Équations aux puissances de modules singuliers

Antonin Riffaut
Institut de Mathématiques de Bordeaux

8 Novembre 2017

Sommaire

Sommaire

Modules singuliers

Soit j la fonction j-invariant classique sur le demi-plan de Poincaré $\mathbb{H} = \{z \in \mathbb{C}\,;\, \operatorname{Im} z > 0\}$. Un *module singulier* est un nombre de la forme $j(\tau)$, avec $\tau \in \mathbb{H}$ un nombre quadratique imaginaire.

Modules singuliers

Soit j la fonction j-invariant classique sur le demi-plan de Poincaré $\mathbb{H} = \{z \in \mathbb{C}\,;\, \operatorname{Im} z > 0\}$. Un *module singulier* est un nombre de la forme $j(\tau)$, avec $\tau \in \mathbb{H}$ un nombre quadratique imaginaire.
Le nombre $j(\tau)$ est un entier algébrique, de degré

$$[\mathbb{Q}(j(\tau) : \mathbb{Q}] = [\mathbb{Q}(\tau, j(\tau)) : \mathbb{Q}(\tau)] = h_\Delta,$$

le nombre de classes de l'ordre quadratique $\mathcal{O}_\Delta = \mathbb{Z}[(\Delta + \sqrt{\Delta})/2]$, où Δ est le discriminant du polynôme minimal de τ sur $\mathbb{Z}$.

Modules singuliers

Soit j la fonction j-invariant classique sur le demi-plan de Poincaré $\mathbb{H} = \{z \in \mathbb{C}\,;\, \operatorname{Im} z > 0\}$. Un *module singulier* est un nombre de la forme $j(\tau)$, avec $\tau \in \mathbb{H}$ un nombre quadratique imaginaire.
Le nombre $j(\tau)$ est un entier algébrique, de degré

$$[\mathbb{Q}(j(\tau) : \mathbb{Q}] = [\mathbb{Q}(\tau, j(\tau)) : \mathbb{Q}(\tau)] = h_\Delta,$$

le nombre de classes de l'ordre quadratique $\mathcal{O}_\Delta = \mathbb{Z}[(\Delta + \sqrt{\Delta})/2]$, où Δ est le discriminant du polynôme minimal de τ sur $\mathbb{Z}$.
De plus, $\mathbb{Q}(\tau, j(\tau))/\mathbb{Q}$ est une extension galoisienne abélienne, dont le groupe de Galois est canoniquement isomorphe au groupe des classes de l'ordre $\mathcal{O}_\Delta$.

Points spéciaux sur les courbes algébriques

Un *point spécial* ou *point de multiplication complexe* de $\mathbb{C}^2$ est un point de la forme $(j(\tau), j(\tau'))$, avec $j(\tau), j(\tau')$ deux modules singuliers.

Points spéciaux sur les courbes algébriques

Un *point spécial* ou *point de multiplication complexe* de $\mathbb{C}^2$ est un point de la forme $(j(\tau), j(\tau'))$, avec $j(\tau), j(\tau')$ deux modules singuliers.
Question : Une courbe irréductible plane de $\mathbb{C}^2$, définie par une équation polynomiale $F(x, y) = 0$, peut-elle contenir une infinité de points spéciaux ?

Points spéciaux sur les courbes algébriques

Un *point spécial* ou *point de multiplication complexe* de $\mathbb{C}^2$ est un point de la forme $(j(\tau), j(\tau'))$, avec $j(\tau), j(\tau')$ deux modules singuliers.
Question : Une courbe irréductible plane de $\mathbb{C}^2$, définie par une équation polynomiale $F(x, y) = 0$, peut-elle contenir une infinité de points spéciaux ?
Réponse :

Théorème (André, 1998)

Seules les *courbes spéciales* contiennent une infinité de points spéciaux.
Les courbes spéciales sont les suivantes :

Points spéciaux sur les courbes algébriques

Un *point spécial* ou *point de multiplication complexe* de $\mathbb{C}^2$ est un point de la forme $(j(\tau), j(\tau'))$, avec $j(\tau), j(\tau')$ deux modules singuliers.
Question : Une courbe irréductible plane de $\mathbb{C}^2$, définie par une équation polynomiale $F(x, y) = 0$, peut-elle contenir une infinité de points spéciaux ?
Réponse :

Théorème (André, 1998)

Seules les *courbes spéciales* contiennent une infinité de points spéciaux.
Les courbes spéciales sont les suivantes :

- les droites verticales $x = j(\tau)$;

Points spéciaux sur les courbes algébriques

Un *point spécial* ou *point de multiplication complexe* de $\mathbb{C}^2$ est un point de la forme $(j(\tau), j(\tau'))$, avec $j(\tau), j(\tau')$ deux modules singuliers.
Question : Une courbe irréductible plane de $\mathbb{C}^2$, définie par une équation polynomiale $F(x, y) = 0$, peut-elle contenir une infinité de points spéciaux ?
Réponse :

Théorème (André, 1998)

Seules les *courbes spéciales* contiennent une infinité de points spéciaux.
Les courbes spéciales sont les suivantes :

- les droites verticales $x = j(\tau)$;
- les droites horizontales $y = j(\tau')$;

Points spéciaux sur les courbes algébriques

Un *point spécial* ou *point de multiplication complexe* de $\mathbb{C}^2$ est un point de la forme $(j(\tau), j(\tau'))$, avec $j(\tau), j(\tau')$ deux modules singuliers.
Question : Une courbe irréductible plane de $\mathbb{C}^2$, définie par une équation polynomiale $F(x, y) = 0$, peut-elle contenir une infinité de points spéciaux ?
Réponse :

Théorème (André, 1998)

Seules les *courbes spéciales* contiennent une infinité de points spéciaux.
Les courbes spéciales sont les suivantes :

- les droites verticales $x = j(\tau)$;
- les droites horizontales $y = j(\tau')$;
- les *courbes modulaires* $Y_0(N)$ $(N > 0)$, d'équation $\Phi_N(x, y) = 0$, où Φ_N est le polynôme modulaire classique de niveau N.

Points spéciaux sur les courbes algébriques

Problématique : "Caractériser" les points spéciaux sur des familles de courbes données.

Points spéciaux sur les courbes algébriques

Problématique : "Caractériser" les points spéciaux sur des familles de courbes données.
On note $(x, y) = (j(\tau), j(\tau'))$. **État de l'art** :

Points spéciaux sur les courbes algébriques

Problématique : "Caractériser" les points spéciaux sur des familles de courbes données.
On note $(x, y) = (j(\tau), j(\tau'))$. **État de l'art** :

- Kühne (2013) : l'équation $x + y = 1$ n'a pas de solution.

Points spéciaux sur les courbes algébriques

Problématique : "Caractériser" les points spéciaux sur des familles de courbes données.
On note $(x, y) = (j(\tau), j(\tau'))$. **État de l'art** :

- Kühne (2013) : l'équation $x + y = 1$ n'a pas de solution.
- Bilu, Masser, Zannier (2013) : l'équation $xy = 1$ n'a pas de solution.

Points spéciaux sur les courbes algébriques

Problématique : "Caractériser" les points spéciaux sur des familles de courbes données.
On note $(x, y) = (j(\tau), j(\tau'))$. **État de l'art** :

- Kühne (2013) : l'équation $x + y = 1$ n'a pas de solution.
- Bilu, Masser, Zannier (2013) : l'équation $xy = 1$ n'a pas de solution.
- Allombert, Bilu, Pizarro-Madariaga (2015) : si (x, y) appartient à une droite non spéciale d'équation $Ax + By = C$, alors soit $x, y \in \mathbb{Q}$, soit $x \neq y$ et x et y engendrent le même corps de nombres de degré 2 sur $\mathbb{Q}$.

Points spéciaux sur les courbes algébriques

Problématique : "Caractériser" les points spéciaux sur des familles de courbes données.
On note $(x, y) = (j(\tau), j(\tau'))$. **État de l'art** :

- Kühne (2013) : l'équation $x + y = 1$ n'a pas de solution.
- Bilu, Masser, Zannier (2013) : l'équation $xy = 1$ n'a pas de solution.
- Allombert, Bilu, Pizarro-Madariaga (2015) : si (x, y) appartient à une droite non spéciale d'équation $Ax + By = C$, alors soit $x, y \in \mathbb{Q}$, soit $x \neq y$ et x et y engendrent le même corps de nombres de degré 2 sur $\mathbb{Q}$.
- Bilu, Luca, Pizarro-Madariaga (2016) : si $xy = A \in \mathbb{Q}^\times$, alors soit $x, y \in \mathbb{Q}^\times$, soit x et y sont de degré 2 et conjugués sur $\mathbb{Q}$.

Indépendance linéaire de modules singuliers

Généralisation du résultat d'Allombert, Bilu et Pizarro-Madariaga :

Théorème d'"indépendance linéaire"

Soient x, y deux modules singuliers *distincts* de discriminants respectifs Δ, Δ', et m, n deux entiers strictement positifs. Supposons que $Ax^m + By^n = C$, pour $A, B, C \in \mathbb{Q}^\times$. Alors x et y engendrent le même corps de nombres de degré $h \leq 3$ sur $\mathbb{Q}$. De plus, si $h = 3$, alors soit $\{\Delta, \Delta'\} = \{-23, -4 \cdot 23\}$, soit $\{\Delta, \Delta'\} = \{-31, -4 \cdot 31\}$.

Indépendance multiplicative de modules singuliers

Généralisation du résultat de Bilu, Luca et Pizarro-Madariaga :

Théorème d'"indépendance multiplicative"

Soient x, y deux modules singuliers non nuls, et m, n deux entiers relatifs non nuls. Supposons que $x^m y^n \in \mathbb{Q}^\times$. Alors l'une des assertions suivantes est vérifiée :

Indépendance multiplicative de modules singuliers

Généralisation du résultat de Bilu, Luca et Pizarro-Madariaga :

Théorème d'"indépendance multiplicative"

Soient x, y deux modules singuliers non nuls, et m, n deux entiers relatifs non nuls. Supposons que $x^m y^n \in \mathbb{Q}^\times$. Alors l'une des assertions suivantes est vérifiée :

(i) $x = y$ et $m + n = 0$;

Indépendance multiplicative de modules singuliers

Généralisation du résultat de Bilu, Luca et Pizarro-Madariaga :

Théorème d'"indépendance multiplicative"

Soient x, y deux modules singuliers non nuls, et m, n deux entiers relatifs non nuls. Supposons que $x^m y^n \in \mathbb{Q}^\times$. Alors l'une des assertions suivantes est vérifiée :

(i) $x = y$ et $m + n = 0$;

(ii) $x, y \in \mathbb{Q}^\times$;

Indépendance multiplicative de modules singuliers

Généralisation du résultat de Bilu, Luca et Pizarro-Madariaga :

Théorème d'"indépendance multiplicative"

Soient x, y deux modules singuliers non nuls, et m, n deux entiers relatifs non nuls. Supposons que $x^m y^n \in \mathbb{Q}^\times$. Alors l'une des assertions suivantes est vérifiée :

(i) $x = y$ et $m + n = 0$;

(ii) $x, y \in \mathbb{Q}^\times$;

(iii) $m = n$ et x et y sont de degré 2 et conjugués sur $\mathbb{Q}$.

Sommaire

Sommaire

Domaine fondamental de l'action de $\mathrm{SL}(2,\mathbb{Z})$ sur $\mathbb{H}$

Soit $\mathcal{D}$ le domaine fondamental standard de l'action de $\mathrm{SL}(2,\mathbb{Z})$ sur $\mathbb{H}$.

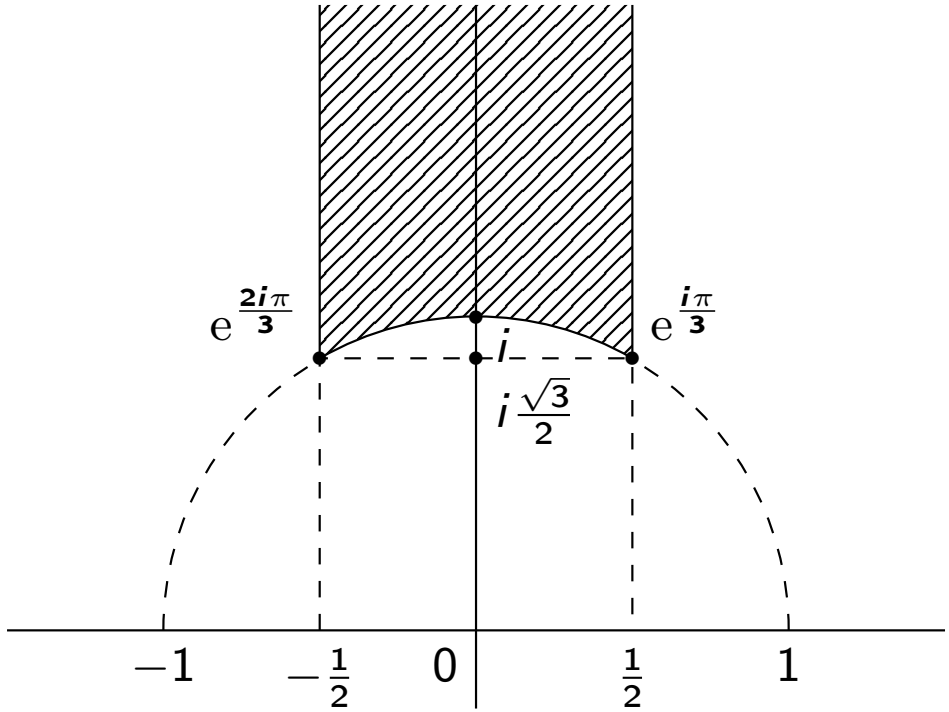

Figure : Domaine fondamental $\mathcal{D}$

La fonction j est $\mathrm{SL}(2,\mathbb{Z})$-invariante, on peut donc la restreindre au domaine $\mathcal{D}$.

Estimations de la fonction j

La fonction j se développe en série de Fourier :

$$j(\tau) = q^{-1} + 744 + 196884q + 21493760q^2 + \ldots, \quad q = q(\tau) = \mathrm{e}^{2i\pi\tau}.$$

Estimations de la fonction j

La fonction j se développe en série de Fourier :

$$j(\tau) = q^{-1} + 744 + 196884q + 21493760q^2 + \ldots, \quad q = q(\tau) = \mathrm{e}^{2i\pi\tau}.$$

On en déduit :

Lemme

Pour $\tau \in \mathcal{D}$, on a

$$\left| |j(\tau)| - |q|^{-1} \right| \leq 2079.$$

Estimations de la fonction j

La fonction j se développe en série de Fourier :

$$j(\tau) = q^{-1} + 744 + 196884q + 21493760q^2 + \ldots, \quad q = q(\tau) = \mathrm{e}^{2i\pi\tau}.$$

On en déduit :

Lemme

Pour $\tau \in \mathcal{D}$, on a

$$\big||j(\tau)| - |q|^{-1}\big| \leq 2079.$$

Lemme

Pour $\tau \in \mathcal{D} \setminus \{\mathrm{e}^{i\pi/3}, \mathrm{e}^{2i\pi/3}\}$, on a

$$|j(\tau)| = |q|^{-1}\mathrm{e}^{v(q)},$$

où $v(q)$ est un nombre réel satisfaisant $|v(q)| \leq 2883|q|$ dès lors que $\operatorname{Im}\tau \geq \log 4158/2\pi \approx 1.326$. Si, de plus, $\operatorname{Im}\tau \geq \log 5766/2\pi \approx 1.378$, alors $|v(q)| \leq 1/2$.

Sommaire

Les conjugués de $j(\tau)$

Soit $j(\tau)$ un module singulier de discriminant Δ et de degré h sur $\mathbb{Q}$. Soit T_Δ l'ensemble des triplets d'entiers (a, b, c) tels que

$$\begin{cases} \gcd(a, b, c) = 1, \\ \Delta = b^2 - 4ac, \\ -a < b \leq a < c \quad \text{ou} \quad 0 \leq b \leq a = c. \end{cases}$$

Les conjugués de $j(\tau)$

Soit $j(\tau)$ un module singulier de discriminant Δ et de degré h sur $\mathbb{Q}$. Soit T_Δ l'ensemble des triplets d'entiers (a, b, c) tels que

$$\begin{cases} \gcd(a, b, c) = 1, \\ \Delta = b^2 - 4ac, \\ -a < b \leq a < c \quad \text{ou} \quad 0 \leq b \leq a = c. \end{cases}$$

Les conjugués de $j(\tau)$ sur $\mathbb{Q}$ sont exactement les

$$j\left(\frac{-b + \sqrt{\Delta}}{2a}\right), \quad (a, b, c) \in T_\Delta.$$

En particulier, $|T_\Delta| = h$.

Les conjugués de $j(\tau)$

Soit $j(\tau)$ un module singulier de discriminant Δ et de degré h sur $\mathbb{Q}$. Soit T_Δ l'ensemble des triplets d'entiers (a, b, c) tels que

$$\begin{cases} \gcd(a, b, c) = 1, \\ \Delta = b^2 - 4ac, \\ -a < b \leq a < c \quad \text{ou} \quad 0 \leq b \leq a = c. \end{cases}$$

Les conjugués de $j(\tau)$ sur $\mathbb{Q}$ sont exactement les

$$j\left(\frac{-b + \sqrt{\Delta}}{2a}\right), \quad (a, b, c) \in T_\Delta.$$

En particulier, $|T_\Delta| = h$.

Remarque : $\frac{-b+\sqrt{\Delta}}{2a} \in \mathcal{D}$.

j-valeur dominante

Dans l'ensemble T_Δ, il existe exactement un triplet $(a, b, c) = 1$, donné explicitement par

$$\left(1, r_4(\Delta), \frac{r_4(\Delta) - \Delta}{4}\right),$$

où $r_4(\Delta) \in \{0, 1\}$ est défini par $\Delta \equiv r_4(\Delta) \bmod 4$.

j-valeur dominante

Dans l'ensemble T_Δ, il existe exactement un triplet $(a, b, c) = 1$, donné explicitement par

$$\left(1, r_4(\Delta), \frac{r_4(\Delta) - \Delta}{4}\right),$$

où $r_4(\Delta) \in \{0, 1\}$ est défini par $\Delta \equiv r_4(\Delta) \bmod 4$. Le conjugué correspondant de $j(\tau)$,

$$J_\Delta = j\left(\frac{-r_4(\Delta) + \sqrt{\Delta}}{2}\right),$$

s'appelle la *j-valeur dominante* de discriminant Δ :

j-valeur dominante

Dans l'ensemble T_Δ, il existe exactement un triplet $(a, b, c) = 1$, donné explicitement par

$$\left(1, r_4(\Delta), \frac{r_4(\Delta) - \Delta}{4}\right),$$

où $r_4(\Delta) \in \{0, 1\}$ est défini par $\Delta \equiv r_4(\Delta) \bmod 4$. Le conjugué correspondant de $j(\tau)$,

$$J_\Delta = j\left(\frac{-r_4(\Delta) + \sqrt{\Delta}}{2}\right),$$

s'appelle la *j-valeur dominante* de discriminant Δ : pour tout conjugué $J_\Delta^\sigma \neq J_\Delta$ avec $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, $|J_\Delta^\sigma| \leq 0.1|J_\Delta|$.

j-valeur dominante

Dans l'ensemble T_Δ, il existe exactement un triplet $(a, b, c) = 1$, donné explicitement par

$$\left(1, r_4(\Delta), \frac{r_4(\Delta) - \Delta}{4}\right),$$

où $r_4(\Delta) \in \{0, 1\}$ est défini par $\Delta \equiv r_4(\Delta) \bmod 4$. Le conjugué correspondant de $j(\tau)$,

$$J_\Delta = j\left(\frac{-r_4(\Delta) + \sqrt{\Delta}}{2}\right),$$

s'appelle la *j-valeur dominante* de discriminant Δ : pour tout conjugué $J_\Delta^\sigma \neq J_\Delta$ avec $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, $|J_\Delta^\sigma| \leq 0.1|J_\Delta|$.
Conséquence : $\mathbb{Q}(j(\tau)^n) = \mathbb{Q}(j(\tau))$, pour tout $n \neq 0$.

Autres éléments explicites de l'ensemble T_Δ

Si $\Delta \equiv 1 \bmod 8$, alors pour tout entier $r \geq 1$, l'ensemble T_Δ possède exactement deux triplets (a, b, c) avec $a = 2^r$ pourvu que $|\Delta|$ soit assez grand.

Autres éléments explicites de l'ensemble T_Δ

Si $\Delta \equiv 1 \bmod 8$, alors pour tout entier $r \geq 1$, l'ensemble T_Δ possède exactement deux triplets (a, b, c) avec $a = 2^r$ pourvu que $|\Delta|$ soit assez grand.
Plus précisément, si $|\Delta| \geq 239$, alors T_Δ possède exactement deux triplets (a, b, c) pour chaque $a \in \{2, 4, 8\}$.

Autres éléments explicites de l'ensemble T_Δ

Si $\Delta \equiv 1 \bmod 8$, alors pour tout entier $r \geq 1$, l'ensemble T_Δ possède exactement deux triplets (a, b, c) avec $a = 2^r$ pourvu que $|\Delta|$ soit assez grand.
Plus précisément, si $|\Delta| \geq 239$, alors T_Δ possède exactement deux triplets (a, b, c) pour chaque $a \in \{2, 4, 8\}$.
En général, T_Δ possède au plus deux triplets (a, b, c) avec $a = 2$.

Sommaire

La courbe modulaire $Y_0(N)$

Soit N un entier naturel non nul. La *courbe modulaire classique* de niveau N, notée $Y_0(N)$, est la courbe algébrique correspondant au quotient de $\mathbb{H}$ par l'action du sous-groupe de congruence

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) \,;\, c \equiv 0 \bmod N \right\}$$

de $\mathrm{SL}(2,\mathbb{Z})$.

La courbe modulaire $Y_0(N)$

Soit N un entier naturel non nul. La *courbe modulaire classique* de niveau N, notée $Y_0(N)$, est la courbe algébrique correspondant au quotient de $\mathbb{H}$ par l'action du sous-groupe de congruence

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) \,;\, c \equiv 0 \bmod N \right\}$$

de $\mathrm{SL}(2,\mathbb{Z})$. Elle peut être réalisée comme une courbe algébrique de $\mathbb{C}^2$ d'équation $\Phi_N(x,y) = 0$, où Φ_N est le *polynôme modulaire classique* de niveau N.

La courbe modulaire $Y_0(N)$

Soit N un entier naturel non nul. La *courbe modulaire classique* de niveau N, notée $Y_0(N)$, est la courbe algébrique correspondant au quotient de $\mathbb{H}$ par l'action du sous-groupe de congruence

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) \,;\, c \equiv 0 \bmod N \right\}$$

de $\mathrm{SL}(2,\mathbb{Z})$. Elle peut être réalisée comme une courbe algébrique de $\mathbb{C}^2$ d'équation $\Phi_N(x,y) = 0$, où Φ_N est le *polynôme modulaire classique* de niveau N.
Le polynôme Φ_N est symétrique et vérifie

$$\forall \tau \in \mathbb{H},\ \Phi_N(j(\tau), j(N\tau)) = 0.$$

Description de Φ_N et le cas particulier $N = 2$

Pour $\tau \in \mathbb{H}$, on a

$$\Phi_N(X, j(\tau)) = \prod_{\sigma \in C(N)} (X - j(\sigma\tau)),$$

où

$$C(N) = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \; ; \; ad = N,\ a > 0,\ 0 \leq b < d,\ \gcd(a, b, d) = 1 \right\}.$$

Description de Φ_N et le cas particulier $N = 2$

Pour $\tau \in \mathbb{H}$, on a

$$\Phi_N(X, j(\tau)) = \prod_{\sigma \in C(N)} (X - j(\sigma\tau)),$$

où

$$C(N) = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \; ; \; ad = N,\ a > 0,\ 0 \leq b < d,\ \gcd(a, b, d) = 1 \right\}.$$

En particulier, pour $N = 2$,

$$C(2) = \left\{ \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} \right\},$$

Description de Φ_N et le cas particulier $N = 2$

Pour $\tau \in \mathbb{H}$, on a

$$\Phi_N(X, j(\tau)) = \prod_{\sigma \in C(N)} (X - j(\sigma\tau)),$$

où

$$C(N) = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \; ; \; ad = N,\ a > 0,\ 0 \leq b < d,\ \gcd(a, b, d) = 1 \right\}.$$

En particulier, pour $N = 2$,

$$C(2) = \left\{ \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} \right\},$$

et donc

$$\Phi_2(X, j(\tau)) = (X - j(2\tau)) \left(X - j\left(\frac{\tau}{2}\right)\right) \left(X - j\left(\frac{\tau + 1}{2}\right)\right).$$

Description de Φ_N et le cas particulier $N = 2$

Pour $\tau \in \mathbb{H}$, on a

$$\Phi_N(X, j(\tau)) = \prod_{\sigma \in C(N)} (X - j(\sigma\tau)),$$

où

$$C(N) = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \; ; \; ad = N,\ a > 0,\ 0 \leq b < d,\ \gcd(a, b, d) = 1 \right\}.$$

En particulier, pour $N = 2$,

$$C(2) = \left\{ \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} \right\},$$

et donc

$$\Phi_2(X, j(\tau)) = (X - j(2\tau)) \left(X - j\left(\frac{\tau}{2}\right)\right) \left(X - j\left(\frac{\tau + 1}{2}\right)\right).$$

Cela permet de déterminer facilement si un point spécial $(j(\tau), j(\tau'))$ appartient à $Y_0(2)$.

Sommaire

Sommaire

Réduction

Soient $x = j(\tau), y = j(\tau')$ deux modules singuliers distincts, de discriminants respectifs Δ, Δ' et de degrés ≥ 3 sur $\mathbb{Q}$, satisfaisant

$$Ax^m + By^n = C,$$

pour $m, n \in \mathbb{N}^*$ et $A, B, C \in \mathbb{Q}^\times$.

Réduction

Soient $x = j(\tau), y = j(\tau')$ deux modules singuliers distincts, de discriminants respectifs Δ, Δ' et de degrés ≥ 3 sur $\mathbb{Q}$, satisfaisant

$$Ax^m + By^n = C,$$

pour $m, n \in \mathbb{N}^*$ et $A, B, C \in \mathbb{Q}^\times$.

- $\mathbb{Q}(x^m) = \mathbb{Q}(y^n)$, donc $\mathbb{Q}(x) = \mathbb{Q}(y)$.

Réduction

Soient $x = j(\tau), y = j(\tau')$ deux modules singuliers distincts, de discriminants respectifs Δ, Δ' et de degrés ≥ 3 sur $\mathbb{Q}$, satisfaisant

$$Ax^m + By^n = C,$$

pour $m, n \in \mathbb{N}^*$ et $A, B, C \in \mathbb{Q}^\times$.

- $\mathbb{Q}(x^m) = \mathbb{Q}(y^n)$, donc $\mathbb{Q}(x) = \mathbb{Q}(y)$.
- On peut supposer que x et y sont simultanément dominants.

Réduction

Soient $x = j(\tau), y = j(\tau')$ deux modules singuliers distincts, de discriminants respectifs Δ, Δ' et de degrés ≥ 3 sur $\mathbb{Q}$, satisfaisant

$$Ax^m + By^n = C,$$

pour $m, n \in \mathbb{N}^*$ et $A, B, C \in \mathbb{Q}^\times$.

- $\mathbb{Q}(x^m) = \mathbb{Q}(y^n)$, donc $\mathbb{Q}(x) = \mathbb{Q}(y)$.
- On peut supposer que x et y sont simultanément dominants.
- Si $\mathbb{Q}(\tau) \neq \mathbb{Q}(\tau')$, on connait tous les couples (Δ, Δ') possibles.

Réduction

Soient $x = j(\tau), y = j(\tau')$ deux modules singuliers distincts, de discriminants respectifs Δ, Δ' et de degrés ≥ 3 sur $\mathbb{Q}$, satisfaisant

$$Ax^m + By^n = C,$$

pour $m, n \in \mathbb{N}^*$ et $A, B, C \in \mathbb{Q}^\times$.

- $\mathbb{Q}(x^m) = \mathbb{Q}(y^n)$, donc $\mathbb{Q}(x) = \mathbb{Q}(y)$.
- On peut supposer que x et y sont simultanément dominants.
- Si $\mathbb{Q}(\tau) \neq \mathbb{Q}(\tau')$, on connait tous les couples (Δ, Δ') possibles.
- Si $\mathbb{Q}(\tau) = \mathbb{Q}(\tau')$, on peut supposer que $\Delta = 4\Delta'$, et on peut choisir

$$\tau = \sqrt{\Delta'} \quad \text{et} \quad \tau' = \frac{-r_4(\Delta') + \sqrt{\Delta'}}{2}.$$

Réduction

Soient $x = j(\tau), y = j(\tau')$ deux modules singuliers distincts, de discriminants respectifs Δ, Δ' et de degrés ≥ 3 sur $\mathbb{Q}$, satisfaisant

$$Ax^m + By^n = C,$$

pour $m, n \in \mathbb{N}^*$ et $A, B, C \in \mathbb{Q}^\times$.

- $\mathbb{Q}(x^m) = \mathbb{Q}(y^n)$, donc $\mathbb{Q}(x) = \mathbb{Q}(y)$.
- On peut supposer que x et y sont simultanément dominants.
- Si $\mathbb{Q}(\tau) \neq \mathbb{Q}(\tau')$, on connait tous les couples (Δ, Δ') possibles.
- Si $\mathbb{Q}(\tau) = \mathbb{Q}(\tau')$, on peut supposer que $\Delta = 4\Delta'$, et on peut choisir

$$\tau = \sqrt{\Delta'} \quad \text{et} \quad \tau' = \frac{-r_4(\Delta') + \sqrt{\Delta'}}{2}.$$

On observe alors que $(x, y) \in Y_0(2)$. De plus, $\Delta' \equiv 1 \bmod 8$.

Sommaire

Éliminer les grands discriminants

Pour $|\Delta'| \geq 1024$, le point spécial (x, y) admet 4 conjugués (x_i, y_i) sur $\mathbb{Q}$ de la forme suivante :

i	x_i	y_i
1	$j(\sqrt{\Delta'})$	$j\left(\frac{-1+\sqrt{\Delta'}}{2}\right)$
2	$j\left(* + \frac{\sqrt{\Delta'}}{8}\right)$	$j\left(\frac{-1+\sqrt{\Delta'}}{4}\right)$
3	$j\left(* + \frac{\sqrt{\Delta'}}{16}\right)$	$j\left(* + \frac{\sqrt{\Delta'}}{8}\right)$
4	$j\left(* + \frac{\sqrt{\Delta'}}{32}\right)$	$j\left(* + \frac{\sqrt{\Delta'}}{16}\right)$.

Éliminer les grands discriminants

Pour $|\Delta'| \geq 1024$, le point spécial (x, y) admet 4 conjugués (x_i, y_i) sur $\mathbb{Q}$ de la forme suivante :

i	x_i	y_i
1	$j(\sqrt{\Delta'})$	$j\left(\frac{-1+\sqrt{\Delta'}}{2}\right)$
2	$j\left(* + \frac{\sqrt{\Delta'}}{8}\right)$	$j\left(\frac{-1+\sqrt{\Delta'}}{4}\right)$
3	$j\left(* + \frac{\sqrt{\Delta'}}{16}\right)$	$j\left(* + \frac{\sqrt{\Delta'}}{8}\right)$
4	$j\left(* + \frac{\sqrt{\Delta'}}{32}\right)$	$j\left(* + \frac{\sqrt{\Delta'}}{16}\right)$.

Pour $i, j \in \{2, 3, 4\}$, $i < j$, la colinéarité des points $(x_1^m, y_1^n), (x_i^m, y_i^n)$ et (x_j^m, y_j^n) se traduit par

$$\left(\frac{x_1}{x_i}\right)^m \left(\frac{y_1}{y_i}\right)^{-n} - 1 = \frac{\left(\frac{y_j}{y_i}\right)^n + \left(\frac{x_j}{x_1}\right)^m - \left(\frac{y_j}{y_1}\right)^n - \left(\frac{x_j}{x_i}\right)^m}{1 - \left(\frac{y_j}{y_i}\right)^n - \left(\frac{x_j}{x_1}\right)^m}.$$

Éliminer les grands discriminants

On en déduit que $\left| \left(\frac{x_1}{x_i}\right)^m \left(\frac{y_1}{y_i}\right)^{-n} - 1 \right|$ est proche de 0, ce qui permet d'encadrer le quotient m/n.

Éliminer les grands discriminants

On en déduit que $\left| \left(\frac{x_1}{x_i}\right)^m \left(\frac{y_1}{y_i}\right)^{-n} - 1 \right|$ est proche de 0, ce qui permet d'encadrer le quotient m/n.
Numériquement :

Éliminer les grands discriminants

On en déduit que $\left| \left(\frac{x_1}{x_i}\right)^m \left(\frac{y_1}{y_i}\right)^{-n} - 1 \right|$ est proche de 0, ce qui permet d'encadrer le quotient m/n.
Numériquement :

- pour $(i,j) = (2,3)$, on obtient

$$0.279 \leq \frac{m}{n} \leq 0.294;$$

Éliminer les grands discriminants

On en déduit que $\left| \left(\frac{x_1}{x_i}\right)^m \left(\frac{y_1}{y_i}\right)^{-n} - 1 \right|$ est proche de 0, ce qui permet d'encadrer le quotient m/n.
Numériquement :

- pour $(i,j) = (2,3)$, on obtient

$$0.279 \leq \frac{m}{n} \leq 0.294;$$

- pour $(i,j) = (3,4)$, on obtient

$$0.392 \leq \frac{m}{n} \leq 0.409.$$

Éliminer les grands discriminants

On en déduit que $\left| \left(\frac{x_1}{x_i}\right)^m \left(\frac{y_1}{y_i}\right)^{-n} - 1 \right|$ est proche de 0, ce qui permet d'encadrer le quotient m/n.
Numériquement :

- pour $(i,j) = (2,3)$, on obtient

$$0.279 \leq \frac{m}{n} \leq 0.294;$$

- pour $(i,j) = (3,4)$, on obtient

$$0.392 \leq \frac{m}{n} \leq 0.409.$$

Les deux encadrements se contredisent, si bien que $|\Delta'| \geq 1024$ est impossible.

Éliminer les petits discriminants

Désormais, on suppose que $|\Delta'| < 1024$.

Éliminer les petits discriminants

Désormais, on suppose que $|\Delta'| < 1024$.
Pour chaque Δ', on peut déterminer et calculer explicitement tous les conjugués (x_i, y_i) de (x, y) sur $\mathbb{Q}$, et exploiter comme précédemment la colinéarité des points (x_i^m, y_i^n) pour encadrer m/n. Cela permet d'éliminer tous les discriminants Δ' sauf $-23, -31, -39, -47, -55, -63, -79, -103, -127$.

Éliminer les petits discriminants

Désormais, on suppose que $|\Delta'| < 1024$.
Pour chaque Δ', on peut déterminer et calculer explicitement tous les conjugués (x_i, y_i) de (x, y) sur $\mathbb{Q}$, et exploiter comme précédemment la colinéarité des points (x_i^m, y_i^n) pour encadrer m/n. Cela permet d'éliminer tous les discriminants Δ' sauf $-23, -31, -39, -47, -55, -63, -79, -103, -127$.
Pour tous ces discriminants, excepté -23 et -31, le point (x, y) admet exactement 3 conjugués (x_i, y_i) avec $|x_1| > |x_2| > |x_3|$. On peut alors encadrer m/n et calculer deux constantes c_1, c_2 telles que

$$|\alpha^m \beta^{-n} + (-1)^\varepsilon| \leq c_1 \cdot c_2^n,$$

avec $\alpha = x_1/x_2$ et

$$(\beta, \varepsilon) = \begin{cases} (y_1/y_2, 1) & \text{si } |y_2| > |y_3|, \\ (y_2/y_3, 0) & \text{si } |y_2| < |y_3|. \end{cases}$$

Éliminer les petits discriminants

On utilise alors les estimations connues sur les formes linéaires logarithmiques (Matveev, 2000) pour en déduire une majoration de n (et donc de m également).

Éliminer les petits discriminants

On utilise alors les estimations connues sur les formes linéaires logarithmiques (Matveev, 2000) pour en déduire une majoration de n (et donc de m également).
En remarquant de plus que

$$\left|\theta - \frac{m}{n}\right| \leq \frac{c_1' \cdot c_2^n}{n \log |\alpha|},$$

avec $\theta = \log|\beta| / \log|\alpha|$ et $c_1' > 0$, on en déduit qu'en écrivant m/n sous forme irréductible p/q, la fraction p/q est une réduite du développement en fraction continue de θ.

Éliminer les petits discriminants

On utilise alors les estimations connues sur les formes linéaires logarithmiques (Matveev, 2000) pour en déduire une majoration de n (et donc de m également).
En remarquant de plus que

$$\left|\theta - \frac{m}{n}\right| \leq \frac{c_1' \cdot c_2^n}{n \log |\alpha|},$$

avec $\theta = \log|\beta| / \log|\alpha|$ et $c_1' > 0$, on en déduit qu'en écrivant m/n sous forme irréductible p/q, la fraction p/q est une réduite du développement en fraction continue de θ.
On peut donc énumérer tous les couples (p, q) possibles et vérifier par un calcul que l'estimation précédente est erronée pour chacun de ces couples.

Sommaire

Le cas $\mathbb{Q}(\tau) \neq \mathbb{Q}(\tau')$

Tous les couples (Δ, Δ') sont donnés par le tableau suivant.

Table : Corps L tels que $L = \mathbb{Q}(j(\tau)) = \mathbb{Q}(j(\tau'))$ et $\mathbb{Q}(\tau) \neq \mathbb{Q}(\tau')$

Corps L	$[L : \mathbb{Q}]$	Δ
$\mathbb{Q}$	1	$-3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163$
$\mathbb{Q}(\sqrt{2})$	2	$-24, -32, -64, -88$
$\mathbb{Q}(\sqrt{3})$	2	$-36, -48$
$\mathbb{Q}(\sqrt{5})$	2	$-15, -20, -35, -40, -60, -75, -100, -115, -235$
$\mathbb{Q}(\sqrt{13})$	2	$-52, -91, -403$
$\mathbb{Q}(\sqrt{17})$	2	$-51, -187$
$\mathbb{Q}(\sqrt{2}, \sqrt{3})$	4	$-96, -192, -288$
$\mathbb{Q}(\sqrt{3}, \sqrt{5})$	4	$-180, -240$
$\mathbb{Q}(\sqrt{5}, \sqrt{13})$	4	$-195, -520, -715$
$\mathbb{Q}(\sqrt{2}, \sqrt{5})$	4	$-120, -160, -280, -760$
$\mathbb{Q}(\sqrt{5}, \sqrt{17})$	4	$-340, -595$
$\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$	8	$-480, -960$

Le cas $\mathbb{Q}(\tau) \neq \mathbb{Q}(\tau')$

Tous les couples (Δ, Δ') sont donnés par le tableau suivant.

Table : Corps L tels que $L = \mathbb{Q}(j(\tau)) = \mathbb{Q}(j(\tau'))$ et $\mathbb{Q}(\tau) \neq \mathbb{Q}(\tau')$

Corps L	$[L : \mathbb{Q}]$	Δ
$\mathbb{Q}$	1	$-3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163$
$\mathbb{Q}(\sqrt{2})$	2	$-24, -32, -64, -88$
$\mathbb{Q}(\sqrt{3})$	2	$-36, -48$
$\mathbb{Q}(\sqrt{5})$	2	$-15, -20, -35, -40, -60, -75, -100, -115, -235$
$\mathbb{Q}(\sqrt{13})$	2	$-52, -91, -403$
$\mathbb{Q}(\sqrt{17})$	2	$-51, -187$
$\mathbb{Q}(\sqrt{2}, \sqrt{3})$	4	$-96, -192, -288$
$\mathbb{Q}(\sqrt{3}, \sqrt{5})$	4	$-180, -240$
$\mathbb{Q}(\sqrt{5}, \sqrt{13})$	4	$-195, -520, -715$
$\mathbb{Q}(\sqrt{2}, \sqrt{5})$	4	$-120, -160, -280, -760$
$\mathbb{Q}(\sqrt{5}, \sqrt{17})$	4	$-340, -595$
$\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$	8	$-480, -960$

On élimine chaque couple possible comme précédemment.

Sommaire

Idée de la démonstration

Soient $x = j(\tau), y = j(\tau')$ deux modules singuliers, de discriminants respectifs Δ, Δ', satisfaisant $x^m y^n = A$ pour $m, n \in \mathbb{Z}^*$ et $A \in \mathbb{Q}^\times$.

Idée de la démonstration

Soient $x = j(\tau), y = j(\tau')$ deux modules singuliers, de discriminants respectifs Δ, Δ', satisfaisant $x^m y^n = A$ pour $m, n \in \mathbb{Z}^*$ et $A \in \mathbb{Q}^\times$.

- $\mathbb{Q}(x^m) = \mathbb{Q}(y^n)$, donc $\mathbb{Q}(x) = \mathbb{Q}(y)$.

Idée de la démonstration

Soient $x = j(\tau), y = j(\tau')$ deux modules singuliers, de discriminants respectifs Δ, Δ', satisfaisant $x^m y^n = A$ pour $m, n \in \mathbb{Z}^*$ et $A \in \mathbb{Q}^\times$.

- $\mathbb{Q}(x^m) = \mathbb{Q}(y^n)$, donc $\mathbb{Q}(x) = \mathbb{Q}(y)$.
- Si $mn < 0$, par exemple $m > 0$ et $n < 0$, on a $x^m - Ay^{-n} = 0$. Les arguments de la précédente preuve peuvent être réutilisés pour réduire à un nombre fini de couples (Δ, Δ') à examiner.

Idée de la démonstration

Soient $x = j(\tau), y = j(\tau')$ deux modules singuliers, de discriminants respectifs Δ, Δ', satisfaisant $x^m y^n = A$ pour $m, n \in \mathbb{Z}^*$ et $A \in \mathbb{Q}^\times$.

- $\mathbb{Q}(x^m) = \mathbb{Q}(y^n)$, donc $\mathbb{Q}(x) = \mathbb{Q}(y)$.
- Si $mn < 0$, par exemple $m > 0$ et $n < 0$, on a $x^m - Ay^{-n} = 0$. Les arguments de la précédente preuve peuvent être réutilisés pour réduire à un nombre fini de couples (Δ, Δ') à examiner.
- Si $mn > 0$, on encadre A en explicitant des conjugués de (x, y) sur $\mathbb{Q}$. Cela permet à nouveau de réduire à un nombre fini de couples (Δ, Δ') à examiner.

Idée de la démonstration

Soient $x = j(\tau), y = j(\tau')$ deux modules singuliers, de discriminants respectifs Δ, Δ', satisfaisant $x^m y^n = A$ pour $m, n \in \mathbb{Z}^*$ et $A \in \mathbb{Q}^\times$.

- $\mathbb{Q}(x^m) = \mathbb{Q}(y^n)$, donc $\mathbb{Q}(x) = \mathbb{Q}(y)$.
- Si $mn < 0$, par exemple $m > 0$ et $n < 0$, on a $x^m - Ay^{-n} = 0$. Les arguments de la précédente preuve peuvent être réutilisés pour réduire à un nombre fini de couples (Δ, Δ') à examiner.
- Si $mn > 0$, on encadre A en explicitant des conjugués de (x, y) sur $\mathbb{Q}$. Cela permet à nouveau de réduire à un nombre fini de couples (Δ, Δ') à examiner.
- Pour éliminer les cas particuliers : pour $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, on a

$$\left(\frac{x}{x^\sigma}\right)^m = \left(\frac{y^\sigma}{y}\right)^n.$$

Idée de la démonstration

Soient $x = j(\tau), y = j(\tau')$ deux modules singuliers, de discriminants respectifs Δ, Δ', satisfaisant $x^m y^n = A$ pour $m, n \in \mathbb{Z}^*$ et $A \in \mathbb{Q}^\times$.

- $\mathbb{Q}(x^m) = \mathbb{Q}(y^n)$, donc $\mathbb{Q}(x) = \mathbb{Q}(y)$.
- Si $mn < 0$, par exemple $m > 0$ et $n < 0$, on a $x^m - Ay^{-n} = 0$. Les arguments de la précédente preuve peuvent être réutilisés pour réduire à un nombre fini de couples (Δ, Δ') à examiner.
- Si $mn > 0$, on encadre A en explicitant des conjugués de (x, y) sur $\mathbb{Q}$. Cela permet à nouveau de réduire à un nombre fini de couples (Δ, Δ') à examiner.
- Pour éliminer les cas particuliers : pour $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, on a

$$\left(\frac{x}{x^\sigma}\right)^m = \left(\frac{y^\sigma}{y}\right)^n.$$

On démontre alors algorithmiquement que x/x^σ et y/y^σ sont multiplicativement indépendants pour un σ adéquat.

Conclusion

Merci pour votre attention !