Master 2 Algèbre Appliquées
Université Paris-Saclay
2016 - 2017

COMPTAGE DE POINTS DE COURBES ELLIPTIQUE SUR DES CORPS FINIS

par Daniel RESENDE

le 17 février 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 ($O(\log^9 p)$).

Sommaire

Introduction

Les courbes elliptiques définissent une lois de groupe sur les corps finis $\mathbf{F}_q$ qui est difficile pour le problème du logarithme discret. On retrouve par conséquent son utilisation dans plusieurs schémas cryptographiques comme Diffie-Hellman (avec ECDH) ou El-Gamal (avec ECDSA). Cependant, l'utilisation de schémas à l'aide de courbes elliptiques nécessite d'avoir un grand nombre premier qui divise l'ordre d'un sous-groupe cyclique de la courbe de $E(\mathbf{F}_q)$. Nous avons donc besoin de connaitre le cardinal de $E(\mathbf{F}_q)$.

Figure 1 – Portrait René Schoof

Il existe aujourd'hui de nombres algorithme de comptage de points d'une courbes elliptiques sur un corps finis $\mathbf{F}_q$:

- L'algorithme Baby Step Giant Step basé sur le théorème de Hasse,
- L'algorithme Schoof en 1985 que l'on va étudier dans ce mémoire,
- L'algorithme SEA [Schoof, Elkies, Atkin] en 1995 qui est une amélioration de l'algorithme de Schoof,
- L'algorithme de Satoh en 2005 basé sur le relèvement canonique sur les $\mathbf{Z}$ q-adiques,
- L'algorithme AGM [Mestre] basé sur le calcul de suites arithmetico-géométriques.

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 $\mathbf{F}_q$ avec $q = p^n$ et p premier différent de 2 et 3. Pour c'est deux derniers cas, l'algorithme est sensiblement le même.

1 Courbes elliptiques sur $\mathbf{F}_q$

Soit $\mathbf{F}_q$ un corps fini à p éléments de caractéristiques $p \neq 2, 3$.
Soit E une courbe elliptique définie sur $\mathbf{F}_q$. On obtient l'équation affine de Weierstraß :

$$y^2 = x^3 + ax + b \tag{1}$$

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

Définition 1.1. Soit Φ l'endomorphisme de Frobénius d'une courbe elliptique E tel que

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

Définition 1.2 (Trace)**.** Soit E une courbe elliptique sur $\mathbf{F}_q$. La trace de $E(\mathbf{F}_q)$ est l'entier $t = q+1-\#E(\mathbf{F}_q)$.

Proposition 1.1
Soit la trace t de $E(\mathbf{F}_q)$, on a alors

$$\phi^2 - t\phi + q = 0 \tag{2}$$

Théorème 1.i (de Hasse)
Soit E une courbe elliptique sur $\mathbf{F}_q$ et la trace t de $E(\mathbf{F}_q)$. On a

$$\mid t \mid \leq 2\sqrt{q}, \tag{3}$$

et par conséquent

$$\mid \#E(\mathbf{F}_q) - (q + 1) \mid \leq 2\sqrt{q} \tag{4}$$

Nous allons maintenant nous concentrer sur les sous-groupe de n-torsions $E[n]$ avec $n \in \mathbf{Z}_{\geq -1}$ tel que $p \nmid n$. Et on introduit la notion de polynôme de division.

Définition 1.3 (Polynôme de division)**.** Soit $n \in \mathbb{Z}^*$, le polynôme de division ψ_n est la fonction polynôme de $K[E]$ de coefficient dominent n et de diviseur

$$div(\psi_n) = (E[n]) - n^2(\vartheta)$$

Proposition 1.2 (Caractérisation du polynôme de division)
On construit le polynôme de division par récurrence sur $n \in \mathbf{Z}_{\geq 1}$:

1. $\psi_{-1}(X,Y) = -1,\ \psi_0(X,Y) = 0,\ \psi_1(X,Y) = 1,\ \psi_2(X,Y) = 2Y,$
2. $\psi_3(X,Y) = 3X^4 + 6aX^2 + 12bX - a^2,$
3. $\psi_4(X,Y) = 4Y(X^6 + 5aX^4 + 20bX^3 - 5a^2X^2 - 4bX - 8b^2 - a^3,$
4. $\psi_{2n}(X,Y) = \psi_n(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2)/2Y,$
5. $\psi_{2n+1}(X,Y) = \psi_{n+2}\psi_n^3 - \psi_{n+1}^3\psi_{n-1},$
6. $\psi_{-n} = \psi_n.$

Démonstration. Voir [**?**]. □

Dans l'algorithme de Schoof, nous utiliserons une variante du polynôme de division.

Définition 1.4. Soit $n \in \mathbb{Z}^*$, le polynôme f_n est une fonction polynôme de $K[E]$ définie par les relations suivantes :

$$f(n) = \begin{cases} \bar{\psi_n}(X,Y) & \text{si } n \text{ est pair} \\ \bar{\psi_n}(X,Y)/Y & \text{si } n \text{ est impair} \end{cases}$$

où $\bar{\psi_n}$ est la réduction de ψ_n par les termes en Y^2 par l'équation (E).

Proposition 1.3 (Caractérisation de f_n)
On construit f_n par récurrence sur $n \in \mathbf{Z}_{\geq 1}$:

1. $f_{-1}(X) = -1,\ f_0(X) = 0,\ f_1(X) = 1,\ f_2(X) = 2,$
2. $\psi_3(X) = 3X^4 + 6aX^2 + 12bX - a^2,$
3. $\psi_4(X) = 4Y(X^6 + 5aX^4 + 20bX^3 - 5a^2X^2 - 4bX - 8b^2 - a^3,$
4. $f_{2n}(X,Y) = f_n(f_{n+2}f_{n-1}^2 - f_{n-2}f_{n+1}^2),$
5. $$f(n) = \begin{cases} \bar{\psi_n}(X,Y) & \textit{si n est pair} \\ \bar{\psi_n}(X,Y)/Y & \textit{si n est impair} \end{cases}$$
6. $f_{2n+1}(X,Y) = \psi_{n+2}\psi_n^3 - \psi_{n+1}^3\psi_{n-1},$

Démonstration. Voir [**?**]. □

2 Algorithme de Schoof

2.1 Cas général

Cette algorithme consiste à calculer la trace du frobénius modulo tous les $l < l_{max}$ tel que l_{max} soit le plus grand nombre premier vérifiant :

$$\prod_{l \text{ premier},\ p \nmid l}^{l_{max}} l > 4\sqrt{q}. \tag{5}$$

Une fois calculé la trace modulo toutes les l-torsions, on utilise le Théorème des Restes Chinois (CRT) pour obtenir la trace dans $\mathbf{F}_q$. Puis on utilise le théoreme de Hasse pour avoir le cardinal de la courbe E sur $\mathbf{F}_q$.

Théorème 2.i (Algorithme de Schoof)
Voici le descriptif de l'algorithme de Schoof :

Algorithme 1 Algorithme de Shoof

Require: Une courbe elliptique E sur $\mathbf{F}_q$ un polynôme quelconque.
Ensure: Le cardinal de $E(\mathbf{F}_q)$.

```
M ← 2, l ← 3 ;
S ← {(t mod 2, 2)} ; {Cas pour l = 2}
while M < 4√q do
  k ← q mod l ;
  for τ = 0 to (l−1)/2 do
    if ∀P ∈ E[l], φ²(P) + [k]P = ±[τ]φ(P) then
      S ← S ∪ {(τ, l)} or S ← S ∪ {(−τ, l)} {Selon les cas}
      break ;
    end if
  end for
  M ← M ∗ l ;
  l ← nextprime(l) ; {Donne le prochain nombre premier après l}
end while
∀t ∈ S, trace ← CRT(t) ; {Effectue le théorème des restes chinois}
return q + 1 − trace.
```

Démonstration.

Cas mod 2 Dans ce cas, on cherche les points de 2-torsions, *i.e.*les points spéciaux de la courbes.

$$t = 1 \, mod \, 2 \Leftrightarrow \#E(\mathbf{F}_q)[2] = 1 \Leftrightarrow X^3{+}aX{+}b \text{ est irreductible sur } \mathbf{F}_q \Leftrightarrow pgcd(X^3{+}aX{+}b, X^q{-}X) = 1$$

□

2.2 Amélioration de Schoof

Dans son article original, Schoof (voir [tR85]) propose une amélioration possible de son algorithme.
— Si $\forall P$ nonzéro $\phi_l^2 P = \pm kP$ avec $q \equiv k[l]$
— Sinon on fait le cas général.

Algorithme 2 Algorithme de Shoof amélioré

Require: Une courbe elliptique E sur $\mathbf{F}_q$ un polynôme quelconque.
Ensure: Le cardinal de $E(\mathbf{F}_p)$.

```
M ← 2, l ← 3 ;
S ← {(t mod 2, 2)} ; {Cas pour l = 2}
while M < 4√q do
  k ← q mod l ;
  if φ_l^2 P = ±kP then
    if (k/l) = −1 then
      S ← S ∪ {(0, l)}
    else
      on recherche w tel que k = w^2 mod l
      if ±w est une valeur propre de φ_l then
        S ← S ∪ {(w, l)} or S ← S ∪ {(−w, l)} {Selon les cas}
      else
        S ← S ∪ {(0, l)}
      end if
    end if
  else
    for τ = 0 to (l−1)/2 do
      if ∀P ∈ E[l], φ^2(P) + [k]P = ±[τ]φ(P) then
        S ← S ∪ {(τ, l)} or S ← S ∪ {(−τ, l)} {Selon les cas}
        break ;
      end if
    end for
  end if
  M ← M ∗ l ;
  l ← nextprime(l) ; {Donne le prochain nombre premier après l}
end while
∀t ∈ S, trace ← CRT(t) ; {Effectue le théorème des restes chinois}
return q + 1 − trace.
```

3 Étude de la complexité

Références

[tIF99] Smart N. Blake I. F., Seroussi G. *Elliptic curves in cryptography*, volume 265. Cambridge university press, 1999.

[tR85] Schoof René. Elliptic curves over finite fields and the computation of square roots mod p. *Mathematics of computation*, 44(170) :483–494, 1985.

[tR06] Pomerance C. Crandall R. *Prime numbers : a computational perspective*, volume 182. Springer Science & Business Media, 2006.