

TP7 : Factorisation d'entiers par la méthode de Pollard

Méthode de Pollard

Exercice 1 : Ecrire une fonction correspondant à l'algorithme de Pollard donné en cours pour trouver des facteurs de l'entier m : on part d'un x_0 au hasard puis on construit la suite

$$x_{i+1} = (x_i^2 + 1) \bmod m \text{ et on calcule les } \text{pgcd}(x_{2i} - x_i, m) .$$

Si on trouve un pgcd différent de 1 on retourne les deux facteurs de m obtenus ainsi que l'indice i

sinon on s'arrête lorsque $2 m^{\left(\frac{1}{4}\right)} < i$ et on rend FAIL.

- Tester cette fonction avec un entier qui a deux grands facteurs premiers : $m = p_1 p_2$ en ajustant la taille de p_1 et p_2 jusqu'à obtenir un temps de calcul notable tout en restant supportable.
- Faire plusieurs exécutions pour le même entier en partant de x_0 différents.

Exercice 2 : Tester la fonction **facteurs** du TP6 (algorithme naïf) avec les entiers m de l'exercice 1.

Trouver des entiers $m = p_1 p_2$ pour lesquels le temps de la fonction **facteurs** soit raisonnable. Quelle stratégie envisagez-vous pour factoriser un entier quelconque ?

S'il vous reste quelques minutes

Exercice 3 : Adapter la fonction de l'exercice 1 pour qu'elle traite un entier m produit de plus de deux grands facteurs premiers :

- lorsqu'on décompose m on n'est pas sûr que les facteurs soient premiers, on rappelle donc la fonction sur chaque facteur,
- on met un test de primalité en début de fonction pour ne pas travailler sur un facteur (très probablement) premier.

Et pour une poignée de minutes de plus

Ecrire un algorithme complet de factorisation de m en utilisant l'algorithme naïf pour extraire les facteurs premiers inférieurs à 10^5 (par exemple) et l'algorithme de Pollard sur ce qu'il reste de m .