

# Formules de Thomae et isogénies

Romain COSSET

CNRS

Laboratoire: LORIA (Nancy), Équipe: CACAO

26 mars 2010

1 Fonctions thêta

2 Généralisation des formules de Thomae

3 Isogénies

# FONCTIONS THÊTA

## Fonctions thêta analytiques

Ce sont des fonctions de  $\mathbb{C}^g$  dans  $\mathbb{C}$ .

Soient  $z \in \mathbb{C}^g$ ,  $(a, b) \in \mathbb{Q}^{2g}$  et  $\Omega \in \mathcal{H}_g$ .

$$\theta(z, \Omega) = \sum_{n \in \mathbb{Z}^g} \exp(\pi i^t n \Omega n + 2\pi i^t n \cdot z)$$

$$\begin{aligned} \theta[a, b](z, \Omega) &= \sum_{n \in \mathbb{Z}^g} \exp(\pi i^t (n+a) \Omega (n+a) + 2\pi i^t (n+a) \cdot (z+b)) \\ &= \exp(\pi i^t a \Omega a + 2\pi i^t a \cdot (z+b)) \theta(z + \Omega a + b, \Omega) \end{aligned}$$

$(a, b)$  est appelé la caractéristique de la fonction thêta.

Nous allons considérer

- $z$  modulo  $\Lambda = \mathbb{Z}^g + \Omega \mathbb{Z}^g$ .
- les caractéristiques  $(a, b)$  modulo  $\mathbb{Z}^{2g}$ .

# Variétés abéliennes

## Variété abélienne

C'est un groupe algébrique complet connexe.

Cad. une variété algébrique avec une loi de groupe algébrique.

Exemples de variétés abéliennes :

- les courbes elliptiques
- les jacobiniennes de courbes.

# Variétés abéliennes

## Variété abélienne

C'est un groupe algébrique complet connexe.

Cad. une variété algébrique avec une loi de groupe algébrique.

Exemples de variétés abéliennes :

- les courbes elliptiques
- les jacobiniennes de courbes.

Elles sont utilisées en cryptographie car

- Le problème du logarithme discret y est (souvent) difficile.
- Il y existe des couplages.

# Variétés abéliennes

Une variété abélienne  $A$  de dimension  $g$  (principalement polarisée) est analytiquement isomorphe à  $\mathbb{C}^g / (\mathbb{Z}^g + \Omega\mathbb{Z}^g)$  pour un certain  $\Omega \in \mathcal{H}_g$ .

Pour  $n \geq 3$ , la variété  $A$  se plonge dans  $\mathbb{P}^{n^g-1}(\mathbb{C})$  à l'aide des fonctions thêta de niveau  $n$ .

## Niveau d'une fonction thêta

- Niveau  $(n, n)$

$$\theta \left[ \frac{a}{n}, \frac{b}{n} \right] (nz, \Omega) \quad \text{avec } a, b \in \mathbb{Z}^g$$

- Niveau  $n$

$$\theta \left[ 0, \frac{b}{n} \right] \left( z, \frac{\Omega}{n} \right) \quad \text{avec } b \in \mathbb{Z}^g$$



## Niveau d'une fonction thêta

- Niveau  $(n, n)$

$$\theta \left[ \frac{a}{n}, \frac{b}{n} \right] (nz, \Omega) \quad \text{avec } a, b \in \mathbb{Z}^g$$

- Niveau  $n$

$$\theta \left[ 0, \frac{b}{n} \right] \left( z, \frac{\Omega}{n} \right) \quad \text{avec } b \in \mathbb{Z}^g$$

Les fonctions thêta de niveau  $(n, n)$  et  $n^2$  fournissent deux plongement isomorphes de la variété abélienne dans  $\mathbb{P}^{n^{2g}-1}(\mathbb{C})$ .

## Niveau d'une fonction thêta

- Niveau  $(n, n)$

$$\theta \left[ \frac{a}{n}, \frac{b}{n} \right] (nz, \Omega) \quad \text{avec } a, b \in \mathbb{Z}^g$$

- Niveau  $n$

$$\theta \left[ 0, \frac{b}{n} \right] \left( z, \frac{\Omega}{n} \right) \quad \text{avec } b \in \mathbb{Z}^g$$

Les fonctions thêta de niveau  $(n, n)$  et  $n^2$  fournissent deux plongement isomorphes de la variété abélienne dans  $\mathbb{P}^{n^2g-1}(\mathbb{C})$ .

Arithmétique :

- Niveau  $4 = (2, 2)$
- Niveau  $2$  : surface de Kummer  $A/\{\pm 1\}$

# Formules de Thomae

$$\text{Jac}(C) \xrightarrow{\sim} \mathbb{C}^g / (\mathbb{Z}^g + \Omega\mathbb{Z}^g) \hookrightarrow \mathbb{P}^{n^g-1}(\mathbb{C})$$

## Formules de Thomae

Elles relient des puissances des thêta constantes avec les paramètres de la courbe.

Formules existantes :

- Courbes elliptiques et hyperelliptiques ; niveau (2,2). (Thomae)
- Courbes elliptiques ; niveau (3,3). (Thomae)
- ...

# Formules de Thomae

$$\text{Jac}(C) \xrightarrow{\sim} \mathbb{C}^g / (\mathbb{Z}^g + \Omega\mathbb{Z}^g) \hookrightarrow \mathbb{P}^{n^g-1}(\mathbb{C})$$

## Formules de Thomae

Elles relient des puissances des thêta constantes avec les paramètres de la courbe.

Formules existantes :

- Courbes elliptiques et hyperelliptiques ; niveau (2,2). (Thomae)
- Courbes elliptiques ; niveau (3,3). (Thomae)
- ...

Exemple pour la courbe  $\mathcal{E} : y^2 = x(x-1)(x-\lambda) :$

$$\left( \frac{\theta \left[ 0, \frac{1}{2} \right] (0)}{\theta [0,0] (0)} \right)^4 = 1 - \frac{1}{\lambda} \quad \left( \frac{\theta \left[ \frac{1}{2}, 0 \right] (0)}{\theta [0,0] (0)} \right)^4 = \lambda$$

# GÉNÉRALISATION DES FORMULES DE THOMAE

# Cas du genre 1

Soit une courbe elliptique sur un corps  $K$  quelconque.

Outils :

- Surfaces de Riemann
- Couplage de Tate

Étant donnée la  $r$ -torsion sur la courbe elliptique, on obtient les thêta constantes de niveau  $(r, r)$  à la puissance  $r' = 2 \text{ppcm}(2, r)$ .

# Cas du genre 1

Soit une courbe elliptique sur un corps  $K$  quelconque.

Outils :

- Surfaces de Riemann
- Couplage de Tate

Étant donnée la  $r$ -torsion sur la courbe elliptique, on obtient les thêta constantes de niveau  $(r, r)$  à la puissance  $r' = 2\text{ppcm}(2, r)$ .

Programme magma :

ENTRÉE : Une courbe elliptique, un point de  $r$ -torsion correspondant à  $a\tau + b$ .

SORTIE : La thêta constante  $\theta[a, b](0, \tau)^{r'}$

## Exemple en genre 1

Soit  $C : y^2 = x(x-1)(x-\lambda)$  associée à  $\tau_\lambda \in \mathcal{H} : C(\mathbb{C}) \simeq \mathbb{C}/(\mathbb{Z} + \tau_\lambda\mathbb{Z})$ .

Points de 2-torsion :

$$\infty \leftrightarrow 0 \quad (0,0) \leftrightarrow \tau_\lambda/2 \quad (1,0) \leftrightarrow 1/2 \quad (\lambda,0) \leftrightarrow 1/2 + \tau_\lambda/2$$



## Exemple en genre 1

Soit  $C : y^2 = x(x-1)(x-\lambda)$  associée à  $\tau_\lambda \in \mathcal{H} : C(\mathbb{C}) \simeq \mathbb{C}/(\mathbb{Z} + \tau_\lambda \mathbb{Z})$ .

Points de 2-torsion :

$$\infty \leftrightarrow 0 \quad (0,0) \leftrightarrow \tau_\lambda/2 \quad (1,0) \leftrightarrow 1/2 \quad (\lambda,0) \leftrightarrow 1/2 + \tau_\lambda/2$$

Soit  $P = (x_0, y_0)$  de 6-torsion tel que  $3 * P = (0,0)$ .

Supposons que  $P$  s'envoie sur le point  $\tau_\lambda/6$ , alors

$$\left( \frac{\theta[1/6,0](0)}{\theta(0)} \right)^{12} = \frac{\lambda-1}{4} x_0^3 + \frac{3\lambda-2}{16} x_0^2 + \frac{-12\lambda^2+13\lambda-2}{8} x_0 + \dots$$

$$\left( \frac{\theta[2/6,0](0)}{\theta(0)} \right)^{12} = \frac{-\lambda+1}{4\lambda} x_0^3 + \frac{-2\lambda+3}{16} x_0^2 + \frac{-2\lambda^2+13\lambda-12}{8} x_0 + \dots$$

$$\left( \frac{\theta[3/6,0](0)}{\theta(0)} \right)^{12} = \lambda^3$$

## Cas du genre $\geq 2$

En genre  $\geq 2$ , la méthode précédente (basée sur les surfaces de Riemann) ne marche pas.

## Cas du genre $\geq 2$

En genre  $\geq 2$ , la méthode précédente (basée sur les surfaces de Riemann) ne marche pas.

Pour tout  $a, b \in \mathbb{Z}^g$  et tout  $\alpha, \beta \in \mathbb{Z}^g$ ,

$$\theta \left[ \begin{array}{c} a \\ n \end{array}, \begin{array}{c} b \\ n \end{array} \right] \left( \Omega \frac{\alpha}{r} + \frac{\beta}{r}, \Omega \right) = \omega \theta \left[ \begin{array}{c} a \\ n \end{array} + \frac{\alpha}{r}, \begin{array}{c} b \\ n \end{array} + \frac{\beta}{r} \right] (0, \Omega)$$

Soit  $P$  un point de  $r$ -torsion dont on connaît les coordonnées par les fonctions thêta de niveau  $(n, n)$ . On a alors les thêta constantes de niveau  $(nr, nr)$ .

## Cas du genre $\geq 2$

En genre  $\geq 2$ , la méthode précédente (basée sur les surfaces de Riemann) ne marche pas.

Pour tout  $a, b \in \mathbb{Z}^g$  et tout  $\alpha, \beta \in \mathbb{Z}^g$ ,

$$\theta \left[ \begin{matrix} a & b \\ n & n \end{matrix} \right] \left( \Omega \frac{\alpha}{r} + \frac{\beta}{r}, \Omega \right) = \omega \theta \left[ \begin{matrix} a & \alpha & b & \beta \\ n & r & n & r \end{matrix} \right] (0, \Omega)$$

Soit  $P$  un point de  $r$ -torsion dont on connaît les coordonnées par les fonctions thêta de niveau  $(n, n)$ . On a alors les thêta constantes de niveau  $(nr, nr)$ .

La variété abélienne  $A = \text{Jac}(C)$  se plonge dans  $\mathbb{P}^{n^2g-1}$  grâce aux fonctions thêta de niveau  $(n, n)$ .

On trouve  $P = \left[ \theta \left[ \begin{matrix} a & b \\ n & n \end{matrix} \right] (z_P, \Omega) \right]_{a, b \in \mathbb{Z}^g}$  un point de  $r$ -torsion.

## Cas du genre $\geq 2$

En genre  $\geq 2$ , la méthode précédente (basée sur les surfaces de Riemann) ne marche pas.

Pour tout  $a, b \in \mathbb{Z}^g$  et tout  $\alpha, \beta \in \mathbb{Z}^g$ ,

$$\theta \left[ \frac{a}{n}, \frac{b}{n} \right] \left( \Omega \frac{\alpha}{r} + \frac{\beta}{r}, \Omega \right) = \omega \theta \left[ \frac{a}{n} + \frac{\alpha}{r}, \frac{b}{n} + \frac{\beta}{r} \right] (0, \Omega)$$

Soit  $P$  un point de  $r$ -torsion dont on connaît les coordonnées par les fonctions thêta de niveau  $(n, n)$ . On a alors les thêta constantes de niveau  $(nr, nr)$ .

La variété abélienne  $A = \text{Jac}(C)$  se plonge dans  $\mathbb{P}^{n^{2g}-1}$  grâce aux fonctions thêta de niveau  $(n, n)$ .

On trouve  $P = \left[ \lambda_P \theta \left[ \frac{a}{n}, \frac{b}{n} \right] (z_P, \Omega) \right]_{a, b \in \mathbb{Z}^g}$  un point de  $r$ -torsion.

On doit calculer  $\lambda_P$ .

## Facteur projectif $\lambda_P$

Grâce aux formules d'addition (affine) on peut calculer

- $\lambda_P^r$  pour  $r$  impair.
- $\lambda_P^{2r}$  pour  $r$  pair.

On obtient les  $\theta \left[ \frac{a}{r}, \frac{b}{r} \right] (0, \Omega)^{2r}$  avec  $a, b \in \mathbb{Z}^g$ .

On a des formules à la Thomae pour le niveau  $(r, r)$ .

# Extraction de racines

Étude de l'action des sous groupes de  $\mathrm{Sp}(2g, \mathbb{Z})$  sur  $\mathbb{C}^g \times \mathcal{H}_g$

Les formules de Thomae fournissent les puissances quatrièmes des thêta constantes de niveau  $(2, 2)$ .

On peut extraire ces racines (quitte à prendre un isomorphisme).

- genre 1 : **ok**.
- genre 2 : **ok** mais utilisation des formules de Frobenius...
- genre  $\geq 3$  : Ok pour certaines et les carrés des autres.

De même il est possible d'obtenir les thêta constantes de niveaux  $(2r, 2r)$  en genre 1 et 2 pour  $r$  impair.

## Descente de niveau

Supposons donnée les thêta constantes de niveau  $ln$ , on veut obtenir les thêta constantes de niveau  $n$  :

$$\theta \left[ 0, \frac{b}{ln} \right] \left( 0, \frac{\Omega}{ln} \right) \longrightarrow \theta \left[ 0, \frac{b'}{n} \right] \left( 0, \frac{\Omega}{n} \right)$$

Application aux formules de Thomae :

Si on a les thêta constantes de niveau  $n^2 = (n, n)$ , on obtient celle de niveau  $n$ .



# Formule de Koizumi

## Formule de Koizumi

Exprime  $\prod_{i=1}^m \theta \left[ K_1^{(i)}, K_2^{(i)} \right] (Z^{(i)}, \gamma_i \Omega)$  en fonction d'une somme de  $\prod_{i=1}^m \theta \left[ L_1^{(i)} + P_1^{(i)}, L_2^{(i)} + P_2^{(i)} \right] (W^{(i)}, \delta_i \Omega)$

## Formule de Koizumi

Soient  $\Gamma = \text{diag}(\gamma_1, \dots, \gamma_m)$  et  $\Delta = \text{diag}(\delta_1, \dots, \delta_m)$  avec  $\gamma_i, \delta_i \in \mathbb{Q}_+^*$ .

Soient  $K_1, K_2 \in M_{g \times m}(\mathbb{Q})$  des caractéristiques pour  $m$  fonctions thêta.

Soient  $L_1, L_2 \in M_{g \times m}(\mathbb{Q})$  des caractéristiques pour  $m$  fonctions thêta.

Soient  $Z \in M_{g \times m}(\mathbb{C})$  et  $W \in M_{g \times m}(\mathbb{C})$  des variables pour  $m$  fonctions thêta.

### Formule de Koizumi

Exprime  $\prod_{i=1}^m \theta \left[ K_1^{(i)}, K_2^{(i)} \right] (Z^{(i)}, \gamma_i \Omega)$  en fonction d'une somme de

$\prod_{i=1}^m \theta \left[ L_1^{(i)} + P_1^{(i)}, L_2^{(i)} + P_2^{(i)} \right] (W^{(i)}, \delta_i \Omega)$

## Formule de Koizumi

Soient  $\Gamma = \text{diag}(\gamma_1, \dots, \gamma_m)$  et  $\Delta = \text{diag}(\delta_1, \dots, \delta_m)$  avec  $\gamma_i, \delta_i \in \mathbb{Q}_+^*$ .

Supposons qu'il existe  $T \in \text{GL}_m(\mathbb{Q})$  tel que  ${}^t T \Gamma T = \Delta$ .

Soient  $K_1, K_2 \in M_{g \times m}(\mathbb{Q})$  des caractéristiques pour  $m$  fonctions thêta.

Soient  $L_1, L_2 \in M_{g \times m}(\mathbb{Q})$  telles que  $L_1 = K_1 {}^t T^{-1}$ ,  $L_2 = K_2 T$ .

Soient  $Z \in M_{g \times m}(\mathbb{C})$  et  $W \in M_{g \times m}(\mathbb{C})$  avec  $W = ZT$ .

### Formule de Koizumi

Exprime  $\prod_{i=1}^m \theta \left[ K_1^{(i)}, K_2^{(i)} \right] (Z^{(i)}, \gamma_i \Omega)$  en fonction d'une somme de

$\prod_{i=1}^m \theta \left[ L_1^{(i)} + P_1^{(i)}, L_2^{(i)} + P_2^{(i)} \right] (W^{(i)}, \delta_i \Omega)$

avec  $P_1 \in M {}^t T^{-1} / (M \cap M {}^t T^{-1})$  et  $P_2 \in MT / (M \cap MT)$  où  $M = M_{g \times m}(\mathbb{Z})$ .

# Applications de la formule de Koizumi

La formule de Koizumi contient :

- Formules de Riemann
- Équivalence entre le niveau  $(n, n)$  et le niveau  $n^2$ .
- Formules d'additions
- ...

# Applications de la formule de Koizumi

La formule de Koizumi contient :

- Formules de Riemann
- Équivalence entre le niveau  $(n, n)$  et le niveau  $n^2$ .
- Formules d'additions
- ...

On veut du niveau  $n$  à partir du niveau  $n^2$ .

Pour avoir du  $\Omega/n$  et du  $\Omega/n^2$  on prend  $\Gamma = \frac{1}{n} \text{Id}_m$  et  $\Delta = \frac{1}{n^2} \text{Id}_m$ .

On cherche une matrice  $T \in \text{GL}_m(\mathbb{Q})$  telle que

$${}^t T \left( \frac{1}{n} \text{Id}_m \right) T = \frac{1}{n^2} \text{Id}_m$$

C'est à dire telle que

$${}^t T T = \frac{1}{n} \text{Id}_m$$

## Choix de la matrice $T$

Choix de la matrice  $T$  telle que  ${}^t T T = \frac{1}{n} \text{Id}_m$

- Pour  $n = a^2$ ,  $T = \left[ \frac{1}{a} \right]$
- Pour  $n = a^2 + b^2$ ,  $T = \frac{1}{n} \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$  (multiplication par  $(a + ib)^{-1}$ ).
- Pour  $n = a^2 + b^2 + c^2 + d^2$ , matrice de la multiplication par  $(a + ib + jc + kd)^{-1}$  dans la base  $(1, i, j, k)$ .

## Choix de la matrice $T$

Choix de la matrice  $T$  telle que  ${}^t T T = \frac{1}{n} \text{Id}_m$

- Pour  $n = a^2$ ,  $T = \left[ \frac{1}{a} \right]$
- Pour  $n = a^2 + b^2$ ,  $T = \frac{1}{n} \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$  (multiplication par  $(a + ib)^{-1}$ ).
- Pour  $n = a^2 + b^2 + c^2 + d^2$ , matrice de la multiplication par  $(a + ib + jc + kd)^{-1}$  dans la base  $(1, i, j, k)$ .

Pour tout entier  $n$ , on obtient une matrice  $T$  (non unique).

Soit  $n \in \mathbb{N}$ , quelle est la dimension minimale  $m$  de  $T$  ?

- si  $m = 1$  alors  $n$  est un carré.
- si  $m = 2$  alors  $n$  est somme de deux carrés
- si  $m = 3$  alors  $n$  est somme de trois carrés et n'est pas premier.

# Algorithme

ENTRÉE : Une courbe hyperelliptique  $\mathcal{C}$  de genre  $g = 2$  donnée sous forme de Weierstrass et un niveau  $r \in \mathbb{N}$ .

SORTIE : Les thêta constantes de niveau  $r$ .

- 1 Calcul des puissances des thêta de niveau  $(2, 2)$ .
- 2 Extraire les racines.
- 3 Calcul de la  $r$ -torsion dans  $\text{Jac}(\mathcal{C})$ .
- 4 Obtenir la  $r$ -torsion exprimée avec les fonctions thêta de niveau  $(2, 2)$ .
- 5 Calcul des puissances thêta de niveau  $(r, r)$ .
- 6 Extraire les racines.
- 7 Descendre de niveau.



# ISOGÉNIES

# Comment prendre des isogénies

On s'intéresse à des  $\ell$ -isogénies pour  $\ell$  premier impair.

On utilise les fonctions thêta de niveau  $n\ell$  avec  $n = 2$  ou  $4$ .

# Comment prendre des isogénies

On s'intéresse à des  $\ell$ -isogénies pour  $\ell$  premier impair.

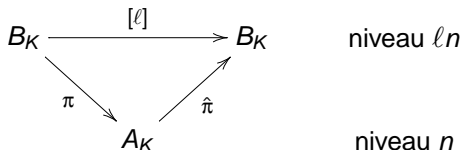
On utilise les fonctions thêta de niveau  $n\ell$  avec  $n = 2$  ou  $4$ .

Pour avoir une  $\ell$ -isogénie, on peut

- oublier des coordonnées (descente de niveau) :

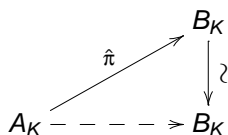
$$\theta \left[ 0, \frac{b}{\ell n} \right] \left( 0, \frac{\Omega}{\ell n} \right) \xrightarrow{\pi} \theta \left[ 0, \frac{b'}{n} \right] \left( 0, \frac{\Omega}{n} \right) = \theta \left[ 0, \frac{b'}{n} \right] \left( 0, \frac{\Omega/\ell}{n} \right)$$

- prendre l'isogénie duale (montée de niveau).



# Diagramme commutatif

Avec les formules de Koizumi, on peut descendre de niveau sans prendre d'isogénie :



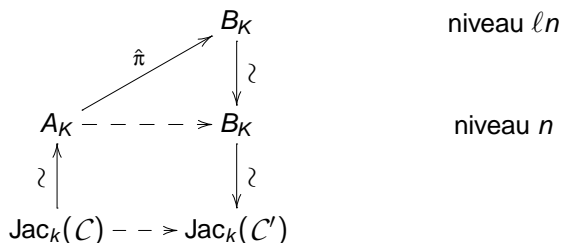
niveau  $ln$

niveau  $n$

## Diagramme commutatif

Avec les formules de Koizumi, on peut descendre de niveau sans prendre d'isogénie .

Attention : pour des courbes définies sur un corps, il faut en général prendre une extension de corps  $K/k$  pour utiliser les thêta constantes.



## Diagramme commutatif

Avec les formules de Koizumi, on peut descendre de niveau sans prendre d'isogénie .

Attention : pour des courbes définies sur un corps, il faut en général prendre une extension de corps  $K/k$  pour utiliser les thêta constantes.

L'isogénie est définie par son noyau  $Ker$ . Il est plus facile de prouver la rationalité de ce dernier du côté de la jacobienne.

$$\begin{array}{ccccc} & & & & B_K & \text{niveau } \ell n \\ & & & \nearrow \hat{\pi} & \downarrow \wr & \\ Ker \hookrightarrow & A_K & \dashrightarrow & B_K & & \text{niveau } n \\ & \uparrow \wr & & \downarrow \wr & & \\ Ker \hookrightarrow & Jac_k(C) & \dashrightarrow & Jac_k(C') & & \end{array}$$

## En pratique

- On utilise  $n = 2$  ou  $4$ .
- On a plusieurs choix de racines à faire.
- La courbe finale  $C'$  est sur  $K/k$  et doit être transformée en une courbe rationnelle sur  $k$ .
- Expression de l'isomorphisme  $\text{Jac}_k(C) \xrightarrow{\sim} A_K$  : OK pour  $g = 1, 2, 3$ .

## En pratique

- On utilise  $n = 2$  ou  $4$ .
- On a plusieurs choix de racines à faire.
- La courbe finale  $C'$  est sur  $K/k$  et doit être transformée en une courbe rationnelle sur  $k$ .
- Expression de l'isomorphisme  $\text{Jac}_k(C) \xrightarrow{\sim} A_K$  : OK pour  $g = 1, 2, 3$ .
- Programme magma : en cours.
- Complexité : calcul de la  $\ell$ -torsion.



# CONCLUSION

# Résultats obtenus

- On obtient des formules à la Thomae pour
  - ▶ Genre 1, niveau quelconque.
  - ▶ Genre 2, niveau quelconque.
  - ▶ Genre  $\geq 3$ , niveau  $(r, r)$  si on connaît le niveau  $(2, 2)$ .
  - ▶ Genre  $\geq 3$ , niveau  $r$  si on connaît le niveau  $(r, r)$ .
  
- On peut prendre des  $\ell$ -isogénies sans changer de niveau.

# Travaux futurs

- Finir de programmer les algorithmes.
- Étudier leur complexité.
  
- Continuer à étudier l'action des sous-groupes  $\mathrm{Sp}(2g)$ .
- Genre  $g \geq 3$ .