Exponentiation

Anca Nitulescu
anca.nitulescu@ens.fr

Ecole Normale Supérieure, Paris

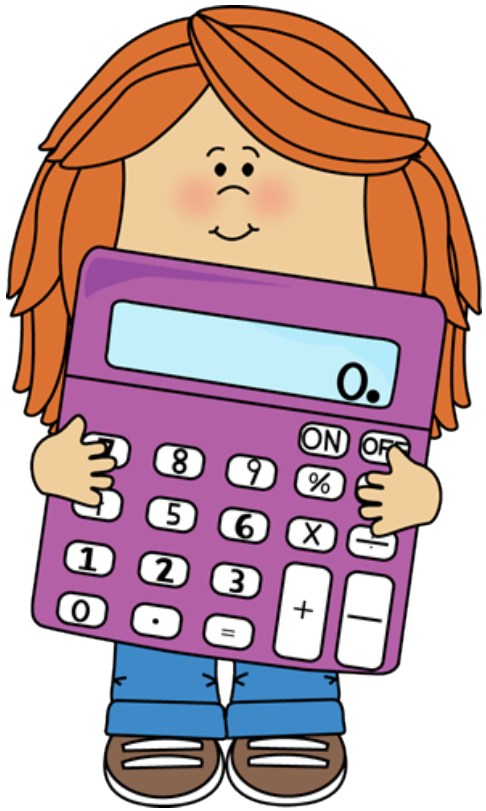
5 octobre 2016

Algorithme

Définition

Algorithme = Suite finie d'opérations élémentaires constituant un schéma de calcul ou de résolution d'un problème

(Petit Larousse)



Exponentiation

Algorithme naïf

Calcul de $n-1$ multiplications successives :

$$x^n = x \cdot x \cdot x \ldots x$$

Optimisation

Pour $n = 2^k$

$$x^n = \left(\ldots \left(\left(x^2 \right)^2 \right)^2 \ldots \right)^2$$

k multiplications au lieu de $n = 2^k$

Exponentiation

Algorithme naïf

Calcul de $n-1$ multiplications successives :

$$x^n = x \cdot x \cdot x \ldots x$$

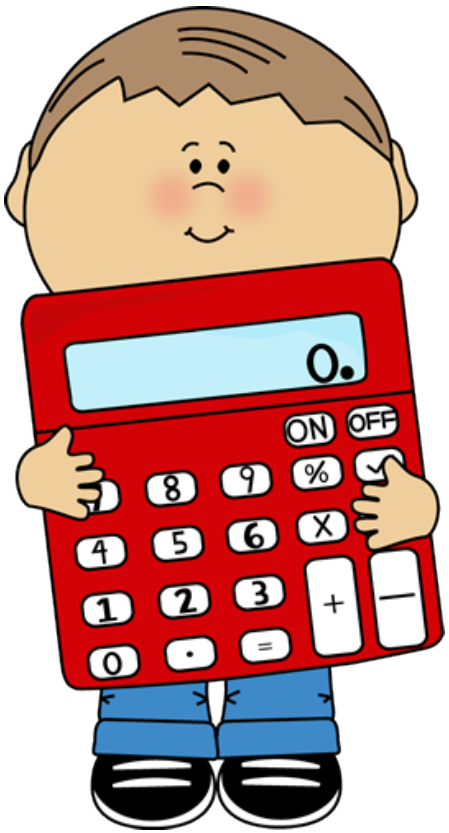
Idée

Décomposer len écriture binaire : $n = 16 = 2^4$

$$x^{16} = \left(\left(\left(x^2\right)^2\right)^2\right)^2$$

4 multiplications au lieu de $n = 2^4 = 16$

Exponentiation



Exemple

Pour calculer x^{11} :

- $11 = 8 + 2 + 1 = 2^3 + 2^1 + 2^0$
- Calcul de 1, x^2, $x^8 = \left(\left(x^2\right)^2\right)^2$
- $x^{11} = x^8 \cdot x^2 \cdot x$