$a \wedge b = 1 \iff (a+b) \wedge ab = 1$

Samuel Rochetin

Vendredi 22 janvier 2016

Résumé

L'exercice suivant est classique : « montrer que si a et b sont premiers entre eux, alors $a+b$ et ab sont premiers entre eux ». Le but de ce document est de présenter cinq méthodes de résolution différentes, accessibles à un élève de terminale S, spécialité mathématique. Bien qu'elles soient toutes élémentaires, aucune n'est immédiate, c'est précisément ce qui rend cet exercice savoureux.

1 Le sens indirect

Tout d'abord, remarquons que la réciproque est vraie. Il suffit s'appliquer le théorème de Bézout.

$$\begin{aligned}
(a+b) \wedge ab = 1 &\iff \exists (u,v) \in \mathbb{Z}^2, (a+b)u + abv = 1 \\
&\iff \exists (u,v) \in \mathbb{Z}^2, a(u+bv) + bu = 1 \\
&\implies \exists (u',v') \in \mathbb{Z}^2, au' + bv' = 1 && \text{en posant } u' = u+bv \text{ et } v' = u \\
&\iff a \wedge b = 1
\end{aligned}$$

2 Le sens direct

2.1 Par le théorème de Bézout

2.1.1 Première méthode

Nous exprimons a comme combinaison linéaire de $a+b$ et ab.

$$\begin{aligned}
a \wedge b = 1 &\iff \exists (u,v) \in \mathbb{Z}^2, au + bv = 1 \\
&\iff \exists (u,v) \in \mathbb{Z}^2, a^2u + abv = a && \text{en multipliant par } a \neq 0 \\
&\iff \exists (u,v) \in \mathbb{Z}^2, (a+b)au + ab(v-u) = a && \text{car } a^2 = a(a+b) - ab
\end{aligned}$$

Posons $d = (a+b) \wedge ab$. d divise toute combinaison linéaire de $a+b$ et ab, donc d divise a d'après ci-dessus. Par symétrie du problème, on obtient d divise b. Donc d est un diviseur commun à a et b. Par définition du PGCD, $1 \leq d \leq a \wedge b = 1$. D'où $d = 1$.

2.1.2 Deuxième méthode

Nous démontrons d'abord le lemme suivant.

Proposition 2.1.1. *Si x est premier avec y et z, alors x est premier avec yz.*

Démonstration. Le théorème de Bézout donne :

$$\begin{aligned}
x \wedge y = 1 &\iff \exists (u,v) \in \mathbb{Z}^2, xu + yv = 1 \\
&\iff \exists (u,v) \in \mathbb{Z}^2, x(uz) + (yz)v = z
\end{aligned}$$

Posons $d = x \wedge yz$. d divise toute combinaison linéaire de x et yz, donc d divise z d'après ci-dessus. Donc d est un diviseur commun à x et z. Par définition du PGCD, $1 \leq d \leq x \wedge z = 1$. Donc $d = 1$. □

Nous voulons appliquer ce lemme à $x = a+b, y = a, z = b$. Il suffit donc de montrer que $(a+b) \wedge a = 1$ et $(a+b) \wedge b = 1$.

$$\begin{aligned}
a \wedge b = 1 &\iff \exists (u,v) \in \mathbb{Z}^2, au + bv = 1 \\
&\iff \exists (u,v) \in \mathbb{Z}^2, au + bv + av - av = 1 \\
&\iff \exists (u,v) \in \mathbb{Z}^2, (a+b)v + a(u-v) = 1 \\
&\iff (a+b) \wedge a = 1
\end{aligned}$$

Nous obtenons de même $(a+b) \wedge b = 1$.

2.1.3 Troisième méthode

Il existe une méthode permettant d'exprimer directement 1 comme combinaison linéaire de $a+b$ et ab.

$$\begin{aligned} a \wedge b = 1 &\iff \exists (u,v) \in \mathbb{Z}^2, au + bv = 1 \\ &\implies \exists (u,v) \in \mathbb{Z}^2, (au+bv)^2 = 1 \\ &\iff \exists (u,v) \in \mathbb{Z}^2, (au)^2 + 2abuv + (bv)^2 + abu^2 - abu^2 + abv^2 - abv^2 = 1 \quad \text{ajout et retrait de termes} \\ &\iff \exists (u,v) \in \mathbb{Z}^2, (a+b)(au^2+bv^2) - ab(u-v)^2 = 1 \end{aligned}$$

2.2 Par le lemme d'Euclide

2.2.1 Rappel sur les nombres premiers

Définition 2.2.1. *Un nombre premier est un entier naturel possédant exactement deux diviseurs positifs.*

Exemple 2.2.1. 1 *n'est pas un nombre premier. Le plus petit nombre premier est* 2. *Retenons que si p est un nombre premier, alors $p > 1$.*

Proposition 2.2.1. *Soit p un nombre premier. $\forall a \in \mathbb{Z}$, p divise a ou $p \wedge a = 1$.*

Démonstration. $\mathscr{D}_+(p) = \{1, p\}$ et $\mathscr{D}_+(a) = \{1, \ldots, |a|\}$. 1er cas : $p \in \mathscr{D}(a)$, c'est-à-dire p divise a. 2ème cas : $p \notin \mathscr{D}(a)$, ainsi $p \wedge a = \max\left(\mathscr{D}_+(p) \cap \mathscr{D}_+(a)\right) = 1$. □

Le lemme d'Euclide constitue la proposition suivante.

Proposition 2.2.2. *Soit p un nombre premier. Si p divise ab, alors p divise a ou p divise b.*

Démonstration. Première preuve : p divise ab. D'après la proposition 2.2.1, il n'y a que deux possibilités : soit p divise a et c'est fini, soit $p \wedge a = 1$ et par le théorème de Gauss, p divise b. Deuxième preuve : sans faire appel au théorème de Gauss, qui est une généralisation du lemme. Par l'absurde, supposons qu'il existe a et b non divisibles par p tels que p divise ab. Quitte à changer b en $-b$, nous pouvons supposer b entier naturel. Posons $E := \{x \in \mathbb{N}, p \text{ ne divise pas } x \text{ et } p \text{ divise } ax\}$. E est une partie non vide de $\mathbb{N}$ car $b \in E$. Donc E admet un plus petit élément x_0. La division euclidienne de p par x_0 donne l'existence de $q \in \mathbb{N}$ et d'un entier r vérifiant $0 \leq r < x_0$ tels que $p = x_0 q + r$. En multipliant par a, il vient $ar = ap - ax_0 q$. Donc p divise ar. Par ailleurs, supposons $r = 0$. Alors $p = x_0 q$. Or, p est premier donc $x_0 = 1$ ou $q = 1$. Si $x_0 = 1$, alors p divise $a \times 1$ car $x_0 \in E$. Contradiction. Si $q = 1$, alors $p = x_0$ donc p divise x_0. Contradiction. Donc $r \neq 0$. En outre, $r = p - x_0 q < p$. Donc $0 < r < p$ donc p ne divise pas r. Donc $r \in E$, ce qui contredit la minimalité de x_0. □

2.2.2 Première méthode

Nous voulons montrer que $(a+b) \wedge ab = 1$. Il suffit de montrer que $(a+b) \wedge ab$ n'admet pas de diviseur premier, d'après l'exemple 2.2.1 du rappel.

Raisonnons par l'absurde : supposons qu'il existe un nombre premier p divisant $a+b$ et ab. p divise ab donc d'après le lemme d'Euclide, p divise a ou p divise b. Supposons que p divise a. Alors p divise $(a+b) - a = b$. Donc p est un diviseur commun à a et b. Par définition du PGCD, $p \leq a \wedge b = 1$. Or, $p > 1$. Contradiction.

2.2.3 Deuxième méthode

Nous démontrons d'abord le lemme suivant.

Proposition 2.2.3. *Soit p un nombre premier. Si p divise a^2, alors p divise a.*

Démonstration. Première preuve : il s'agit du lemme d'Euclide, dans le cas particulier où $b = a$. Deuxième preuve : p divise a^2, donc $\exists k \in \mathbb{Z}, a \times a = kp$, donc a divise kp. Supposons $p \wedge a = 1$. D'après le théorème de Gauss, a divise k. Alors $\exists k' \in \mathbb{Z}, k = ak'$, d'où en reportant dans la relation précédente et en divisant par $a \neq 0$, $a = k'p$, c'est-à-dire p divise a. Cela contredit la proposition 2.2.1. Troisième preuve : p est un diviseur premier de a^2, donc p apparaît comme facteur premier dans la décomposition de a^2. Or, les facteurs premiers de a^2 sont exactement ceux de a élevés à une puissance double. Donc p apparaît dans la décomposition de a, c'est-à-dire p divise a. Remarque : la réciproque de cette proposition est évidemment vraie. □

Raisonnons par l'absurde : supposons qu'il existe un nombre premier p divisant $a+b$ et ab. p divise toute combinaison linéaire de $a+b$ et ab, en particulier $a(a+b) - ab = a^2$. Donc p divise a. Par symétrie du problème, p divise b. Etc.