Algorithme d'Euclide

L'**algorithme d'Euclide** est un algorithme permettant de déterminer le plus grand commun diviseur (P.G.C.D.) de deux entiers dont on ne connaît pas la factorisation. Il est déjà décrit dans le livre VII des *Éléments* d'Euclide sous la forme de l'anthyphérèse.

Sommaire

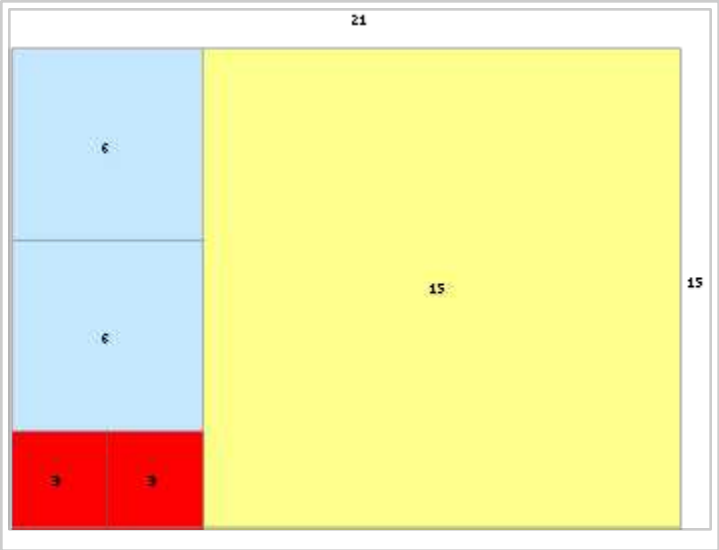
Description

Explications géométriques

Dans la tradition grecque, en comprenant un nombre entier comme une longueur et un couple d'entiers comme un rectangle, leur PGCD est la longueur du côté du plus grand carré permettant de carreler entièrement ce rectangle. L'algorithme décompose ce rectangle en carrés, de plus en plus petits, par divisions euclidiennes successives, de la longueur par la largeur, puis de la largeur par le reste, jusqu'à un reste nul.

Dans le rectangle de dimensions L=21 par l=15 représenté à droite, par exemple,

on peut glisser un carré de côté 15 mais il reste un rectangle de côtés 15 et 6, dans lequel on peut glisser deux carrés de côté 6 mais il reste un rectangle de côtés 6 et 3 que l'on peut carreler entièrement de carrés de côté 3. Les carrés de côté 6 ou 15 peuvent aussi se carreler en carrés de côté 3. Le rectangle entier peut se carreler en carrés de côté 3. Il n'existe pas de carré plus grand permettant un tel carrelage.



Voir en fin de document l'algorithme d'Euclide appliqué à cet exemple

Explications arithmétiques

On considère que `pgcd(a,0) = a` et que pour b ≠ 0 `pgcd(a,b) = pgcd(b, a mod b)`. On progresse dans l'algorithme en diminuant à chaque étape les nombres considérés par calcul du modulo.

Généralisation

Cet algorithme repose sur la structure d'anneau euclidien de l'anneau **Z** des entiers relatifs, plus particulièrement sur la propriété de division euclidienne. Il se généralise donc à bien d'autres anneaux, en particulier les anneaux de polynômes à coefficients dans un corps. L'algorithme se généralise pour permettre le calcul des coefficients de Bézout.

L'algorithme est effectif à condition de disposer d'un algorithme effectif de division euclidienne. La possibilité de disposer d'un tel algorithme rend de nombreux autres calculs effectifs, notamment, en algèbre linéaire, le calcul de facteurs invariants.

Remarque préliminaire

Puisque l'algorithme a pour objet le calcul d'un PGCD, il est possible de se restreindre aux entiers positifs, un PGCD de deux entiers relatifs étant égal au PGCD de leurs valeurs absolues.

Description de l'algorithme

Soient deux entiers naturels a et b, dont on cherche le PGCD. Le cas où a ou b est nul ne nécessite aucun algorithme ; on l'exclut. Une suite d'entiers $(a_n)_n$ est définie par récurrence de pas 2, plus précisément par divisions euclidiennes successives ; la suite est initialisée par $a_0 = a$, $a_1 = b$, puis propagée par la règle de récurrence : tant que a_{n+1} est non nul, a_{n+2} est défini comme le reste de la division euclidienne de a_n par a_{n+1}.

On commence donc par calculer le reste de la division de a par b, qu'on note r ; puis on remplace a par b, puis b par r, et on réapplique le procédé depuis le début.

On obtient ainsi une suite, qui vaut 0 à un certain rang ; le PGCD cherché est le terme précédent de la suite.

Si $a < b$, la première itération de la boucle a pour effet de « permuter a et b ». Plus précisément : dans ce cas, la division euclidienne de a par b s'écrit $a = b.0 + a$ donc $a_2 = a$, si bien que la suite produite par l'algorithme appliqué au couple (a, b) commence par a, suivie de la suite produite par l'algorithme appliqué au couple (b, a).

Exemple

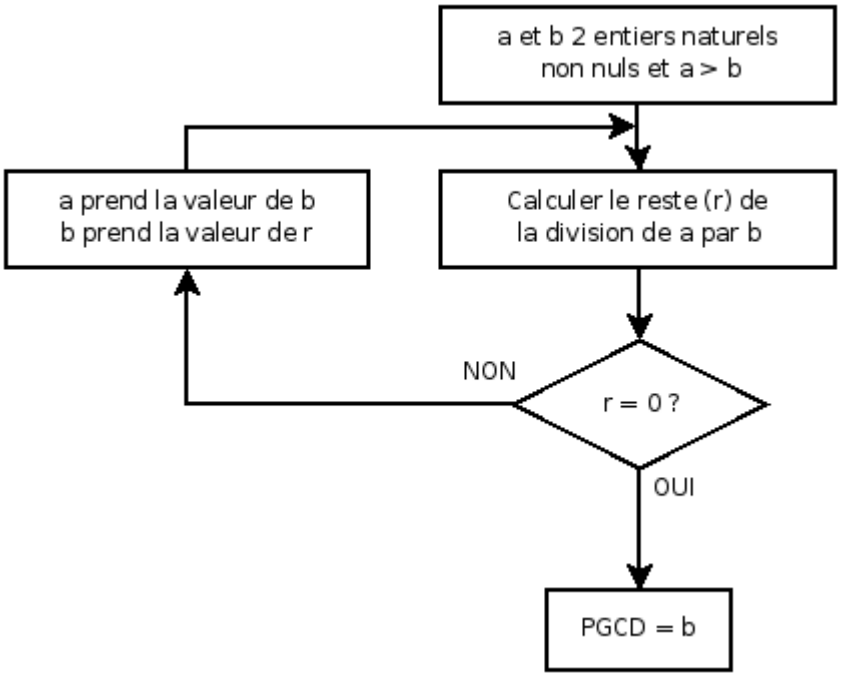
Calculons, par exemple, le PGCD de 1071 et de 1029 à l'aide de l'algorithme d'Euclide :

1071 = 1029 × 1 + 42

1029 = 42 × 24 + **21**

42 = 21 × 2 + 0

Il faut prendre le dernier reste avant le zéro, donc PGCD(1071 ; 1029) = 21



Remarque historique

Au début, Euclide a formulé le problème de façon géométrique : comment trouver une « unité de mesure » commune pour deux longueurs de segments. Il procède par soustractions répétées de la longueur du plus court segment sur la longueur du plus long. Cela correspond à une adaptation de la méthode naïve de calcul de la division

Complément, exemple de l'algorithme d'Euclide
reprenant le shéma de l'extrait en première page

Recherche du PGCD de 21 et 15

21 > 15

- division 21:15= 1,4

partie entière de 1,4 =1

21 = 15*1 + reste de la divison

reste de la division = 21 – 1* 15 =6
la division de 21 par 15. Dans cette division, 21 est le *dividende* et 15 est le *diviseur*.
dividende = *diviseur* x *quotient* + *reste*, avec *reste* < *diviseur*
le quotient est 1, le reste est 6

le reste n'est pas égal à zéro , nous poursuivons

le diviseur (15) devient le dividende dans l'étape suivante et le reste (6) devient le diviseur

- division 15:6= 2,5

partie entière de 2,5 =2

15 = 2*6 + reste de la divison

reste de la division = 15 – 2* 6=15-12= 3

le reste n'est pas égal à zéro , nous poursuivons

- division 6:3= 2

partie entière 2 =2

6 = 2*3+ reste de la divison

reste de la division = 6 – 2* 3=0

le PGCD est 3 ; la division par 3 a donné un reste égal à zéro !