Université Bordeaux 1 | **N1MA8W02 – Master 1**
Mathématiques | Année 2014–2015

Algèbre et calcul formel
Corrigé du devoir surveillé du 4 mars 2015

Exercice 1 – [Interpolation d'Hermite]
On utilise la formule de Taylor pour les polynômes : si P est un polynôme de $\mathbb{Q}[x]$ de degré n, alors

$$P(x) = \sum_{i=0}^{n} \frac{(x-a)^i}{i!} P^{(i)}(a).$$

Soient

$$P_1 = 1 + (x-1) + 2\frac{(x-1)^2}{2} = x^2 - x + 1$$
$$P_2 = 1 + 2(x-2) = 2x - 3$$

Alors P satisfait les conditions de l'énoncé si et seulement si

$$\begin{cases} P \equiv P_1 \mod (x-1)^3 \\ P \equiv P_2 \mod (x-2)^2 \end{cases}$$

Grâce à la commande `crt`, on trouve : $P = 5x^4 - 27x^3 + 52x^2 - 42x + 13$.

Exercice 2 – [Tri fusion]
Voir le fichier sage de la correction.

Exercice 3 – [Algorithme d'Euclide binaire]
1) $a = 60$, $b = 20$.

- Pas 2 : on appelle `Euclide(30,10)`. Il faudra à la fin multiplier le résultat par 2.
- Pas 2 : on appelle `Euclide(15,5)`. Il faudra à la fin multiplier le résultat par 2.
- Pas 4 : on appelle `Euclide(5,5)`.
- Pas 1 : on retourne 5
- On termine le programme `Euclide(30,10)` en multipliant par 2 : on retourne 10.
- On termine le programme `Euclide(60,20)` en multipliant par 2 : on retourne 20.

On trouve donc 20. C'est le pgcd de 20 et 60.

2) À chaque appel, on remplace (a, b) par (a', b'), où $a' \leqslant a/2$ ou $b' \leqslant b/2$. Ainsi, après $\lfloor \log_2(a) \rfloor + \lfloor \log_2(b) \rfloor$ appels, $a = b = 1$, et l'algorithme se termine (s'il ne s'est pas terminé avant).

Reste à examiner la complexité binaire de chaque opération. La division par 2 consiste juste à enlever un 0 dans l'écriture binaire du nombre considéré. La multiplication par 2 consiste à ajouter un 0. Les opérations les plus longues sont les différences $a - b$ et les comparaisons, qui sont en $O(\log n)$. On en déduit que l'algorithme est en $O((\log n)^2)$.

3) La question précédente prouve que l'algorithme se termine. Reste à voir qu'il calcul bien $\mathrm{pgcd}(a, b)$. Cela vient des points suivants.

- $\mathrm{pgcd}(a, a) = a$.
- Si a et b sont pairs, $\mathrm{pgcd}(a, b) = 2\,\mathrm{pgcd}(a/2, b/2)$.
- Si a est pair et si b est impair, $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(a/2, b)$.
- Si a et b sont impairs, $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(a - b, b) = \mathrm{pgcd}(\frac{a-b}{2}, b)$.

4)

Algorithme 1. AEEB (Algorithme d'Euclide étendu binaire)

Entrées: Deux entiers strictement positifs a et b
Sorties: (d, u, v) où $d = \mathrm{pgcd}(a, b)$ et où $d = au + bv$

Si $a = b$, alors
  retourner $(a, 1, 0)$
Si a et b sont pairs, alors
  $(d, u, v) \longleftarrow$ `AEEB(a/2,b/2)`
  retourner $(2d, u, v)$
Si l'un exactement des deux entiers est pair, mettons a, alors
  $(d, u, v) \longleftarrow$ `AEEB(a/2,b)`
  Si u est pair, alors
    retourner $(d, u/2, v)$
  Si u est impair, alors
    retourner $(d, (u - b)/2, v + a/2)$
Si a et b sont impairs, et mettons que $a > b$, alors
  $(d, u, v) \longleftarrow$ `AEEB((a-b)/2,b)`
  Si u est pair, alors
    retourner $(d, u/2, v - u/2)$
  Si u est impair, alors
    retourner $(d, (u - b)/2, v + (a - u)/2)$

Détaillons le cas où a est pair et b impair. Les autres cas se traitent de la même manière. Dans ce cas, si l'on appelle `AEEB(a/2,b)`, on obtient (d, u, v) où $d = \mathrm{pgcd}(a, b)$ et où

$$\frac{a}{2}u + bv = d.$$

Alors $\mathrm{pgcd}(a, b) = d$. Si u est pair, $u/2$ est un entier et

$$a\frac{u}{2} + bv = d.$$

Si u est impair, alors comme b est aussi impair, $(u - b)/2$ est un entier et

$$a\frac{u-b}{2} + b\left(\frac{a}{2} + v\right) = d.$$