*Master 2 Algèbre Appliquées*
Université Paris-Saclay
2016 - 2017



# COMPTAGE DE POINTS DE COURBES ELLIPTIQUE SUR DES CORPS FINIS

*par* Daniel RESENDE

le 24 janvier 2017

Résumé. — Il s'agit de la description de l'algorithme de René Schoof. Celui-ci fût le premier algorithme de comptage de points de courbes elliptique sur des corps finis en un temps polynomial ($O(\log^9 p)$).

*Remarque.* — Les éléments biographiques sont tirés de [**?**].

## Sommaire

# Introduction

Dans ce projet, je vais vous présenter un algorithme de comptage de points de courbes elliptique sur des corps finis. Je me restreindrais à des corps finis $\mathbf{F}_p$ avec $p$ premier différent de 2 et 3. Pour c'est deux derniers cas, l'algorithme est sensiblement le même.

# Contexte historique

# Courbes elliptiques sur $\mathbf{F}_p$

Soit $\mathbf{F}_p$ un corps fini à $p$ éléments de caractéristiques $p \neq 2, 3$.

Soit $E$ une courbe elliptique définie sur $\mathbf{F}_p$. On obtient l'équation affine de Weierstraß :

$$y^2 = x^3 + ax + b$$

avec $a, b \in \mathbf{F}_p$ et $\Delta = -16(4a^3 + 27b^2) \neq 0$.

Définition 2.1. — *Soit $\Phi$ l'endomorphisme de Frobénius d'une courbe elliptique $E$ tel que*

$$\begin{array}{rccc} \Phi : & E(\bar{\mathbf{F}}_p) & \longrightarrow & E(\bar{\mathbf{F}}_p) \\ & (x, y) & \longmapsto & (x^p, y^p). \end{array}$$

## Quelques résultats mathématiques marquants

Une des réussites d'Euler a été la démonstration du grand théorème de Fermat dans un cas particulier [†].

Théorème 3.i (de Fermat, cas $n = 3$). — *L'équation* $x^3 + y^3 + z^3 = 0$ *n'admet aucune solutions entières lorsque* $xyz \neq 0$.

*Démonstration.* On renvoie à [**?**, p. 134]. □

Le théorème 3.i est un résultat de théorie des nombres, mais Euler a touché à d'autres domaines. Citons par exemple ce résultat de topologie.

Théorème 3.ii. — *Il n'est pas possible de traverser tous les ponts de Könisberg en ne passant qu'une seule fois sur chaque pont.*

[†] Fermat lui-même n'avait de démonstration que dans le cas $n = 4$.