Master 2 Algèbre Appliquées
Université Paris-Saclay
2016 - 2017

COMPTAGE DE POINTS DE COURBES ELLIPTIQUE SUR DES CORPS FINIS

par DANIEL RESENDE

le 15 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 ($O(\log^9 p)$).

Remarque. — Les éléments biographiques sont tirés de ..

SOMMAIRE

Introduction

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

Contexte historique

Courbes elliptiques sur $\mathbf{F}_p$

Soit $\mathbf{F}_p$ un corps fini à p éléments de caractéristiques $p \neq 2, 3$.

Soit E une courbe elliptique définie sur $\mathbf{F}_p$. On obtient l'équation affine de Weierstraß :

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

avec $a, b \in \mathbf{F}_p$ 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*

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

Algorithme de Schoof

Cas général

Algorithme 1 Algorithme de Shoof

Require: Une courbe elliptique E sur $\mathbf{F}_p$ 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 ;
    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.
```

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.

Quelques résultats mathématiques marquants

Une des réussites d'Euler a été la démonstration du grand théorème de Fermat dans un cas particulier [†].

[†] Fermat lui-même n'avait de démonstration que dans le cas $n = 4$.

THÉORÈME 3.I (de Fermat, cas $n = 3$). — *L'équation* $x^3 + y^3 + z^3 = 0$ *n'admet aucune solutions entières lorsque* $xyz \neq 0$.

Démonstration. On renvoie à [tR85] □

Le théorème 3.I est un résultat de théorie des nombres, mais Euler a touché à d'autres domaines. Citons par exemple ce résultat de topologie.

THÉORÈME 3.II. — *Il n'est pas possible de traverser tous les ponts de Könisberg en ne passant qu'une seule fois sur chaque pont.*

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.