Comptage de points sur les courbes elliptiques en petite caractéristique

B. Allombert

IMB
CNRS/Université Bordeaux 1

20/11/2012

Lignes directrices

Présentation du problème

Principe de l'algorithme de Satoh (d'après Vercauteren)

Présentation du problème

Soit E une courbe elliptique ordinaire définie sur un corps fini $\mathbb{F}_q$ ($q = p^n$) et donnée pour $(a, b) \in \mathbb{F}_q^2$ par

$$\begin{aligned} E_{a,b} : \quad & y^2 = x^3 + ax + b & p \geq 5 \\ E_{a,b} : \quad & y^2 = x^3 + ax^2 + b & p = 3 \\ E_{a,b} : \quad & y^2 + xy = x^3 + ax^2 + b & p = 2 \end{aligned}$$

On note $E_{a,b}(\mathbb{F}_q) = \{(x, y) \in \mathbb{F}_q^2 | E_{a,b}\} \cup \{\infty\}$
But : Un algorithme qui étant donné q, a et b détermine le cardinal $|E_{a,b}(\mathbb{F}_q)|$ en temps polynomial en $\log(q)$.

Endomorphisme de Frobenius φ

Le Frobenius $\varphi \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_q)$

$$\varphi \left| \begin{array}{ccc} \overline{\mathbb{F}}_p & \longrightarrow & \overline{\mathbb{F}}_p \\ x & \mapsto & x^q \end{array} \right.$$

détermine le Frobenius sur E :

$$\varphi_E \left| \begin{array}{ccc} E(\overline{\mathbb{F}}_p) & \longrightarrow & E(\overline{\mathbb{F}}_p) \\ (x,y) & \mapsto & (x^q, y^q) \end{array} \right.$$

Théorie de Galois : Soit $(x,y) \in E(\overline{\mathbb{F}}_p)$, alors $(x,y) \in E(\mathbb{F}_q)$ ssi $\varphi_E(x,y) = (x,y)$, i.e (x,y) est un point fixe du Frobenius.

Principe général

Formule du point fixe de Lefschetz appliquée au Frobenius φ.

$$|E(\mathbb{F}_q)| = 1 - \mathrm{Trace}(\varphi^* | H_1(E)) + q$$

où H_1 est défini par une théorie de cohomologie de Weil.

- Cohomologie ℓ-adique : Algorithmes de Schoof, SEA. complexité : $\tilde{O}(log(q)^4)$
- Cohomologie de Monsky–Washnitzer : Algorithme de Kedlaya, en $\tilde{O}(pn^3)$
- Cohomologie cristalline : Algorithme de Satoh en $\tilde{O}(p^2n^3)$, algorithme de Harley en $\tilde{O}(n^2)$ pour $p = 2$. But : un algorithme en $\tilde{O}(p^2n^2)$.

Endomorphisme de Frobenius σ

Le Frobenius $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$

$$\varphi \left| \begin{array}{ccc} \overline{\mathbb{F}}_p & \longrightarrow & \overline{\mathbb{F}}_p \\ x & \mapsto & x^p \end{array} \right.$$

détermine le Frobenius entre $E_{a,b}$ et $E_{\sigma(a),\sigma(b)}$:

$$\sigma_E \left| \begin{array}{ccc} E_{a,b}(\overline{\mathbb{F}}_p) & \longrightarrow & E_{\sigma(a),\sigma(b)}(\overline{\mathbb{F}}_p) \\ (x,y) & \mapsto & (x^p, y^p) \end{array} \right.$$

$$\varphi = \sigma^n$$

Σ permet de séparer la complexité en p et n.

Relèvement p-adique

Soit $\mathbb{Q}_q$ l'unique extension non-ramifiée de $\mathbb{Q}_p$ de degré n. Si $T \in \mathbb{Z}_p[X]$ est unitaire et irreductible modulo p, alors

$$\mathbb{Q}_q \cong \mathbb{Q}_p[X]/T(X)$$

$$\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) \cong \mathrm{Gal}(\mathbb{Q}_q/\mathbb{Q}_p)$$

Soit Σ l'image de σ par cet isomorphisme, alors

$$\Sigma(x) = x^p \pmod{p}$$

$$\Sigma^n = id$$

Résultats théoriques

- Deuring : Il existe un courbe $\tilde{E}$ sur $\mathbb{Q}_q$ qui se réduit sur E mod p et tel que Trace$\varphi_{\tilde{E}} =$ Traceφ_E.
- Hasse-Weil : $|\text{Trace}(\varphi_E)| \leq 2\sqrt{q}$
- Lubin-Serre-Tate : Soit j le j-invariant de E. Soit Φ_p le polynôme modulaire de niveau p. Le j-invariant de $\tilde{E}$ est l'unique $J \equiv j \pmod{p}$ tel que $\Phi_p(J, \Sigma(J)) = 0$, où Φ_p est le polynôme modulaire de niveau p.

Paramétrisation des courbes

Paramétrisation par le j-invariant (car. 0) : La courbe

$$E_j : y^2 = x^3 + 3gx + 2g$$

où $g = \frac{j}{j-1728}$ a pour j-invariant j.
On pose donc $\tilde{E} = E_J$ et on relève σ_E en $\sigma_{\tilde{E}}$:

$$\sigma_{\tilde{E}} \left| \begin{array}{ccc} E_J & \longrightarrow & E_{\Sigma(J)} \\ (x,y) & \mapsto & (\Sigma(x), \Sigma(y)) \end{array} \right.$$

Formule de Vélu

La formule de Vélu permet de calculer l'action de l'isogénie $\sigma_{\tilde{E}}$ sur la différentielle canonique ω.
Soit $\sigma^*_{\tilde{E}}(\omega) = c$, alors $\sigma^*_{\tilde{E}_{\Sigma^k}}(\omega) = \Sigma^k(c)$.

$$\tilde{E} \xrightarrow{\sigma_{\tilde{E}}} \tilde{E}_\Sigma \xrightarrow{\sigma_{\tilde{E}_\Sigma}} \tilde{E}_{\Sigma^2} \longrightarrow \ldots \longrightarrow \tilde{E}_{\Sigma^n} = \tilde{E}$$

$$\tilde{E} \xrightarrow{c} \tilde{E}_\Sigma \xrightarrow{\Sigma(c)} \longrightarrow \ldots \longrightarrow \tilde{E}_{\Sigma^n} = E$$

$$\tilde{E} \xrightarrow{c\Sigma(c)\ldots\Sigma^{n-1}(c)} \tilde{E}_{\Sigma^n} = \tilde{E}$$

$$\varphi^*_{\tilde{E}}(\omega) = c\Sigma(c)\ldots\Sigma^{n-1}(c) = \mathrm{Norm}_{\mathbb{Q}_q/\mathbb{Q}_p}(c)$$

Théorème : $\mathrm{Trace}(\varphi_E) = c + q/c$

Résumé de l'algorithme

1. Calcul de e tel que $p^e > 4\sqrt{(}q)$.
2. Calcul de j
3. Résolution de $\Phi_p(J, \Sigma(J))$ à la précision p^e.
4. Calcul de $c = \sigma^*_{\tilde{E}}(\omega) \pmod{p^e}$.
5. Calcul de $\mathrm{Norm}(c) \pmod{p^e}$.
6. Retour de $1 - t + q$ où $|t| \leq 2\sqrt{q}$ et $t \equiv \mathrm{Norm}(c) \pmod{p^e}$.

Difficultés

- On travaille dans $\mathbb{Z}[X]/(T, p^e)$ dont les objets sont de tailles $O(\log(p)n^2)$. Pour obtenir une complexité en $\tilde{O}(n^2)$, il faut faire seulement des opérations quasi-linéaires.
- Évaluer Σ en moins de $\tilde{O}(\sqrt{n})$ opérations semble impossible.
- Σ n'est pas $\mathbb{Q}_q$-dérivable.
- En pratique il est difficile de calculer la norme en temps quasi-linéaire.

Algorithme de Newton multivarié

Soit $F : \mathbb{Q}_p^n \longrightarrow \mathbb{Q}_p^n$ différentiable, et x tel que $F(x) = 0 \pmod{p^n}$.

- On veut trouver x_1 tel que $F(x_1) = 0 \pmod{p^{2n}}$.
- On pose $x_1 = x + p^n h$, alors $F(x_1) = F(x) + DF_x(p^n h) + O(p^{2n})$
- On résoud l'équation linéaire

$$DF_x(h) = F(x)p^{-n} \pmod{p^n}$$

Algorithme de Dixon

Soit D une application linéaire inversible mod p. On se donne un inverse mod p.

- On veut résoudre $D(A) = B \pmod{p^{2n}}$
- On écrit

$$A = A_0 + p^n A_1$$

$$D(A_0) + p^n D(A_1) = B \pmod{p^{2n}}$$

- On résoud

$$D(A_0) = B \pmod{p^n}$$

puis

$$D(A_1) = (B - D(A_0))p^{-n} \pmod{p^n}$$

en appelant récursivement l'algorithme.

Calcul de J

Nous voulons résoudre $\Phi_p(X, \Sigma(X)) = 0$ dans $\mathbb{Q}_q$ avec l'algorithme de Newton. Σ est différentiable sur $\mathbb{Q}_q$ vu comme $\mathbb{Q}_p$-espace vectoriel de dimension n.

$$\Phi_p(X, Y) \equiv (X^p - Y)(X - Y^p) \pmod{p}$$

$$D\Phi_{p(X,\Sigma(X))}(H) = H\frac{\partial \Phi_p}{\partial X}(X, \Sigma(X)) + \Sigma(H)\frac{\partial \Phi_p}{\partial Y}(X, \Sigma(X))$$

$$\frac{\partial \Phi_p}{\partial X}_{(X,\Sigma(X))} \equiv 0 \pmod{p}$$

$$\frac{\partial \Phi_p}{\partial Y}_{(X,\Sigma(X))} \equiv X^{p^2} - X \pmod{p}$$

$$D\Phi_{p(X,\Sigma(X))}(H) = \Sigma(H)(X^{p^2} - X) \pmod{p}$$

Inversible si $j \notin \mathbb{F}_{p^2}$.

Variante AGM

Mestre : si $p = 2$, la moyenne arithmético-géométrique appliquée au paramétrage

$$E : y^2 = x(x-1)(x-L^2)$$

permet de remplacer $\Phi_2 = X^3 + (-Y^2 + 1488\,Y - 162000) \times X^2 + (1488\,Y^2 + 40773375\,Y + 8748000000) \times X + (Y^3 - 162000\,Y^2 + 8748000000\,Y - 157464000000000)$ par l'équation plus simple

$$\Sigma(L) = \frac{1+L}{2\sqrt{L}}$$

i.e $P(L, \Sigma(L)) = 0$ avec

$$P(X, Y) = 4XY^2 - (1+X)^2$$

calcul de Σ pour $p = 2$

Harley(p=2) :

- Au lieu de relever $T(X)$ puis de calculer $\Sigma(X)$, On relève $T(X)$ tel que $\Sigma(X) = X^2 \pmod{2^e}$
- Cela revient à résoudre $T(X^2) = T(X)T(-X) \pmod{2^n}$
- Ou bien en posant $T = T_0(X^2) + XT_1(X^2)$ à résoudre $T - (T_0^2 - XT_1^2) = 0$
- La différentielle étant $D(H) \mapsto H - (2H_0T_0 - 2XT_1H_1)$ avec $H = H_0(X^2) + XH_1(X^2)$.
- $D(H) = H \pmod 2$ est inversible.
- On applique les algorithmes de Newton et Dixon.

Calcul de Σ pour $p > 2$

On veut relever $T(X)$ pour que $\Sigma(X) = X^p \pmod{p^e}$

- Soit ω une racine p-ième formelle. Il faut relever T de sorte que $T(X^p) = \prod_{i=0}^{p-1} T(\omega^i X)$
- Ce qui revient à $T(X) = \text{Norm}(T(Y) \pmod{Y^p - X})$
- on pose $F(T) = T(X) - \text{Norm}(T(Y) \pmod{Y^p - X})$
- $DF_T(H) = H(X) - \text{Trace}(NH(Y) \pmod{Y^p - X})$ avec $N = \prod_{i=1}^{p-1} T(\omega^i X)$

Calcul de la trace

Si

$$H = \sum_{i=0}^{p-1} H_i(X^p)X^i$$

et

$$N = \sum_{i=0}^{p-1} N_i(X^p)X^i$$

alors en utilisant l'orthogonalité des caractères,

$$\text{Trace}(NH) = pH_0(Y)N_0(Y) + pY\sum_{i=1}^{p-1} H_i(Y)N_{p-i}(Y)$$

Donc $DF_T(H) = H \pmod p$ est inversible

Calcul de $F(T)$ et de N

On pose

$$P_a(T) = \prod_{i=1}^{a} (T(\omega^i X))$$

La formule d'addition

$$P_(a+b)(T) = P_a(T)\,(P_b(T)(\omega^a X))$$

permet de calculer $N = P_{p-1}$ par "exponentiation binaire".
$F(T) = TN$
On applique encore les algorithmes de Newton et Dixon.

Calcul de $\Sigma(A \pmod T)$, $p > 2$

Par définition nous avons $\Sigma(A) = A(X^p) \pmod T$. Nous précalculons $X_k = X^{kn} \pmod T$ pour $k = 0$ à $p - 1$. Nous écrivons

$$A(X^p) = \sum_{k=0}^{p-1} A_i(X) X^{kn}$$

avec $\deg A_i < n$.

$$S = \sum_{k=0}^{p-1} A_i(X) X_k \pmod T$$

$\deg S < 2n$ et $\Sigma(A) = S \pmod T$. (environ deux fois plus rapide).

Calcul de la norme

On se ramène à $c \equiv 1 \pmod{p}$ en utilisant le morphisme de Teichmuller.
On utilise la formule de Dwork :

$$\mathrm{Norm}_{\mathbb{Q}_q/\mathbb{Q}_p}(c) = \exp(\mathrm{Trace}(\log(c)))$$

Calcul du logarithme

- On suppose $c \equiv 1 \pmod{p}$.
- On choisit $k = [n^{\frac{1}{3}}]$
- On calcule $c^{p^k} \pmod{p^{e+k}}$.
- Nous avons $c^{p^k} = 1 \pmod{p^{k+1}}$
- On calcule b tel que $\frac{1+b}{1-b} = c^{p^k}$ de sorte que $\log(c^{p^k}) = 2\text{atanh}(b) \pmod{p^{e+k}}$.
- On a $v_p(b) \geq k$
- On retourne $2\text{atanh}(b)p^{-k} \pmod{e}$.

Calcul de l'arctangente hyperbolique

- On calcule

$$\operatorname{atanh}(b) = \sum_{i=1}^{\frac{e+k}{2k}} \frac{b^{2i+1}}{2i+1} \pmod{p^{e+k}}$$

  par l'algorithme de Brent&Kung (Pas de bébé-Pas de géant).
- $O(n^{\frac{1}{3}})$ multiplications mais $O(n^{\frac{2}{3}})$ additions.
- en prenant $k = \frac{1}{2}$, on obtient $O(n^{\frac{1}{2}})$ multiplications et additions, plus lent en pratique.