

TD 2 - Arithmétique : exponentiation rapide

Le principe d'exponentiation rapide décrit ci-dessous repose sur la décomposition de l'exposant en base 2 et l'utilisation de l'algorithme de Hörner.

Décrivons la méthode sur un exemple : soit à calculer a^{11} où a est par exemple un entier.

- On commence par décomposer l'exposant $n = 11$ en base 2 :
on obtient $11 = 1 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 1 \times 2^0$ soit encore $11 = \overline{1011}$.
- On associe ensuite à cette décomposition le polynôme P :
 $P(X) = 1 \times X^3 + 0 \times X^2 + 1 \times X^1 + 1 \times X^0$; P est tel que $11 = P(2)$.
- On utilise le schéma de Hörner :
 $P(X) = 1 + X \times (1 + X \times (0 + X \times (1)))$ et $11 = 1 + 2 \times (1 + 2 \times (0 + 2 \times (1)))$.
- La substitution donne :

$$a^{11} = \left(\left(\left((a^1)^2 \times a^0 \right)^2 \times a^1 \right)^2 \times a^1 \right)$$

Remarque : dans cette écriture, si on lit les exposants de a de la gauche vers la droite, on retrouve la décomposition de 11 en base 2, $11 = \overline{1011}$.

Travail demandé :

Écrire une fonction Scilab qui prenne en argument l'entier a et l'exposant entier naturel n , et qui retourne a^n suivant le schéma décrit ci-dessus.

1. Pour simplifier le script, on peut utiliser la commande Scilab dec2bin qui retourne la décomposition en base 2 d'un entier écrit en base 10.
Attention : cette fonction retourne une chaîne de caractères qu'il est nécessaire d'interpréter comme une suite de chiffres 0 ou 1. Il faudra, par conséquent, séparer chaque caractère de la chaîne ce qui peut se faire par la commande strsplit suivie de la commande evstr qui permet de convertir le caractère 0 ou 1 en nombre.
Par ailleurs, la longueur d'une chaîne de caractères s'obtient par la commande *length*.
2. Implémenter ensuite la formule d'exponentiation rapide à l'aide d'une boucle `for ... end`, boucle qui « suit » le calcul de la parenthèse la plus intérieure vers la plus extérieure.
Afficher le résultat.

Script Scilab

```
// Exponentiation rapide
// -----
a=input('nombre a : ');
n=input('exposant entier : ');
// conversion en base 2 de l'exposant n
N=evstr(strsplit(dec2bin(n)));
// -----
l=length(N);
x=a;
for i=2:l
    x=x*x;
    if N(i)==1 then x=x*a
    end
end
// affichage de a^n
disp(x);
```