Remontée de l'algorithme d'Euclide

Caroline Pintoux et Hélène Arnaud

On dispose de deux nombres entiers positifs premiers entre eux $a > b$, et on cherche un couple de nombres entiers (u, v) qui satisfasse l'équation :

$$au + bv = 1.$$

1 Petit rappel sur la division euclidienne

Par *division euclidienne*, on désigne la division usuelle des entiers, telle qu'on l'apprend en primaire, non poussée. Par exemple, la division euclidienne de 255 par 7 donne :

$$\begin{array}{r|l} 2\ 5\ 5 & 7 \\ \cline{2-2} 4\ 5 & 3\ 6 \\ 3 & \end{array}$$

c'est à dire

$$255 = 7 \times 36 + 3.$$

Le nombre 36 est le *quotient* de la division, et 3 en est le *reste*.

2 Remontée de l'algorithme d'Euclide

Pour deux entiers $a > b$ premiers entre eux, on note $a_0 = a$ et $a_1 = b$, et on commence par effectuer la division euclidienne de a_0 par a_1,

$$a_0 = a_1 b_1 + a_2.$$

Le reste de cette division est noté a_2, et son quotient b_1.

En effectuant les divisions euclidiennes successives de a_n par a_{n+1}, on construit ainsi deux suites $(a_n)_n$ et $(b_n)_n$ d'entiers :

- La suite (a_n) est celle des restes successifs des divisions euclidiennes : a_{n+2} est le reste de la division euclidienne de a_n par a_{n+1}.
- La suite (b_n) est celle des quotients des divisions euclidiennes successives : b_{n+1} est le quotient entier de la division de a_n par a_{n+1}.

$$a_n = a_{n+1} b_{n+1} + a_{n+2}.$$

On peut montrer qu'en procédant ainsi, on arrive toujours à $a_k = 1$ pour un certain indice k. A ce moment là, on arrête l'algorithme, et on va pouvoir le "remonter".

Pour remonter l'algorithme et trouver les coefficients de Bezout (u, v) dans

$$au + bv = 1,$$

on se sert de nos deux suites en gardant en permanence $a_0 = a$ et $a_1 = b$ en évidence, et en cherchant les coefficients qui se trouvent devant ces deux quantités. On part de $1 = a_k = a_{k-2} - b_{k-1}a_{k-1}$ et on *remonte* dans la suite des divisions euclidiennes, exprimant les termes des deux suites en fonction des termes précédents jusqu'à n'avoir plus que $1 = a_0u + a_1v$.

On y verra plus clair sur des exemples

3 Deux exemples

1. Soient $a = a_0 = 165$ et $b = a_1 = 56$. Alors, les divisions euclidiennes successives s'écrivent

$$\begin{aligned} a_0 &= 2 \times a_1 + 53 \\ a_1 &= 1 \times 53 + 3 \\ 53 &= 17 \times 3 + 2 \\ 3 &= 1 \times 2 + 1. \end{aligned}$$

La remontée va s'effectuer de la façon suivante :

$$\begin{aligned} 1 &= 3 - 1 \times 2 \\ 1 &= 3 - 1 \times [53 - 17 \times 3] \\ 1 &= \{a_1 - 1 \times 53\} - 1 \times [53 - 17 \times \{a_1 - 1 \times 53\}] \\ 1 &= \{a_1 - 1 \times (a_0 - 2a_1)\} - 1 \times [(a_0 - 2a_1) - 17 \times \{a_1 - 1 \times (a_0 - 2a_1)\}] \end{aligned}$$

et après simplification de la dernière ligne, on obtient

$$1 = 56a_1 - 19a_0,$$

donc $u = -19$ et $v = 56$.

2. Avec $a = a_0 = 7590$ et $b = a_1 = 1547$, on cherche à remonter l'algorithme d'Euclide suivant

$$\begin{aligned} a_0 &= 4 \times a_1 + 1402 \\ a_1 &= 1 \times 1402 + 145 \\ 1402 &= 9 \times 145 + 97 \\ 145 &= 1 \times 97 + 48 \\ 97 &= 2 \times 48 + 1, \end{aligned}$$

d'où la remontée

$$\begin{aligned} 1 &= 97 - 2 \times 48 \\ 1 &= 97 - 2 \times (145 - 1 \times 97) \\ 1 &= [1402 - 9 \times 145] - 2 \times (145 - 1 \times [1402 - 9 \times 145]) \\ 1 &= [1402 - 9 \times \{a_1 - 1 \times 1402\}] - 2 \times (\{a_1 - 1 \times 1402\} - 1 \times [1402 - 9 \times \{a_1 - 1 \times 1402\}]) \\ 1 &= [(a_0 - 4a_1) - 9 \times \{a_1 - 1 \times (a_0 - 4a_1)\}] \\ &-2 \times (\{a_1 - 1 \times (a_0 - 4a_1)\} - 1 \times [(a_0 - 4a_1) - 9 \times \{a_1 - 1 \times (a_0 - 4a_1)\}]), \end{aligned}$$

et on trouve finalement

$$1 = 32a - 157b,$$

donc $u = 32$ et $v = -157$.