Compter les points sur une courbe elliptique

Jérémie Coulaud

12 janvier 2019

Table des matières

1 Introduction aux courbes elliptiques **2**

2 Compter les points sur une courbe **2**
2.1 Algorithme naif 2
2.2 Shanks 2
2.3 Schoof 2

1 Introduction aux courbes elliptiques

2 Compter les points sur une courbe

On va considérer dans la suite que la caractéristique du corps utilisée pour définir nos courbes elliptiques est plus grande que 3. On peut donc écrire notre courbe elliptique sur $\mathbb{F}_p$ sous leur forme réduite $y^2 = x^3+ax+b$

2.1 Algorithme naif

On note $E : y^2 = f(x)$, compter les points de E revient donc pour chaque valeur de $x \in \mathbb{F}_p$ à regarder si $f(x)$ est un carré modulo p. On calcule donc le symbole de Legendre de $f(x)$, on a les cas suivant :

- $\left(\frac{f(x)}{p}\right) = -1$, $f(x)$ 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.

Au final en considérant le point à l'infini on peut calculer le nombre de points de E :

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

Soit :

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

La complexité est en la taille de p. Cette méthode est pratique quand p est petit mais devient impraticable s'il est trop grand.

2.2 Shanks

Il s'agit d'un algorithme Baby steps-giant steps de complexité exponentielle.

2.3 Schoof

Soit E une courbe elliptique défini sur $\mathbb{F}_p$ avec p premier > 3 sous sa forme réduite

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

On rappelle le théorème de Hasse-Weil :

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

Pour trouver le nombre de points de E il faut donc déterminer t. L'idée de Schoof est de calculer t modulo de petits nombres premiers puis d'utiliser le théorème des restes chinois.