Niveau : 1 **Jaune**

Le théorème de Bézout

1 Théorème de Bézout

Le théorème suivant est fondamental dans la théorie, et l'algorithme que nous allons mettre en place pour le démontrer (algorithme d'Euclide étendu) est tout aussi important que le théorème lui-même.

Théorème 1.1 *Si pgcd*$(a, b) = d$*, il existe deux entiers* u *et* v *tels que* $ua + vb = d$*.*

Preuve. L'existence d'un couple (u, v) répondant à la question est prouvée par sa production grâce à l'algorithme suivant. □

1.1 Algorithme d'Euclide étendu

Là encore nous supposerons que $a \geq 0$ et $b > 0$. Le cas général s'en déduit.
Voici un algorithme (algorithme d'Euclide étendu, adaptation de l'algorithme précédent) qui permet de trouver explicitement un couple (u, v) qui convient.

$R0 := a$; $\quad (a \geq 0)$
$R1 := b$; $\quad (b > 0)$
$U0 := 1$; $U1 := 0$;
$V0 := 0$; $V1 := 1$;
Tant que $R1 > 0$ **faire**
$\quad Q := Quotient\_Division(R0, R1)$;
$\quad R := Reste\_Division(R0, R1)$;
$\quad U := U0 - Q * U1$;
$\quad V := V0 - Q * V1$;
$\quad R0 := R1$; $R1 := R$;
$\quad U0 := U1$; $U1 := U$;
$\quad V0 := V1$; $V1 := V$;
fintq ;

Remarquons qu'il s'agit d'une amélioration de l'algorithme d'Euclide donné précédemment pour le calcul du pgcd. Comme précédemment l'algorithme se termine avec $R1 = 0$ et $R0 = \text{pgcd}(a, b)$.
Montrons que les conditions :

$$\begin{cases} U0a + V0b &= R0 \\ U1a + V1b &= R1 \\ R1 \geq 0 \end{cases}$$

sont un invariant de boucle. Pour cela notons $R0', R1', U0', U1', V0', V1'$ les nouvelles valeurs de $R0, R1, U0, U1, V0, V1$ en sortie d'un tour de boucle.

On a :

$$R0 = Q * R1 + R,$$

$$U := U0 - Q * U1,$$

$$V := V0 - Q * V1,$$

puis $R0' = R1$, $R1' = R = R0 - Q * R1$, $U0' = U1$, $U1' = U = U0 - Q * U1$, $V0' = V1$, $V1' = V = V0 - Q * V1$. Si bien que :

$$U0'a + V0'b = U1a + V1b = R1 = R0'.$$

La première condition est bien réalisée en sortie. De même on a :

$$U1'a + V1'b = U0a + V0b - Q * (U1a + V1b) = R0 - Q * R1 = R'1,$$

et la deuxième condition est aussi réalisée.
Il est facile de voir qu'à l'instant initial ces deux conditions sont bien réalisées. En sortie on a $R1 = 0$ et $R0 = \text{pgcd}(a, b)$ si bien que $U0$ et $V0$ contiennent une solution du problème.

2 Cas de nombres premiers entre eux

On a une réciproque partielle du résultat précédent qui traite du cas où a et b sont premiers entre eux. On obtient alors le théorème de Bézout. Ce théorème est très important ; nous verrons qu'il est lié au calcul de l'inverse dans les classes résiduelles modulo un entier n.

Théorème 2.1 *Deux entiers a et b sont premiers entre eux si et seulement s'il existe u et v tels que $au + bv = 1$.*

Preuve. La partie directe est conséquence du théorème précédent. Si maintenant on a l'existence d'un tel couple (u, v), il est visible que tout nombre qui divise a et b divise 1. □

Remarque : L'algorithme d'Euclide étendu s'applique, bien entendu, à la détermination effective d'un couple (u, v) répondant à la question.
Comme conséquence de ces résultats on a le lemme d'Euclide-Gauss :

Théorème 2.2 *Si c divise ab et si c est premier avec a alors c divise b.*

Preuve. Si c est premier avec a on peut trouver u et v tels que $ua + vc = 1$, donc $uab + vcb = b$. Comme c divise ab, donc uab, et aussi vcb, il divise leur somme b. □

On peut maintenant se poser la question suivante : soient a et b deux entiers dont l'un au moins est non nul, et d leur plus grand commun diviseur. Nous supposerons encore $a \geq 0$ et $b > 0$. Comment trouver toutes les solutions de $au + bv = d$?
Remarquons que ce sont aussi toutes les solutions de $a'u + b'v = 1$ où $a' = a/d$ et $b' = b/d$. On sait alors que a' et b' sont premiers entre eux. Notons (u_0, v_0) une solution (dont on connaît l'existence et qu'on peut trouver par l'algorithme d'Euclide étendu). Si (u, v) est une autre solution alors :

$$a'(u - u_0) + b'(v - v_0) = 0.$$

Donc b' divise $a'(u - u_0)$ et comme b' est premier avec a', on conclut que b' divise $u - u_0$, donc que :

$$u = u_0 + kb'.$$

Si bien que :

$$a'kb' + b'(v - v_0) = 0,$$

et donc :

$$v = v_0 - ka'.$$

Ainsi pour tout couple (u, v) répondant à la question il existe un entier k tel que :

$$u = u_0 + kb'$$

et :

$$v = v_0 - ka'.$$

Réciproquement tout couple de cette forme répond à la question.
Cherchons une solution minimale c'est-à-dire une solution où les nombres u, v sont « petits ». Excluons le cas trivial où l'un des deux nombres a', b' est 1. Alors on peut trouver par division euclidienne par b' une solution (u_1, v_1) telle que :

$$0 < u_1 < b'.$$

On calcule alors :

$$v_1 = \frac{1 - a'u_1}{b'},$$

d'où :

$$\frac{1}{b'} - a' < v_1 < 0,$$

ou encore :

$$-a' < v_1 < 0.$$

Cette remarque est particulièrement utile lorsque l'un des nombres a' ou b' est petit. Par exemple si $b' = 3$ alors $u_1 = 1$ ou $u_1 = 2$. Il suffit alors d'essayer lequel des nombres $1 - a'$ et $1 - 2a'$ est divisible par 3 pour obtenir une solution.