Fonctions récursives - exponentiation effiace

laurent.jospin.59@free.fr, `http://jospin.lstl.fr`

Lycée Saint-Louis, Paris

Le mot clef **`rec`** de Caml permet de définir des fonctions récursives telles que :

```
let rec factorielle n = match n with
| 0 -> 1
| k -> k * factorielle (k-1);;
```

On a ainsi :

```
factorielle 3  =  3 * factorielle 2
               =  3 * (2 * factorielle 1)
               =  3 * (2 * (1 * factorielle 0))
               =  3 * (2 * (1 * 1))
               =  6
```

1. Ecrire une fonction récursive qui calcule $\binom{n}{k}$ par récurrence à l'aide de la formule du triangle de Pascal :

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

pour tous entiers naturels n et k tels que $0 < k < n$.

De plus, on rappelle que : $\displaystyle\binom{n}{n} = \binom{n}{0} = 1$ pour tout entier naturel n .

1 Exponentiation

Soit E un ensemble muni d'une loi de composition interne associative notée $*$ et on note 1 l'élément neutre. On s'intéresse au calcul des puissances entières de a. La multiplication sur E est considérée comme l'opération coûteuse de nos programmes (on pourra par exemple imaginer que $E = \mathbb{K}[X]$ ou $E = \mathscr{M}_k(\mathbb{K})$ pour justifier cette considération). On ne comptera pas la multiplication par 1 comme une multiplication dans les nombres de multiplications demandés et on évitera cette multiplication autant que possible dans les programmes.

Pour tout $a \in E$, on définit a^n par : $a^0 = 1$, et par récurrence $a^{n+1} = a^n * a$.

2. En se basant uniquement sur cette définition, ecrire une fonction récursive `puissance n a` qui calcule a^n. On utilisera la multiplication entière. Préciser le nombre de multiplications en fonction de n. Quel est le type de `puissance 3` et que représente `puissance 3` ?

3. Soit $k \in \mathbb{N}$. Justifier que tout entier compris entre 2^k et $2^{k+1} - 1$ s'écrit avec exactement $k + 1$ bits (significatifs). En déduire le nombre de bits significatifs d'un entier n non nul en fonction de n.

4 (Méthode binaire)**.** En remarquant que $\forall p \in \mathbb{N}^* \begin{cases} a^{2p} = a^p * a^p \\ a^{2p+1} = a^p * a^p * a \end{cases}$, écrire une fonction *récursive* plus efficace pour calculer a^n. Préciser le nombre de multiplications effectuées en fonction du nombre $\nu(n)$ de 1 dans son écriture binaire, puis montrer que le nombre $C(n)$ de multiplications sur l'entrée n est en $\Theta(\log_2 n)$ (c'est-à-dire qu'il existe $a, b \in \mathbb{R}_+^*$ tel que $a \log_2 n \leqslant C(n) \leqslant b \log_2 n$ pour tout n à partir d'un certain rang).

5. Justifier que le calcul de a^{15} correspond à un pire cas pour l'algorithme puis montrer que le calcul de a^{15} n'est pas optimal avec cet algorithme.

6 (Méthode des facteurs)**.** La méthode peut, en réalité, être adaptée en fonction du plus petit diviseur p non trivial de n. En effet si, $n = pq$, donner une méthode pour calculer a^n.

7. En déduire une fonction *récursive* basée sur la méthode des facteurs qui commencera par tester (uniquement) si n est divisible par 2, 3, 5 ou 7 et effectuera les calculs adaptés dans ces cas, puis sinon se raménera au cas $n - 1$.

8. Montrer que pour tout entier k, la méthode binaire est meilleure que la méthode des facteurs pour $n = 33 \times 2^k$ et que la méthode des facteurs est meilleure que la méthode binaire pour $n = 15 \times 2^k$.

2 Flèches de Knuth

Donald Knuth définit pour $a,b \in \mathbb{N}$: $a \uparrow b = a^b$, $a \uparrow\uparrow b = a^{a^{\cdot^{\cdot^{\cdot^{a}}}}}$ avec b exemplaires de a, et plus généralement pour $n > 1$, $a \uparrow^n 0 = 1$ et pour tout entier $b \geqslant 0$, $a \uparrow^n b = a \uparrow^{n-1} (a \uparrow^n (b-1))$. Cette notation est parfois utilisée pour exprimer des majorants dans des problèmes combinatoires complexes.

9. Définir une fonction récursive `fleches_Knuth n a b` qui calcule $a \uparrow^n b$ pour tous entiers naturels a,b,n.

10. L'exécution de `fleches_Knuth 2 3 4 ;;` produit le résultat `- : int = -2124021781892527813`. Calculer une valeur approchée du nombre de bits nécessaires pour écrire l'entier $3 \uparrow\uparrow 4$ puis justifier le résultat obtenu.