Division euclidienne. Algorithme d'Euclide

Anca Nitulescu
anca.nitulescu@ens.fr

Ecole Normale Supérieure, Paris

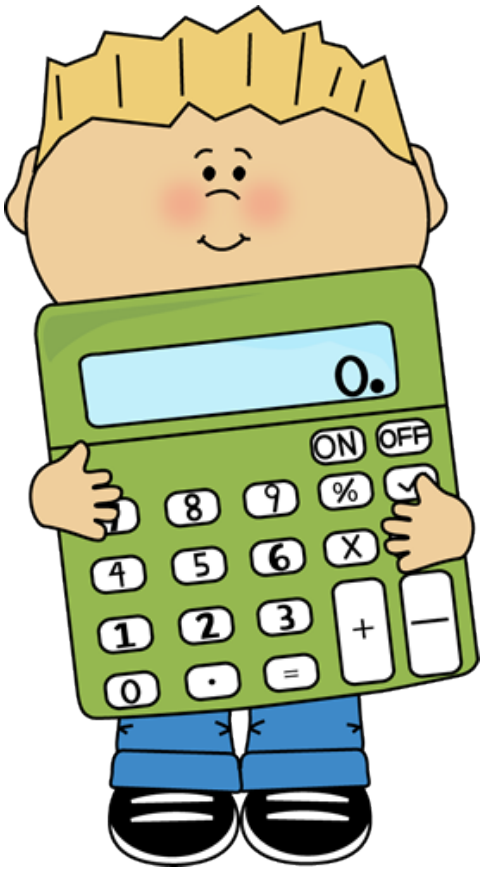
5 octobre 2016

Algorithme

Définition

Algorithme = Suite finie d'opérations élémentaires constituant un schéma de calcul ou de résolution d'un problème

(Petit Larousse)



Mathématiques ≠ Informatique

Problèmes pratiques

La pratique = Ligne de séparation entre les maths et l'info :

- **Mathématiques :** on résout un problème en montrant l'existence d'une solution.
- **Informatique :** on cherche à construire cette solution en s'intéressant à l'effcacitè de la construction.

Un algorithme permet un traitement (informatique) automatisé si :

- la solution existe
- l'algorithme soit performant

Algorithme d'Euclide

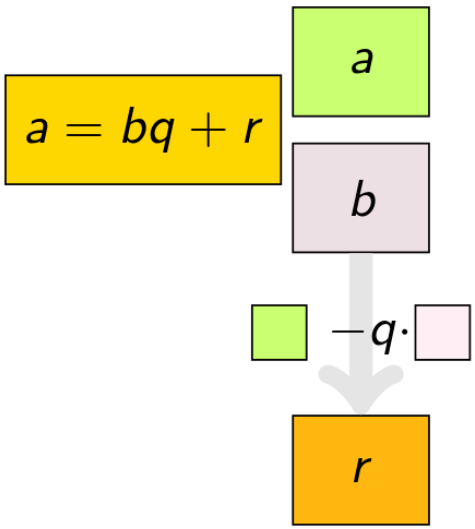
But

Algorithme de calcul du $d = \mathbf{pgcd}(a, b)$.

PGCD

- **Définition** : plus grand entier d divisant à la fois **a** et **b**
- **Propriétés** : si $a > b$ alors on a $\mathbf{a} = \mathbf{b}q + r$
  - les diviseurs communs à **a** et **b** sont les mêmes que les diviseurs communs à **b** et **r**
  - donc $\mathbf{pgcd}(a, b) = \mathbf{pgcd}(b, r)$

Algorithme d'Euclide : Exemple



a	b	q
546738492	6754024	
6754024	6416572	80
6416572	337452	1
337452	4984	19
4984	3524	67
3524	1460	1
1460	604	2
604	252	2
252	100	2
100	52	2
52	48	1
48	4	1
4	0	12

Algorithme d'Euclide étendu

But

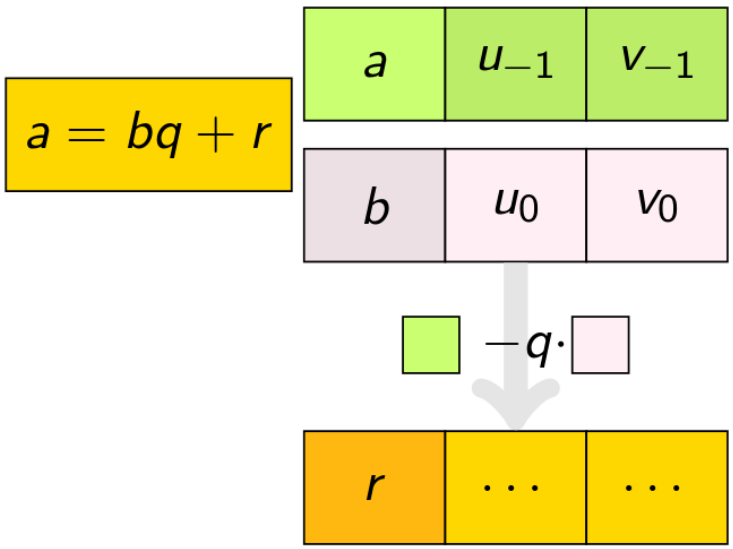
Agorithme de calcul des coeficients (u, v) tels que

$$\mathbf{a}u + \mathbf{b}v = d = \text{pgcd}(a, b)$$

Théorème de Bézout

- **Définition :** (u, v) sont les *coefficients de Bézout* pour les deux entiers naturels **a** et **b**
- **Propriétés :** **a** et **b** sont premiers entre eux si et seulement s'il existe deux entiers relatifs (u, v) tels que $au + bv = 1$.

Algorithme d'Euclide étendu : Exemple



a	u	v	q
4864	1	0	
3458	0	1	1
1406	1	−1	2
646	−2	3	2
114	5	−7	5
76	−27	38	1
38	32	−45	2
0	...	...	

$$38 = 32a - 45b = 32 \times 4864 - 45 \times 3458$$