Preuve et Analyse des Algorithmes
Examen 2h

17 février 2010

1 Reduction

On considère l'algorithme ci-dessous. Les nombres sont représentés par des tableaux de chiffres en base B.

```
1  Residue( z : nombre, m : entier )
2  variable r : chiffre
3           i : indice
4  debut
5    i ← taille(z) − 1
6    r ← 0
7    tantque ( i ≥ 0 )
8        r ← r ∗ B + z[i]
9        r ← r mod m
10       i ← i − 1
11   ftq
12   retourner r
13 fin
```

(a) Que fait cet algorithme ?

(b) On suppose que toutes les opérations arithmétiques d'effectuent à temps constant. Quelle est la forme du temps de calcul de cet algorithme ?

```
#define  MAX 100
#define  B    16

typedef  unsigned int chiffre;
typedef  chiffre nombre [ MAX ];

typedef  unsigned int entier;
```

(c) Donner une implantation en langage C de cet algorithme utilisant les définitions ci-dessus.

(d) Quelle est la taille binaire d'un entier ?

(e) Quel est le domaine de validité de votre implantation.

2 Euclide à la main

Résoudre le problème de Bâchet-Bézout pour les entiers $a = 57$, et $b = 33$.

L'entier 33 est-il inversible modulo 57 ?

3 Invention

Il s'agit d'écrire un algorithme `pgcdb(a, b)` pour caculer le PGCD de deux entiers positifs **sans** utiliser l'opération de **réduction modulaire**. Vous utiliserez les règles :

1. si a et b sont pairs alors

$$\text{PGCD}(a, b) = 2\,\text{PGCD}(a/2, b/2)$$

2. si a est pair et si b est impair alors

$$\text{PGCD}(a, b) = \text{PGCD}(a/2, b)$$

3. si $a \geq b$ alors

$$\text{PGCD}(a, b) = \text{PGCD}(a - b, b)$$

4. si $a \neq 0$ alors

$$\text{PGCD}(a, 0) = a$$