

## Exercices d'algorithmique

### 1 Un premier calcul de $a^n$

**Question 1.** Proposer un algorithme écrit en pseudo-code de calcul de  $a^n$  qui utilise uniquement l'opération multiplication (on utilisera une boucle **Tant que** et la variable de boucle  $c$  sera initialisée à  $n$ ).

**Question 2.** Démontrer la terminaison de l'algorithme.

**Question 3.** Démontrer la correction de l'algorithme en utilisant un invariant de boucle.

**Question 4.** Donner la complexité de l'algorithme.

### 2 Exponentiation rapide

On considère l'algorithme suivant, dit d'*exponentiation rapide*, qui calcule la puissance  $n$ -ième d'un nombre  $a$  :

```

Fonction exp(a, n)
  r ← 1
  k ← a
  c ← n
  Tant que c > 0
    Si c est impair
      r ← r × k
    k ← k × k
    c ← ⌊ $\frac{c}{2}$ ⌋
  ...

```

**Question 5.** Faire tourner l'algorithme à la main pour  $n=6$  et  $n=7$ . Quel est le rôle de la variable  $r$ ? Compléter la fonction **exp** pour qu'elle renvoie le résultat.

**Question 6.** Démontrer que cet algorithme se termine, puis démontrer que cet algorithme est correct, en considérant l'invariant de boucle :

$$k_i^{c_i} r_i = a^n$$

**Question 7.** Donner la complexité de l'algorithme.