

# Compter les points sur une courbe elliptique

Jeremie Coulaud

18 février 2019

# Table of contents

Introduction

Algorithme naïf

Algorithme de Schoof

- Frobenius

- Polynômes de division

- Choix des premiers /

- Expérimentations

Algorithme SEA

- Analyse Complexe

- Isogénie

- Polynômes modulaires

- Premier d'Elkies

# Introduction

blabla

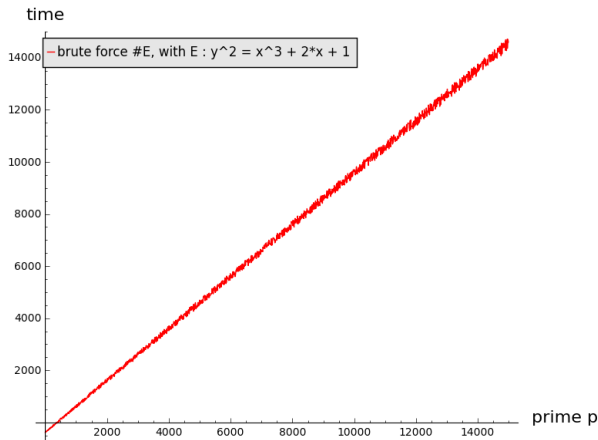
# Algorithme naïf

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

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

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

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 divisions défini 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 :

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



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

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

En posant :

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

## Frobenius et Schoof

$$\phi_p^2(P) + [p_I]P = [\tau_I]\phi_p(P) \quad \forall P \in E[I] \quad (3)$$

Or pour tout  $P = (x, y) \in E[I]$ ,  $f_I(x) = 0$  et  $y^2 - x^3 - ax - b = 0$ .

On peut donc travailler dans l'anneau :

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

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

$$(x^{p^2}, y^{p^2}) + [p_I](x, y) = [\tau_I](x^p, y^p) \quad (4)$$

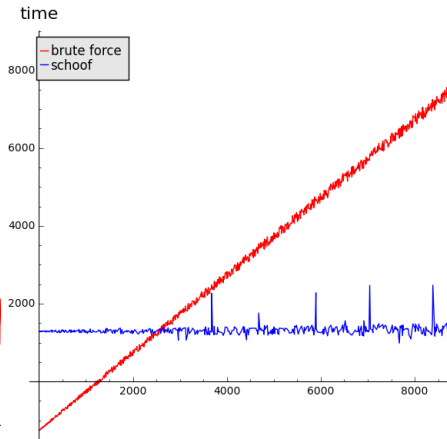
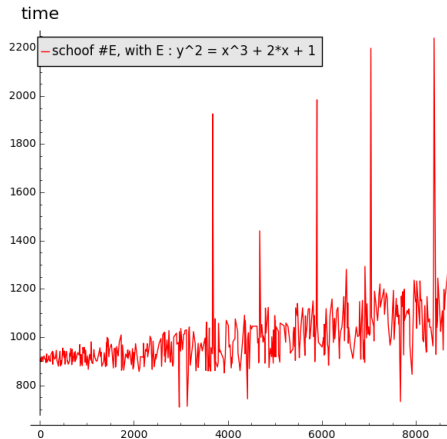
## Choix des premiers /

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

**Cas 1 = 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



# Analyse Complexe

## Definition

Tout sous groupe discret de  $\mathbb{C}$  non nul et non isomorphe à  $\mathbb{Z}$  peut s'écrire sous la forme  $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ , avec  $\omega_1, \omega_2 \in \mathbb{C}$ ,

$\operatorname{Im}\left(\frac{\omega_2}{\omega_1}\right) \neq 0, \tau = \frac{\omega_2}{\omega_1}$ . C'est un réseau de  $\mathbb{C}$  de rang 2, qu'on note :

$$\Gamma = \mathbb{Z} + \tau\mathbb{Z}$$

## Definition

On appelle tore le quotient  $T = \mathbb{C}/\Gamma$

Soit  $\Gamma$  un réseau de  $\mathbb{C}$ , on a la  $\wp$ -fonction de Weierstrass :

$$\wp(z) = \frac{1}{z^2} + \sum_{w \in \Gamma, w \neq 0} \left( \frac{1}{(z-w)^2} - \frac{1}{w^2} \right)$$

et sa dérivée :

$$\wp' = -2 \sum_{\omega \in \Gamma} \frac{1}{(z-\omega)^3}$$

### Theorem

*Soit  $E/\mathbb{C}$  une courbe elliptique sous forme réduite sur le corps des complexes. Il existe alors un réseau  $\Gamma$  tel que l'application suivante soit une bijection :*

$$\begin{aligned} \mathbb{C}/\Gamma &\rightarrow E \\ z + \Gamma &\mapsto \begin{cases} (\wp(z), \frac{\wp'(z)}{2}) & z \notin \Gamma \\ O & z \in \Gamma \end{cases} \end{aligned}$$

La fonction  $\wp$  satisfait l'équation différentielle suivante :

$$\wp'(z)^2 = 4\wp^3(z) + A\wp + B$$

# Isogénie

## Definition

Soit  $E_1/K$  et  $E_2/K$  deux courbes elliptiques. Si  $E_1$  et  $E_2$  ont le même  $j$ -invariant alors elles sont isomorphiques sur  $\bar{K}$ .

## Definition

Soit  $T_1 = \mathbb{C}/\Gamma_1$  et  $T_2 = \mathbb{C}/\Gamma_2$  deux tores. Un morphisme de  $E_1$  vers  $E_2$  est une application holomorphe  $\mu$  de  $T_1$  vers  $T_2$  qui soit un morphisme de groupe. Si ce morphisme est non constant alors on dit que c'est une isogénie.

Deux courbes elliptiques  $E_1/K$  et  $E_2/K$  sont isogènes s'il existe une isogénie  $\psi : E_1 \mapsto E_2$ . Le degré de l'isogénie est le degré du noyau de  $\psi$ .

# Polynômes modulaires

Le  $n$ -ème polynôme modulaire est noté  $\Phi_n(X, Y)$  et il est :

- symétrique
- de degré  $n + 1$  en chaque variable
- de coefficients de termes de plus haut degré 1
- de coefficients dans  $\mathbb{Z}$

## Definition

Soit  $E_1/\mathbb{C}$  et  $E_2/\mathbb{C}$  deux courbes elliptiques de  $j$ -invariant respectivement  $j_{E_1}$  et  $j_{E_2}$ . Le  $n$ -ième polynôme modulaire vérifie  $\Phi_n(j_{E_1}, j_{E_2}) = 0$  si et seulement si il existe une isogénie entre  $E_1$  et  $E_2$  dont le noyau est cyclique de degré  $n$ .



## Example

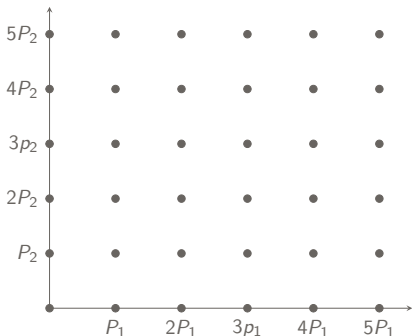
Pour  $n = 3$  on a le polynôme :

$$\begin{aligned}\Phi_3(x, y) = & x^4 - x^3y^3 + y^4 \\ & + 2232(x^3y^2 + x^2y^3) \\ & - 1069956(x^3y^2 + x^2y^3) \\ & + 36864000(x^3 + y^3) \\ & + 2587918086x^2y^2 \\ & + 8900222976000(x^2y + xy^2) \\ & + 452984832000000(x^2 + y^2) \\ & - 770845966336000000xy \\ & + 1855000000000(x + y)\end{aligned}$$

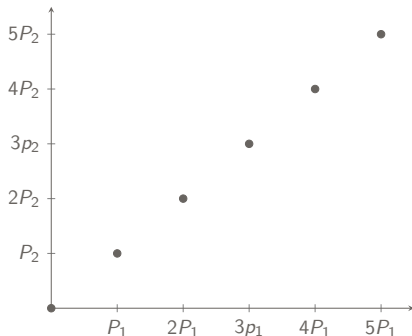
# Algorithme SEA

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

Représentation de  $E[6]$



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



Soit  $l$  un petit premier,  $\phi$  l'endomorphisme de Frobenius de polynôme caractéristique :

$$\chi_l(x) = x^2 - t_l x + p_l, \quad \text{avec } t \equiv t_l \pmod{l}, \quad p \equiv p_l \pmod{l}$$

$$\Delta_{\chi_l} = t_l^2 - 4p_l$$

### Definition

Si  $\Delta_{\chi_l}$  est un carré non nul dans  $\mathbb{F}_l$ , alors  $l$  est un premier de Elkies, sinon c'est un premier de Atkins.

Étude de la factorisation de  $\Phi_l$  pour savoir si  $\Delta_{\chi_l}$  est un carré.

$$\Phi_l(x, j) = h_1(x) \dots h_s(x) :$$

- $(1, 1, r, \dots, r)$ ,  $\Delta_{\chi_l}$  est un carré,  $\phi|_{E[l]}$  est diagonalisable,  $l$  est un premier de Elkies
- Calcul  $\gcd(\Phi_l(x, j), x^p - x)$

# Premier d'Elkies

## Premier d'Elkies

$\phi_p$  est diagonalisable de valeurs propres  $\lambda, \mu$ .

$$\chi_I(x) = x^2 - t_I x + p_I = (x - \lambda)(x - \mu)$$

Donc :

$$t_I \equiv \lambda + \mu \pmod{I}$$

- $\exists P_1 \in E[I]$  tel que  $\phi_I(P_1) = \lambda P_1$
- $C_1$  est le groupe cyclique d'ordre  $I$  engendré par  $P$
- $C_1$  est stable par le Frobenius

On peut construire le polynôme de degré  $I$  :

$$g_I(x) = \prod_{\pm P \in C_1^*} (x - x_P), \quad \text{où } P = (x_P, y_P)$$