J. reine angew. Math. **505** (1998), 203–208

Journal für die reine und angewandte Mathematik

Finitude des couples d'invariants modulaires singuliers sur une courbe algébrique plane non modulaire

Par *Yves André* à Paris

Abstract. Let S be an irreducible algebraic curve in the affine complex plane. Assume that S is neither a horizontal line, nor a vertical line, nor a modular curve $Y_0(N)$ (for any integer $N \geqq 1$). Then there are only finitely many points P of S such that both coordinates of P are singular moduli (i.e. invariants of elliptic curves with complex multiplication).

1. Le résultat

La courbe modulaire $Y_0(N)$ est la courbe algébrique plane irréductible d'équation $P_N(x,y) = 0$, où P_N est le polynôme unitaire caractérisé (au signe près pour $N = 1$) par la propriété suivante: si E et E' sont deux courbes elliptiques d'invariants modulaires respectifs j et j', alors il existe une isogénie cyclique de degré N de E vers E' si et seulement si $P_N(j,j') = 0$. Par exemple

$$P_1(x,y) = x - y,$$

$$P_2(x,y) = x^3 + y^3 - x^2y^2 + 2^4.3.31(x^2y + xy^2) - 2^4.3^4.5^3(x^2 + y^2) + 3^4.5^3.4027xy + 2^8.3^7.5^6(x + y) - 2^{12}.3^9.5^9\ ^1).$$

Pour $N > 1$, P_N est symétrique en x et y.

Il est clair que si $P_N(j,j') = 0$ et si j est un invariant modulaire singulier, alors il en est de même de j'. A fortiori, $Y_0(N)$ contient une infinité de points (j,j') tels que j et j' sont des invariants modulaires singuliers. Nous nous proposons de caractériser les courbes modulaires par cette propriété.

Théorème. *Soit S une courbe algébrique irréductible dans le plan affine, qui ne soit ni une droite horizontale, ni une droite verticale. Alors S est une courbe modulaire $Y_0(N)$ si*

[1]) cf. [Co], p. 379. The coefficient of the term xy seems to be mistaken in [C], p. 186.

et seulement si S contient une infinité de points (j,j') tels que j et j' soient des invariants modulaires singuliers.

Des résultats partiels dans cette direction avaient été obtenus en Décembre 1995 par l'auteur (cas où la fermeture de S dans $\mathbb{P}^1 \times \mathbb{P}^1$ ne rencontre $\{\infty\} \times \mathbb{P}^1$ qu'en l'infini ou en des invariants modulaires singuliers, cf. [A], 5.5), et, indépendamment, par B. Edixhoven (sous l'hypothèse de Riemann généralisée, [E]).

Le théorème est le premier cas de conjectures beaucoup plus ambitieuses sur la distribution des points *CM* sur les sous-variétés des variétés de Shimura, pour la discussion desquelles nous renvoyons à [A].

Pour la démonstration, nous allons donc supposer l'existence d'une suite infinie (j_n,j_n') de points complexes de S tels que j_n (resp. j_n') soit l'invariant modulaire d'une courbe elliptique E_n (resp. E_n') à multiplication complexe par un ordre quadratique $\mathcal{O}_{D_n}$ (resp. $\mathcal{O}_{D_n'}$) de discriminant négatif D_n (resp. D_n'). Nous noterons f_n (resp. f_n') le conducteur de $\mathcal{O}_{D_n}$ (resp. $\mathcal{O}_{D_n'}$). Comme les points (j_n,j_n') sont algébriques sur $\mathbb{Q}$, on en déduit que S est définie sur une extension finie de $\mathbb{Q}$. Quitte à remplacer S par la réunion de ses conjuguées (et à abandonner l'irréductibilité géométrique), nous pouvons alors supposer, et nous supposerons, que S est définie sur $\mathbb{Q}$. Comme S est irréductible sur $\mathbb{Q}$, il suffit de montrer qu'*il existe une sous-suite infinie de (j_n,j_n') portée par une courbe $Y_0(N)$*.

Nous noterons (d,d') le bidegré de S (par hypothèse, d et d' sont non nuls).

2. Première réduction, via la théorie du corps de classes

Lemme 1. *Pour n assez grand, on a $\mathbb{Q}(\sqrt{D_n}) = \mathbb{Q}(\sqrt{D_n'})$; de plus, le quotient D_n'/D_n ne prend qu'un nombre fini de valeurs.*

Nous ferons appel à la notion de «ring class field» (RCF), cf. [C], 8.1.6. Rappelons qu'une extension abélienne $K/\mathbb{Q}(\sqrt{D})$ est RCF (selon le conducteur $f \geqq 1$) si presque tout idéal premier de $\mathbb{Q}(\sqrt{D})$ congru à un entier rationnel modulo f se décompose dans K (K est donc un corps de classes de rayon particulier).

Le théorème de Weber nous dit que $\mathbb{Q}(\sqrt{D_n}, j_n)/\mathbb{Q}(\sqrt{D_n})$ est RCF (selon le conducteur f_n, cf. [C], 11). Comme d'autre part $\mathbb{Q}(\sqrt{D_n}, \sqrt{D_n'})/\mathbb{Q}(\sqrt{D_n})$ est RCF (selon $D_n.D_n'$, loc. cit. 8.2.1), on en déduit que $\mathbb{Q}(\sqrt{D_n}, \sqrt{D_n'}, j_n)/\mathbb{Q}(\sqrt{D_n})$ est RCF (selon $f_n.D_n.D_n'$). De même, $\mathbb{Q}(\sqrt{D_n}, \sqrt{D_n'}, j_n')$ est RCF pour $\mathbb{Q}(\sqrt{D_n'})$. Il suit que le corps

$$K_n := \mathbb{Q}(\sqrt{D_n}, \sqrt{D_n'}, j_n) \cap \mathbb{Q}(\sqrt{D_n}, \sqrt{D_n'}, j_n')$$

est RCF à la fois pour $\mathbb{Q}(\sqrt{D_n})$ et pour $\mathbb{Q}(\sqrt{D_n'})$.

Si $\mathbb{Q}(\sqrt{D_n}) \neq \mathbb{Q}(\sqrt{D_n'})$, ceci entraîne que K_n est multiquadratique sur $\mathbb{Q}$ (loc. cit. 8.3.12). Puisque $\mathrm{Gal}(\mathbb{Q}(\sqrt{D_n}, j_n)/\mathbb{Q}(\sqrt{D_n}))$ s'identifie au groupe de classes d'idéaux de $\mathcal{O}_{D_n'}$ on en déduit que le degré $[\mathbb{Q}(\sqrt{D_n}, \sqrt{D_n'}, j_n) : K_n]$ est divisible par le quotient $q(\mathcal{O}_{D_n})$ du nombre de classes d'idéaux de $\mathcal{O}_{D_n}$ par le nombre de classes d'idéaux d'ordre $\leqq 2$ de $\mathcal{O}_{D_n}$. Or $[\mathbb{Q}(\sqrt{D_n}, \sqrt{D_n'}, j_n) : K_n] = [\mathbb{Q}(\sqrt{D_n}, \sqrt{D_n'}, j_n, j_n') : \mathbb{Q}(\sqrt{D_n}, \sqrt{D_n'}, j_n')]$ est borné par d, du fait que S est supposée définie sur $\mathbb{Q}$. Comme l'inégalité $q(\mathcal{O}_{D_n}) \leqq d$ (resp. $q(\mathcal{O}_{D_n'}) \leqq d'$) n'admet qu'un nombre fini de solutions D_n (resp. D_n') d'après Chowla (cf. [N], 8.8), on en déduit que $\mathbb{Q}(\sqrt{D_n}) = \mathbb{Q}(\sqrt{D_n'})$ pour n assez grand.

Notons d_n le discriminant de $\mathbb{Q}(\sqrt{D_n})$. On a $D_n = f_n^2 d_n$, $D_n' = f_n'^2 d_n$. Soit f_n'' le plus petit multiple commun de f_n et de f_n', et posons $D_n'' = f_n''^2 d_n$. Alors

$$[\mathbb{Q}(\sqrt{D_n}, j_n, j_n') : \mathbb{Q}(\sqrt{D_n})]$$

est le nombre de classes d'idéaux de $\mathcal{O}_{D_n''}$. En comparant au nombre de classes d'idéaux de $\mathcal{O}_{d_n}$, on obtient la formule

$$[\mathbb{Q}(\sqrt{D_n}, j_n, j_n') : \mathbb{Q}(\sqrt{D_n}, j_n')] = (f_n''/f_n') \prod_{p \mid (f_n''/f_n)} (1 - p^{-1}\chi(p)),$$

où χ désigne le symbole de Kronecker relatif à $\mathcal{O}_{d_n}$; de même pour

$$[\mathbb{Q}(\sqrt{D_n}, j_n, j_n') : \mathbb{Q}(\sqrt{D_n}, j_n)].$$

Comme ces degrés sont bornés (par d et par d' respectivement), on en déduit que f_n''/f_n' et f_n''/f_n, et donc aussi D_n'/D_n, ne prennent qu'un nombre fini de valeurs.

Remarque. Ce lemme a aussi été démontré par B. Edixhoven [E], sans recourir aux RCF.

3. Seconde reduction, via une mesure de transcendance

Comme S est définie sur $\mathbb{Q}$, on peut remplacer chaque point (j_n, j_n') par n'importe quel conjugué. Nous pouvons donc supposer, et nous supposerons désormais, que $j_n = j\left(\frac{D_n + \sqrt{D_n}}{2}\right)$ (i.e. que $E_n \cong \mathbb{C}/\mathcal{O}_{D_n}$).

Le développement de Fourier de la fonction modulaire j montre alors que $\log|j_n| \approx \pi\sqrt{|D_n|}$ $\left(\text{i.e. } \frac{\log|j_n|}{\pi\sqrt{|D_n|}} \to 1\right)$; en particulier, $|j_n| \to \infty$.

Lemme 2. *On a aussi* $|j_n'| \to \infty$.

Soit $\bar{S}$ la fermeture de S dans $\mathbb{P}^1 \times \mathbb{P}^1$. Supposons, par l'absurde, que le lemme soit faux. Alors il existe un point (∞, j') de l'ensemble fini $\bar{S} \cap \{\infty\} \times \mathbb{A}^1$, et une fonction

croissante $\sigma : \mathbb{N} \to \mathbb{N}$ telle que la suite $(j_{\sigma(n)}, j'_{\sigma(n)})$ tende vers (∞, j') et soit portée par une branche unique de $\bar{S}$ passant par (∞, j'). Le développement de Puiseux au voisinage de (∞, j') montre l'existence d'une constante $\varrho \in \mathbb{Q}_{>0}$ telle que

$$\log|j' - j'_{\sigma(n)}| \approx -\varrho.\log|j_{\sigma(n)}| \approx -\varrho\pi\sqrt{|D_{\sigma(n)}|}\,.$$

Soit τ' (resp. $\tau'_{\sigma(n)}$) l'unique point du domaine fondamental standard de $\mathrm{SL}_2(\mathbb{Z})$ tel que $j' = j(\tau')$ (resp. $j'_{\sigma(n)} = j(\tau'_{\sigma(n)})$). Si $\mathrm{Re}\,\tau' \neq -\frac{1}{2}$, $\tau'_{\sigma(n)}$ tend vers τ'. Plus précisément, en développant j au voisinage de τ', on obtient

$$\log|j' - j'_{\sigma(n)}| \approx \kappa.\log|\tau' - \tau'_{\sigma(n)}|, \quad \text{avec } \kappa = 3, 2 \text{ ou } 1$$

selon que $j' = 0$, $j' = 1728$, ou $j' \neq 0$, 1728 respectivement. Il existe donc une constante $c > 0$ telle que

$$(*) \qquad \log|\tau' - \tau'_{\sigma(n)}| \approx -c\sqrt{|D_{\sigma(n)}|}\,.$$

Si $\mathrm{Re}\,\tau' = -\frac{1}{2}$, on obtient la même estimation après passage à une sous-suite de $\tau'_{\sigma(n)}$ et remplacement éventuel de τ' par $\tau' + 1$.

Notons que $j(\tau')$ est algébrique sur $\mathbb{Q}$, puisque $\bar{S}$ est définie sur $\mathbb{Q}$. Dans [M], I, 1.1, D. Masser a établi pour tout nombre algébrique $\alpha \neq \tau'$ de degré fixé δ une inégalité

$$(**) \qquad \log|\tau' - \alpha| > -Ch'(\alpha)^{3+\varepsilon},$$

où C est une constante ne dépendant que de $(\tau', \delta, \varepsilon)$, et où $h'(\alpha)$ désigne le maximum de 1 et de la hauteur logarithmique de α (le cas où τ' est algébrique découle plus simplement, avec $3 + \varepsilon$ remplacé par 1, de l'inégalité de Liouville). Appliquons (**) à $\alpha = \tau'_{\sigma(n)}$: on a $\delta = 2$; en écrivant $A_n(\tau'_{\sigma(n)})^2 + B_n\tau'_{\sigma(n)} + C_n = 0$ avec A_n, B_n, C_n entiers premiers entre eux et vérifiant $|B_n| \leqq A_n \leqq C_n$, $D'_{\sigma(n)} = B_n^2 - 4A_nC_n$ (compte tenu de ce que $\tau'_{\sigma(n)}$ est dans le domaine fondamental), on obtient

$$h'(\tau'_{\sigma(n)}) = \max\left(1, \frac{1}{2}\log C_n\right) = O(\log|D'_{\sigma(n)}|)\ (= O(\log|D_{\sigma(n)}|)$$

d'après le lemme 1). On tire de là et de (**) une inégalité

$$(***) \qquad \log|\tau' - \tau'_{\sigma(n)}| > -C'(\log|D_{\sigma(n)}|)^{3+\varepsilon},$$

qui contredit (*) pour n assez grand. Ceci démontre le lemme.

4. Conclusion de la preuve

Compte tenu des lemme précédents, on peut désormais supposer, quitte à remplacer (j_n, j'_n) par une sous-suite, que les (j_n, j'_n) se situent sur une branche unique de $\bar{S}$ passant

par (∞,∞), et que le quotient f_n'/f_n prend une seule valeur, notée f. On a alors $D_n = f_n^2 d_n$, $D_n' = f^2.f_n^2 d_n$. Ecrivons le couple (τ_n, τ_n') d'éléments du domaine fondamental standard de $\mathrm{SL}_2(\mathbb{Z})$ d'image

$$(j_n = j(\tau_n), j_n' = j(\tau_n'))$$

sous la forme

$$\left(\tau_n = \frac{c_n + f_n\sqrt{d_n}}{2},\ \tau_n' = \frac{b_n + f.f_n\sqrt{d_n}}{2a_n}\right),$$

avec a_n, b_n, c_n entiers, $a_n \geqq |b_n|$, $c_n = 0$ ou 1 (cf. e.g. [L], 8.1).

Le développement de Puiseux au voisinage de (∞,∞) montre l'existence d'une constante $\varrho \in \mathbb{Q}_{>0}$ telle que $\log|j_n'| \approx \varrho.\log|j_n|$. D'autre part, le développement de Fourier de la fonction modulaire j montre alors que $\log|j_n| \approx \pi f_n\sqrt{|d_n|}$, $\log|j_n'| \approx \pi f.\dfrac{f_n\sqrt{|d_n|}}{a_n}$, d'où l'on tire la valeur, constante, de l'entier a_n : $a_n = f\varrho$.

Quitte à remplacer derechef (j_n, j_n') par une sous-suite, et à passer aux conjugués complexes si besoin est, on peut aussi supposer que b_n prend une valeur constante $\geqq 0$.

On en conclut que pour des entiers naturels k, l, m convenables, premiers entre eux dans leur ensemble (avec $k \leqq \dfrac{m}{2}$ et $\mathrm{pgcd}(l,m) \leqq 2$), S contient tous les points

$$\left(j(\tau_n), j\left(\frac{k + l\tau_n}{m}\right)\right).$$

Comme ces points sont portés par $Y_0(l.m)$, ceci entraîne finalement que $S = Y_0(l.m)$. q.e.d.

Une légère variante du résultat principal (qui s'en déduit immédiatement) s'énonce ainsi:

Variante. *Soient S_1 et S_2 deux courbes modulaires, et soit S une courbe algébrique irréductible tracée sur le produit $S_1 \times S_2$. On suppose que S contient une infinité de points CM.*

Alors S est ou bien une fibre d'une des deux projections, ou bien une composante irréductible d'une correspondance de Hecke.

Références bibliographiques

[A] *Y. André*, Distribution des points *CM* sur les sous-variétés des variétés de modules de variétés abéliennes, prépublication, Jussieu 1997.

[Co] *H. Cohen*, A course in computational algebraic number theory, Springer Verlag, 1993.

[C] *H. Cohn*, Introduction to the construction of class fields, Cambridge stud. **6** (1985).

[E] *B. Edixhoven*, Special points on the product of two modular curves, Compos. Math., à paraître.

[L] *S. Lang*, Elliptic functions, Addison-Wesley, 1973.

[M] *D. Masser*, Elliptic functions and transcendence, Springer Lect. Notes Math. **437** (1975).
[N] *W. Narkiewicz*, Elementary and analytic theory of algebraic numbers, 2ème éd., Springer Verlag / Polish Scientific Publishers, 1990.

Institut de Mathématiques, 4 place Jussieu, Tour 46-00, 5ème étage, case 247, F-75252 Paris Cedex 05
e-mail: andre@math.jussieu.fr

Eingegangen 17. Juli 1997, in revidierter Fassung 26. Mai 1998