Compter les points sur une courbe elliptique

Jeremie Coulaud

15 février 2019

Table of contents

Introduction

blabla

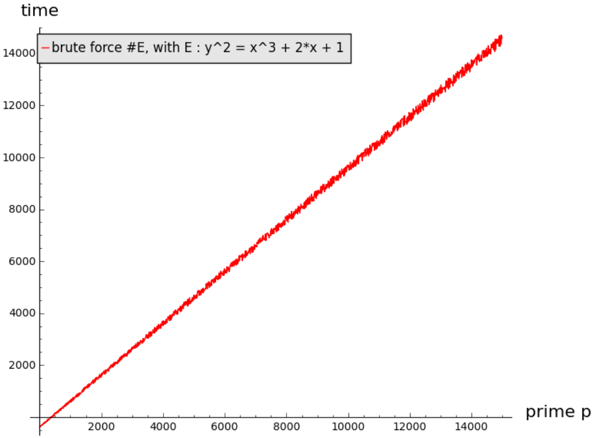
Algorithme naïf

$$y^2 = x^3 + ax + b = f(x)$$

- $\left(\dfrac{f(x)}{p}\right) = -1$, $f(x)$ n'est pas un carré modulo p, on ne trouve aucun point appartenant à la courbe.
- $\left(\dfrac{f(x)}{p}\right) = 0$, $f(x)$ est divisible par p, on trouve 1 point sur la courbe.
- $\left(\dfrac{f(x)}{p}\right) = 1$, $f(x)$ est un carré modulo p, on trouve 2 points sur la courbe.

$$\#E(\mathbb{F}_p) = 1 + p + \sum_{x \in \mathbb{F}_p} \left(\frac{f(x)}{p} \right)$$

Complexité en la taille de p



Algorithme de Schoof

Théorème Hasse-Weil

$\#E(\mathbb{F}_p) = p + 1 - t$ avec $|t| \leq 2\sqrt{p}$ trace de l'endomorphisme de Frobenius de E.

Pour trouver l'ordre de $E(\mathbb{F}_p)$ il faut trouver t
Idée de Schoof : trouver $t \pmod{l}$, avec l petit premier et utiliser les restes chinois pour trouver t

Frobenius

Soit E une courbe elliptique défini sur $\mathbb{F}_p$, l'endomorphisme de Frobenius est défini par

$$\begin{array}{cccc} \phi_p & : & E(\mathbb{F}_p) & \rightarrow & E(\mathbb{F}_p) \\ & & (x, y) & \mapsto & (x^p, y^p) \end{array}$$

On lui associe son polynôme caractéristique :

$$\phi_p^2 - t\phi_p + p = 0$$