Compter les points sur une courbe elliptique

Jeremie Coulaud

17 février 2019

Table of contents

Introduction

blabla

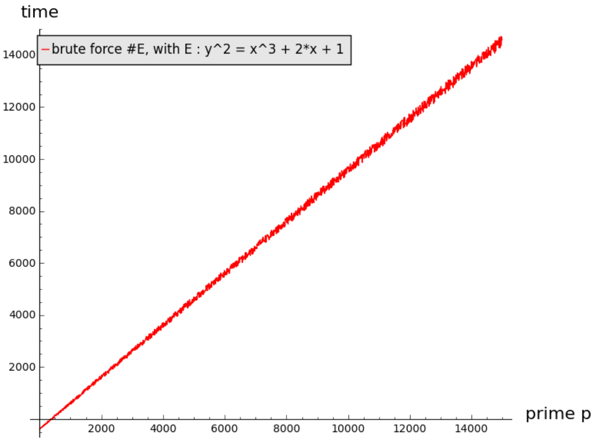
Algorithme naïf

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

- $\left(\dfrac{f(x)}{p}\right) = -1$, $f(x)$ 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 $|t| \leqslant 2\sqrt{p}$ 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 :

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

1ère application : calcul de $\#E(\mathbb{F}_{p^n})$

- r_1, r_2 racines de $\chi_p(x)$
- $Tr(\phi_{p^n}(x,y)) = r_1^n + r_2^n$
- Hass-Weil : $\#E(\mathbb{F}_{p^n}) = p^n + 1 - r_1^n - r_2^n$

Polynômes de division

On appelle $f_n(X)$ le n-ième polynôme de divisons définit sur $\mathbb{Z}[x]$par :

$$f_0(x) = 0$$
$$f_1(x) = 1$$
$$f_2(x) = 1$$
$$f_3(x) = 3x^4 + 6ax^2 + 12bx - a^2$$
$$f_4(x) = 2x^6 + 10ax^4 + 40bx^3 - 10a^2x^2 - 8abx - 2(a^3 + 8b^2)$$

On pose $F(X) = 4x^3 + 4ax + 4b$, et on a :

$$\begin{cases} f_{2n} & = f_n(f_{n+2}f_{n-1}^2 - f_{n-2}f_{n+1}^2) \\ f_{2n+1} & = \begin{cases} F^2 f_{n+2}f_n^3 - f_{n-1}f_{n+1}^3 & \text{si} \quad n \text{ est pair} \\ f_{n+2}f_n^3 - f_{n-1}f_{n+1}^3 F^2 & \text{si} \quad n \text{ est impair} \end{cases} \end{cases} \tag{1}$$

Ces polynômes s'annulent sur les points de l-torsion et permettent de calculer :

$$[m]P = \begin{cases} O_E & \text{si} \qquad P \in E[m] \\ \left(x - \frac{\psi_{m-1}(x,y)\psi_{m+1}(x,y)}{\psi_m^2(x,y)}, \frac{\psi_{2m}(x,y)}{\psi_m^4(x,y)}\right) & \text{sinon} \end{cases} \tag{2}$$

En posant :

$$\psi_m = \begin{cases} 2yf_m & \text{si m est pair} \\ f_m & \text{sinon} \end{cases}$$

Frobenius et Schoof

$$\phi_p^2(P) + [p_l]P = [t_l]\phi_p(P) \quad \forall P \in E[l] \tag{3}$$

Or pour tout $P = (x, y) \in E[l]$, $f_l(x) = 0$ et $y^2 - x^3 - ax - b = 0$. On peut donc travailler dans l'anneau :

$$\frac{\mathbb{F}_p[x, y]}{(f_l(x), y^2 - x^3 - ax - b)}$$

La question est donc pour quel valeur $0 \leqslant \tau \leqslant \frac{l-1}{2}$ l'équation suivante est vérifié :

$$(x^{p^2}, y^{p^2}) + [p_l](x, y) = [\tau_l](x^p, y^p) \tag{4}$$

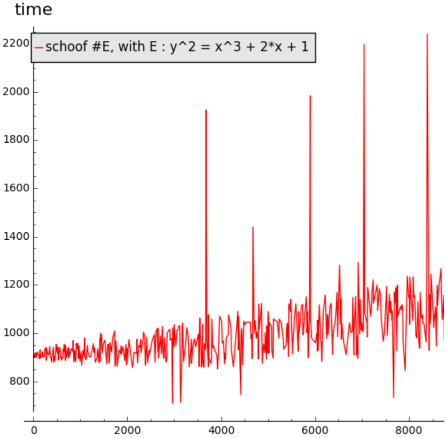
Choix des premiers l

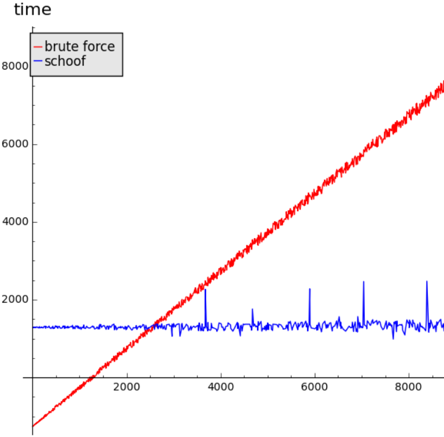
- $S = (l_1, \dots l_n)$ tel que $\prod l_i > 4\sqrt{p}$
- Petits l_i pour que f_l soit de plus petit degré possible.

Cas l = 2 : $t_2 \equiv 0 \pmod 2 \Leftrightarrow E(\mathbb{F}_p)$ a un élément d'ordre 2

- Point 2-torsion est de la forme $(x, 0)$
- $x^3 + ax + b$ à une racine dans $\mathbb{F}_p$
- Calcul $\gcd(x^p - x,\, x^3 + ax + b) \neq 1$

Expérimentations

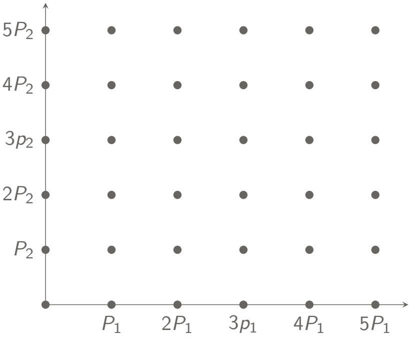




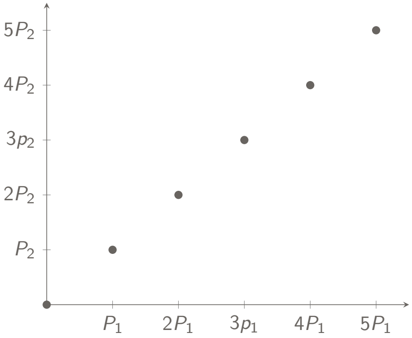
Algorithme SEA

Amélioration de l'algorithme de Schoof par Elkies et Atkins.

Représentation de $E[6]$



Représentation d'un sous groupe de $E[6]$



Isogénie

Polynômes modulaires