# 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 ………………………………………………………………………………………………………………………………….3

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

Développements mathématiques ……………………………………………………………………………………………………….4

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

1. PHP……………………………………………………………………………………………………………………………………
2. GMP………………………………………………………………………………………………………………………………….
3. WAMP………………………………………………………………………………………………………………………………

Présentation et commentaires des résultats obtenus………………………………………………………………………….

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

Annexes………………………………………………………………………………………………………………………………………………

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).

2- Contexte du projet

Ce projet présente des algorithmes de calcul rapide de nombres de la forme mn, où m et n sont deux entiers positifs. De tels algorithmes sont utilisés dans de nombreux domaines où l’on a besoin de manipuler de grands entiers, par exemple en cryptographie.

3-Objectif du projet

Analyser et programmer plusieurs algorithmes d’exponentiation rapide de nombres entiers (et de classes de congruence d’entiers). Le but était de concevoir plusieurs façons de calculer des exponentiations et de comparés leur rapidité et leurs complexités afin de savoir lequel est le plus optimal et donc le moins couteux.

# Développements mathématiques

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 polynôme 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 algorithme 1 : Voir annexe 1.

Question de l’énoncé :

1. A) Ici on travaille en base de 2, on a donc :

B) Le nombre d’opérations additions et multiplication par boucle ne comptant que pour une seule opération on a :

1. Pour justifier l’encadrement suivant il faut comprendre la chose suivante : quand on met un nombre en base 2, il est composé de 1 et/ou de 0. Donc grâce à la formule (\*) alors 2d est inférieur ou égale à n

Explications :

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 quelques 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.

# Présentation des différents outils informatique

1. PHP



Pour réaliser ce projet nous avons décidé d’utiliser le langage de programmation PHP, PHP est un langage de programmation libre multi plateforme, principalement utilisé pour produire des pages Web dynamiques via un serveur HTTP, mais pouvant également fonctionner comme n'importe quel langage interprété de façon locale. PHP est un langage impératif orienté objet.

PHP est un langage qui a été créé en 1994 par Rasmus Lerdorf. C’est un langage extrêmement utilisé, il a permis la création de site tels que Facebook, Wikipédia et bien plus encore.

1. GMP

De plus nous avons utilisé une librairie de fonctions PHP qui se nomme GMP, *GNU Multiple Précision*, qui permet de manipuler des entiers d’une taille arbitraire. Parmi ces fonctions nous avons notamment utilisé *gmp\_mod* une fonction qui permet de mettre un nombre de type GMP au modulo souhaiter. *gmp\_mul* une fonction qui permet de multiplier deux nombres de type GMP.

1. WAMP

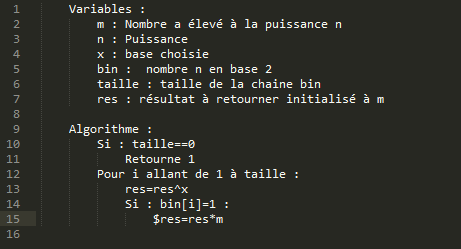


Wamp est une plate-forme de développement Web sous Windows pour des applications Web dynamiques à l’aide du serveur Apache2, du langage de scripts PHP et d’une base de données MySQL. (Mamp pour OS, LAMP pour Linux). Elle nous a permis de travailler avec GMP car cette librairie est déjà installée. Nous l’avons donc utilisé dans le but de tester et voir le rendu de notre code.

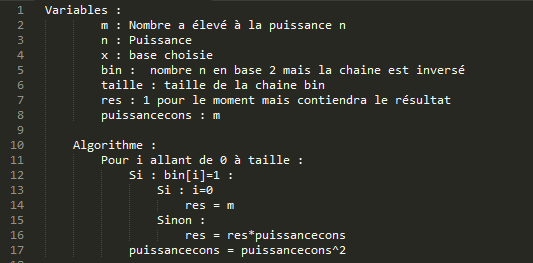
# Présentation et commentaires des résultats obtenus

# Annexes

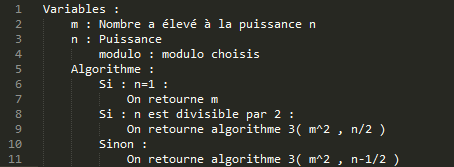
**Annexe 1 : Pseudo code** 1er **algorithme (Hornër)**



**Annexe 2 : Pseudo code 2ème algorithme (puissances successives)**



Annexe 3 : Pseudo code 3ème algorithme (parité des puissances)



# 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>

<http://php.net/manual/fr/book.gmp.php>

Cours sur la cryptographie de David Hébert.