

Résumé de CM8

Identité de Bézout

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

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, $\text{pgcd}(a, b) = 1$.

$\Rightarrow$) Comme

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

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

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 $\text{pgcd}(a, b)|d$. $\square$

Comment peut on calculer un pair $(u, v) \in \mathbb{Z}^2$ vérifiant $au + bv = \text{pgcd}(a, b)$?

Il suffit de reprendre les divisions successives effectuées en algorithme d'Euclide.

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

$$a = qb + r \quad 0 \leq r < |b|.$$

Si $r = 0$, $0 \cdot a + \frac{|b|}{b} \cdot b = |b| = \text{pgcd}(a, b)$ est une identité de Bézout. Supposons que $r \neq 0$. Alors, il existe $n \in \mathbb{N}^*$ vérifiant la propriété suivante:

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

Réécrivons ces égalités:

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

On lit les formules du bas vers le haut:

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

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

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

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

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 $a \mid bc$, cette dernière implique $a \mid c$. □

Équation diophantienne

Ici, on travaille sur une équation diophantienne

$$ax + by = d, \tag{1}$$

où $a, b \in \mathbb{N}^*$ et $d \in \mathbb{N}^*$ qui est un multiple de $D := \text{pgcd}(a, b)$. Quitte à rétrécir, on suppose que $\text{pgcd}(a, b) = 1$. (Pourquoi ?)

On a vu que cette équation admet *une* solution $(x_0, y_0) \in \mathbb{Z}^2$. La question que l'on se pose est

Comment peut-on trouver *les* solutions de l'équation (1) ?

Soustrayant de l'équation (1) par $ax_0 + by_0 = d$, on obtient

$$a(x - x_0) + b(y - y_0) = 0 \iff a(x - x_0) = b(y_0 - y).$$

Comme a et b sont premiers entre eux et que a divise $b(y_0 - y)$, le lemme de Gauss implique que $y_0 - y$ est un multiple de a , i.e., $\exists k \in \mathbb{Z}$ tel que $y_0 - y = ak$. Ceci implique que

$$a(x - x_0) = b \cdot ak \iff x - x_0 = bk.$$

On en déduit que l'ensemble des solutions de l'équation (1), i.e., $\{(x, y) \mid (x, y) \in \mathbb{Z}^2 \text{ vérifie (1)}\}$ est

$$\left\{ (x_0 + bk, y_0 - ak) \mid k \in \mathbb{Z} \right\}.$$

(Est-il claire que, $\forall k \in \mathbb{Z}$, $(x, y) = (x_0 + bk, y_0 - ak)$ est une solution de l'équation (1) ?)

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, $\dots$, 257(= 2^8+1), $\dots$, 65537(= $2^{16}+1$), $\dots$ □

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 $d \geq 2$ 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 $p_1, p_2, \dots, p_k$ 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 ($1 \leq i \leq k$) ne divise jamais N , le nombre premier p_i ne peut être un des p_i ($1 \leq i \leq k$), d'où on a $k + 1$ nombres premiers : $p_1, p_2, \dots, p_k$ et p . □