L'algorithme d'Euclide

Pierre Lescanne

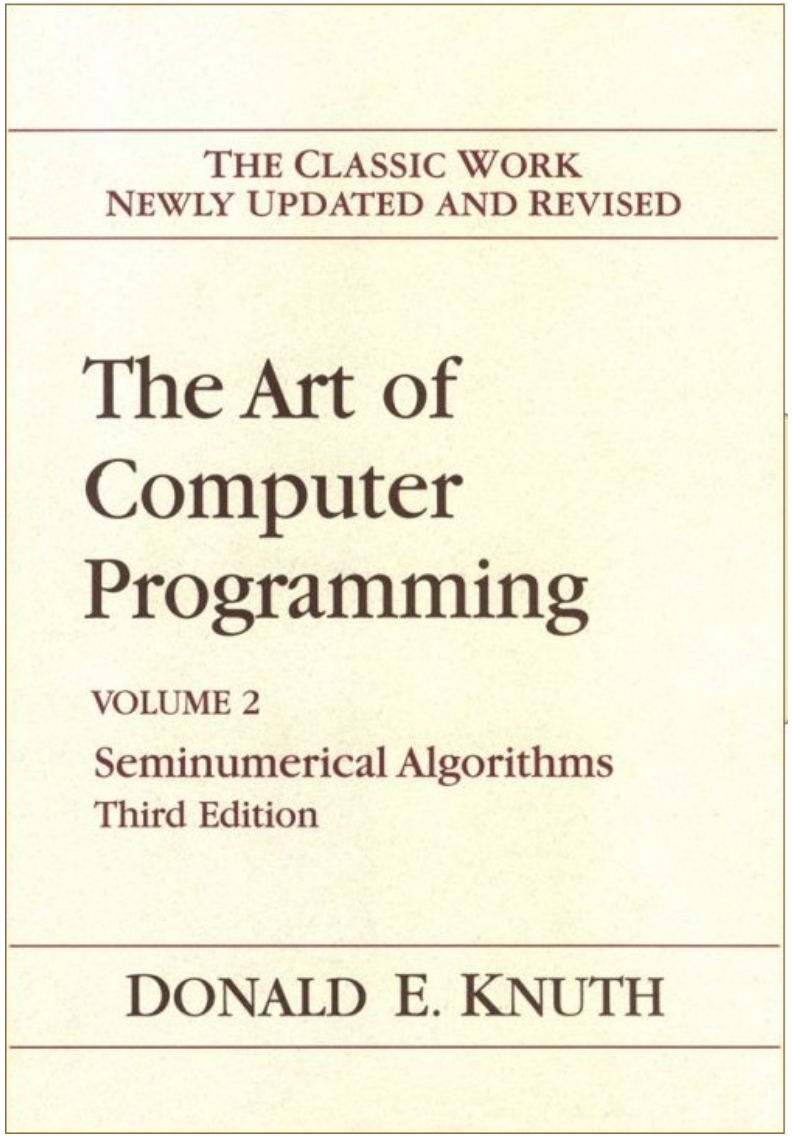
dernière mise à jour: *18 janvier 2006 – 09 : 07*

Plan

Source

Cete exposé est inspiré de l'ouvrage de Don Knuth

The art of computer programming Vol.2



Knuth

Sûrement le plus grand scientifique informaticien contemporain.

The art of computer programming a été désigné par American Scientist, parmi les douze meilleurs livres scientifiques du siècle.
avec

1. la mécanique quantique de Dirac,
2. la relativité d'Einstein,
3. les fractales de Mandelbrot,
4. la liaison chimique de Pauling,
5. la fondation des mathématiques de Russel et Withehead,
6. la théorie des jeux de von Neumannn et Morgenstern,
7. la cybernétique de Wiener,
8. la symétrie orbitale de Woodward et Hoffmann,
9. l'électrodynamique quantique de Feynman,
10. la recherche de structure de Smith,
11. les œuvres complètes d'Einstein.

Plan

Euclide

Euclide (né vers -325, mort vers -265 à Alexandrie) étudia à Athènes à l'École des successeurs de Platon et il s'établit à Alexandrie sur l'invitation de Ptolémée II, roi d'Égypte.

Ses Éléments sont constitués de 13 livres :

- qui sont une synthèse des mathématiques connues à son époque,
- auxquelles Euclide apporte des compléments, des démonstrations et de la rigueur,
- qui traitent d'arithmétique, d'algèbre et de géométrie.

L'algorithme d'Euclide

L'algorithme d'Euclide de calcul du plus grand commun diviseur se trouve dans le livre 7 propositions 1 et 2.

Il n'est pas probablement pas de lui.
Les experts pensent que la méthode était déjà connue 200 ans auparavant.
Au moins dans sa forme soustractive, elle était connue d'Eudoxe.

Le plus vieil algorithme non trivial connu,
car il contient explicitement une itération.

Plan

Le plus grand commun diviseur

Le plus grand commun diviseur $pgcd(m, n)$ de m et n est le plus grand entier qui divise à la fois m et n.
Si

$$m = 2^{m_2} 3^{m_3} 5^{m_5} 7^{m_7} 11^{m_{11}} \ldots = \prod_{p \text{ premier}} p^{m_p}$$

alors

$$pgcd(m, n) = \prod_{p \text{ premier}} p^{min(m_p, n_p)}.$$

Cette formule est inapplicable en pratique, car elle nécessite de factoriser un nombre en facteurs premiers,

ce que l'on se sait pas faire efficacement.

L'algorithme d'Euclide annoté (1/3)

Proposition. Étant donné deux entiers positifs, trouver leur plus grand commun diviseur.

L'initialisation

Soit A et C deux entiers positifs ; on doit trouver leur plus grand commun diviseur. Si C divise A, alors C est un diviseur commun de C et A puisqu'il se divise lui-même. Il est aussi clairement le plus grand puisqu'aucun entier plus grand que C ne divise C.

L'itération

Si C ne divise pas A, alors je soustrais de façon continue le plus petit des nombres A ou C du plus grand, jusqu'à ce qu'un nombre divise le précédent. Ceci arrivera à un moment ou à un autre, puisque s'il reste une unité, il divise le nombre précédent.

L'algorithme d'Euclide annoté (2/3)

Preuve que le résultat est un diviseur commun

Soit maintenant E le reste de A divisé par C ; soit F le reste de C divisé par E.

Supposons que F est un diviseur de E. Puisque F divise E et E divise $C - F$, F divise aussi $C - F$; mais il se divise lui-même, donc il divise C. Puisque C divise $A - E$ alors F divise $A - E$. Mais il divise aussi E alors, il divise A. Donc c'est un diviseur commun de A et C.

L'algorithme d'Euclide (3/3)

Preuve que le résultat est le plus grand diviseur commun

J'affirme maintenant que c'est le plus grand. En effet, si F n'est pas le plus grand diviseur commun de A et C, un nombre plus grand doit les diviser tous les deux. Soit G un tel nombre.

Maintenant puisque G divise C tandis que C divise $A - E$, alors G divise $A - E$. G divise A tout entier, donc il doit diviser le reste E. Mais E divise $C - F$; par conséquent, G divise $C - F$. Or G divise C entier, donc il divise le reste F ; c'est-à-dire qu'un nombre plus grand divise un nombre plus petit.

C'est impossible.

Commentaires

L'algorithme a été simplifié.
Les Grecs ne considèrent pas l'unité comme un «diviseur» d'un entier.
Plus précisément,

- l'unité n'est pas un nombre,
- le zéro n'existe pas

Étant donnés deux entiers positifs,

- ou bien il sont tous les deux égaux à l'unité,
- ou plus il sont premiers entre eux,
- ou bien ils ont un pgcd.

Commentaires

Euclide duplique ses explications et donne deux propositions séparées.

Commentaires

En fait, Euclide fournit un algorithme fondé sur des soustractions

$$\begin{aligned} pgcd(m,n) &= pgcd(m-n,n) \quad \text{si } m > n \\ pgcd(m,n) &= pgcd(m,n-m) \quad \text{si } m < n \\ pgcd(m,n) &= m \quad \text{si } m|n \end{aligned}$$

et prouve un algorithme fondé sur des divisions entières «divisions euclidiennes»

$$\begin{aligned} pgcd(m,n) &= pgcd(m \bmod n,n) \quad \text{si } m > n \\ pgcd(m,n) &= pgcd(m,n \bmod m) \quad \text{si } m < n \\ pgcd(m,n) &= m \quad \text{si } m|n \end{aligned}$$

Commentaires

En fait, il ne fait la preuve que sur trois étapes d'itération !
Car il ne connaît pas la preuve par récurrence[1].
En fait, ça n'est pas la seule occurrence d'une preuve pour le cas $n = 3$

censée valoir pour le cas général.

[1] que le vingtième siècle a commencé seulement à découvrir !

Commentaires

En fait, il ne fait la preuve que sur trois étapes d'itération !
Car il ne connaît pas la preuve par récurrence.
En fait, ça n'est pas la seule occurrence d'une preuve pour le cas $n = 3$

censée valoir pour le cas général.

Il n'empêche qu'Euclide est un pionnier !