$(4a + 9b) \wedge (3a + 7b) = a \wedge b$

Samuel Rochetin

Mardi 26 janvier 2016

Résumé

L'exercice suivant est classique : « montrer que $\mathrm{PGCD}(4a + 9b, 3a + 7b) = \mathrm{PGCD}(a, b)$ ». Bien entendu, les combinaisons linéaires $4a + 9b$ et $3a + 7b$ ne doivent rien au hasard : la dernière section de ce document explique comment les coefficients $4, 9, 3, 7$ sont choisis. À noter que les entiers relatifs a et b ne peuvent pas être simultanément nuls, car $\mathrm{PGCD}(0, 0)$ n'existe pas.

1 Par combinaisons linéaires

1.1 Première méthode

Soit E l'ensemble des diviseurs communs à a et b. Soit F l'ensemble des diviseurs communs à $4a+9b$ et $3a+7b$. Soit $d \in E$. d divise toute combinaison linéaire de a et b, en particulier d divise $4a+9b$ et $3a+7b$, donc $d \in F$. D'où $E \subset F$. Soit $d' \in F$. d' divise $4a+9b$ et $3a+7b$ donc d' divise $7(4a+9b)-9(3a+7b) = a$ et $-3(4a+9b)+4(3a+7b) = b$, donc $d' \in E$. D'où $F \subset E$. D'où $E = F$. Donc le plus grand élément de E est égal au plus grand élément de F.

Il s'agit donc d'un argument de double inclusion d'ensembles.

1.2 Deuxième méthode

Posons $d = a \wedge b$ et $d' = (4a + 9b) \wedge (3a + 7b)$. d divise toute combinaison linéaire de a et b, en particulier d divise $4a + 9b$ et $3a + 7b$. Par définition du PGCD, $d \leq d'$. En outre, d' divise $4a + 9b$ et $3a + 7b$ donc d' divise $7(4a + 9b) - 9(3a + 7b) = a$ et $-3(4a + 9b) + 4(3a + 7b) = b$. d' divise a et b, donc par définition du PGCD, $d' \leq d$. D'où $d = d'$.

Il s'agit donc d'un argument de double inégalité.

1.3 Troisième méthode

Nous avons besoin du point de cours suivant.

Proposition 1.3.1. *Si d divise a et b, alors d divise $a \wedge b$.*

Démonstration. Première preuve : d'après une proposition de cours, il existe a', b' premiers entre eux tels que $a = a'(a \wedge b)$ et $b = b'(a \wedge b)$. D'après le théorème de Bézout, il existe donc u, v tels que $a'u + b'v = 1$. En multipliant par $a \wedge b$, nous obtenons ainsi : $\exists (u, v) \in \mathbb{Z}, au + bv = a \wedge b$. d divise toute combinaison linéaire de a et b, donc d divise $a \wedge b$. Deuxième preuve : notons $\mathscr{D}(a, b)$ l'ensemble des diviseurs communs à a et b, r le reste de la division euclidienne de a par b. D'après l'algorithme d'Euclide, $\mathscr{D}(a, b) = \mathscr{D}(b, r) = \cdots = \mathscr{D}(a \wedge b, 0)$. En particulier, nous avons donc $\mathscr{D}(a, b) \subset \mathscr{D}(a \wedge b, 0)$. Tout diviseur de a et b divise donc $a \wedge b$. Remarque : la réciproque est triviale, puisqu'elle découle de la transitivité. En effet, si d divise $a \wedge b$, comme $a \wedge b$ divise a et b, alors d divise a et b. □

Nous avons également besoin du lemme suivant, qui est évident.

Proposition 1.3.2. *Si a divise b et b divise a, alors $a = \pm b$.*

Démonstration. a divise b donc $\exists k \in \mathbb{Z}, b = ak$. b divise a donc $\exists k' \in \mathbb{Z}, a = bk'$. Comme $b \neq 0$ puisque b divise a, alors en injectant puis simplifiant, il vient $kk' = 1$, c'est-à-dire $k = k' = 1$ ou $k = k' = -1$, c'est-à-dire $a = b$ ou $a = -b$. □

Reprenons la méthode précédente. Au lieu d'écrire $d \leq d'$ puis $d' \leq d$, la proposition **??** nous permet d'écrire d divise d' puis d' divise d. Or, d et d' sont tous les deux positifs, donc d'après la proposition **??**, $d = d'$.

Il s'agit donc d'un argument de division mutuelle des PGCD.

2 Par un lemme d'Euclide

Cette méthode directe repose sur le point de cours suivant, appelé parfois lemme d'Euclide (à ne pas confondre avec le lemme d'Euclide portant sur les nombres premiers). Dans cette proposition, a et b sont deux entiers relatifs non simultanément nuls, pour la raison évoquée dans l'introduction.

Proposition 2.0.1. $\forall k \in \mathbb{Z}, a \wedge b = b \wedge (a - kb)$.

Démonstration. Il s'agit d'une égalité de PGCD du même type que celle de l'énoncé de départ, il suffit donc d'appliquer l'une des trois méthodes précédentes. □

Utilisons cette proposition en cascade en choisissant à chaque étape une valeur judicieuse de k.

$$\begin{aligned}(4a+9b) \wedge (3a+7b) &= (3a+7b) \wedge (a+2b) && k=1\\ &= (a+2b) \wedge b && k=3\\ &= b \wedge a && k=2\\ &= a \wedge b\end{aligned}$$

3 Comment fabriquer un tel exercice ?

3.1 La symétrie du problème

Les trois premières méthodes révèlent une certaine symétrie du problème, qui provient de la relation de Bézout. En effet, $au + bv = 1$ montre que a et b sont premiers entre eux mais aussi que u et v sont premiers entre eux, de coefficients de Bézout particuliers a et b.

3.2 Exemple

Pour fabriquer un tel exercice, il suffit de choisir deux nombres premiers entre eux. Par exemple 5 et 8. Ce seront les coefficients devant b. Ensuite, choisir un couple de coefficients (u, v) solution de la relation de Bézout $5u+8v = 1$, par exemple $(-11, 7)$. u et v seront, au signe près, les coefficients devant a. Enfin, former deux combinaisons linéaires de a et b en prenant soin de « croiser » les coefficients. Ainsi, $11a + 5b$ et $7a + 8b$ ne conviennent pas mais $7a + 5b$ et $11a + 8b$ conviennent.