Équations différentielles p-adiques pour le calcul d'isogénies en petite caractéristique

Elie Eid
Univ. Rennes 1

Séminaire LFANT

15 décembre 2020

Soit p un nombre premier, $\mathbb{Q}_p$ le corps des nombres p-adiques et K une extension finie de $\mathbb{Q}_p$.

Une EDO p-adique du premier ordre est une équation de la forme

$$y'(t) = F(y(t), t)$$

où l'inconnue $y(t)$ est une fonction $U \subset K \longrightarrow K$.

Soit p un nombre premier, $\mathbb{Q}_p$ le corps des nombres p-adiques et K une extension finie de $\mathbb{Q}_p$.

Une EDO p-adique du premier ordre est une équation de la forme

$$y'(t) = F(y(t), t)$$

où l'inconnue $y(t)$ est une fonction $U \subset K \to K$.

Quelques questions intéressantes :

- Existence de solutions et unicité.
- Propriétés des solutions : rayon de convergence, ...
- Méthode de résolution.

- Calcul de la fonction Zeta d'une variété algébrique.

  Equations différentielles hypergéométriques :

$$t(1-t)y''(t)+(c-(a+b+1)t)y'(t)-aby(t)=0.$$

- Calcul de la fonction Zeta d'une variété algébrique.

  Equations différentielles hypergéométriques :

$$t(1-t)y''(t)+(c-(a+b+1)t)y'(t)-aby(t)=0.$$

- Calcul de sommes et produits composés de polynômes définis sur des corps finis.

$$f=\prod_{i=1}^{d}(x-\alpha_i) \text{ et } g=\prod_{i=1}^{e}(x-\beta_i),$$

$$f\oplus g=\prod_{i,j}(x-\alpha_i+\beta_j), \quad f\otimes g=\prod_{i,j}(x-\alpha_i\beta_j).$$

- Calcul de la fonction Zeta d'une variété algébrique.

  Equations différentielles hypergéométriques :

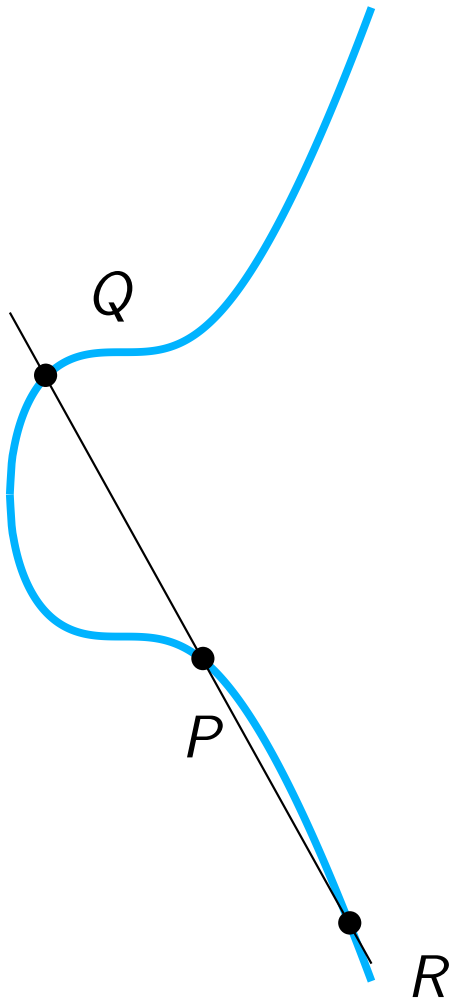
$$t(1-t)y''(t)+(c-(a+b+1)t)y'(t)-aby(t)=0.$$

- Calcul de sommes et produits composés de polynômes définis sur des corps finis.

$$f=\prod_{i=1}^{d}(x-\alpha_i) \text{ et } g=\prod_{i=1}^{e}(x-\beta_i),$$

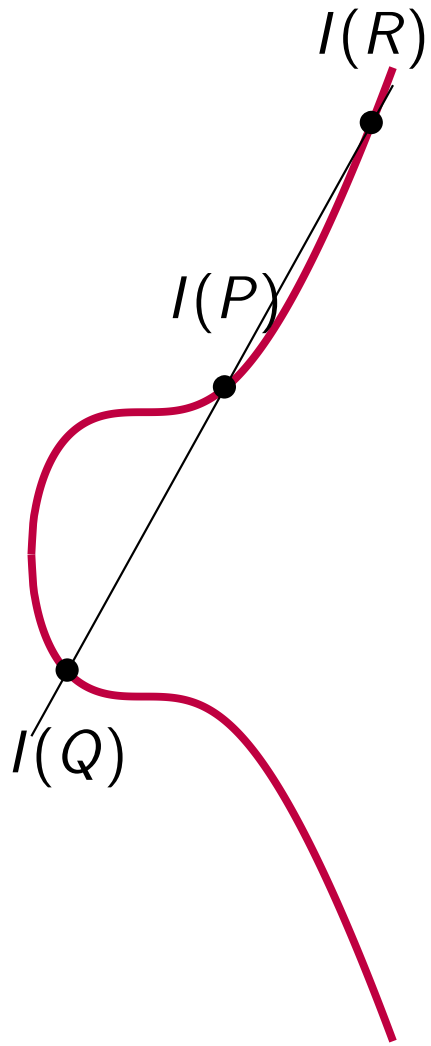
$$f\oplus g=\prod_{i,j}(x-\alpha_i+\beta_j), \quad f\otimes g=\prod_{i,j}(x-\alpha_i\beta_j).$$

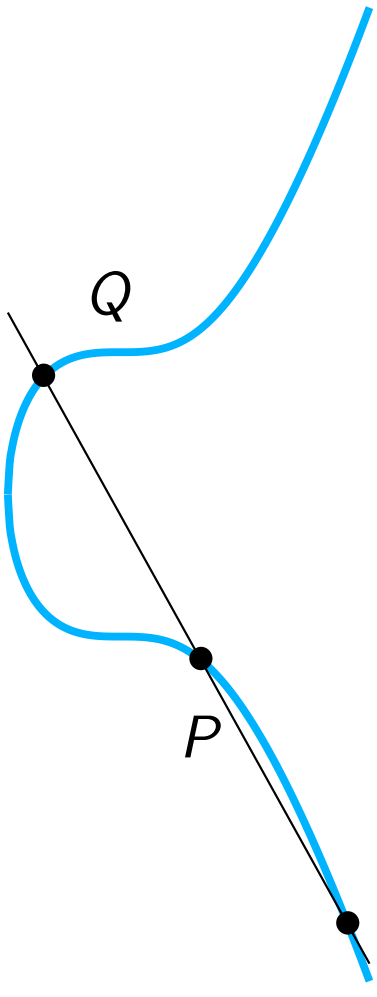
- Calcul d'isogénies.



$$I \longrightarrow$$

$$I(x,y) = \Big(h(x), yg(x)\Big)$$

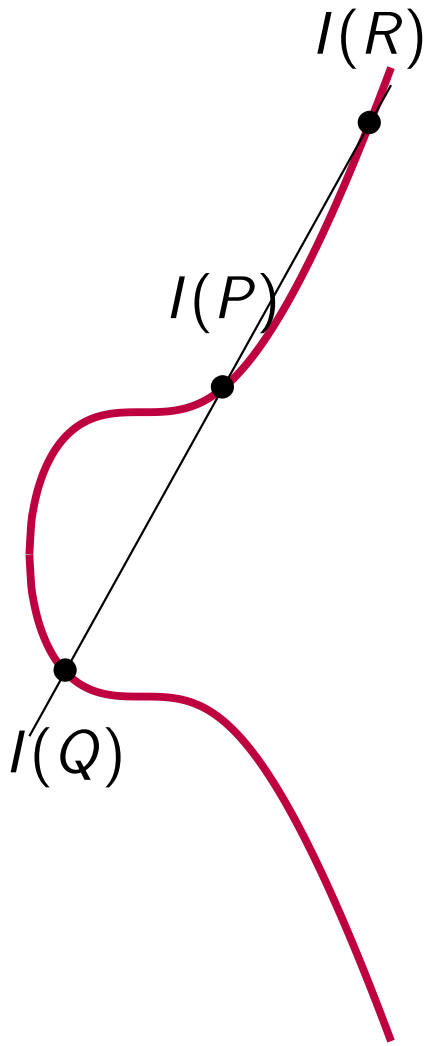


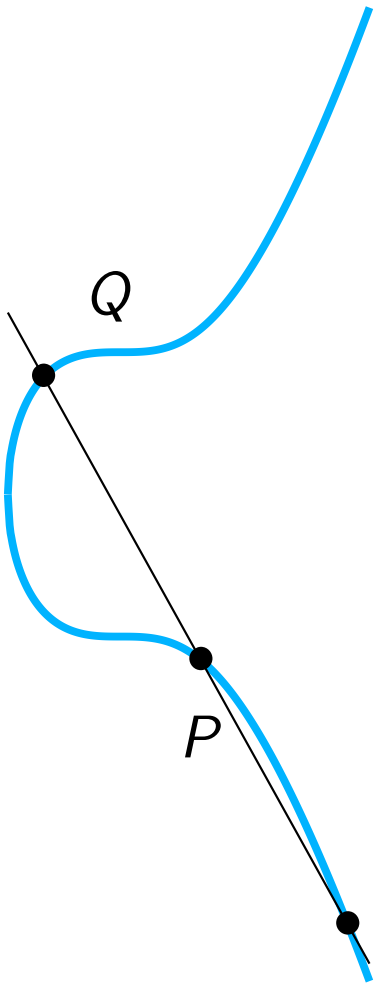


$$\xrightarrow{\quad I \quad}$$

$$I(x,y) = \Big(h(x), yg(x)\Big)$$

$$H^0(E,\Omega^1_E) = <\omega> \text{ avec } \omega = dx/y$$



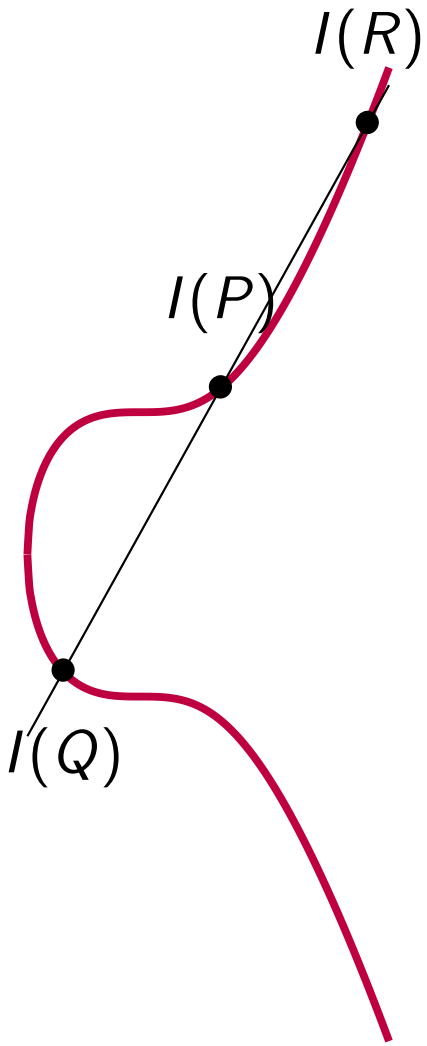


$$\xrightarrow{\quad I \quad}$$

$$I(x,y) = \Big(h(x), yg(x)\Big)$$

$$H^0(E,\Omega^1_E) = <\omega> \text{ avec } \omega = dx/y$$

$$\Longrightarrow g(x) = ch'(x)$$



$$E/k \xrightarrow{I(x,y)=(h(x),cyh'(x))} \widetilde{E}/k \qquad char(k) \neq 2$$

$$E/k \xrightarrow{I(x,y)=(h(x),cyh'(x))} \widetilde{E}/k \qquad char(k) \neq 2$$

$$E : y^2 = x^3 + a_2x^2 + a_4x + a_6$$

$$\widetilde{E} : y^2 = x^3 + \widetilde{a_2}x^2 + \widetilde{a_4}x + \widetilde{a_6}$$

$$E/k \xrightarrow{I(x,y)=(h(x),cyh'(x))} \widetilde{E}/k \qquad char(k) \neq 2$$

$$E : y^2 = x^3 + a_2x^2 + a_4x + a_6$$

$$\widetilde{E} : y^2 = x^3 + \widetilde{a_2}x^2 + \widetilde{a_4}x + \widetilde{a_6}$$

$$\Longrightarrow c^2\left(x^3 + a_2x^2 + a_4x + a_6\right)h'^2 = x^3 + \widetilde{a_2}h^2 + \widetilde{a_4}h + \widetilde{a_6}$$

$$E/k \xrightarrow{I(x,y)=(h(x),cyh'(x))} \widetilde{E}/k \qquad char(k) \neq 2$$

$$E : y^2 = x^3 + a_2x^2 + a_4x + a_6$$
$$\widetilde{E} : y^2 = x^3 + \widetilde{a_2}x^2 + \widetilde{a_4}x + \widetilde{a_6}$$

$$\Longrightarrow c^2(x^3 + a_2x^2 + a_4x + a_6)\,h'^2 = x^3 + \widetilde{a_2}h^2 + \widetilde{a_4}h + \widetilde{a_6}$$

Au voisinage de ∞: $U(t)y'^2 = V(y(t))$ et $y(0) = 0$

Soit g un entier ≥ 2. Soit

$$H : y^2 = f(x)$$

une courbe hyperelliptique de genre g définie sur un corps k ($\text{carac}(k) \neq 2$) et $J(H)$ la Jacobienne de H.

Soit g un entier ≥ 2. Soit

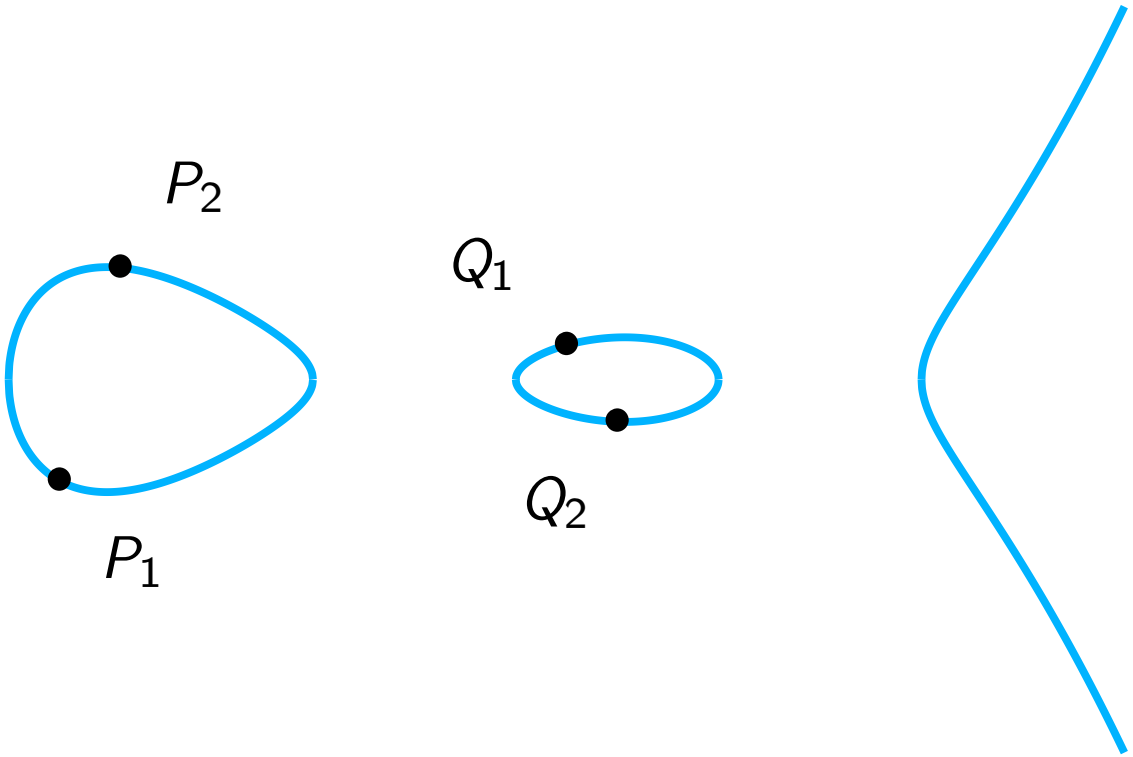
$$H : y^2 = f(x)$$

une courbe hyperelliptique de genre g définie sur un corps k ($\text{carac}(k) \neq 2$) et $J(H)$ la Jacobienne de H.

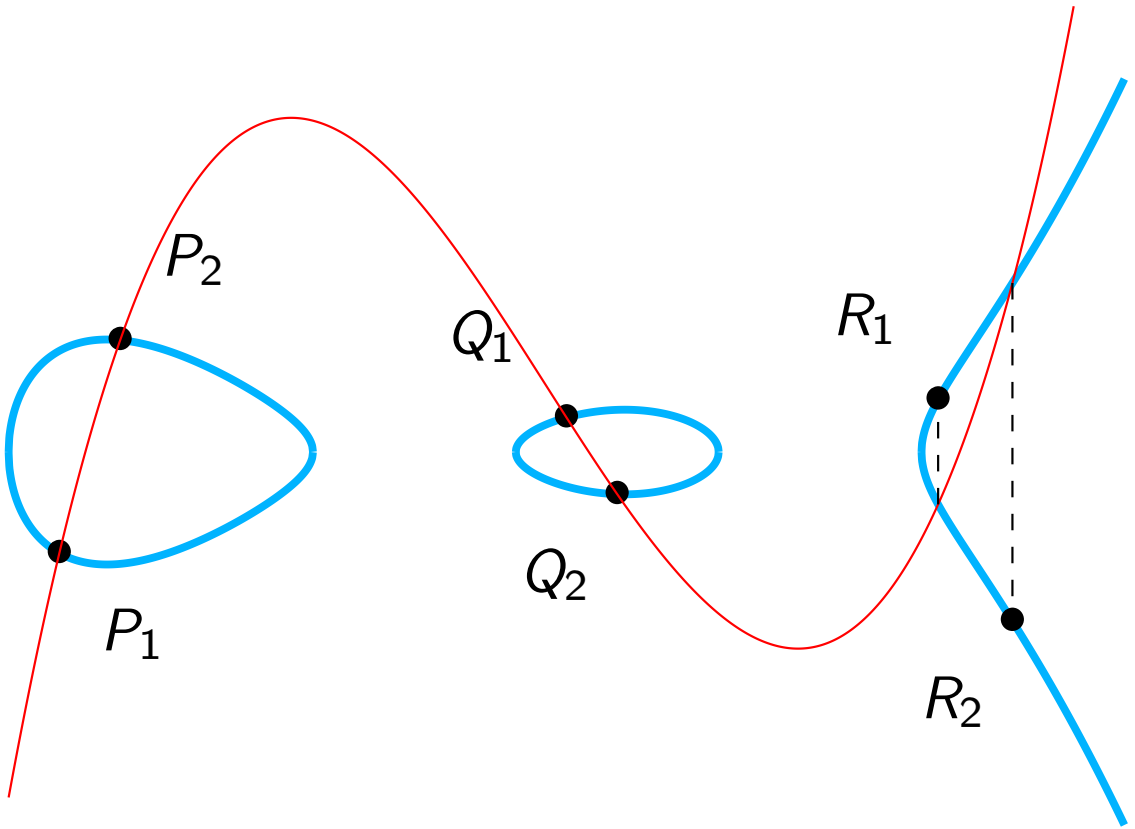
On représente les éléments dans $J(H)$ en utilisant le morphisme birationnel suivant

$$\begin{array}{ccc} J(H) & \longrightarrow & H^{(g)} \\ x & \mapsto & \{P_1, \cdots, P_g\} \end{array}$$

g=2



g=2



$$\{P_1, P_2\} + \{Q_1, Q_2\} = \{R_1, R_2\}.$$

Représentation de Mumford

Un point "générique" $x = \{(x_1, y_1), \cdots, (x_g, y_g)\}$ est représenté par $(U(X), V(X))$ avec

$$U(X) = X^g + \sigma_1 X^{g-1} + \cdots + \sigma_g$$

où

$$\sigma_i = (-1)^i \sum_{1 \leq j_1 < j_2 < \cdots < j_i \leq g} x_{j_1} x_{j_2} \cdots x_{j_i}$$

et

$$V(X) = \rho_1 X^{g-1} + \cdots + \rho_g = \sum_{j=0}^{g-1} y_j \left(\prod_{i=0, i \neq j}^{g-1} \frac{X - x_i}{x_j - x_i} \right).$$

Représentation de Mumford

Un point "générique" $x = \{(x_1, y_1), \cdots, (x_g, y_g)\}$ est représenté par $(U(X), V(X))$ avec

$$U(X) = X^g + \sigma_1 X^{g-1} + \cdots + \sigma_g$$

où

$$\sigma_i = (-1)^i \sum_{1 \leq j_1 < j_2 < \cdots < j_i \leq g} x_{j_1} x_{j_2} \cdots x_{j_i}$$

et

$$V(X) = \rho_1 X^{g-1} + \cdots + \rho_g = \sum_{j=0}^{g-1} y_j \left(\prod_{i=0, i \neq j}^{g-1} \frac{X - x_i}{x_j - x_i} \right).$$

On représente x soit par $\{(x_1, y_1), \cdots, (x_g, y_g)\}$ soit par le $2g$-uplet $(\sigma_1, \cdots, \sigma_g, \rho_1, \cdots, \rho_g)$.

Représentation rationnelle d'une isogénie

Soient $H_1 : v^2 = f_1(u)$ et $H_2 : y^2 = f_2(x)$ deux courbes hyperelliptiques de genre g.
On suppose qu'il existe une isogénie $I : J(H_1) \to J(H_2)$.
Soit $P \in H_1$. Soit $j_P : H_1 \to J(H_1)$ le **morphisme de Jacobi** d'origine P.

Représentation rationnelle d'une isogénie

Soient $H_1 : v^2 = f_1(u)$ et $H_2 : y^2 = f_2(x)$ deux courbes hyperelliptiques de genre g.
On suppose qu'il existe une isogénie $I : J(H_1) \longrightarrow J(H_2)$.
Soit $P \in H_1$. Soit $j_P : H_1 \longrightarrow J(H_1)$ le **morphisme de Jacobi** d'origine P.
$I \circ j_P$ induit un unique morphisme I_P définit comme suit

$$\begin{array}{rcl} I_P : H_1 & \longrightarrow & H_2^{(g)} \simeq J(H_2) \\ Q = (u, v) & \mapsto & I([Q - P]) \end{array}$$

Représentation rationnelle d'une isogénie

Soient $H_1 : v^2 = f_1(u)$ et $H_2 : y^2 = f_2(x)$ deux courbes hyperelliptiques de genre g.
On suppose qu'il existe une isogénie $I : J(H_1) \longrightarrow J(H_2)$.
Soit $P \in H_1$. Soit $j_P : H_1 \longrightarrow J(H_1)$ le **morphisme de Jacobi** d'origine P.
$I \circ j_P$ induit un unique morphisme I_P définit comme suit

$$\begin{array}{rcl} I_P : H_1 & \longrightarrow & H_2^{(g)} \simeq J(H_2) \\ Q = (u, v) & \mapsto & I([Q - P]) \end{array}$$

I_P est représenté par $2g$ fractions rationnelles
$\sigma_1(u, v), \cdots, \sigma_g(u, v), \rho_1(u, v), \cdots, \rho_g(u, v)$.

Représentation rationnelle d'une isogénie

Soient $H_1 : v^2 = f_1(u)$ et $H_2 : y^2 = f_2(x)$ deux courbes hyperelliptiques de genre g.
On suppose qu'il existe une isogénie $I : J(H_1) \longrightarrow J(H_2)$.
Soit $P \in H_1$. Soit $j_P : H_1 \longrightarrow J(H_1)$ le **morphisme de Jacobi** d'origine P.
$I \circ j_P$ induit un unique morphisme I_P définit comme suit

$$\begin{array}{rcl} I_P : H_1 & \longrightarrow & H_2^{(g)} \simeq J(H_2) \\ Q = (u, v) & \mapsto & I([Q - P]) \end{array}$$

I_P est représenté par $2g$ fractions rationnelles $\sigma_1(u,v), \cdots, \sigma_g(u,v), \rho_1(u,v), \cdots, \rho_g(u,v)$.

On dit que le $2g$-uplet $(\sigma_1, \cdots, \sigma_g, \rho_1, \cdots, \rho_g)$ est **une représentation rationnelle** de I.

EDO associée à une représentation rationnelle

Le morphisme I_P agit sur les espaces vectoriels $H^0(J(H_2), \Omega^1_{J(H_2)})$ et $H^0(H_1, \Omega^1_{H_1})$ pour donner l'application linéaire

$$I_P^* : H^0(J(H_2), \Omega^1_{J(H_2)}) \longrightarrow H^0(H_1, \Omega^1_{H_1})$$

EDO associée à une représentation rationnelle

Le morphisme I_P agit sur les espaces vectoriels $H^0(J(H_2),\Omega^1_{J(H_2)})$ et $H^0(H_1,\Omega^1_{H_1})$ pour donner l'application linéaire

$$I_P^* : H^0(J(H_2),\Omega^1_{J(H_2)}) \longrightarrow H^0(H_1,\Omega^1_{H_1})$$

Des bases respectives de $H^0(H_1,\Omega^1_{H_1})$ et $H^0(J(H_2),\Omega^1_{J(H_2)})$ sont données par

$$B_1 = \left\{ u^i \frac{du}{v} \, ; i \in \{0,\dots,g-1\} \right\}$$

et

$$B_2 = \left\{ \sum_{j=1}^{g} x_j^i \frac{dx_j}{y_j} \, ; i \in \{0,\dots,g-1\} \right\}.$$

Soit $(m_{ij})_{ij}$ la matrice de l'application I_P^* dans le couple de bases (B_2, B_1). On a ainsi le système différentiel suivant

$$\begin{cases} \dfrac{dx_1}{y_1} + \cdots + \dfrac{dx_g}{y_g} = \left(m_{11} + \ldots + m_{1g} \cdot u^{g-1}\right)\dfrac{du}{v} \\ \dfrac{x_1 \cdot dx_1}{y_1} + \cdots + \dfrac{x_g \cdot dx_g}{y_g} = \left(m_{21} + \ldots + m_{2g} \cdot u^{g-1}\right)\dfrac{du}{v} \\ \vdots \qquad\qquad\qquad\qquad \vdots \\ \dfrac{x_1^{g-1} \cdot dx_1}{y_1} + \cdots + \dfrac{x_g^{g-1} \cdot dx_g}{y_g} = \left(m_{g1} + \ldots + m_{gg} \cdot u^{g-1}\right)\dfrac{du}{v} \\ y_1^2 = f_2(x_1), \quad \cdots \quad , y_g^2 = f_2(x_g)\,. \end{cases}$$

Soit $Q = (u_Q, v_Q)$ un point de H_1. Soit t un paramètre local au voisinage de Q $(t = u - u_Q)$. Le système différentiel s'écrit

$$\begin{cases} \dfrac{x_1'(t)}{y_1(t)} + \cdots + \dfrac{x_g'(t)}{y_g(t)} = G_1(t) \\ \dfrac{x_1(t)\cdot x_1'(t)}{y_1(t)} + \cdots + \dfrac{x_g(t)\cdot x_g'(t)}{y_g(t)} = G_2(t) \\ \vdots \qquad\qquad \vdots \\ \dfrac{x_1(t)^{g-1}\cdot x_1'(t)}{y_1(t)} + \cdots + \dfrac{x_g(t)^{g-1}\cdot x_g'(t)}{y_g(t)} = G_g(t) \\ y_1(t)^2 = f_2(x_1(t)), \quad \cdots \quad , y_g(t)^2 = f_2(x_g(t)). \end{cases}$$

Soit k un corps fini de caractéristique $p > 0$.

- Les équations différentielles construites pour le calcul d'isogénies peuvent avoir plusieurs solutions.

Soit k un corps fini de caractéristique $p > 0$.

- Les équations différentielles construites pour le calcul d'isogénies peuvent avoir plusieurs solutions.

  Ceci est du à l'existence d'isogénies inséparables. Par exemple : $[\ell], [\ell + p], [\ell + p^2]$... donnent plusieurs solutions à la même équadiff.

Soit k un corps fini de caractéristique $p > 0$.

- Les équations différentielles construites pour le calcul d'isogénies peuvent avoir plusieurs solutions.

  Ceci est du à l'existence d'isogénies inséparables. Par exemple : $[\ell], [\ell + p], [\ell + p^2]$... donnent plusieurs solutions à la même équadiff.

- On relève sur un corps de caractéristique 0 : une extension de $\mathbb{Q}_p$.

Soit k un corps fini de caractéristique $p > 0$.

- Les équations différentielles construites pour le calcul d'isogénies peuvent avoir plusieurs solutions.

  Ceci est du à l'existence d'isogénies inséparables. Par exemple : $[\ell], [\ell + p], [\ell + p^2]$... donnent plusieurs solutions à la même équadiff.

- On relève sur un corps de caractéristique 0 : une extension de $\mathbb{Q}_p$.
- On résout l'équation différentielle sur cette extension puis on réduit modulo p.

Soit k un corps fini de caractéristique $p > 0$.

- Les équations différentielles construites pour le calcul d'isogénies peuvent avoir plusieurs solutions.

  Ceci est du à l'existence d'isogénies inséparables. Par exemple : $[\ell], [\ell + p], [\ell + p^2]$... donnent plusieurs solutions à la même équadiff.

- On relève sur un corps de caractéristique 0 : une extension de $\mathbb{Q}_p$.
- On résout l'équation différentielle sur cette extension puis on réduit modulo p.
- Résoudre dans $\mathbb{Q}_p \Longrightarrow$ perte de précision p-adique.

Quelle précision doit-on avoir ?

Quelle précision doit-on avoir ?

- $g = 1$ et $p \geq 3$

  [Lercier-Sirvent,08] $\sim 2\log^2(\deg(I))$ chiffres de précision.

Quelle précision doit-on avoir ?

- $g = 1$ et $p \geq 3$

  [Lercier-Sirvent,08] $\sim 2\log^2(\deg(I))$ chiffres de précision.

  [Lairez-Vaccon,16] $\sim 2\log(\deg(I))$ chiffres de précision (optimale !).

Quelle précision doit-on avoir ?

- $g = 1$ et $p \geq 3$

  [Lercier-Sirvent,08] $\sim 2\log^2(\deg(I))$ chiffres de précision.

  [Lairez-Vaccon,16] $\sim 2\log(\deg(I))$ chiffres de précision (optimale !).

- $g = 1$ et $p = 2$

  [Caruso-E.-Lercier,19] $\sim 2\log(\deg(I))$ chiffres de précision (optimale !).

Quelle précision doit-on avoir ?

- $g = 1$ et $p \geq 3$

  [Lercier-Sirvent,08] $\sim 2\log^2(\deg(I))$ chiffres de précision.

  [Lairez-Vaccon,16] $\sim 2\log(\deg(I))$ chiffres de précision (optimale !).

- $g = 1$ et $p = 2$

  [Caruso-E.-Lercier,19] $\sim 2\log(\deg(I))$ chiffres de précision (optimale !).

- $g > 1$ et $p \geq 3$

  [E.,20] $\sim \log(\deg(\rho_g))$ chiffres de précision (optimale !).

Lemme de précision Soit $f : \mathbb{Q}_p^r \longrightarrow \mathbb{Q}_p^s$ une application localement analytique.

Lemme de précision Soit $f : \mathbb{Q}_p^r \longrightarrow \mathbb{Q}_p^s$ une application localement analytique.
Soit $x \in \mathbb{Q}_p^r$ tel que $df(x)$ est surjective.

Lemme de précision Soit $f : \mathbb{Q}_p^r \longrightarrow \mathbb{Q}_p^s$ une application localement analytique.
Soit $x \in \mathbb{Q}_p^r$ tel que $df(x)$ est surjective.
Pour toute boule ouverte centrée B "suffisament petite", on a

$$f(x+B) = f(x) + df(x)(B).$$

Soit K une extension de $\mathbb{Q}_p$.

Soit K une extension de $\mathbb{Q}_p$.

Si $g = 1$, l'équation différentielle prend la forme

$$U(t)y'^2(t) = V(y(t))$$

avec U et V des carrés inversibles dans $\mathcal{O}_K[\![t]\!]$ et $y(t) \in \mathcal{O}_K[\![t]\!]$.

Soit K une extension de $\mathbb{Q}_p$.

Si $g = 1$, l'équation différentielle prend la forme

$$U(t)y'^2(t) = V(y(t))$$

avec U et V des carrés inversibles dans $\mathcal{O}_K[\![t]\!]$ et $y(t) \in \mathcal{O}_K[\![t]\!]$.

Cette équation prend la forme

$$h(y(t))y' = g(t).$$

Soit K une extension de $\mathbb{Q}_p$.

Si $g = 1$, l'équation différentielle prend la forme

$$U(t)y'^2(t) = V(y(t))$$

avec U et V des carrés inversibles dans $\mathcal{O}_K[\![t]\!]$ et $y(t) \in \mathcal{O}_K[\![t]\!]$.

Cette équation prend la forme

$$h(y(t))y' = g(t).$$

Si $g > 2$, le système différentiel prend la forme

$$H(X(t)) \cdot X'(t) = G(t).$$

$X(t)$ est le vecteur $(x_1(t), \cdots, x_g(t)) \in \left(\mathcal{O}_K[\![t]\!]\right)^g$.

Itération de Newton

$$X_n = X_m + (H(X_m))^{-1} \int (G - H(X_m) \cdot X_m') \, dt.$$

Remarque :

$$\int O(p^k) t^{p-1} dt = O(p^{k-1}) t^p.$$

$\Longrightarrow$ on perd $O(\log^2(N))$ chiffres de précision pour calculer une approx. de X mod. t^N.

En pratique

- On travaille avec une précision fixe : dans l'anneau $\mathbb{Z}/p^k\mathbb{Z}$.

En pratique

- On travaille avec une précision fixe : dans l'anneau $\mathbb{Z}/p^k\mathbb{Z}$.
- On fixe H et on varie G. On pose alors

$$f : G(t) \mapsto X(t)$$

tel que $X(t)$ est la solution de l'équation $H(X(t)) \cdot X'(t) = G(t)$.

En pratique

- On travaille avec une précision fixe : dans l'anneau $\mathbb{Z}/p^k\mathbb{Z}$.
- On fixe H et on varie G. On pose alors

$$f : G(t) \mapsto X(t)$$

tel que $X(t)$ est la solution de l'équation $H(X(t)) \cdot X'(t) = G(t)$.

- La différentielle df est donnée par

$$df(G(t))(dG(t)) = (H(X(t))^{-1} \int dG(t)\, dt.$$

Si on connait G et H modulo $(p^{1+\lfloor \log_p(n) \rfloor}, t^{n+1})$, on obtient la solution $X(t) \mod (p, t^{n+1})$ en appliquant l'itération suivante

$$X_n = X_m + (H(X_m))^{-1} \int (G - H(X_m) \cdot X_m') \, dt$$

Soit k un corps fini de caractéristique 2. Soit K une extension de $\mathbb{Q}_2$.

Soit k un corps fini de caractéristique 2. Soit K une extension de $\mathbb{Q}_2$.

L'équation d'une courbe elliptique ordinaire sur k est de la forme

$$y^2 + xy = x^3 + a_2x^2 + a_6.$$

Soit k un corps fini de caractéristique 2. Soit K une extension de $\mathbb{Q}_2$.

L'équation d'une courbe elliptique ordinaire sur k est de la forme

$$y^2 + xy = x^3 + a_2x^2 + a_6.$$

La série $U(t)$ de l'équation différentielle $U(t)y'^2(t) = V(y(t))$ est de la forme

$$U(t) = t(t-4a)g^2(t)$$

avec $a \in \mathcal{O}_K^*$ et $g \in \mathcal{O}_K[\![t]\!]$.

Soit k un corps fini de caractéristique 2. Soit K une extension de $\mathbb{Q}_2$.

L'équation d'une courbe elliptique ordinaire sur k est de la forme

$$y^2 + xy = x^3 + a_2x^2 + a_6.$$

La série $U(t)$ de l'équation différentielle $U(t)y'^2(t) = V(y(t))$ est de la forme

$$U(t) = t(t-4a)g^2(t)$$

avec $a \in \mathcal{O}_K^*$ et $g \in \mathcal{O}_K[\![t]\!]$.
$\Longrightarrow$ un point singulier de norme $1/4$.

$g = 2$

On considère la courbe H_1 donnée par l'équation

$$H_1/\mathbb{F}_{19} : y^2 = x^5 + 16x^4 + 11x^3 + 3x^2 + 5x + 17.$$

$V \subset J(H_1)[11]$ s.g. isotrope max.

Trouvons H_2 et $I : J(H_1) \longrightarrow J(H_2) = J(H_1)/V$.

$g = 2$

On considère la courbe H_1 donnée par l'équation

$$H_1/\mathbb{F}_{19} : y^2 = x^5 + 16x^4 + 11x^3 + 3x^2 + 5x + 17.$$

$V \subset J(H_1)[11]$ s.g. isotrope max.

Trouvons H_2 et $I : J(H_1) \longrightarrow J(H_2) = J(H_1)/V$.

La précision 19-adique qu'on aura besoin : $1 + \lfloor \log_{19}(110) \rfloor = 2$.

On relève l'équation de H_1 dans $\mathbb{Q}_{19}$:

$$\mathscr{H}_1/\mathbb{Q}_{19} : y^2 = x^5 + (16 + O(19^2))\,x^4 + (11 + O(19^2))\,x^3 + (3 + O(19^2))\,x^2 + (5 + O(19^2))\,x + 17 + O(19^2).$$

On relève l'équation de H_1 dans $\mathbb{Q}_{19}$:

$$\mathscr{H}_1/\mathbb{Q}_{19} : y^2 = x^5 + (16 + O(19^2))x^4 + (11 + O(19^2))x^3 + (3 + O(19^2))x^2 + (5 + O(19^2))x + 17 + O(19^2).$$

Soit $\mathscr{V}$ le relevé de V dans une extension finie de $\mathbb{Q}_{19}$.

Soit $\mathscr{H}_2$ la courbe telle que $J(\mathscr{H}_2) = J(\mathscr{H}_1)/\mathscr{V}$.

On relève l'équation de H_1 dans $\mathbb{Q}_{19}$:

$$\mathscr{H}_1/\mathbb{Q}_{19} : y^2 = x^5 + (16 + O(19^2))x^4 + (11 + O(19^2))x^3 + (3 + O(19^2))x^2 + (5 + O(19^2))x + 17 + O(19^2).$$

Soit $\mathscr{V}$ le relevé de V dans une extension finie de $\mathbb{Q}_{19}$.

Soit $\mathscr{H}_2$ la courbe telle que $J(\mathscr{H}_2) = J(\mathscr{H}_1)/\mathscr{V}$.
On trouve une équation de $\mathscr{H}_2$ en utilisant l'algorithme de Couveignes :

$$\mathscr{H}_2/\mathbb{Q}_{19} : y^2 = (2 + O(19^2))x^5 - (176 + O(19^2))x^4 - (100 + O(19^2))x^3 + (2546 + O(19^2))x^2 - (68 + O(19^3))x,$$

La matrice de normalisation $(m_{ij})_{ij}$ est égale à

$$\begin{pmatrix} 95 + O(19^2) & 233 + O(19^2) \\ 155 + O(19^2) & 228 + O(19^2) \end{pmatrix}.$$

La matrice de normalisation $(m_{ij})_{ij}$ est égale à

$$\begin{pmatrix} 95 + O(19^2) & 233 + O(19^2) \\ 155 + O(19^2) & 228 + O(19^2) \end{pmatrix}.$$

Le calcul de (m_{ij}) se fait en envoyant le point

$$P_1(t) = \left(t + O(19^2), 146 - 21\,t + 179\,t^2 + O\left(19^2, t^3\right)\right) \in \mathscr{H}_1\left(\mathbb{Q}_{19}[\![t]\!]\right)$$

à

$$\left\{R_1 = \left(-36 + 353\,t + O\left(19^2, t^2\right), -13 + 326\,t + O\left(19^2, t^2\right)\right),\right.$$
$$\left.R_2 = \left(-129 + 102\,t + O\left(19^2, t^2\right), -47 + 2\,t + O\left(19^2, t^2\right)\right)\right\}$$

dans $\mathscr{H}_2\left(\mathbb{Q}_{19}[\![t]\!]\right)^{(2)}$.

On choisit alors $X_0 = (-36 + O(19^2), -129 + O(19^2))$ comme condition initiale.

On choisit alors $X_0 = (-36 + O(19^2), -129 + O(19^2))$ comme condition initiale.

L'algorithme de résolution du système différentiel nous donne $x_1(t)$, $x_2(t)$, $y_1(t)$ et $y_2(t)$.

$$x_1(t) = -36 - 8t - 58t^2 - 90t^3 - 90t^4 - 145t^5 - 124t^6 + \ldots$$

et

$$x_2(t) = -129 + 102t + 100t^2 + 94t^3 + 45t^4 + 91t^5 + 29t^6 + \ldots$$

On choisit alors $X_0 = (-36 + O(19^2), -129 + O(19^2))$ comme condition initiale.

L'algorithme de résolution du système différentiel nous donne $x_1(t)$, $x_2(t)$, $y_1(t)$ et $y_2(t)$.

$$x_1(t) = -36 - 8t - 58t^2 - 90t^3 - 90t^4 - 145t^5 - 124t^6 + \ldots$$

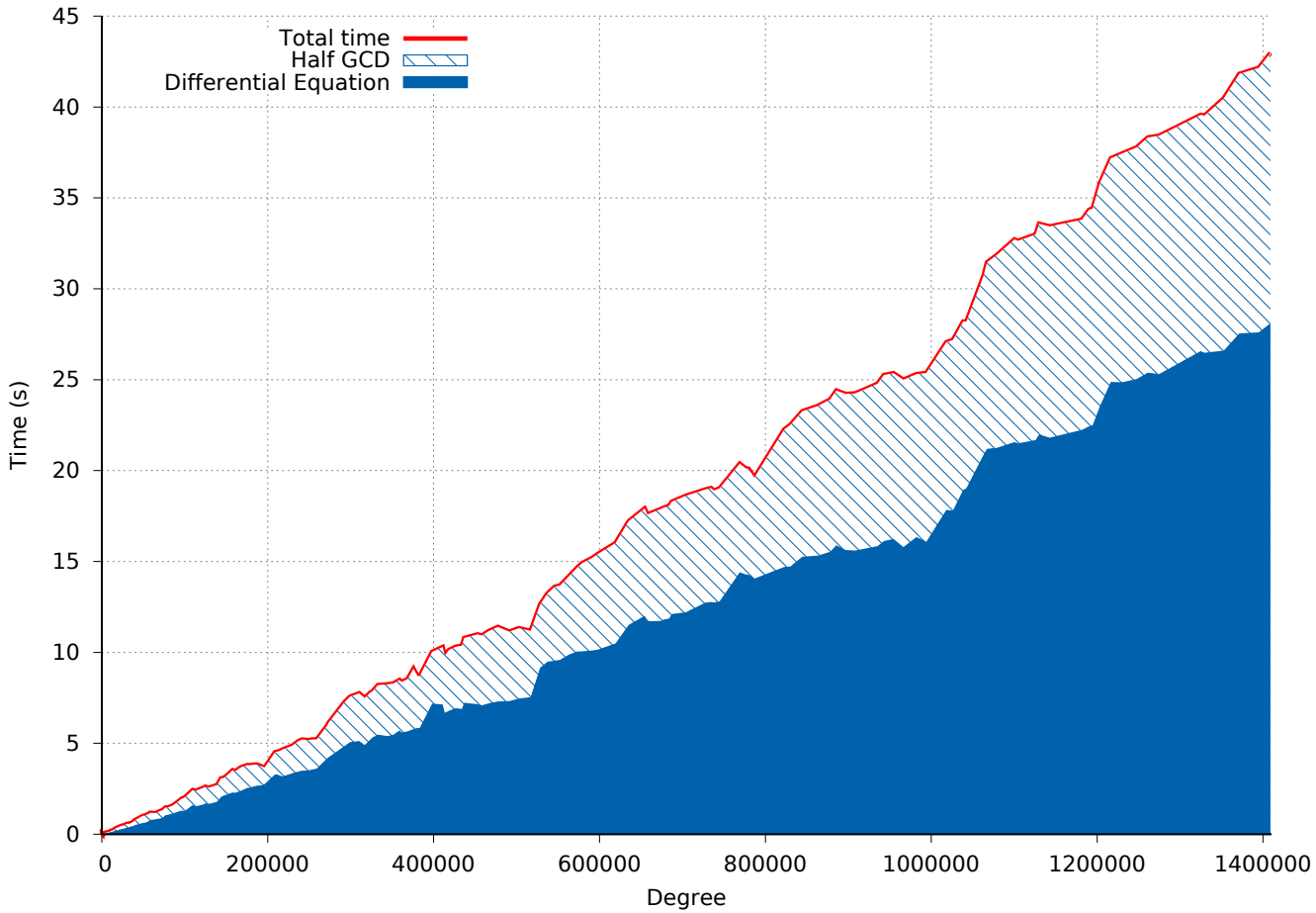
et

$$x_2(t) = -129 + 102t + 100t^2 + 94t^3 + 45t^4 + 91t^5 + 29t^6 + \ldots$$

Ce qui donne les fractions rationnelles $\sigma_1, \sigma_2, \rho_1$ et ρ_2.

Expérimentations

$\mathbf{p = 2, g = 1}$



Expérimentations

p = 7