGCD**

Soient a et b deux entiers naturels non nuls tels que a soit impair et supérieur ou égal à 3.

Montrer que :

$$(2^a - 1) \wedge (2^b + 1) = 1\,.$$

74 **Equation diophantienne**

Déterminer tous les couples (a,b) de $(\mathbb{N}^*)^2$ tels que :

$$a < b \text{ et } (a \vee b) - (a \wedge b) = 77\,.$$

75 **Equation diophantienne**

Déterminer tous les couples (a,b) d'entiers naturels tels que :

$$a \leqslant b\,,\ a + b = 256 \text{ et } a \wedge b = 16\,.$$

76 **Equation diophantienne**

Résoudre dans $\mathbb{Z}^2$ les équations suivantes d'inconnues (x,y) :

1) $7x - 19y = 1$ 2) $7x - 19y = 9$.

77 **Equation diophantienne**

Résoudre dans $\mathbb{Z}^2$ l'équation d'inconnue (x,y) :

$$3675x - 5145y = 4410\,.$$

78 **Equation diophantienne**

Résoudre dans $\mathbb{Z}^2$ l'équation d'inconnue (x,y) :

$$323x - 391y = 612\,.$$

79 **Anneau Z/nZ**

Montrer que dans l'anneau $\mathbb{Z}/1700\mathbb{Z}$, l'élément $\overline{429}$ est inversible et déterminer son inverse.

80 ★★ **Nombres premiers entre eux**

Soit n un entier naturel non nul.

On note :

$$S_n = \sum_{k=1}^{n} k^3\,.$$

1) Calculer pour tout entier naturel n non nul, $S_n \wedge S_{n+1}$.

2) Montrer que :

$$\forall n \in \mathbb{N}^*, (S_n \wedge S_{n+1}) \wedge S_{n+2} = 1\,.$$

81 **Nombres premiers entre eux**

Pour tout entier naturel n non nul, on pose :

$$a_n = 15n^2 + 8n + 6 \text{ et } b_n = 30n^2 + 21n + 13\,.$$

1) Montrer que pour tout entier naturel n non nul :

$$b_n - 2a_n \mid a_n - 5\,.$$

2) En déduire que pour tout entier naturel n non nul, les entiers a_n et b_n sont premiers entre eux.

82 **PGCD** 🖫

Montrer que : $\forall (a,b) \in \mathbb{N}^* \times \mathbb{N}^*, a \wedge b = 1 \Rightarrow (a+b) \wedge (a-b) \in \{1, 2\}$.

83 ★ **Nombres premiers entre eux**

Soient n et d deux entiers naturels non nuls.

1) Montrer que d divise n et $n+2$, alors d est égal à 1 ou à 2.

2) En déduire que parmi quatre entiers naturels non nuls consécutifs, il y en a toujours un qui est premier avec chacun des trois autres.

84 **Nombres premiers entre eux** 🖫

Montrer que : $\forall n \in \mathbb{N}^*, (n\,! + 1) \wedge ((n+1)\,! + 1) = 1$.

On utilisera l'exercice 72.

85 **Système d'équations diophantiennes**

Soit k un entier relatif.

1) Quels sont les restes possibles de la division de k^2 par 7 ?

2) Déterminer les entiers relatifs x tels que $x^2 \equiv 2\ [7]$.

3) L'équation d'inconnue x : $\overline{3}x^2 = \overline{7}x + \overline{2}$ a-t-elle des solutions dans l'ensemble $\mathbb{Z}/7\mathbb{Z}$?

4) Dans $\mathbb{Z}/7\mathbb{Z}$, quel est l'inverse de $\overline{3}$? Celui de $\overline{4}$?

5) Résoudre dans $\mathbb{Z}^2$ le système d'équations d'inconnu (x,y) :

$$\begin{cases} 8x^2 + xy \equiv 3\ [7] \\ x^2 - xy \equiv 1\ [7] \end{cases}.$$

86 **Système d'équations diophantiennes**

Soit k un entier relatif.

1) Quels sont les restes possibles de la division de k^2 par 11 ?

2) Déterminer les entiers relatifs x tels que $x^2 \equiv 1\ [11]$.

3) Déterminer les entiers relatifs x tels que $x^2 \equiv 3\ [11]$.

4) Dans l'anneau $\mathbb{Z}/11\mathbb{Z}$, quel est l'inverse de $\overline{2}$? l'inverse de $\overline{3}$? l'inverse de $\overline{5}$?

5) Résoudre dans $(\mathbb{Z}/11\mathbb{Z})^2$ le système d'équations d'inconnu (x,y) :

$$\begin{cases} \overline{4}x^2 + y^2 = \overline{2} \\ xy = \overline{3} \end{cases}.$$