PGCD et solutions entières d'équations

Définition (pgcd): Soit a et b des entiers relatifs dont l'un au moins est non nul.
On appelle *plus grand diviseur commun* de a et b (ou $pgcd(a,b)$) et on note $a \wedge b$ le plus grand élément de l'ensemble des diviseurs communs de a *et* b. On convient que $0 \wedge 0 = 0$.

Propriétés immédiates : Soit a et b des entiers relatifs

$pgcd(a,b) = pgcd(|a|,|b|)$ | Si a est multiple de b alors $pgcd(a,b) = |b|$

Définition : On dit que les entiers relatifs non nuls a et b sont premiers entre eux lorsque $pgcd(a,b) = 1$

Propriété : détermination du PGCD avec l'algorithme d'Euclide (l'algorithme des divisions euclidiennes successives)
Idée phare : $pgcd(a,b) = pgcd(b,r)$ où $r = a - qb$ est le reste dans la division euclidienne de a par b.

En répétant ce procédé on aboutit nécessairement à $pgcd(d,0)$ et d est alors le nombre cherché.

Exemple : $pgcd(546;60)$:
$546 = 60 \times 9 + 6$ donc $pgcd(546,60) = pgcd(60,6)$ puis $60 = 10 \times 6 + 0$ donc $pgcd(60,6) = 6$

Propriété (identité de Bézout)
Soit a et b des entiers relatifs. Il existe des entiers relatifs u et v tels que $au + bv = pgcd(a,b)$.
(on peut déterminer un u et un v en remontant l'algorithme d'Euclide)

Corollaire (Théorème de Bézout ; nombre premier entre eux)
« il existe u et v tels que $au + bv = 1$ » est équivalent à « a et b premiers entre eux ».

Remarque :Les coefficients u et v ne sont pas uniques. $2 = 4(-1) + 6(1)$ et aussi $2 = 4(2) + 6(-1)$

Exemple de l'algorithme d'Euclide : Pour 15 et 21 on a $pgcd(21,15) = 3$ et on obtient $21 \times (-2) + 15 \times 3 = 3$

$21 = 1 \times 15 + 6$ | $3 = 15 + (-2) \times (21 - 15) = 3 \times 15 + (-2) \times 21$
$15 = 2 \times 6 + 3$ | $3 = 15 - 2 \times 6$
$6 = 2 \times 3 + 0$ | En remontant

Propriété : $pgcd(ka', kb') = |k| \times pgcd(a', b')$ (les diviseurs communs à a et b divisent le $pgcd$. En effet $au + bv = pgcd(a,b)$.)
Exemples : $pgcd(12,18) = pgcd(6 \times 2; 6 \times 3) = 6 \times pgcd(2,3) = 6 \times 1 = 6$

Théorème de Gauss *(le "prince des mathématiques")*. Si a divise bc et a et b premiers entre eux alors a divise c
Corollaire : Si b et c sont premiers entre eux et divisent a alors bc divise a.

Définition (équation diophantienne (Diophante d'Alexandrie au *III*^{e} siècle après JC)
Une équation diophantienne est une équation polynomiale à coefficients entiers à une ou plusieurs inconnues dont les solutions sont cherchées parmi les nombres entiers.

Propriété (équations diophantiennes linéaires du 1er degré à 2 inconnues x et y)
$ax + by = c$ n'admet soit aucune solution soit une infinité de couples solutions dépendants de l'un d'eux (x_0, y_0) :

- Si $pgcd(a,b) = 1$ alors il existe une infinité de couples solutions : $S = \{(x_0 + kb; y_0 - ka), k \in \mathbb{Z}\}$.
- Si $pgcd(a,b) \neq 1$
  - Si c n'est pas multiple du pgcd alors $S = \emptyset$
  - Si c est multiple du pgcd alors en divisant par ce pgcd l'équation devient

$\frac{a}{pgcd(a,b)} x + \frac{b}{pgcd(a,b)} y = \frac{c}{pgcd(a,b)} \Leftrightarrow a'x + b'y = c'$ avec $pgcd(a',b') = 1$. $S = \{(x_0 + kb'; y_0 - ka'), k \in \mathbb{Z}\}$

La solution particulière (x_0, y_0) est soit évidente soit déterminée en remontant l'algorithme d'Euclide.

Remarque :
$ax + by = c$ est une équation de droite, il s'agit en fait de déterminer les points à coordonnées entières de la droite.

Une application : Déterminer, lorsqu'il existe, un inverse modulo un entier. Par exemple résoudre $8x \equiv 1\ [23]$ revient résoudre $8x = 1 + 23k \Leftrightarrow 8x + (-23)k = 1$. Ici $pgcd(8,23) = 1$ donc x et k existent, donc 8 est inversible.

Des Démonstrations

Théorème de Bézout :
L'ensemble des « $au + bv$ positifs » ont un plus petit élément, notons le c. Montrons que $c = pgcd(a, b)$
En remontant algo Euclide, on montre que $pgcd(a, b)$ s'écrit $au + bv$ donc $pgcd(a, b) \geqslant c$
Mais $pgcd(a, b)$ divise a et b donc $au + bv$ donc c donc $pgcd(a, b) \leqslant c$

Théorème de Gauss
a divise bc dont il existe k tel que $bc = ka$. D'autre part a et b premiers entre eux, donc il existe u et v de $\mathbb{Z}$ tels que $au + bv = 1$, en multipliant par c on obtient $cau + cbv = c$ puis comme $bc = ka$, $cau + akv = c$ et enfin $a(cu + kv) = c$ qui prouve que a divise c.

Démo2 : Si $a \wedge b = 1$ alors $ac \wedge bc = |c|$ puis si a divise bc , comme il divise bien sûr ac, il divise $ac \wedge bc = |c|$

Corollaire : Si b et c sont premiers entre eux et divisent a alors bc divise a.
$a = bk$ et $a = ck'$ donc $bk = ck'$ comme $b \wedge c = 1$,b ne divise pas c donc il divise k' donc $k' = bk''$ d'où $a = cbk''$

Des Exemples

Exemple de détermination de u et v. $pgcd(3080{,}525) = 35$

$3080 = 5 \times 525 + 455$ $525 = 1 \times 455 + 70$ $455 = 6 \times 70 + 35$ $70 = 2 \times 35$	$35 = 7 \times (3080 - 5 \times 525) - 6 \times 525 = 7 \times 3080 + (-41) \times 525$ $35 = 455 - 6 \times (525 - 455) = 7 \times 455 - 6 \times 525$ $35 = 455 - 6 \times 70$ En remontant

Une présentation efficace sous forme d'un tableau (de Lamé-Lucas)

			nb de 3080	nb de 525
		3080	1	0
		525	0	1
3080 - 5×525	=	455	1	-5
525 – 1x455	=	70	-1	6
455 – 6x70	=	35	7	-41
		0		

Pour ceux qui le souhaitent, faire un programme qui retourne u et v lorsqu'on lui donne a et b.

Exemple de résolution d'équation diophantienne : Résolvons "$5x + 2y = 4$".

- $pgcd(2{,}5) = 1$ donc l'équation admet des solutions.
- Avec l'algorithme d'Euclide où de tête, on cherche une solution particulière : $5 \times (1) + 2 \times (-2) = 1$ puis en multipliant par 4, $5 \times (4) + 2 \times (-8) = 4$
  donc $(x_0 = 4, y_0 = -8)$ est une solution particulière.
- Les solutions sont donc $(4 - 2k; -8 + 5k)$ avec k parcourant $\mathbb{Z}$

On peut aussi, sans théorème, procéder ainsi, après avoir trouvé une solution particulière.

- On effectue une soustraction pour supprimer le second membre : $(5x + 2y = 4) - (5x_0 + 2y_0 = 4)$ donne $5(x - x_0) + 2(y - y_0) = 0$ soit $5(x - x_0) = -2(y - y_0)$
- Le théorème de Gauss donne 5 divise $(y - y_0)$ donc $y = y_0 + 5k$
  En remplaçant on obtient $x = x_0 - 2k$

Les solutions sont $(4 - 2k; -8 + 5k)$ avec k parcourant $\mathbb{Z}$.
$k = 0$ donne $(4; -8)$, $k = 1$ donne $(6; -13)$, $k = 2$ donne $(8; -18)$...

Culture : la plus célèbre des équations diophantiennes est celle du polymathe français Pierre de Fermat (surnommé le "prince des amateurs" car il n'était pas mathématicien de métier, il était magistrat à Toulouse en 1650).
Il s'agit pour n fixé, de résoudre $x^n + y^n = z^n$.

- Pour $n = 1$, les triplets solutions sont triviaux, par exemple $(x = 1, y = 1, z = 2)$
- Pour $n = 2$, les triplets solutions sont les triplets pythagoriciens, on sait en trouver.
- Pour $n \geqslant 3$, il aura fallu attendre l'année 1994 (soit 300 ans) pour prouver qu'il n'y a pas de solution !