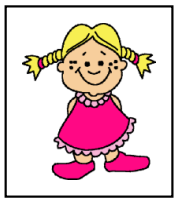
Un algorithme à la Kedlaya pour compter les points de revêtements cycliques de la droite projective

Cécile GONÇALVES

Équipe GRACE
Inria Saclay
LIX - Laboratoire d'Informatique de l'École Polytechnique
Sous la direction de Benjamin Smith et François Morain

Mercredi 10 Octobre 2012

Publics : un groupe G d'ordre n et g un générateur de G.
Par exemple G est l'ensemble des entiers modulo p.



Alice choisit un entier a au hasard

Bob choisit un entier b au hasard

Alice calcule $A = g^a$

Bob calcule $B = g^b$

Alice reçoit B

Bob reçoit A

Alice calcule $B^a = g^{ba}$

Bob calcule $A^b = g^{ab}$

Leur clé secrète est $K = g^{ab}$

Publics : un groupe G d'ordre n et g un générateur de G.
Par exemple G est l'ensemble des entiers modulo p.

La sécurité du protocole repose sur le problème suivant :

Problème de Diffie-Hellman calculatoire (CDHP)

Étants donnés G, g, g^a et g^b, construire g^{ab}.

Maurer et Wolf : CDHP équivalent au problème suivant :

Problème du logarithme discret (DLP)

Étant donnés G, g et h, trouver un entier x tel que $h = g^x$.

On cherche G tel que DLP(G) est difficile à résoudre.

Définition : courbe hyperelliptique de genre g

Une courbe hyperelliptique $\mathcal{C}$ de genre g est une équation de la forme :

$$\mathcal{C} : y^2 + h(x)y = f(x), \text{ définie sur } \mathbb{F}_q$$

avec h et f deux polynômes et $deg(f) = d = 2g + 1$ ou $2g + 2$ et $deg(h) \leqslant g$.

Les courbes fournissent de bons candidats de groupes car :

- Elles ont un groupe G que l'on note $J(\mathcal{C})$ qui leur est associé, avec $\#J(\mathcal{C}) \sim O(q^g)$.
- On dispose d'une arithmétique efficace.
- Pas de meilleure attaque connue que les attaques génériques pour $g = 1$ ou 2 .

La difficulté à résoudre le DLP repose sur le choix du groupe G, notamment sur son cardinal :

Conséquence de la réduction de Pohlig-Hellman

Résoudre le DLP dans un groupe de taille n est aussi difficile que de le résoudre dans un groupe de taille p, où p est le plus grand facteur premier de n.

Pour calculer la taille de $J(\mathcal{C})$, on compte les points sur la courbe.

Définition : Fonction zêta d'une courbe

Soit $\mathcal{C}$ une courbe définie sur $\mathbb{F}_q$, où $q = p^n$.

$$Z(\mathcal{C}/\mathbb{F}_q; t) = \exp\left(\sum_{n\geq 1} N_k \frac{t^k}{k}\right) \text{ , où } N_k = \#\mathcal{C}(\mathbb{F}_{q^k})$$

Théorème de Weil

$$Z(\mathcal{C}/\mathbb{F}_q; t) = \frac{L(t)}{(1-qt)(1-t)},$$

avec :

- $L(t) = 1 + a_1 t + \ldots + a_{g-1} t^{g-1} + a_g t^g + q a_{g-1} t^{g+1} + \ldots + q^{g-1} a_1 t^{2g-1} + q^g t^{2g}$
- $|a_i| \leq \binom{2g}{i} q^{i/2}$
- g éléments $N_k \Leftrightarrow L \Leftrightarrow$ Zêta

$$\boxed{\#J(\mathcal{C}) = L(1)}$$

Exemple :

$$y^2 = x^3 + x + 1, \text{ sur } \mathbb{F}_q, \text{ avec } q = 2^{160} + 7.$$

Comptage naïf :

$x = 0, y^2 = 1$: donne deux solutions : $(0, -1)$ et $(0, 1)$.

$\vdots$

$x = 3, y^2 = 31$: ne donne pas de solution.

$\vdots$

$x = 2^{160} + 6, y^2 = -1$: ne donne pas de solution.

Le nombre de points sur la courbe est :

$$N = 3^2 \times 13 \times 1249146698573421297609986216263988125818008660 9.$$

Cette méthode d'énumération prend beaucoup de temps... $(O(q))$.

On peut faire mieux...

$\mathcal{C}$ définie sur $\mathbb{F}_q$ de caractéristique p.

Frobenius arithmétique d'ordre p :

$$\sigma : \begin{cases} \overline{\mathbb{F}}_q \longrightarrow \overline{\mathbb{F}}_q \\ x \longmapsto x^p \end{cases} \qquad \mathrm{Fix}(\sigma^k) = \mathbb{F}_{p^k}, \text{ pour } k \in \mathbb{N}^*.$$

$\mathcal{C}$ définie sur $\mathbb{F}_q$ de caractéristique p.

Frobenius arithmétique d'ordre p :

$$\sigma : \begin{cases} \overline{\mathbb{F}}_q \longrightarrow \overline{\mathbb{F}}_q \\ x \longmapsto x^p \end{cases} \qquad \mathrm{Fix}(\sigma^k) = \mathbb{F}_{p^k}, \text{ pour } k \in \mathbb{N}^*.$$

Définition étendue à $\mathcal{C}$: Frobenius géométrique d'ordre p :

$$\varphi : \begin{cases} \mathcal{C} \longrightarrow \mathcal{C} \\ P = (x, y) \longmapsto (x^p, y^p) \end{cases} \qquad \mathrm{Fix}(\varphi^k) = \mathcal{C}(\mathbb{F}_{p^k}), \text{ pour } k \in \mathbb{N}^*.$$

s'étend en un endomorphisme de $J(\mathcal{C})$.

$\mathcal{C}$ définie sur $\mathbb{F}_q$ de caractéristique p.

Frobenius arithmétique d'ordre p :

$$\sigma : \begin{cases} \overline{\mathbb{F}}_q \longrightarrow \overline{\mathbb{F}}_q \\ x \longmapsto x^p \end{cases} \qquad \mathrm{Fix}(\sigma^k) = \mathbb{F}_{p^k}, \text{ pour } k \in \mathbb{N}^*.$$

Définition étendue à $\mathcal{C}$: Frobenius géométrique d'ordre p :

$$\varphi : \begin{cases} \mathcal{C} \longrightarrow \mathcal{C} \\ P = (x, y) \longmapsto (x^p, y^p) \end{cases} \qquad \mathrm{Fix}(\varphi^k) = \mathcal{C}(\mathbb{F}_{p^k}), \text{ pour } k \in \mathbb{N}^*.$$

s'étend en un endomorphisme de $J(\mathcal{C})$.

Proposition

Le polynôme L est le polynôme réciproque du polynôme caractéristique du Frobenius agissant sur $J(\mathcal{C})$:
Si

$$P(t) = \chi_\varphi(t) = a_0 + a_1 t + \ldots + a_{2g} t^{2g},$$

alors

$$L(t) = a_{2g} + a_{2g-1} t + \ldots + a_1 t^{2g-1} + a_0 t^{2g}$$

But : créer des algorithmes :

- praticables, c'est à dire que l'on peut faire tourner en temps raisonnable.
- les plus rapides possibles.
- avec une implémentation robuste.

Algorithmes :

- à la Schoof (1985)
- à la Satoh (1999)
- à la Kedlaya et méthodes de déformation (2001)

Si l'on veut compter les points d'une telle courbe,

$$y^2 + h(x)y = f(x), \text{ définie sur } \mathbb{F}_q \text{ , avec } q = p^n \text{ et } f \text{ de degré } d.$$

on utilisera l'algorithme le mieux adapté selon le tableau suivant :

Dépendance en :	Schoof	Satoh	Kedlaya
$\log(p)$	polynomial	exponentiel (gros)	exponentiel (petit)
n	polynomial (gros)	polynomial (petit)	polynomial
d	exponentiel	exponentiel	polynomial

Entrée : courbe superelliptique $\mathcal{C} : y^r = f(x)$ définie sur $\mathbb{F}_{p^n}$, $p \nmid r$ et f un polynôme de degré d premier à r.

$$\mathcal{C} \text{ de genre } \quad g = \frac{(r-1)(d-1)}{2}.$$

Sortie : polynôme de Weil : $P(t) = t^{2g} + a_1 t^{2g-1} + \ldots$, avec $|a_i| \leq \binom{2g}{i} p^{ni/2}$.

Complexité : $\widetilde{O}(pn^3 d^4)$.

Entrée : courbe superelliptique $\mathcal{C} : y^r = f(x)$ définie sur $\mathbb{F}_{p^n}$, $p \nmid r$ et f un polynôme de degré d premier à r.

$$\mathcal{C} \text{ de genre } \quad g = \frac{(r-1)(d-1)}{2}.$$

Sortie : polynôme de Weil : $P(t) = t^{2g} + a_1 t^{2g-1} + \ldots$, avec $|a_i| \leq \binom{2g}{i} p^{ni/2}$.
Complexité : $\widetilde{O}(pn^3 d^4)$.

0. Estimer la précision p-adique requise.

Entrée : courbe superelliptique $\mathcal{C} : y^r = f(x)$ définie sur $\mathbb{F}_{p^n}$, $p \nmid r$ et f un polynôme de degré d premier à r.

$$\mathcal{C} \text{ de genre } \quad g = \frac{(r-1)(d-1)}{2}.$$

Sortie : polynôme de Weil : $P(t) = t^{2g} + a_1 t^{2g-1} + \ldots$, avec $|a_i| \leq \binom{2g}{i} p^{ni/2}$.
Complexité : $\widetilde{O}(pn^3 d^4)$.

0. Estimer la précision p-adique requise.
1. Choisir un relèvement de $\mathcal{C}$ à $\mathbb{Z}_{p^n}$.
2. Choisir une base de l'espace des formes différentielles (de $H^1_{MW}(\mathcal{C}, \mathbb{Q}_p)$).

Entrée : courbe superelliptique $\mathcal{C} : y^r = f(x)$ définie sur $\mathbb{F}_{p^n}$, $p \nmid r$ et f un polynôme de degré d premier à r.

$$\mathcal{C} \text{ de genre } \quad g = \frac{(r-1)(d-1)}{2}.$$

Sortie : polynôme de Weil : $P(t) = t^{2g} + a_1 t^{2g-1} + \ldots$, avec $|a_i| \leq \binom{2g}{i} p^{ni/2}$.
Complexité : $\widetilde{O}(pn^3 d^4)$.

0. Estimer la précision p-adique requise.
1. Choisir un relèvement de $\mathcal{C}$ à $\mathbb{Z}_{p^n}$.
2. Choisir une base de l'espace des formes différentielles (de $H^1_{MW}(\mathcal{C}, \mathbb{Q}_p)$).
3. Calculer la matrice M' de l'action du Frobenius dans $H^1_{MW}(\mathcal{C}, \mathbb{Q}_p)$:
   - Relever le Frobenius d'ordre p dans $H^1_{MW}(\mathcal{C}, \mathbb{Q}_p)$.
   - Calculer l'action du Frobenius d'ordre p sur les formes différentielles.

Entrée : courbe superelliptique $\mathcal{C} : y^r = f(x)$ définie sur $\mathbb{F}_{p^n}$, $p \nmid r$ et f un polynôme de degré d premier à r.

$$\mathcal{C} \text{ de genre } \quad g = \frac{(r-1)(d-1)}{2}.$$

Sortie : polynôme de Weil : $P(t) = t^{2g} + a_1 t^{2g-1} + \ldots$, avec $|a_i| \leq \binom{2g}{i} p^{ni/2}$.
Complexité : $\widetilde{O}(pn^3 d^4)$.

0. Estimer la précision p-adique requise.
1. Choisir un relèvement de $\mathcal{C}$ à $\mathbb{Z}_{p^n}$.
2. Choisir une base de l'espace des formes différentielles (de $H^1_{MW}(\mathcal{C}, \mathbb{Q}_p)$).
3. Calculer la matrice M' de l'action du Frobenius dans $H^1_{MW}(\mathcal{C}, \mathbb{Q}_p)$:
   - Relever le Frobenius d'ordre p dans $H^1_{MW}(\mathcal{C}, \mathbb{Q}_p)$.
   - Calculer l'action du Frobenius d'ordre p sur les formes différentielles.
   - Obtenir la matrice M du Frobenius d'ordre p en appliquant une réduction.

Entrée : courbe superelliptique $\mathcal{C} : y^r = f(x)$ définie sur $\mathbb{F}_{p^n}$, $p \nmid r$ et f un polynôme de degré d premier à r.

$$\mathcal{C} \text{ de genre } \quad g = \frac{(r-1)(d-1)}{2}.$$

Sortie : polynôme de Weil : $P(t) = t^{2g} + a_1 t^{2g-1} + \ldots$, avec $|a_i| \leq \binom{2g}{i} p^{ni/2}$.
Complexité : $\widetilde{O}(pn^3 d^4)$.

0. Estimer la précision p-adique requise.
1. Choisir un relèvement de $\mathcal{C}$ à $\mathbb{Z}_{p^n}$.
2. Choisir une base de l'espace des formes différentielles (de $H^1_{MW}(\mathcal{C}, \mathbb{Q}_p)$).
3. Calculer la matrice M' de l'action du Frobenius dans $H^1_{MW}(\mathcal{C}, \mathbb{Q}_p)$:
   - Relever le Frobenius d'ordre p dans $H^1_{MW}(\mathcal{C}, \mathbb{Q}_p)$.
   - Calculer l'action du Frobenius d'ordre p sur les formes différentielles.
   - Obtenir la matrice M du Frobenius d'ordre p en appliquant une réduction.
   - Calculer la matrice $M' = M.M^{\sigma} \ldots M^{\sigma^{n-1}}$.
4. Calculer le polynôme caractéristique P de M'.
5. Renvoyer P.

La taille de $J(\mathcal{C})$ est alors $P(1)$.

Soit p un nombre premier et $q = p^n$.

Définition : L'anneau des entiers p-adiques $\mathbb{Z}_p$

Un entier p-adique x est une série formelle

$$x = \sum_{k \geqslant 0} x_k p^k, \text{ avec } 0 \leqslant x_k \leqslant p-1$$

Il est muni d'une valuation : $v_p(x) = min\{k \in \mathbb{N} \mid x_k \neq 0\}$.

Exemple :
Dans $\mathbb{Z}_5$, $x = -\frac{5}{4} = 5 + 5^2 + \ldots = \sum_{k \geqslant 1} 5^k$ et $v_5(x) = 1$.

Remarque :
$\mathbb{Z}_p$ est naturellement muni de la projection

$$\pi : \left\{ \begin{array}{ccc} \mathbb{Z}_p & \longrightarrow & \mathbb{F}_p \\ x & \longmapsto & x_0 \end{array} \right.$$

Définition : Le corps des p-adiques $\mathbb{Q}_p$

Le corps des fractions de $\mathbb{Z}_p$ est noté $\mathbb{Q}_p$. Ses éléments sont de la forme :

$$x = \sum_{k \geqslant \alpha} x_k p^k, \text{ avec } x_k \in \mathbb{Z}/p\mathbb{Z} \text{ et } \alpha \in \mathbb{Z}$$

Proposition - Définition : Extension non ramifiée de $\mathbb{Q}_p$.

Soit $f \in \mathbb{Z}_p[x]$ un polynôme de degré n tel que $\pi(f)$ est irréductible de degré n. L'anneau

$$\mathbb{Z}_q = \mathbb{Z}_p[x]/\langle f(x) \rangle$$

est un $\mathbb{Z}_p$-module de rang n.

Son corps des fractions, noté $\mathbb{Q}_q$, est une extension non ramifiée de degré n de $\mathbb{Q}_p$.

Exemple : $\mathbb{Q}_4 \cong \mathbb{Q}_2[t]/\langle t^2 + t + 1 \rangle$.

Remarque :
En pratique, les p-adiques sont tronqués à précision fixée N.

Pour relever $\mathcal{C}$, on relève son équation de la manière suivante :

Définition : Relèvement à $\mathbb{Z}_q$

On dit que $\overline{f} \in \mathbb{Z}_q[x]$ est un relèvement de $f \in \mathbb{F}_q[x]$ si $\pi(\overline{f}) = f$, c'est à dire si $\overline{f} \equiv f \bmod p$.

Exemple :

Si

$$\mathcal{C} : y^3 = x^4 + \omega x^3 + \omega^2 x + 1 \quad \text{sur } \mathbb{F}_4 = \mathbb{F}_2[\omega]$$

alors

$$\overline{\mathcal{C}} : y^3 = x^4 + (\omega - 2 + O(2^5))x^3 + (3\omega^2 - 2 + 2^4 + O(2^5))x + (1 + O(2^5))$$

est un relèvement de $\mathcal{C}$ à $\mathbb{Z}_4$, dont les éléments sont tronqués à précision 5.

Remarque : On travaille avec la courbe $\widetilde{\mathcal{C}} = \overline{\mathcal{C}} \setminus \{\text{zéros de } y\}$.

Base de formes différentielles :

$$B = \left\{ x^i \frac{dx}{y^j} \mid i \in [0, \ldots, d-2], j \in [1, \ldots, r-1] \right\}.$$

Action de $\mathcal{F}$ sur l'anneau des coordonnées :

$$\begin{aligned}
\mathcal{F}(x) &= x^p \\
\mathcal{F}(y) &= y^p \left(1 + \left(\mathcal{F}\left(f(x)\right) - f(x)^p\right)\tau^p\right)^{\frac{1}{r}}, \text{ où } \tau = y^{-r}. \\
&= y^p \sum_{i=0}^{\mu} \binom{1/r}{i} \left(\mathcal{F}\left(f(x)\right) - f(x)^p\right)^i \tau^{pi} + O(p^N)
\end{aligned}$$

Base de formes différentielles :

$$B = \left\{ x^i \frac{dx}{y^j} \mid i \in [0, \ldots, d-2], j \in [1, \ldots, r-1] \right\}.$$

Action de $\mathcal{F}$ sur l'anneau des coordonnées :

$$\begin{aligned}
\mathcal{F}(x) &= x^p \\
\mathcal{F}(y) &= y^p \left(1 + \left(\mathcal{F}\left(f(x)\right) - f(x)^p\right)\tau^p\right)^{\frac{1}{r}}, \text{ où } \tau = y^{-r}. \\
&= y^p \sum_{i=0}^{\mu} \binom{1/r}{i} \left(\mathcal{F}\left(f(x)\right) - f(x)^p\right)^i \tau^{pi} + O(p^N)
\end{aligned}$$

Action de $\mathcal{F}$ sur les différentielles : $\mathcal{F}(dx) = d\left(\mathcal{F}(x)\right) = px^{p-1}dx$.

$$\begin{aligned}
\mathcal{F}\left(x^i \tfrac{dx}{y^j}\right) &= px^{p(i+1)-1} \tfrac{dx}{\mathcal{F}(y)^j} \\
&= px^{p(i+1)-1} y^{-jp} \textstyle\sum_{i \geqslant 0} \binom{-j/r}{i} \left(\mathcal{F}(f(x)) - f(x)^p\right)^i \tau^{pi} dx \\
&= px^{p(i+1)-1} y^{-a} \left(\textstyle\sum_{i \geqslant 0} \binom{-j/r}{i} \left(\mathcal{F}(f(x)) - f(x)^p\right)^i \tau^{pi}\right) \tfrac{dx}{y^\ell} \\
&= \textstyle\sum_{i=0}^{\mu} R_k \tau^k \tfrac{dx}{y^\ell} + O(p^N), \text{ avec } a \text{ et } \ell \text{ tels que } jp = ar + \ell.
\end{aligned}$$

But : Exprimer $\omega = \sum_{0 \leqslant k \leqslant \mu} R_k(x)\tau^k \frac{dx}{y^\ell}$ en fonction des vecteurs de B.

Les df sont nulles dans $H^1_{MW}(\mathcal{C}, \mathbb{Q}_p)$.

$\longrightarrow$ Soustraire des formes différentielles de cette forme.

But : Exprimer $\omega = \sum_{0 \leqslant k \leqslant \mu} R_k(x)\tau^k \frac{dx}{y^\ell}$ en fonction des vecteurs de B.

Les df sont nulles dans $H^1_{MW}(\mathcal{C}, \mathbb{Q}_p)$.

$\longrightarrow$ Soustraire des formes différentielles de cette forme.

Entrée : $\omega = \left(\sum_{0 \leqslant k \leqslant M} R_k(x)\tau^k\right) \frac{dx}{y^\ell}$

Sortie : $\omega' = T(x)\frac{dx}{y^\ell}$, avec $deg(T) \leqslant d-2$ et ω' équivalente à ω.

But : Exprimer $\omega = \sum_{0 \leqslant k \leqslant \mu} R_k(x)\tau^k \frac{dx}{y^\ell}$ en fonction des vecteurs de B.

Les df sont nulles dans $H^1_{MW}(\mathcal{C}, \mathbb{Q}_p)$.

$\longrightarrow$ Soustraire des formes différentielles de cette forme.

Entrée : $\omega = \left(\sum_{0 \leqslant k \leqslant M} R_k(x)\tau^k\right) \frac{dx}{y^\ell}$

Sortie : $\omega' = T(x)\frac{dx}{y^\ell}$, avec $deg(T) \leqslant d-2$ et ω' équivalente à ω.

1. Faire baisser le degré en τ de ω pour obtenir $S(x)\frac{dx}{y^\ell}$:
   Utiliser autant de fois que nécessaire la relation :

$$\boxed{R\tau^k \frac{dx}{y^\ell} = \left(A + \frac{r}{r(k-1)+\ell} B'\right)\tau^{k-1}\frac{dx}{y^\ell} \text{ si } R = A\overline{f} + B\overline{f}'}$$

But : Exprimer $\omega = \sum_{0 \leqslant k \leqslant \mu} R_k(x)\tau^k \frac{dx}{y^\ell}$ en fonction des vecteurs de B.

Les df sont nulles dans $H^1_{MW}(\mathcal{C}, \mathbb{Q}_p)$.

$\longrightarrow$ Soustraire des formes différentielles de cette forme.

Entrée : $\omega = \left(\sum_{0 \leqslant k \leqslant M} R_k(x)\tau^k\right) \frac{dx}{y^\ell}$

Sortie : $\omega' = T(x)\frac{dx}{y^\ell}$, avec $deg(T) \leqslant d-2$ et ω' équivalente à ω.

1. Faire baisser le degré en τ de ω pour obtenir $S(x)\frac{dx}{y^\ell}$:
   Utiliser autant de fois que nécessaire la relation :

$$\boxed{R\tau^k \frac{dx}{y^\ell} = \left(A + \frac{r}{r(k-1)+\ell} B'\right)\tau^{k-1}\frac{dx}{y^\ell} \text{ si } R = A\overline{f} + B\overline{f}'}$$

2. Faire baisser le degré de S jusqu'à ce qu'il soit inférieur ou égal à $d-2$.
   Utiliser autant de fois que nécessaire la relation :

$$\boxed{\left(r(\delta - d + 1)x^{\delta+d}\overline{f} + (r-\ell)x^{\delta-d+1}\overline{f}'\right)\frac{dx}{y^\ell} \equiv 0}$$

Ce qui précède nous fournit la matrice :

$$M = \mathrm{Mat}_{\boldsymbol{B}}(\mathcal{F})$$

du Frobenius d'ordre p, à coefficients dans $\mathbb{Q}_{\boldsymbol{q}}$.

On retrouve la matrice du Frobenius d'ordre q grâce à la relation :

$$\mathrm{Mat}_{\boldsymbol{B}}(\mathcal{F}^{\boldsymbol{n}}) = M.M^{\sigma} \ldots M^{\sigma^{\boldsymbol{n-1}}}$$

où $M_{i,j}^{\sigma} = \sigma\left(M_{i,j}\right)$.

Le polynôme caractéristique de cette dernière matrice nous fournit le polynôme réciproque du numérateur de la fonction Zêta.

But : Bien estimer la précision p-adique N.

Lemme [G.] : Perte de précision dans l'algorithme de réduction

- Étape 1 : Passage de $R\tau^k \frac{dx}{y^\ell}$ à $S\frac{dx}{y^\ell}$: perte d'au plus $\lfloor \log_p(r(k-1)+\ell) \rfloor$
- Étape 2 : Passage de $S\frac{dx}{y^\ell}$ à $T\frac{dx}{y^\ell}$, avec $\deg(T) < d-1$: perte d'au plus $\lfloor \log_p(r(m+1)-\ell d) \rfloor$.

Théorème [G.] :

Pour tenir compte des pertes de précision, on utilise des p-adiques tronqués à précision N telle que :

$$N = \min_{n\in\mathbb{N}} \left\{ n - \lfloor \log_p(p(rn-1)-r) \rfloor \geqslant N_0 + \lfloor \log_p(dp(r-1)+r) \rfloor \right\}.$$

où

$$N_0 = \left\lceil \log_p\left(2\binom{2g}{g} q^{g/2}\right) \right\rceil.$$

Entrée : courbe $\mathcal{C} : y^r = f(x)$ définie sur $\mathbb{F}_q$, avec $q = p^n$, $p \nmid r$ et f un polynôme de degré d **quelconque**.

$$\mathcal{C} \text{ de genre } \quad g = \frac{(r-1)(d-1)}{2} - \frac{\text{pgcd}(r,d)-1}{2}.$$

Sortie : polynôme de Weil : $P(t) = t^{2g} + a_1 t^{2g-1} + \ldots$, avec $|a_i| \leq \binom{2g}{i} p^{ni/2}$.
Complexité : $\widetilde{O}(pn^3 d^4)$.

Entrée : courbe $\mathcal{C} : y^r = f(x)$ définie sur $\mathbb{F}_q$, avec $q = p^n$, $p \nmid r$ et f un polynôme de degré d **quelconque**.

$$\mathcal{C} \text{ de genre } \quad g = \frac{(r-1)(d-1)}{2} - \frac{\text{pgcd}(r,d)-1}{2}.$$

Sortie : polynôme de Weil : $P(t) = t^{2g} + a_1 t^{2g-1} + \ldots$, avec $|a_i| \leq \binom{2g}{i} p^{ni/2}$.
Complexité : $\widetilde{O}(pn^3 d^4)$.

On voudrait procéder comme dans le cas superelliptique.

Entrée : courbe $\mathcal{C} : y^r = f(x)$ définie sur $\mathbb{F}_q$, avec $q = p^n$, $p \nmid r$ et f un polynôme de degré d **quelconque**.

$$\mathcal{C} \text{ de genre } \quad g = \frac{(r-1)(d-1)}{2} - \frac{\text{pgcd}(r,d)-1}{2}.$$

Sortie : polynôme de Weil : $P(t) = t^{2g} + a_1 t^{2g-1} + \ldots$, avec $|a_i| \leq \binom{2g}{i} p^{ni/2}$.
Complexité : $\widetilde{O}(pn^3 d^4)$.

On voudrait procéder comme dans le cas superelliptique.

Proposition :

La courbe $\mathcal{C}$ a $\text{pgcd}(r,d)$ points à l'infini qui ont une contribution dans l'espace des formes différentielles.

Entrée : courbe $\mathcal{C} : y^r = f(x)$ définie sur $\mathbb{F}_q$, avec $q = p^n$, $p \nmid r$ et f un polynôme de degré d **quelconque**.

$$\mathcal{C} \text{ de genre } \quad g = \frac{(r-1)(d-1)}{2} - \frac{\text{pgcd}(r,d)-1}{2}.$$

Sortie : polynôme de Weil : $P(t) = t^{2g} + a_1 t^{2g-1} + \ldots$, avec $|a_i| \leq \binom{2g}{i} p^{ni/2}$.
Complexité : $\widetilde{O}(pn^3 d^4)$.

On voudrait procéder comme dans le cas superelliptique.

Proposition :

La courbe $\mathcal{C}$ a $\text{pgcd}(r,d)$ points à l'infini qui ont une contribution dans l'espace des formes différentielles.

Conséquence : En procédant de la même manière que Gaudry et Gürel, le polynôme ainsi calculé a un facteur qu'il faut retirer :

$$\chi_{\mathcal{F}^n}(t) = P(t)U(t).$$

Théorème : Lien entre les Frobenius arithmétique et géométrique

Dans l'espace $H^1_{MW}(\mathcal{C}, \mathbb{Q}_p)$,

$$\mathcal{F}^n = q\left(\Sigma^{n*}\right)^{-1}.$$

Théorème : Lien entre les Frobenius arithmétique et géométrique

Dans l'espace $H^1_{MW}(\mathcal{C}, \mathbb{Q}_p)$,

$$\mathcal{F}^n = q\left(\Sigma^{n*}\right)^{-1}.$$

La matrice du Frobenius agissant sur les points à l'infini de $\mathcal{C}$ est de la forme

$$\begin{bmatrix} 1 & 0 \\ 0 & \widetilde{M} \end{bmatrix}.$$

Théorème : Lien entre les Frobenius arithmétique et géométrique

Dans l'espace $H^1_{MW}(\mathcal{C}, \mathbb{Q}_p)$,

$$\mathcal{F}^n = q\left(\Sigma^{n*}\right)^{-1}.$$

La matrice du Frobenius agissant sur les points à l'infini de $\mathcal{C}$ est de la forme

$$\begin{bmatrix} 1 & 0 \\ 0 & \widetilde{M} \end{bmatrix}.$$

Théorème [G.] :

Le polynôme P que l'on cherche à calculer est :

$$P(t) = \frac{\chi_{\Sigma^n}(t)}{\chi_{q\widetilde{M}^{-1}}(t)}$$

où $\chi_{\Sigma^n}(t)$ a été calculé en procédant de la même manière que Gaudry et Gürel.

Courbe aléatoire de genre 4 définie sur $\mathbb{F}_{5^3} = \mathbb{F}_5[t]/\langle t^3 + 3t + 3\rangle$:

$$y^3 = x^6 + t^{55}x^5 + t^{23}x^4 + t^{10}x^3 + t^{18}x^2 + t^{65}x + 2.$$

Courbe aléatoire de genre 4 définie sur $\mathbb{F}_{5^3} = \mathbb{F}_5[t]/\langle t^3 + 3t + 3\rangle$:

$$y^3 = x^6 + t^{55}x^5 + t^{23}x^4 + t^{10}x^3 + t^{18}x^2 + t^{65}x + 2.$$

$$L(T) = 5^{12}T^8 + 5^9 a_1 T^7 + 5^6 a_2 T^6 + 5^3 a_3 T^5 + a_4 T^4 + a_3 T^3 + a_2 T^2 + a_1 T + 1$$

où

$$a_1 = 0, \quad a_2 = 104, \quad a_3 = 0 \quad \text{et } a_4 = -5250.$$

Courbe aléatoire de genre 4 définie sur $\mathbb{F}_{5^3} = \mathbb{F}_5[t]/\langle t^3 + 3t + 3\rangle$:

$$y^3 = x^6 + t^{55}x^5 + t^{23}x^4 + t^{10}x^3 + t^{18}x^2 + t^{65}x + 2.$$

$$L(T) = 5^{12}T^8 + 5^9 a_1 T^7 + 5^6 a_2 T^6 + 5^3 a_3 T^5 + a_4 T^4 + a_3 T^3 + a_2 T^2 + a_1 T + 1$$

où

$$a_1 = 0, \quad a_2 = 104, \quad a_3 = 0 \quad \text{et } a_4 = -5250.$$

Primitive MAGMA : 42 minutes.

Courbe aléatoire de genre 4 définie sur $\mathbb{F}_{5^3} = \mathbb{F}_5[t]/\langle t^3 + 3t + 3\rangle$:

$$y^3 = x^6 + t^{55}x^5 + t^{23}x^4 + t^{10}x^3 + t^{18}x^2 + t^{65}x + 2.$$

$$L(T) = 5^{12}T^8 + 5^9 a_1 T^7 + 5^6 a_2 T^6 + 5^3 a_3 T^5 + a_4 T^4 + a_3 T^3 + a_2 T^2 + a_1 T + 1$$

où

$$a_1 = 0, \quad a_2 = 104, \quad a_3 = 0 \quad \text{et } a_4 = -5250.$$

Primitive MAGMA : 42 minutes.

Notre algorithme en Magma : 18 secondes.

Théorème [G.]

En utilisant la base B dans les algorithmes précédents,

- si $p \geqslant 2g$, la matrice du Frobenius est à coefficients dans $\mathbb{Z}_q$.
- si $p < 2g$, la matrice du Frobenius a des coefficients dans $\mathbb{Q}_q$ dont les dénominateurs sont bornés par $\lfloor \log_p(2g-1) \rfloor$.

- Lorsqu'on la matrice M a des coefficients dans $\mathbb{Q}_q \backslash \mathbb{Z}_q$: perte de contrôle de la précision.

  $\Rightarrow$ On souhaiterait que les coefficients soient dans $\mathbb{Z}_q$.

Théorème [G.]

En utilisant la base B dans les algorithmes précédents,

- si $p \geqslant 2g$, la matrice du Frobenius est à coefficients dans $\mathbb{Z}_q$.
- si $p < 2g$, la matrice du Frobenius a des coefficients dans $\mathbb{Q}_q$ dont les dénominateurs sont bornés par $\lfloor \log_p(2g-1) \rfloor$.

- Lorsqu'on la matrice M a des coefficients dans $\mathbb{Q}_q \backslash \mathbb{Z}_q$: perte de contrôle de la précision.
  $\Rightarrow$ On souhaiterait que les coefficients soient dans $\mathbb{Z}_q$.

En suivant l'approche de Harrison pour les courbes hyperelliptiques :
Utiliser

$$B' = \left\{ x^i \frac{dx}{y^{r+j}} \mid i \in [0, \ldots, d-2], j \in [1, \ldots, r-1] \right\}.$$

Conjecture [G.]

En utilisant la base B', les coefficients de M sont toujours entiers.

Conséquences :
On peut affiner les bornes de précision.

Dans notre algorithme :

Théorème [G.]

Dans l'espace $H^1_{MW}(\mathcal{C}, \mathbb{Q}_p)$, en utilisant la base B',

$$\mathcal{F}^n = (\Sigma^{n*})^{-1}.$$

Le polynôme P que l'on cherche à calculer est :

$$P(t) = \frac{\chi_{\Sigma^n}(t)}{\chi_{\widetilde{M}^{-1}}(t)}$$

où $\chi_{\Sigma^n}(t)$ a été calculé en procédant de la même manière que Gaudry et Gürel.

Exploitation d'endomorphismes spécifiques explicites (pour tous les algorithmes à la Kedlaya) :

- Multiplication réelle
- Automorphismes cycliques

Algorithme de Vercauteren :

- Recherche d'une base mieux adaptée.

Algorithme de Hubrechts sur $\mathbb{F}_{2^n}$:

- Explorer les méthodes de déformation.
- Implémentation.