Algorithme d'Euclide

Novembre 2013
dernière compilation : 7 novembre 2017

L'objectif de cette séance de travaux pratiques est de vérifier expérimentalement les résultats du cours concernant le calcul du PGCD de deux entiers : le théorème de G. Lamé, l'approche binaire et l'algorithme d'Euclide étendu.

1 Nombre d'itération

Etant donnés deux entiers positifs a et b, $b \leq a$, on note $I(a,b)$ le nombre d'itérations de l'algorithme d'Euclide pour déterminer $\text{PGCD}(a,b)$.

1. Implanter `ullong pgcd(ullong a,ullong b)` en utilisant l'algorithme itératif. Vérifier le bon fonctionnement de votre fonction.
2. Pour un entier a, on note $\varphi(a)$ le nombre d'entiers b tels que $0 < b < a$ et $\text{PGCD}(a,b) = 1$. Ecrire un programme `phi.c` qui calcule $\varphi(a)$ pour des entiers $a < n$, le paramètre n étant passé sur la ligne de commande.
3. Proposer une formule pour $\phi(a)$!
4. Implanter `ullong iter(ullong a,ullong b)` qui retourne le nombre d'itérations de l'algorithme d'Euclide.
5. Utiliser `gnuplot` pour représenter le graphe de la fonction

$$a \mapsto \sup_{0 \leq b \leq a} I(a,b).$$

6. idem pour le coût moyen

$$a \mapsto \frac{1}{a} \sum_{0 \leq b \leq a} I(a,b).$$

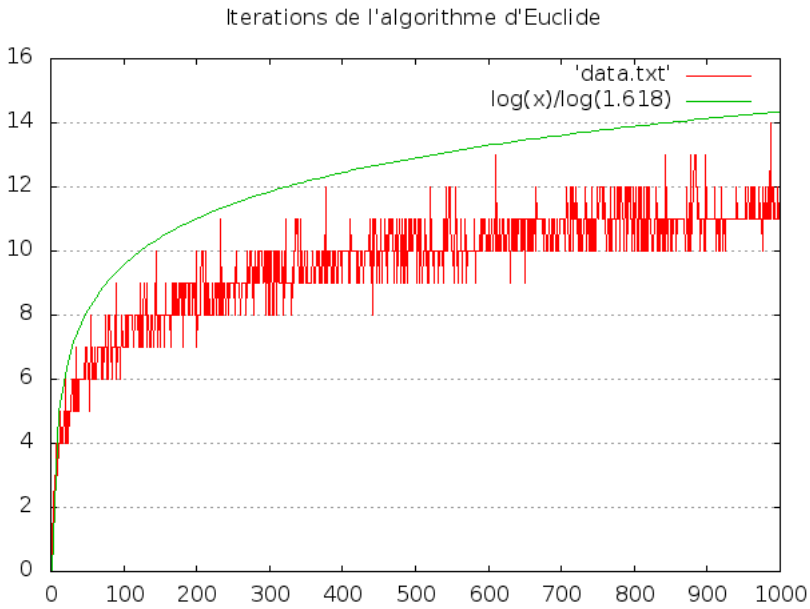

FIGURE 1 – Complexité de l'algorithme d'Euclide

7. idem pour le coût moyen

$$a \mapsto \frac{1}{\varphi(a)} \sum_{\substack{\text{PGCD}(a,b)=1 \\ 0 \leq b \leq a}} I(a,b).$$

où $\varphi(a)$ est la fonction d'Euler.

2 Euclide étendu

Résoudre le problème du PGCD étendu pour deux entiers a et b c'est déterminer deux entiers relatifs u et v tel que

$$au + bv = \text{PGCD}(a,b)$$

1. Implanter une version récursive `void bbr(ullong a, ...*u, ullong b, ...*v)` de l'algorithme d'Euclide.
2. Implanter une version itérative `void bbi(ullong a, ...*u, ullong b, ...*v)` de l'algorithme d'Euclide.
3. Vérifier le bon fonctionnement de ces deux implantations.

4. Faire une version “verbeuse” qui tracent les étapes intermédiaires de l’algorithme itératif.

3 PGCD binaire

— Implanter l’algorithme du PGCD binaire sur les entiers de 64 bits.
— Comparer les performance du PGCD binaire avec celui de l’algorithme d’Euclide.