# Rapport de projet : Exponentiation rapide

## Année : 2016/2017

## S4 MA – IUT de Villetaneuse



## Groupe : Gatto Nathan, Wong Jason et Dos Santos Jérémy

## Tuteur : M. Bonino

# Sommaire :

INTRODUCTION ……………………………………………………………………………………………………………………………………

1. Présentation du projet ………………………………………………………………………………………………………
2. Contexte du projet …………………………………………………………………………………………………………...
3. Objectifs du projet …………………………………………………………………………………………………………….

Développements mathématiques ………………………………………………………………………………………………………..

Pseudo-Codes ………………………………………………………………………………………………………………………………………

Présentation des différents outils informatique …………………………………………………………………………………..

Conclusion et commentaires personnels sur le projet………………………………………………………………………….

Bibliographie………………………………………………………………………………………………………………………………………..

# Introduction

1 – Présentation du projet

Tout d’abord nous allons commencer par expliquer ce qu’est l’exponentiation rapide. C’est une méthode mathématiques utilisé pour calculer rapidement de grandes puissances entières qu’on peut éventuellement mettre à un certain modulo. On l’appelle aussi « Square and multiply ». Cette méthode est très utilisée en informatique notamment pour des méthodes de cryptage (RSA),

1er algorithme (Écriture de Hörner) :

On souhaite faire le calcul rapide d’une puissance de la forme , pour cela, on veut tout d’abord décomposer la puissance, c’est-à-dire n.On commence passer le nombre n à la base 2( en binaire), qui correspond à un polynome de la forme :

où : - les correspondent au nombre de rang i donnés dans l’écriture de n. - x correspond à la base, ici on utilise la base 2. - d le nombre de chiffres dans l’écriture binaire de n.

Puis on met en facteur les x le plus possible.

puis

on continue jusqu’à avoir l’écriture de Hörner du polynôme P

Enfin, on va utiliser cette écriture pour notre calcul de puissance. Pour cela, on remplace n par son écriture de Hörner et on calcule .

Exemple :

On veut calculer

Le nombre 9 correspond à 1001 en base 2, soit au polynôme :

où l’on va mettre les x en facteurs :

puis

On obtient donc où x correspond à la base utilisée, soit 2 dans notre cas.

Pseudo-code :

Variables :

m : Nombre a élevé à la puissance n

n : Puissance

x : base choisie

bin : nombre n en base 2

taille : taille de la chaine bin

res : résultat à retourner initialisé à m

Algorithme :

Si : taille==0

Retourne 1

Pour i allant de 1 à taille :

res=res^x

Si : bin[i]=1 :

res=res\*m

Explication :

Si la puissance n = 0, la taille de la chaine bin qui est la longueur du nombre en base 2 sera 0 et l’algorithme retournera 1 car .

Sinon, on remarque que quelque soit le chiffre au rang i du nombre binaire, on fait toujours le même calcul : on met à la puissance x le résultat, on fait une multiplication du nombre m seulement si le chiffre au rang i est 1.

Donc on crée une boucle dans laquelle on calcule res=res^x et on vérifie si le chiffre au rang i est 1, si c’est le cas, on fait l’opération res=res\*m

# Bibliographie

Site web consultés :

<https://hal.inria.fr/inria-00540485v2/document>

<http://www.maths-algo.fr/index.php/informatique/problemes-d-informatique/arithmetique/exponentiation-rapide>