Arithmétique. Cours

Algorithme d'euclide.

Remarque

Avec des grands nombres il peut être fastidieux de trouver des diviseurs communs. On a alors recours à l'algorithme d'Euclide.

Théorème

Soient a et b deux entiers naturels non nuls tels que b ne divise pas a.
La suite des divisions euclidiennes suivantes :

$$a = bq_0 + r_0 \text{ avec } r_0 < b$$
$$b = r_0q_1 + r_1 \text{ avec } r_1 < r_0$$
$$r_0 = r_1q_2 + r_2 \text{ avec } r_2 < r_1$$
$$r_1 = r_2q_3 + r_3 \text{ avec } r_3 < r_2$$
$$\ldots.$$
$$r_{n-2} = r_{n-1}q_n + r_n \text{ avec } r_n < r_{n-1}$$

s'arrête sur un dernier reste nul : r_n. Le dernier reste non nul r_{n-1} est le $PGCD$ de a et de b

Preuve

Montrons que $PGCD(a,b) = PGCD(b,r_0)$
Soit A l'ensemble des diviseurs de a, B l'ensemble des diviseurs de B et R l'ensemble des diviseurs de r_0

$$d \in A \cap B \Rightarrow \begin{Bmatrix} d \mid a \\ et \\ d \mid b \end{Bmatrix} \Rightarrow \exists (k,k')\ ds\ \mathbb{N}^*\ tels\ que \begin{Bmatrix} a = kd \\ et \\ b = k'd \end{Bmatrix} \Rightarrow kd = k'dq_0 + r_0 \Rightarrow d(k - q_0k') = r_0 \Rightarrow d|R \Rightarrow d \in B \cap R$$

Donc : $A \cap B \subset B \cap R$

Réciproquement :

$$d \in B \cap R \Rightarrow \begin{Bmatrix} d \mid b \\ et \\ d \mid r_0 \end{Bmatrix} \Rightarrow \exists (k,k')\ ds\ \mathbb{N}^*\ tels\ que \begin{Bmatrix} b = kd \\ et \\ r_0 = k'd \end{Bmatrix} \Rightarrow a = kdq_0 + k'd \Rightarrow a = d(kq_0 + k') \Rightarrow d|a \Rightarrow d \in B \cap A$$

Donc : $B \cap R \subset A \cap B$

La double inclusion réciproque nous amène à $\boldsymbol{A \cap B = B \cap R}$. Ces deux ensembles étants identiques, leur plus grand élément l'est aussi. Il vient $\boldsymbol{PGCD(a,b) = PGCD(b,r_0)}$

En reprenant la suite des divisions successives nous avons donc :

$$\boldsymbol{PGCD(a,b) = PGCD(b,r_0) = PGCD(r_0,r_1) = PGCD(r_1,r_2) = \cdots PGCD(r_{n-1},r_n)}\ (*)$$

La suite des $((r_p))_{p\in\mathbb{N}}$ est une suite strictement décroissante de $\mathbb{N}$. Elle est donc finie et son dernier élément r_n est nul. $(*)$ nous amène donc à $\boldsymbol{PGCD(a,b) = PGCD(r_{n-1},r_n) = PGCD(r_{n-1},0) = r_{n-1}}$

Le $PGCD$ de a et b est bien le dernier reste non nul.

Exemple

Déterminons le $PGCD$ de 1958 et 4539

$$4539 = 1958 * 2 + 623$$
$$1958 = 623 * 3 + 89$$
$$623 = 89 * 7 + 0$$

Il vient $\boldsymbol{PGCD(4539,1958) = PGCD(1958,623) = PGCD(623,89) = PGCD(89,0) = 89}$