(

Variables :

(résultat)

(base à la puissance avec l’indice de la boucle en cours)

Conversion de l'exposant en binaire.

On parcourt l'exposant en binaire (eme coefficient) :

- si le coefficient vaut on multiplie le résultat par et on en extrait le reste modulo

- on remplace par

On retourne le résultat

Complexité :

# Inverse modulaire

Algorithme d'Euclide éten rE1=du (recherche des coefficients de l'équation de Bézout)

On calcule , , tels que

Tant que :

On retourne puisque donc

Complexité :