Algorithmes en arithmétique

Samuel Rochetin

Vendredi 2 février 2018

Résumé

Ce document liste les principaux algorithmes d'arithmétique étudiés en Terminale S, spécialité mathématiques. Les algorithmes sont écrits en pseudo-code dans leur version itérative et non récursive et ne vérifient pas les conditions sur les entiers naturels en entrée.

Liste des algorithmes

Algorithme 1 Liste des diviseurs positifs

Entrées: $n \in \mathbb{N}^*$
Sorties: les entiers naturels divisant n

1: $k \leftarrow 1$
2: **tant que** $k \leq \sqrt{n}$ **faire**
3: **si** $\frac{n}{k} = \left\lfloor \frac{n}{k} \right\rfloor$ **alors**
4: **si** $k \neq \frac{n}{k}$ **alors**
5: **retourner** $k, \frac{n}{k}$
6: **sinon**
7: **retourner** k
8: **fin si**
9: **fin si**
10: $k \leftarrow k + 1$
11: **fin tant que**

L'algorithme prend soin de ne pas afficher deux fois le même diviseur dans le cas où n est un carré parfait.

Algorithme 2 Division euclidienne

Entrées: $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$
Sorties: le quotient et le reste de la division euclidienne de a par b

1: $q \leftarrow 0$
2: $r \leftarrow a$
3: **tant que** $r \geq b$ **faire**
4: $\quad r \leftarrow r - b$
5: $\quad q \leftarrow q + 1$
6: **fin tant que**
7: **retourner** q, r

Algorithme 3 Ordre multiplicatif

Entrées: $a \in \mathbb{N}, a \geq 2$ et b un entier naturel premier avec a
Sorties: le plus petit entier naturel k non nul tel que $a^k \equiv 1 \pmod{b}$

1: $k \leftarrow 1$
2: **tant que** $\dfrac{a^k - 1}{b} \neq \left\lfloor \dfrac{a^k - 1}{b} \right\rfloor$ **faire**
3: $\quad k \leftarrow k + 1$
4: **fin tant que**
5: **retourner** k

Algorithme 4 Algorithme d'Euclide

Entrées: deux entiers naturels a et b tels que $(a, b) \neq (0, 0)$ et $a \geq b$
Sorties: $a \wedge b$

1: $r \leftarrow a \mod b$
2: **tant que** $r \neq 0$ **faire**
3: $\quad a \leftarrow b$
4: $\quad b \leftarrow r$
5: $\quad r \leftarrow a \mod b$
6: **fin tant que**
7: **retourner** b

Algorithme 5 Coefficients de Bézout

Entrées: deux entiers naturels a et b premiers entre eux
Sorties: deux entiers relatifs u et v tels que $au + bv = 1$

1: $u \leftarrow 1$
2: $c \leftarrow a$
3: **tant que** $\frac{a-1}{b} \neq \left\lfloor \frac{a-1}{b} \right\rfloor$ **faire**
4: $\quad u \leftarrow u + 1$
5: $\quad a \leftarrow u \times c$
6: **fin tant que**
7: $v \leftarrow \frac{1-a}{b}$
8: **retourner** u, v

Algorithme 6 Algorithme d'Euclide étendu

Entrées: deux entiers naturels a et b tels que $(a, b) \neq (0, 0)$ et $a \geq b$
Sorties: $a \wedge b$ et deux entiers relatifs u et v tels que $au + bv = a \wedge b$

1: $u \leftarrow 1$
2: $x \leftarrow 0$
3: $v \leftarrow 0$
4: $y \leftarrow 1$
5: $r \leftarrow a \mod b$
6: **tant que** $r \neq 0$ **faire**
7: $\quad a \leftarrow b$
8: $\quad b \leftarrow r$
9: $\quad q \leftarrow \left\lfloor \frac{a}{b} \right\rfloor$
10: $\quad r \leftarrow a \mod b$
11: $\quad s \leftarrow u - qx$
12: $\quad u \leftarrow x$
13: $\quad x \leftarrow s$
14: $\quad t \leftarrow v - qy$
15: $\quad v \leftarrow y$
16: $\quad y \leftarrow t$
17: **fin tant que**
18: **retourner** a, u, v

Algorithme 7 Test de primalité

Entrées: $n \in \mathbb{N}, n \geq 3$ et n impair
Sorties: un booléen et le plus petit diviseur non trivial de n, s'il existe

$k \leftarrow 3$
$m \leftarrow 0$
tant que $k \leq \sqrt{n}$ **faire**
  si $\frac{n}{k} = \left\lfloor \frac{n}{k} \right\rfloor$ **alors**
    retourner **faux**
    afficher k "divise" n
    $m \leftarrow k$
    $k \leftarrow \frac{n}{k}$
  fin si
  $k \leftarrow k + 2$
fin tant que
si $m = 0$ **alors**
  retourner **vrai**
fin si

On ne teste que les nombres impairs jusqu'à la racine carrée. On pourrait améliorer cet algorithme en ne testant que les nombres premiers jusqu'à la racine carrée.

Algorithme 8 Valuation p-adique

Entrées: $n \in \mathbb{N}^*$ et p un nombre premier
Sorties: l'entier naturel k tel que $p^k \mid n$ et $p^{k+1} \nmid n$

$q \leftarrow 1$
$k \leftarrow -1$
tant que $\frac{n}{q} = \left\lfloor \frac{n}{q} \right\rfloor$ **faire**
  $q \leftarrow q \times p$
  $k \leftarrow k + 1$
fin tant que
retourner k

Algorithme 9 Décomposition en produit de facteurs premiers

Entrées: $n \in \mathbb{N}, n \geq 2$

Sorties: la liste des diviseurs premiers de n répétés valuation de fois

1: $d \leftarrow 2$
2: $i \leftarrow 1$
3: $c \leftarrow 1$
4: **tant que** $d \leq \sqrt{n}$ **faire**
5: **si** $\frac{n}{d} = \left\lfloor \frac{n}{d} \right\rfloor$ **alors**
6: $L[i] \leftarrow d$
7: $i \leftarrow i + 1$
8: $n \leftarrow \frac{n}{d}$
9: **sinon**
10: $d \leftarrow d + c$
11: $c \leftarrow 2$
12: **fin si**
13: **fin tant que**
14: $L[i] \leftarrow n$
15: **retourner** L