Séminaires & Congrès
13, 2006, p. 91–125

JACOBIENS, JACOBIENNES ET STABILITÉ NUMÉRIQUE

par

Jean-Marc Couveignes

***Résumé.* —** On étudie la complexité et la stabilité des calculs dans la jacobienne des courbes de grand genre sur le corps des complexes avec une attention particulière aux courbes modulaires.

***Abstract* (Jacobians and numerical stability). —** This paper is concerned with the complexity and stability of arithmetic operations in the jacobian variety of curves over the field of complex numbers, as the genus grows to infinity. We focus on modular curves.

Table des matières

1. Introduction

Il est traditionnel de calculer dans le groupe des points de la jacobienne d'une courbe algébrique projective lisse et géométriquement irréductible X de genre g en représentant tout élément de ce groupe par un diviseur effectif de degré g, une fois choisi un tel diviseur O comme origine. La somme de deux diviseurs $P - O$ et $Q - O$ est *réduite* par le calcul de l'espace linéaire associé au diviseur $P + Q - O$ suivi de la localisation des zéros d'une fonction non nulle de cet espace.

***Classification mathématique par sujets* (2000). —** 11F11, 11F25, 11F30, 11Y16, 11Y35, 65E05, 65Y20, 68Q15.
***Mots clefs.* —** Jacobienne, approximation, stabilité, formes modulaires, complexité algorithmique, machine de Turing, temps polynomial déterministe.

Comme l'application de Jacobi,

$$S^g X \to J_X$$

de la puissance symétrique g-ième $S^g X$ de X dans sa jacobienne J_X, n'est pas un isomorphisme, la représentation n'est pas unique.

Si le corps de base est un corps fini $\mathbb{F}_q$, les opérations arithmétiques y sont exactes et rapides.

On considère ici le cas où le corps de base est le corps $\mathbb{C}$ des complexes. On se donne un modèle analytique naturel et une mesure sur $X(\mathbb{C})$. On s'intéresse à la complexité des algorithmes utilisés pour ajouter et réduire des diviseurs. Le cadre est celui des machines de Turing classiques. En effet, on peut avoir en vue des applications arithmétiques comme le calcul de nombres de points, ou de coefficients de formes modulaires et les calculs en nombres complexes ne sont alors qu'une étape dans la recherche d'une quantité discrète. Le projet de Bas Edixhoven pour répondre à une question de René Schoof [**6, 7, 3**] se prête à cette approche.

Bien sûr, les machines de Turing ordinaires ne manipulent pas les nombres réels ni complexes mais plutôt des nombres rationnels, décimaux ou binaires. Cependant, on peut voir un nombre réel α comme un oracle qui, pour tout entier positif k, retourne une valeur binaire ou décimale approchée de α à $\exp(-k)$ près. Si une machine de Turing doit résoudre un problème dont les entrées sont des nombres réels, elle reçoit un oracle pour chacun de ces réels. Si la machine de Turing calcule un nombre réel, on lui donne en entrée la précision absolue k requise et elle retourne une valeur approchée à $\exp(-k)$ près du résultat. On dit que la machine est polynomiale si elle répond en temps polynomial en la taille des données et k. On note que la recherche des racines complexes d'un polynôme unitaire à coefficients complexes se fait en temps déterministe polynomial grâce à la méthode de quadrichotomie de Weyl par exemple. On veut dire par là qu'une valeur approchée à $\exp(-k)$ près de chaque racine peut être calculée en temps polynomial en le degré du polynôme, la taille des coefficients (logarithme du maximum des modules des coefficients) et la précision absolue k requise.

On veut savoir si la complexité asymptotique des opérations arithmétiques dans la jacobienne est polynomiale en le genre de la courbe. La première difficulté est de donner un sens précis à cette assertion. Plutôt que de rester dans le vague, on formule et on étudie ces questions dans le cas important et représentatif des courbes modulaires $X_0(p)$ lorsque p est un entier premier qui tend vers l'infini. L'algorithmique de ces courbes est riche et largement explorée. On trouve dans [**4, 5, 8**] des algorithmes pour l'étude homologique des courbes modulaires et des méthodes analytiques expérimentales motivées par la vérification de conjectures arithmétiques et la recherche de points rationnels.

La section 2 décrit le modèle analytique standard de ces courbes ainsi que ses propriétés algorithmiques. On y rappelle d'abord les résultats de Manin, Shokurov, Cremona et Merel concernant le calcul des périodes, et on en donne une expression

quantifiée du point de vue de la complexité algorithmique et de la stabilité numérique. Cette dernière est assurée en dernier ressort par des minorations du volume des périodes et du déterminant jacobien de l'application d'intégration de Jacobi. Ces minorations reposent elles mêmes sur des considérations d'intégralité des coefficients des formes modulaires primitives, propres et normalisées.

On présente dans la section 3 des algorithmes pour les opérations élémentaires dans la jacobienne $J_0(p)$ et pour la résolution effective du problème inverse de Jacobi. La complexité et la stabilité de ces algorithmes sont étudiées avec les outils de la section 2 puis estimées dans les théorèmes 1 et 2. On obtient des algorithmes déterministes polynomiaux en p. Le caractère déterministe de ces algorithmes s'explique en dernier lieu par la connexité du tore analytique complexe $J_0(p)(\mathbb{C})$.

Tous les lemmes et définitions concernant la localisation et la stabilité des zéros de fonctions analytiques sont présentés dans l'appendice A qui est indépendant mais doit être au moins parcouru avant de lire les sections 2 et 3.

Les méthodes, les énoncés et les démonstrations que nous donnons pour les courbes $X_0(p)$ s'étendent sans peine au cas de $X_1(p)$. Pour les courbes modulaires de niveau composé, il faut une majoration des coefficients des développements de Fourier en toutes les pointes ainsi qu'un algorithme pour les calculer.

On trouvera un index à la fin de cet article.

Convention importante. — le symbole $\mathcal{O}$ désigne partout une constante absolue positive et effective, chaque fois différente. La présence de ce symbole dans une formule ou un énoncé signifie que cette formule ou cet énoncé sont vrais si, pour chaque occurence, ce symbole est remplacée par une constante positive effective bien choisie.

2. Courbes modulaires $X_0(p)$

Cette section rappelle, précise et complète quelques résultats métriques et algorithmiques concernant les courbes modulaires $X_0(p)$. On supposera que p est premier et que le genre g de $X_0(p)$ est au moins 2.

Le paragraphe 2.1 introduit quelques notations et un recouvrement non injectif de $X_0(p)$ par deux disques analytiques centrés en chacune des deux pointes.

Les propriétés élémentaires des formes primitives, propres et normalisées sont rappelées dans le paragraphe 2.2 et celles de l'homologie dans le paragraphe 2.3. Le calcul des périodes est abordé dans le paragraphe 2.4. Ces trois paragraphes résument le travail de Manin, Shokurov, Cremona et Merel sur cette question.

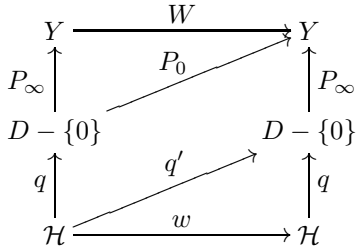
Le paragraphe 2.5 établit une minoration du volume du réseau des périodes. Une formule d'intégration sur les surfaces de Riemann relie ce volume au produit des normes de Petersson des formes primitives, propres et normalisées, ces dernières étant faciles à minorer parce que le développement de Fourier commence par $(1 + O(q))dq$ où $q = \exp(2i\pi\tau)$ est le paramètre de Tate associé à un τ du demi-plan de Poincaré.

Le paragraphe 2.6 établit des majorations simples mais nécessaires des intégrales de Jacobi et définit l'*instabilité* d'un diviseur effectif de degré g. Le paragraphe 2.7 construit un diviseur d'instabilité assez petite. Cela revient à trouver g points dans le modèle canonique de $X_0(p)$ qui ne soient proches d'aucun hyperplan. Autrement dit, le jacobien en ces g points n'est pas trop petit. On prend le parti (maladroit en pratique mais simple en théorie) de chercher les g points dans le voisinage de la pointe à l'infini. Le terme principal du développement du jacobien y est le wronskien. On le minore grâce à l'intégralité des coefficients de son développement de Fourier.

Le paragraphe 2.9 étudie la stabilité de l'application inverse de Jacobi. Celà se réduit à majorer la différence entre cette application et sa linéarisée.

La connaissance d'un g-uplet de points de faible instabilité, donné au paragraphe 2.7, permet de construire au paragraphe 2.10 des sous-ensembles finis de taille modeste et bien distribués dans le tore complexe. Comme les éléments de ces ensembles sont images par l'application de Jacobi de diviseurs connus, il sont des auxiliaires précieux pour la résolution approchée du problème inverse de Jacobi. Ils permettent de discrétiser ce problème.

2.1. Un modèle analytique. — Soit p un nombre premier et $X = X_0(p)$ la courbe modulaire de niveau p associée au sous groupe de congruence $\Gamma = \Gamma_0(p)$ de $\mathrm{SL}_2(\mathbb{Z})$. On note $\mathcal{H}$ le demi-plan de Poincaré et $\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$. La surface de Riemann compacte quotient $\Gamma\backslash\mathcal{H}^*$ est $X(\mathbb{C})$. Son genre est $g = \frac{p+1-3\nu_2-4\nu_3}{12}$ avec $\nu_2 = 1+\left(\frac{-1}{p}\right)$ et $\nu_3 = 1+\left(\frac{-3}{p}\right)$. Il y a ν_2 points elliptiques d'ordre 2 et on note $\mathcal{P}_2$ le diviseur somme de ces points. De même il a ν_3 points elliptiques d'ordre 3 et on note $\mathcal{P}_3$ le diviseur somme de ces points. Voir [**15**, Propositions 1.40 et 1.43]. Le genre de X est compris entre $\frac{p-13}{12}$ et $\frac{p+1}{12}$. Le quotient $\Gamma\backslash\mathcal{H}$ est un ouvert de Zariski de X noté $Y = Y_0(p)$. On note que la largeur de la pointe ∞ est 1 et la largeur de la pointe 0 est p. Pour $\tau \in \mathcal{H}$ on pose $q = q(\tau) = q_\infty(\tau) = \exp(2i\pi\tau)$ et $w(\tau) = -\frac{1}{p\tau}$ et $q' = q'(\tau) = q_0(\tau) = q(w(\tau)) = \exp(\frac{-2i\pi}{p\tau})$. On note $P = P_\infty = P(\tau) = P(q)$ le point de Y associé à τ et $P' = P_0 = P'(\tau) = P'(q) = P(w(\tau)) = W(P) = P(q')$ où W est l'involution d'Atkin-Lehner. On a le diagramme



Étant donnés deux réels R_∞ et R_0 plus petits que 1 on peut se demander si l'union de l'image par P_∞ du disque ouvert $D(0, R_\infty)$ et de l'image par P_0 de $D(0, R_0)$ recouvre $X(\mathbb{C})$.

On pose $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ et $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ de sorte que $S\tau = -1/\tau$ et $T\tau = \tau + 1$. Soit $\mathcal{R}$ le domaine fondamental usuel de $\mathrm{SL}_2(\mathbb{Z})$, délimité par le cercle de centre 0 et de rayon 1 et par les droites d'abscisses $-1/2$ et $1/2$. Alors un domaine fondamental pour Γ est constitué de l'union de $\mathcal{R}$ et des $ST^k\mathcal{R}$ pour k entier de 0 à $p-1$. Ces derniers sont contenus dans l'image par S de l'ensemble des $\tau = a + ib$ avec $b \geq \frac{\sqrt{3}}{2}$. Donc leur image par w est constituée de complexes dont la partie imaginaire est au moins $\frac{\sqrt{3}}{2p}$. Si on choisit $R_0 > \exp(-\frac{\pi\sqrt{3}}{p})$ alors l'image de $D(0, R_0)$ par P_0 recouvre les $ST^k\mathcal{R}$ pour k de 0 à $p-1$.

Comme $\mathcal{R}$ est contenu dans le demi plan des parties imaginaire au moins égales à $\sqrt{3}/2$ on prend $R_\infty > \exp(-\pi\sqrt{3})$ et l'image de $D(0, R_\infty)$ par P_∞ recouvre $\mathcal{R}$.

On pose donc $R_\infty = 0.005$ et $R_0 = 1 - \frac{1}{p}$

On a donc recouvert $X(\mathbb{C})$ par l'image de deux disques analytiques complexes $D_\infty = D(0, R_\infty)$ et $D_0 = D(0, R_0)$.

2.2. Différentielles. — On peut maintenant calculer des espaces de formes différentielles sur X. On fixe donc un entier $d \geq 1$. À toute forme modulaire parabolique f de poids $2d$ sur Γ on associe la différentielle $\omega = (2i\pi)^d f(d\tau)^d$ de degré d. D'après [**15**, Proposition 2.16] on a

$$\mathrm{Div}(\omega) = \mathrm{Div}(f) - d(0) - d(\infty) - \frac{d}{2}\mathcal{P}_2 - \frac{2d}{3}\mathcal{P}_3.$$

On pose donc $\Delta_d = (d-1)(0) + (d-1)(\infty) + \lfloor \frac{d}{2} \rfloor \mathcal{P}_2 + \lfloor \frac{2d}{3} \rfloor \mathcal{P}_3$ et on cherche une base $\mathcal{D}_d$ de l'espace $\mathcal{H}^d(\Delta_d)$ des formes différentielles de degré d et de diviseur $\geq -\Delta_d$.

On prend pour $\mathcal{D}_d$ l'ensemble des $\omega = (2i\pi)^d f(q)(d\tau)^d = \frac{f(q)}{q^d}(dq)^d$ où $f(q)$ est une forme modulaire parabolique primitive[(1)], propre[(2)] et normalisée[(3)] sur $\Gamma = \Gamma_0(p)$ et de poids $2d$. Si f est une telle forme elle admet un développement $f = \sum_{k \geq 1} a_k q_\infty^k$ avec $a_1 = 1$ et pour tout entier $k \geq 1$ on montre que le coefficient a_k est un entier algébrique majoré en module par k^{d+2}. Il suffit de le montrer pour $k = \ell^n$ une puissance d'un premier ℓ. D'après le théorème de Deligne on a $|a_\ell| \leq 2\ell^{d-\frac{1}{2}}$ et d'après [**1**, Theorem 3]

$$|a_{\ell^{n+2}}| \leq |a_\ell a_{\ell^{n+1}}| + \ell^{2d-1}|a_{\ell^n}|$$

donc $|a_{\ell^n}| \leq u_n \ell^{\frac{n(2d-1)}{2}}$ où u_n est la suite récurrente $u_0 = 1$, $u_1 = 2$ et $u_{n+2} = 2u_{n+1} + u_n$. Donc $u_n = \frac{(1+\sqrt{2})^{n+1} - (1-\sqrt{2})^{n+1}}{2\sqrt{2}}$ et $|u_n| \leq 4^n \leq \ell^{2n}$ donc $|a_{\ell^n}| \leq \ell^{2n}\ell^{\frac{n(2d-1)}{2}}$.

Le développement de ω en q_∞ est donc le développement standard, donné par les valeurs propres des opérateurs de Hecke. On peut calculer les coefficients a_k comme valeurs propres des opérateurs de Hecke agissant sur les symboles de Manin-Shokurov suivant [**4, 14, 10**]. Les plongements complexes des valeurs propres peuvent alors être

(1) Cela signifie qu'elle ne provient pas d'une forme de niveau plus petit. Se dit en Anglais *newform*. Cette condition est vide ici puisque le niveau p est premier.

(2) Autrement dit, f est vecteur propre des opérateurs de Hecke.

(3) Son développement de Fourier commence par q.