Quel est le nombre minimal de multiplications pour calculer x<sup>n</sup> dans chaque cas suivant :

n	15	16	23	33	53
min(n)	5	4	6	6	8

## **Explications** (Inspiré de Donald Knuth The Art of Computer Programming)

Il y a deux méthodes classiques (on suppose qu'on peut garder en mémoire les résultats intermédiaires obtenus et donc les réutiliser sans les recalculer).

## La méthode binaire :

Ecrivez n en base 2, puis remplacez dans l'écriture trouvée chaque 1 par SX, chaque 0 par S. Supprimez le SX qui apparaît à gauche.

Interprétez l'écriture obtenue comme le moyen de calculer x <sup>n</sup> : S désigne la mise au carré et X la multiplication par x.

Par exemple 15 = 1111 en binaire donne <del>SX</del>SXSXSX ce qui s'interprète (à condition de commencer par la droite) comme :

$$x^{15} = X(S(X(S(X(S(x))))))$$
 soit  $x * (x * (x * x^2)^2)^2$ 

Donc pour 15, la méthode binaire nécessite 6 multiplications b(15) = 6.

Remarque : avec cette méthode, on n'a besoin de mettre en mémoire que x et le résultat courant.

## La méthode de factorisation

Elle consiste à utiliser une factorisation de n : n = p q où p est le plus petit facteur premier de n et q > 1. On calcule d'abord x p qu'on élève ensuite à la puissance q.

Par exemple, pour x  $^{15}$  on calcule x  $^{3}$  en deux multiplications, puis on élève x  $^{3}$  à la puissance 5 en trois multiplications, y  $^{5}$  = y \* (y  $^{2}$ )  $^{2}$ 

Donc, par la méthode de factorisation, on calcule  $x^{15}$  en 5 multiplications : f(15) = 5.

## Les exemples proposés

- Pour 16 la méthode binaire est la meilleure :  $(((x^2)^2)^2)^2$
- Pour 15, la méthode binaire nécessite 6 multiplications b(15) = 6, alors que par la méthode de factorisation, on calcule  $x^{15}$  en 5 multiplications.
- 23 est le plus petit exemple où la meilleure méthode n'est ni la méthode binaire, ni la méthode par factorisation : b(23) = 7, f(23) = 1 + b(22) = 7 tandis qu'on peut calculer x <sup>23</sup> en 6 multiplications : on calcule x <sup>3</sup> en deux multiplications : x <sup>2</sup> \* x puis x <sup>5</sup> en une multiplication supplémentaire x <sup>3</sup> \* x<sup>2</sup> et x <sup>10</sup> comme carré de x <sup>5</sup> et enfin x <sup>23</sup> = (x <sup>10</sup> \* x <sup>3</sup>) \* x <sup>10</sup>
- Pour 33 la méthode binaire est la meilleure b(33) = 6, f(33) = 7
- Pour 55 la méthode par factorisation est la meilleure b(55) = 9, f(55) = 8