Résumé de CM8

Divisibilité

Définition Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^* := \mathbb{Z}\backslash\{0\}$. Lorsqu'il existe un entier $q \in \mathbb{Z}$ tel que $a = bq$, on dit que a est un **multiple** de b et que b est un **diviseur** de a. On le note par $b|a$. □

Le théorème suivant est fondamental :

Théorème (Division euclidienne). Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^* := \mathbb{Z}\backslash\{0\}$. Alors, il existe un unique couple $(q, r) \in \mathbb{Z}^2$ vérifiant

$$a = qb + r, \qquad 0 \leqslant r < |b|.$$

□

Preuve Comme $\mathbb{R} = \coprod_{q\in\mathbb{Z}}[|b|q, |b|(q+1)[$, $\exists! q \in \mathbb{Z}$ tel que $bq \leqslant a < bq + |b|$, d'où en posant $r = a - bq$, on voit que les deux conditions sont vérifiées. □

PGCD et PPCM

Soit $(a, b) \in \mathbb{Z}^2\backslash\{(0, 0)\}$. Alors, l'ensemble

$$\mathcal{M} := \{\, m \in \mathbb{N} \,|\, a \,|\, m \text{ et } b \,|\, m \,\}$$

est non-vide car $ab \in \mathcal{M}$. Lorsque l'ensemble $\mathcal{M} \cap \mathbb{N}^*$ est non-vide, son plus petite élément est dit le plus petit commun multiple (**PPCM**), noté $\text{ppcm}(a, b)$. Sinon, $0 \in \mathcal{M}$ est dit le PPCM, noté également. L'ensemble

$$\mathcal{D} := \{\, d \in \mathbb{N} \,|\, d \,|\, a \text{ et } d \,|\, b \,\}$$

est non-vide car $1 \in \mathcal{D}$, de plus cet ensemble est fini. Le plus grand élément de $\mathcal{D}$ est dit le petit grand commun diviseur (**PGCD**), noté $\text{pgcd}(a, b)$.

Théorème (PPCM) Soient a et b deux entiers non nuls. Alors, un entier m qui est un multiple commun de a et de b et un multiple de $\text{ppcm}(a, b)$. □

Preuve Posons $l = \text{ppcm}(a, b)$. Alors, $\exists!(q, r) \in \mathbb{Z}^2$ tel que

$$m = ql + r \qquad 0 \leqslant r < l.$$

Comme $r = m - ql$ et m et l sont multiples de a et de b, r l'est aussi. Comme $0 \leqslant r < l$, la minimalité de l implique que $r = 0$, i.e., $m = ql$. □

Théorème (PGCD) Soient a et b deux entiers non nuls. Alors, un entier d qui est un diviseur commun de a et de b et un diviseur de $\text{pgcd}(a, b)$. □

Preuve Posons $m = \text{pgcd}(a, b)$. Il suffit de montrer que $l := \text{ppcm}(m, d) = m$. Comme a est un multiple de m et de d, a est un multiple de l. De même, b est un multiple de l, d'où l est un diviseur commun de a et de b. En particulier, ceci implique que $l \leqslant m$. Par la définition de l, on a $l \geqslant m$, d'où $l = m$. □

Maintenant, montrons le théorème suivant:

Théorème Soient $a, b \in \mathbb{N}^*$. Alors, $a \cdot b = \text{ppcm}(a, b) \cdot \text{pgcd}(a, b)$. □

Preuve Posons $l = \text{ppcm}(a, b)$. Comme l est un multiple de a et de b, il existent $a', b' \in \mathbb{N}^*$ tels que

$$l = ab' = a'b. \tag{1}$$

Comme ab est un multiple commun de a et b, c'est un multiple de l, i.e., il existe $d \in \mathbb{N}^*$ tel que

$$ab = dl. \tag{2}$$

D'après (1), on a $ab = da'b = dab'$, d'où

$$a = da', \qquad b = db'. \tag{3}$$

Posons $m = \text{pgcd}(a, b)$. Comme (3) implique que d est un diviseur commun de a et b, il existe $e \in \mathbb{N}^*$ tel que $m = de$. Comme m est un diviseur de a et b, (3) implique que a', b' sont divisible par e, i.e., il existe $a'', b'' \in \mathbb{N}^*$ tels que $a' = ea'', b' = eb''$. Donc, (1) implique que

$$l = ab''e = ba''e.$$

Si $e > 1$, alors, l/e devient un multiple commun qui est plus petit que l, ce qui est absurde. Donc, on a $e = 1$, i.e., $m = d$ et (2) implique l'énoncé. □

Algorithme d'Euclide

Étant donné deux entiers $a, b \in \mathbb{N}^*$, l'"**algorithme d'Euclide** nous donne une méthode pratique pour calculer le PGCD de a et b. Le théorème précédent nous permet de calculer le PPCM de a et b, ainsi.

Le principe de cet algorithme est suivant: soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$. Par la division euclidienne, il existe un unique $(q, r) \in \mathbb{Z}^2$ tel que $a = bq + r$ et $0 \leqslant r < |b|$. Alors,

$$\text{pgcd}(a, b) = \text{pgcd}(a - bq, b) = \text{pgcd}(b, r). \tag{4}$$

Basé sur ce principe, l'**algorithme d'Euclide** est présenté comme suit.

Soit $a, b \in \mathbb{Z}^*$ tel que $|a| > |b|$. Alors, $\exists!(q, r) \in \mathbb{Z}^2$ tel que

$$a = qb + r \qquad 0 \leqslant r < |b|.$$

Si $r = 0$, alors, $a = qb$ et $\text{pgcd}(a, b) = b$. Supposons que $r \neq 0$. Alors, il existe $n \in \mathbb{N}^*$ vérifiant la propriété suivante:

$$\begin{aligned}
\exists!\,(q_1, r_1) \in \mathbb{Z}^2 \quad &\text{t.q.} \quad b = q_1 r + r_1 \qquad 0 < r_1 < r, \\
\exists!\,(q_2, r_2) \in \mathbb{Z}^2 \quad &\text{t.q.} \quad r = q_2 r_1 + r_2 \qquad 0 < r_2 < r_1, \\
&\vdots \\
\exists!\,(q_{n-1}, r_{n-1}) \in \mathbb{Z}^2 \quad &\text{t.q.} \quad r_{n-3} = q_{n-1} r_{n-2} + r_{n-1} \qquad 0 < r_{n-1} < r_{n-2}, \\
\exists!\,q_n \in \mathbb{Z} \quad &\text{t.q.} \quad r_{n-2} = q_n r_{n-1}.
\end{aligned}$$

Alors, le principe (4) expliqué ci-dessus implique que

$$\begin{aligned}\mathrm{pgcd}(a,b) =& \mathrm{pgcd}(a-qb,b) = \mathrm{pgcd}(b,r)\\ =& \mathrm{pgcd}(b-q_1r,r) = \mathrm{pgcd}(r,r_1)\\ =& \mathrm{pgcd}(r-q_2r_1,r_1) = \mathrm{pgcd}(r_1,r_2)\\ &\vdots\\ =& \mathrm{pgcd}(r_{n-3}-q_{n-1}r_{n-2},r_{n-2}) = \mathrm{pgcd}(r_{n-2},r_{n-1})\\ =& r_{n-1},\end{aligned}$$

d'où $\boxed{\mathrm{pgcd}(a,b) = r_{n-1}}$! □

Le théorème suivant est techniquement important:

Théorème (Bézout) Soient $a, b \in \mathbb{Z}^*$ deux entiers. Alors, a et b sont **premiers entre eux**, i.e., $\mathrm{pgcd}(a,b) = 1$ si et seulement si $\exists\,(u,v) \in \mathbb{Z}^2$ tel que $au + bv = 1$ (identité de Bézout). □

Preuve $\Leftarrow$) Pour un diviseur commun $d \in \mathbb{N}^*$ de a et b, $d|au$ et $d|bv$ implique $d|(au+bv)$, i.e., $d|1$ d'où $d = 1$. Donc, $\mathrm{pgcd}(a,b) = 1$.
$\Rightarrow$) Comme

$$au + bv = a(u+v) + (b-a)v = (a-b)u + b(u+v),$$

on pourra montrer l'énoncé par récurrence sur $\max(a,b)$. □

Voici un corollaire simple et utile de ce théorème :

Corollaire Soient $a, b \in \mathbb{Z}^*$ et $d \in \mathbb{N}^*$. Alors, l'**équation diophantienne** $ax + by = d$ admet une solution $(x,y) \in \mathbb{Z}^2$ si et seulement si $\mathrm{pgcd}(a,b)|d$. □

Alors, comment peut on calculer un pair $(u,v) \in \mathbb{Z}^2$ vérifiant $au + bv = \mathrm{pgcd}(a,b)$?
Il suffit de reprendre les divisions successives effectuées en algorithme d'Euclide:

$$\begin{aligned}\mathbf{a} = q\mathbf{b} + r \quad &\Longrightarrow \quad r = \mathbf{a} - q\mathbf{b}\\ \mathbf{b} = q_1 r + r_1 \quad &\Longrightarrow \quad r_1 = \mathbf{b} - q_1 r\\ r = q_2 r_1 + r_2 \quad &\Longrightarrow \quad r_2 = r - q_2 r_1\\ &\vdots\\ r_{n-4} = q_{n-2} r_{n-3} + r_{n-2} \quad &\Longrightarrow \quad r_{n-2} = r_{n-4} - q_{n-2} r_{n-3}\\ r_{n-3} = q_{n-1} r_{n-2} + r_{n-1} \quad &\Longrightarrow \quad r_{n-1} = r_{n-3} - q_{n-1} r_{n-2}\end{aligned}$$

On lit les formules du bas vers le haut:

1. Remplacer le r_{n-2} avec le côté droit de $r_{n-2} = \cdots$ (une ligne au dessus).
   On aura la formule de la forme $r_{n-1} = (\cdots)r_{n-4} + (\cdots)r_{n-3}$.
2. Remplacer le r_{n-3} avec le côté droit de $r_{n-3} = \cdots$ (une ligne au dessus).
   On aura la formule de la forme $r_{n-1} = (\cdots)r_{n-5} + (\cdots)r_{n-4}$.

3. Répéter cette opération plusieurs fois; vous aurez une formule de la forme
$$r_{n-1} = (\cdots)r_1 + (\cdots)r_2.$$
4. Remplacer le r_2 avec le côté droit de $r_2 = \cdots$ ($3^{\text{ème}}$ ligne).
On aura la formule de la forme $r_{n-1} = (\cdots)r + (\cdots)r_1$.
5. Remplacer le r_1 avec le côté droit de $r_1 = \cdots$ ($2^{\text{ème}}$ ligne).
On aura la formule de la forme $r_{n-1} = (\cdots)\mathbf{b} + (\cdots)r$.
6. Remplacer le r avec le côté droit de $r = \cdots$ ($1^{\text{ère}}$ ligne).
Enfin, on aura la formule de la forme $r_{n-1} = (\cdots)\mathbf{a} + (\cdots)\mathbf{b}$!

Voici un exemple: $a = 625$ et $b = 216$.

$$\begin{aligned}
\mathbf{625} = 2 \cdot \mathbf{216} + 193 \quad &= \quad 42 \cdot \mathbf{216} + (-47) \cdot (\mathbf{625} - 2 \cdot \mathbf{216}) = (-47) \cdot \mathbf{625} + 136 \cdot \mathbf{216} \\
\mathbf{216} = 1 \cdot 193 + 23 \quad &= \quad (-5) \cdot 193 + 42 \cdot (\mathbf{216} - 1 \cdot 193) = 42 \cdot \mathbf{216} + (-47) \cdot 193 \\
219 = 8 \cdot 23 + 9 \quad &= \quad 2 \cdot 23 + (-5) \cdot (193 - 8 \cdot 23) = (-5) \cdot 193 + 42 \cdot 23 \\
23 = 2 \cdot 9 + 5 \quad &= \quad (-1) \cdot 9 + 2 \cdot (23 - 2 \cdot 9) = 2 \cdot 23 + (-5) \cdot 9 \\
9 = 1 \cdot 5 + 4 \quad &= \quad 1 \cdot 5 + (-1) \cdot (9 - 1 \cdot 5) = (-1) \cdot 9 + 2 \cdot 5 \\
5 = 1 \cdot 4 + 1 \quad \Longrightarrow \quad 1 \quad &= \quad 1 \cdot 5 + (-1) \cdot 4
\end{aligned}$$

d'où on obtient l'identité de Bézout $\mathbf{625} \cdot (-47) + \mathbf{216} \cdot 136 = 1$.

Lemme de Gauss

Le théorème suivant est une propriété de $\mathbb{Z}$ très importante :

Théorème (Lemme de Gauss) Soient $a, b \in \mathbb{Z}^*$ deux entiers qui sont premiers entre eux et soit $c \in \mathbb{Z}$ tel que $a \mid bc$. Alors, $a \mid c$. □

Preuve 1 Le nombre bc étant un multiple de a et de b, c'est un multiple de $\text{ppcm}(a, b) = ab$ (car $\text{pgcd}(a, b) = 1$), d'où il existe $d \in \mathbb{Z}^*$ tel que $bc = abd \Leftrightarrow c = ad$, c.-à-d., $a \mid c$. □

Preuve 2 Comme $\text{pgcd}(a, b) = 1$, il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$. Multipliant les deux côtés par c, on obtient $a(cu) + (bc)v = c$. Par l'hypothèse $a|bc$, cette dernière implique $a|c$. □

Nombres premiers

Définition Un entier $p \in \mathbb{N}^*$ est dit **premier** si ses seuls diviseurs positifs sont 1 et p. □

Exemples $2, 3, 5(= 2^2+1), 7, 11, 13, 17(= 2^4+1), 19, 23, 29, 31, 37, 41, 43, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, \cdots, 257(= 2^8 + 1), \cdots, 65537(= 2^{16} + 1), \cdots$ □

Commençons par un lemme technique:

Lemme Soit $n > 2$ un entier et soit p le plus petit diviseur de n supérieur à 1. Alors, p est un nombre premier. □

Preuve Si p n'était pas premier, il y aurait un diviseur de p tel que $d \geqslant 2$ et $d|p$. Comme $p|n$, on en déduit que $d|n$. Ceci contredit à la minimalité de p. □

Comme une application de ce lemme, voici un premier résultat :

Théorème (Euclide) Il existe une infinité de nombres premiers. □

Preuve Supposons qu'il y a k nombres premiers pour un $k \in \mathbb{N}^*$.
Montrons qu'il en existe un autre.
Soient $p_1, p_2, \cdots, p_k$ k nombres premiers deux à deux distincts. Posons

$$N = p_1 p_2 \cdots p_k + 1.$$

Soit $p > 1$ le plus petit diviseur de N. Alors, le lemme ci-dessus montre que p est un nombre premier. De plus, comme p_i $(1 \leqslant i \leqslant k)$ ne divise jamais N, le nombre premier p_i ne peut être un des p_i $(1 \leqslant i \leqslant k)$, d'où on a $k+1$ nombres premiers : $p_1, p_2, \cdots, p_k$ et p. □

Le théorème suivant traite une propriété remarquable sur $\mathbb{Z}$:

Théorème (Décomposition en facteurs premiers) Soit $n \in \mathbb{N}$ un entier tel que $n > 1$. Il existe une unique écriture de n sous la forme $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ où

1. les entiers p_i sont premiers,
2. les exposants α_i sont entiers strictement positifs,
3. $p_1 < p_2 < p_3 < \cdots < p_s$. □

Preuve (l'existence) Démo. par récurrence forte.
Pour $n = 2$, l'énoncé est claire. Fixons $n \geqslant 3$. Soit p le plus petit diviseur (de n) > 1. D'après le lemme ci-dessus, p est premier et, par hypothèse de récurrence, $\dfrac{n}{p}$ admet une telle décomposition.
(l'unicité) Démo. par récurrence forte avec le lemme de Gauss. □

Le théorème suivant est un corollaire simple :

Théorème Soient $a, b \in \mathbb{N}^*$ deux entiers. Soient $p_1, p_2, \cdots, p_s$ nombres premiers deux à deux distincts tels qu'ils existent $\alpha_1, \alpha_2, \cdots, \alpha_s$ et $\beta_1, \beta_2, \cdots, \beta_s \in \mathbb{N}$ tels que

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s} \qquad \text{et} \qquad b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}.$$

Alors,

1. $\text{ppcm}(a, b) = p_1^{\max\{\alpha_1, \beta_1\}} p_2^{\max\{\alpha_2, \beta_2\}} \cdots p_s^{\max\{\alpha_s, \beta_s\}}$,
2. $\text{pgcd}(a, b) = p_1^{\min\{\alpha_1, \beta_1\}} p_2^{\min\{\alpha_2, \beta_2\}} \cdots p_s^{\min\{\alpha_s, \beta_s\}}$. □