Factorisation des grands nombres

Decker Benjamin - Le Boulc'h Erin

Double Licence Mathématiques Informatique - Semestre 6

Sommaire

1 Introduction

Déterminer si un nombre est premier est plus simple que de trouver les facteurs premiers de sa décomposition. On peut être convaincu moralement qu'un nombre est premier/ ou qu'il est décomposable en facteurs premiers non triviaux sans les connaître.

Objectif : Explorer les méthodes de factorisation, notamment pour de grands nombres

2 Factorisation naïve par divisions successives

Principe : trouver le plus petit diviseur de n (diviser n par tous les nombres premiers plus petits que lui et voir si un d'eux le divise), puis itérer la méthode sur le quotient.

3 Méthode de Fermat

Cette méthode repose sur le principe selon lequel un entier peut s'exprimer comme la différence entre deux carrés.

Lemmes nécessaires

- Tous les nombres premiers (sauf 2) sont impairs.
- Un entier se décompose comme $2^k N$ avec k $\in \mathbb{N}$, N un entier impair. Si pair est premier, on a donc la décomposition en facteurs premiers, sinon, N s'exprime comme une différence de carrés.
- Une somme ou une différence de nombres impairs est paire.
- Soit p, q $\in \mathbb{N}$, $pq = \frac{(p+q)}{2} - \frac{(p-q)}{2}$

Méthode On sait qu'un entier est décomposable comme $2^k N$, avec N un entier impair. Si N est premier, on a déjà la décomposition en facteurs premiers qui nous intéresse. Sinon, nous allons décomposer N en produit de deux facteurs impairs (auxquels on appliquera la même procédure s'ils ne sont pas premiers).

On veut trouver S et R tel que N = R^2 - S^2 = (S+R)(S-R). Pour cela, on commence avec c = $\lfloor\sqrt{(N)}\rfloor$ et on va y ajouter k $\in \mathbb{N}^*$ jusqu'à trouver un S^2 convenable. En effet, on pose R = c + k (R est forcément plus grand que N) pour avoir $S^2 = N - R^2 = N - (c+k)^2$. Un S^2 convenable est donc tel que S est un entier. Une fois S et R trouvés, on pourra donc écrire N = (S+R)(S-R)

Exemple Factorisons 15 par la méthode de Fermat. (On sait déjà que 15 = 3 × 5)
15 étant impair, 15 = 2^0N et N = 15
c = $\lfloor\sqrt{(15)}\rfloor$ = 3
Si on prend R = c + 1 = 4, R^2 = 16 et S^2 = N - R^2 = 16 - 15 = 1.
On a donc S = 1 qui est $\sqrt{(1)}$
On retrouve bien N = (R+S)(R-S) = (4+1) × (4-1) = 5 × 3