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). □

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 $\max(a,b)$. □

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 $\text{pgcd}(a,b)|d$. □

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

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

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

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

Réécrivons ces égalités:

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

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 une 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 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 $a|c$. □

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 $\text{pgcd}(a, b) = 1$, car on peut toujours diviser les deux côtés de l'équation (1) par D: $\dfrac{a}{D}x + \dfrac{b}{D}y = \dfrac{d}{D}$.

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

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

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

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

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

$$\Big\{ \big(x_0 + bk, y_0 - ak\big) \,\Big|\, k \in \mathbb{Z} \Big\}.$$

(Est-il claire que, $\forall\, k \in \mathbb{Z}$, $(x, y) = \big(x_0 + bk, y_0 - ak\big)$ 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 $2, 3, 5(= 2^2+1), 7, 11, 13, 17(= 2^4+1), 19, 23, 29, 31, 37, 41, 43, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, \cdots, 257(= 2^8 + 1), \cdots, 65537(= 2^{16} + 1), \cdots$ □

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. □

Voici un théorème assez utile (pour une preuve, voir la Feuille X de TD !):

Le petit théorème de Fermat Soit p un nombre premier et a un entier qui n'est pas un multiple de p. Alors, p divise $a^{p-1} - 1$. □