# Sur les points de torsion des jacobiennes de courbes

**Franck Leprévost**

Université Paris 7
Département de Mathématiques
Tour 45-55
5ème étage
2 place Jussieu
75252 Paris Cedex 05
FRANCE

Max-Planck-Institut
für Mathematik
Gottfried-Claren-Str. 26
53225 Bonn
GERMANY

MPI/95-38

# Sur une conjecture sur les points de torsion rationnels des jacobiennes de courbes

Franck Leprévost

## 1 Enoncé d'une conjecture de Flynn

Flynn formule, en p. 264 de [F-1], la

**Conjecture :** *Il existe une constante $\kappa$ telle que, pour tout entier $g \geq 1$, et pour tout entier $l$ tel que $1 \leq l < \kappa g$, il existe une courbe hyperelliptique définie sur $\mathbf{Q}$, de genre $g$, dont la jacobienne est munie d'un point rationnel d'ordre $l$.*

Le but de cet article est de démontrer de façon constructive cette conjecture, avec la constante $\kappa = 3$. Plus précisément, nous montrons ici les résultats suivants, la notion de famille étant définie plus loin :

**Théorème 1.1** *Soit $g$ un entier $\geq 1$. Pour tout entier $l$ tel que $1 \leq l \leq 2g+1$, il existe une famille géométrique à un paramètre de courbes hyperelliptiques définie sur $\mathbf{Q}$, de genre $g$, dont la jacobienne possède un point rationnel d'ordre $l$.*

**Théorème 1.2** *Soient $g \geq 1$. Si $l$ est un entier pair tel que $2g+2 \leq l \leq 3g$, il existe une famille géométrique à un paramètre de courbes hyperelliptiques de genre $g$ définies sur $\mathbf{Q}$, dont la jacobienne possède un point rationnel d'ordre $l$. Si $l$ est un entier impair tel que $2g+1 \leq l \leq 3g-1$, il existe au moins une courbe hyperelliptique de genre $g$ définie sur $\mathbf{Q}$, dont la jacobienne possède un point rationnel d'ordre $l$.*

Les démonstrations de ces théorèmes sont effectives, comme on va le voir dans les sections suivantes.

**Remarque :** On n'a à l'heure actuelle guère de renseignements sur la valeur maximale de $\kappa$, ni sur l'ordre maximal d'un point rationnel de la jacobienne d'une courbe définie sur $\mathbf{Q}$, hyperelliptique ou non, en fonction du genre $g$ de celle-ci, le record actuel étant, à notre connaissance, $2g(2g+1)$ (*cf.* [L-2], voir [L-1] et [F-2] pour les records précédents). De même, on ne sait pas, pour $g \geq 2$, s'il existe des entiers $l$ qui *ne* peuvent *pas* être l'ordre d'un point rationnel de la jacobienne d'une courbe de genre $g$ définie sur $\mathbf{Q}$.

Afin de définir la notion de famille géométrique à un paramètre de courbes hyperelliptiques, il est nécessaire de rappeler les notions suivantes (*cf.* [M]).

Soit

$$F = a_0 X^n + a_1 X^{n-1} Y + \cdots + a_n Y^n$$

une forme binaire de degré $n$, à coefficients dans un corps $K$ de caractéristique 0. Un *invariant* de $F$ est une expression polynômiale $I(a_0, \ldots, a_n)$ telle que

$$I(a'_0, \ldots, a'_n) = (\det M)^{-k} I(a_0, \ldots, a_n),$$

*Adresse : Université Paris 7, Département de Mathématiques, tour 45-55, 5ème étage, 2 place Jussieu, 75252 Paris cedex 05, France. E-mail : leprevot@mathp7.jussieu.fr

si l'on fait subir à $F$ une transformation

$$\begin{cases} X &= rX' + sY' \\ Y &= tX' + uY' \end{cases}$$

où $M = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$ de $\mathrm{GL}_2(\bar{K})$. Le *degré* de $I$ est le degré total de $I$ relativement à $(a_0, \ldots, a_n)$, et $k$ est l'*indice* de $I$. Un *invariant absolu* de $F$ est un quotient de deux invariants de même degré.

Soit $y^2 = f(x)$ l'équation d'une courbe hyperelliptique, où $f(x) = a_0x^{2g+2} + a_1x^{2g+1} + \cdots + a_{2g+2}$ est un polynôme à coefficients dans $K$, de degré $2g+1$ ou $2g+2$, sans racines multiples. On lui associe la forme binaire $F$ définie par

$$F(X, Y) = Y^{2g+2} f(\frac{X}{Y}).$$

Un *invariant* (resp. *invariant absolu*) de $f$ est entendu comme étant celui de la forme binaire $F$ associée.

Par exemple, nous avons le discriminant de la forme binaire $F$, $\mathcal{D}(F)$, qui est un invariant de degré $2(2g+1)$ et d'indice $(2g+2)(2g+1)$. Un autre invariant, de degré 2, d'indice $2g+2$ et noté ici $\mathcal{A}$, s'obtient de manière explicite, avec les notations précédentes, par

$$\mathcal{A}(F) = \sum_{k=0}^{2g+2} (-1)^k \binom{2g+2}{k}^{-1} a_{2g+2-k} a_k.$$

Ainsi, la quantité

$$\gamma(F) = \frac{\mathcal{A}^{2g+1}(F)}{\mathcal{D}(\mathcal{F})}$$

définit un invariant absolu de $f$.

Nous dirons ici qu'une équation $y^2 = f(x)$ où $f(x)$ est un polynôme de degré $2g+1$ ou $2g+2$, à coefficients dans $\mathbf{Q}(t)$ sans racines multiples, définit une *famille géométrique à un paramètre de courbes hyperelliptiques de genre $g$ sur* $\mathbf{Q}$ si l'image de la courbe dans la variété de modules des courbes de genre $g$ est non constante. C'est le cas si et seulement si l'un au moins de ses invariants absolus est une fraction rationnelle non constante. Une telle famille permet, par spécialisation du paramètre en des valeurs rationnelles, d'obtenir une infinité de courbes hyperelliptiques de genre $g$ deux à deux non $\bar{\mathbf{Q}}$-isomorphes.

## 2 $\kappa = 2$

Nous établissons dans cette section le théorème **1.1**. Remarquons tout d'abord que si, pour tout entier $l$ tel que $g+1 \leq l \leq 2g+1$, $(C_l)$ est une famille géométrique à un paramètre de courbes hyperelliptiques de genre $g$ dont la jacobienne possède un point rationnel d'ordre $l$, alors, pour tout entier $m$ tel que $1 \leq m \leq g$, la jacobienne de l'une de ces courbes possède un point rationnel d'ordre $m$. En effet, tout tel $m$ admet un multiple $l$ compris entre $g+1$ et $2g+1$, et la courbe $(C_l)$ convient.

Soit maintenant $K$ un corps de caractéristique 0, $g$ un entier $\geq 1$, et $f$ un élément unitaire de $K[x]$ de degré $2g+2$, tel que l'équation $y^2 = f(x)$ définisse une courbe $(C)$, hyperelliptique et de genre $g$. Notons $+\infty$ et $-\infty$ les deux points rationnels de $(C)$ à l'infini. Avec ces notations, nous avons le lemme général suivant :

**Lemme 2.1** *Soient $l$ un entier $\geq g+1$, et $P$ et $Q$ deux éléments unitaires de $K[x]$ de degrés respectifs $l$ et $l-g-1$, tels que*

$$P^2(x) - Q^2(x)f(x) = \text{constante} \neq 0.$$

*Alors le diviseur $D_\infty = (+\infty) - (-\infty)$ définit un point rationnel de la jacobienne de $(C)$ d'exposant $l$, et d'ordre différent de 1.*

En effet, le diviseur de la fonction $P(x) - yQ(x)$ étant égal à $lD_\infty$, la classe de $D_\infty$ dans la jacobienne de $(C)$ est d'exposant $l$. De plus, si l'ordre de cet élément était égal à 1, $(C)$ serait de genre 0, ce qui est absurde.

Fixons $l$ tel que $g+1 \leq l \leq 2g+1$. Soient $Q$ et $R$ deux éléments unitaires de $K[x]$ de degrés respectifs $l-g-1$ et $2g+2-l$. Alors $P = Q^2R - t$ et $f = (Q^2R - 2t)R$ sont des éléments unitaires de $K(t)[x]$ de degrés respectifs $l$ et $2g+2$, et vérifient l'équation :

$$P^2(x) - Q^2(x)f(x) = t^2.$$

Notons $(C_{Q,R})$ la courbe d'équation $y^2 = f(x)$ obtenue avec un tel $f$. Afin de montrer qu'une telle construction définit une famille à un paramètre de courbes hyperelliptiques de genre $g$ dont la jacobienne est munie d'un point rationnel d'ordre $l$, nous spécialisons $Q$ et $R$ en :

$$\begin{cases} Q(x) &= x^{l-g-1} \\ R(x) &= x^{2g+1-l}(x+1) + a \end{cases}$$

Notons $f_{t,a,l}(x)$ le polynôme et $(C_{1,l})$ la courbe obtenus avec ce choix.

**Lemme 2.2** *Pour tout $g \geq 1$ et tout entier $l$ tel que $g+1 \leq l \leq 2g+1$, le discriminant $\mathcal{D}(f_{t,a,l})$ est non identiquement nul.*

Fixons $l$ dans l'intervalle considéré, et notons $f(t,a,x) = f_{t,a,l}(x)$ pour la démonstration de ce lemme. Supposons que $f(t,a,x)$ ait une racine multiple en $x$ : il existe alors deux éléments $P_1(t,a,x)$ et $P_2(t,a,x)$ de $\mathbf{Q}[t,a,x]$, où $P_2(t,a,x)$ est sans facteur carré, tels que l'on ait l'identité

$$f(t,a,x) = P_1^2(t,a,x)P_2(t,a,x).$$

L'on montre aisément que le degré de $P_1$ en $a$ et $t$ est nul. On déduit de l'identité ci-dessus, en notant plus simplement $P_1(x) = P_1(t,a,x)$, que $P_1^2(x)$ divise toutes les dérivées partielles de $f(t,a,x)$ par rapport à $t$ ou $a$.

Ainsi

$$\frac{\partial}{\partial t}f(t,a,x) = -2x^{2g+1-l}(x+1) - 2a = P_1^2(x)\frac{\partial}{\partial t}P_2(t,a,x),$$

$P_1(x)$ est donc constant, et la courbe $(C_{1,l})$ est hyperelliptique de genre $g$.

Notons $\mathcal{S}_1 = \{2,3\}$, $\mathcal{S}_2 = \{3,4\}$, $\mathcal{S}_3 = \{5,6\}$, $\mathcal{S}_4 = \{7\}$, $\mathcal{S}_5 = \{9\}$ et $\mathcal{S}_g = \emptyset$ pour $g \geq 6$. Le calcul montre :

**Lemme 2.3** *Pour tout $g \geq 1$ et tout entier $l$ tel que $g+1 \leq l \leq 2g+1$, l'invariant $\mathcal{A}(f_{t,a,l})$ est un polynôme en $a$ et en $t$, non identiquement nul. Plus précisément, notons, pour tout entier $n$ tel que $0 \leq n \leq 2g+2$, $\rho_l = (-1)^l \binom{2g+2}{l}^{-1}$. On a $\mathcal{A}(f_{t,a,l}) = -4at(1+2\rho_l) + \mu_l$ où $\mu_l$ est donné dans le tableau ci-dessous pour $l \notin \mathcal{S}_g$.*

| $g \geq 1$ et $l \notin \mathcal{S}_g$ | |
|---|---|
| $l$ | $\mu_l$ |
| $2g+1$ | $-4t(1+2\rho_1)$ |
| $2g$ | $-4t(2\rho_1+\rho_2)$ |
| $2g-1$ | $-4t\rho_2$ |
| $g+2$ | $2a^2(\rho_2+2\rho_{g+1})$ |
| $g+1$ | $2a^2+4(a^2+t^2)\rho_{g+1}$ |
| $g+3 \leq l \leq 2g-2$ | $\mu_l$ |
| si $3l = 4g+4$ | $4a^3\rho_l$ |
| si $3l = 4g+5$ | $4a^3\rho_{l-1}$ |
| si $2l = 3g+3$ | $a^4\rho_{g+1}$ |
| sinon | 0 |

**Remarque :** Les expressions de $\mathcal{A}$ pour $1 \leq g \leq 5$ et $l \in \mathcal{S}_g$ s'obtiennent aisément et n'affectent en rien les résultats qui suivent.

**Lemme 2.4** *Pour tout $g \geq 1$ et $l$ tel que $g+1 \leq l \leq 2g+1$, la courbe $(C_{1,l})$ définit une famille géométrique à un paramètre de courbes de genre $g$.*

Le lemme **2.2** montre que l'invariant absolu $\gamma(f_{t,a,l})$ est un élément bien défini de $\mathbf{Q}(t,a)$.

Les cas $1 \leq g \leq 5$ se traitent directement à l'aide d'un ordinateur. Supposons $g \geq 6$ dans la suite de la démonstration de ce lemme.

Remarquons tout d'abord que :

$$f_{0,a,l}(x) = \left(x^{l-g-1}(x^{2g+2-l}+a)+x^g\right)^2,$$

et

$$f_{t,0,l}(x) = (x+1)x^{2g+1-l}\left(x^{l-1}(x+1)-2t\right),$$

donc, pour tout $l$ tel que $g+1 \leq l \leq 2g+1$ (resp. $g+1 \leq l \leq 2g-1$), une puissance strictement positive de $t$ (resp. $a$) divise le discriminant $\mathcal{D}(f_{t,a,l})$. Ceci établit le lemme pour les $l \in [g+1, 2g-1]$ tels que $\mathcal{A} \neq \mu at$ où $\mu \in \mathbf{Q}^*$.

Notons ici $\mathcal{N} = \{l \in [g+3, 2g-2]\ ;\ \exists \mu \in \mathbf{Q}^*,\ \mathcal{A} = \mu at\} \cup \{2g, 2g+1\}$. Supposons $g+2 \leq l \leq 2g$, $t \neq 0$, et soit $x_0$ tel que $f_{t,a,l}(x_0) = f'_{t,a,l}(x_0) = 0$. De l'équation

$$P^2_{t,a,l}(x) - Q^2_{l-g-1}(x) f_{t,a,l}(x) = t^2,$$

on déduit le système

$$\begin{cases} P^2_{t,a,l}(x_0) & = t^2 \\ P'_{t,a,l}(x_0) & = 0 \end{cases}$$

Réciproquement, si $x_0 \neq 0$ est solution de ce système, $x_0$ est racine multiple de $f_{t,a,l}(x)$. Ceci est le cas avec $x_0 = -\frac{2g+1-l}{2g+2-l}$ et $a_0 = -x_0^{2g+1-l}(x_0+1)$, donc $a - a_0$ divise $\mathcal{D}(f_{t,a,l})$. Il est clair que $a_0 \neq 0$, ce qui, en vertu du lemme **2.3**, montre que $\gamma(f_{t,a,l})$ est non constante pour $l \in \mathcal{N} - \{2g, 2g+1\}$.

Pour $l = 2g$, $a_0 = \frac{2g}{2g^2+3g+3}$ équivaut à $g = 1$, cas que nous avons déjà traité.

Enfin, supposons $l = 2g+1$ et $t \neq 0$. On a

$$\begin{cases} f_{t,a,2g+1}(x) & = (x+a+1)\left(x^{2g}(x+a+1)-2t\right) \\ f'_{t,a,2g+1}(x) & = x^{2g}(x+a+1) - 2t + (x+a+1)x^{2g-1}\left(2g(x+a+1)+x\right) \end{cases}$$

Soit $x_0$ tel que $x_0^{2g+1} + 4tg = 0$ et $a_0 = -\frac{(2g+1)x_0+2g}{2g}$. Le calcul montre que

$$f_{t,a_0,2g+1}(x_0) = f'_{t,a_0,2g+1}(x_0) = 0,$$

si bien que $a - a_0$ divise le discriminant par rapport à $x$ de $f_{t,a,2g+1}$. Comme $x_0 \neq 0$, $a_0 \neq -1$, donc $a - a_0$ ne divise pas $\mathcal{A}(f_{t,a,2g+1})$ et le lemme **2.4** est démontré.

**Lemme 2.5** *Pour tout $g \geq 1$ et tout entier $l$ tel que $g+1 \leq l \leq 2g+1$, l'ordre de la classe de $D_\infty$ dans la jacobienne de $(C_{1,l})$ est égal à $l$.*

Si $l$ est premier, ce lemme est démontré. Supposons donc $l = mn$, où $m$ et $n$ sont deux entiers $\geq 2$, et soit $\psi(x,y) = U(x) - yV(x)$ avec $U$ et $V$ deux éléments de $\mathbf{Q}(a,t)[x]$ premiers entre eux en la variable $x$, telle que

$$(\psi) = mD_\infty.$$

Par suite, il existe $\lambda \in \mathbf{Q}^*$ tel que $\varphi = \lambda\psi^n$.

Supposons $g+2 \leq l \leq 2g+1$, et montrons que, nécessairement, $n=2$. Pour cela, choisissons $t = \frac{1-v^2}{4}$ et $a = \frac{2}{v^2-1}$. Les deux points $R_0 = (0,1)$ et $R_1 = (1, v\frac{v^2+1}{v^2-1})$ sont des points rationnels sur la courbe et l'on a

$$\varphi(R_0) = \frac{v^2-1}{4} \qquad \text{et} \qquad \varphi(R_1) = \frac{(v-1)^3}{4(v+1)}.$$

Donc l'équation

$$\frac{\varphi(R_0)}{\varphi(R_1)} = \left(\frac{\psi(R_0)}{\psi(R_1)}\right)^n$$

s'écrit

$$\psi(R_1)^n (v+1)^2 = \psi(R_0)^n (v-1)^2.$$

On peut supposer cette identité dans $\mathbf{Q}[v]$ et $\psi(R_0)$ et $\psi(R_1)$ premiers entre eux sans nuire à la généralité du problème. Il existe alors un élément non nul $\chi_0$ de $\mathbf{Q}[v]$ tel que $\psi(R_0) = (v+1)\chi_0$, et l'on a :

$$\psi(R_1)^n = (v-1)^2 (v+1)^{n-2} \chi_0^n,$$

ce qui impose $n=2$.

Par suite

$$\lambda(U^2(x) + f_{t,a,l}(x)V^2(x) - 2yU(x)V(x)) = x^l + x^{l-1} + ax^{2l-2g-2} - t - yx^{l-(g+1)},$$

soit encore

$$2\lambda U(x)V(x) = x^{l-(g+1)}$$

et

$$\text{(E)} \qquad \lambda\left(U^2(x) + f_{t,a,l}(x)V^2(x)\right) = x^l + x^{l-1} + ax^{2l-(2g+2)} - t.$$

Le degré du membre de droite de l'égalité (E) est égal à $l$. $U$ et $V$ étant premiers entre eux, supposons dans un premier temps $U(x) = u_0 x^{l-(g+1)}$ $(u_0 \neq 0)$ et $V(x) = \frac{1}{2u_0\lambda}$. En ce cas, le degré du membre de gauche de (E) est celui de $f_{t,a,l}$ *i-e* $2g+2$. Si maintenant $V(x) = v_0 x^{l-(g+1)}$ $(v_0 \neq 0)$ et $U(x) = \frac{1}{2\lambda v_0}$, le degré du membre de gauche de (E) est $\geq 2g+2$. Dans l'un et l'autre cas, on aboutit à une contradiction, et donc, si $g+2 \leq l \leq 2g+1$, la classe du diviseur $D_\infty$ définit un point rationnel de la jacobienne de $C_{1,l}$ d'ordre $l$.

Supposons maintenant $l = g+1$. L'expression de $f_{t,a,l}$ est donnée par :

$$f_{t,a,g+1}(x) = (x^g(x+1) + a - t)^2 - t^2.$$

Prenons $t = \frac{(a-u)(a+u)}{2a}$, où $u$ est une indéterminée. On a alors $f_{t,a,g+1}(0) = u^2$ si bien que $R_0 = (0,u)$ est un point rationnel sur la courbe. De plus $\varphi(R_0) = \frac{(a-u)^2}{2a}$, et l'on a l'identité suivante dans $\mathbf{Q}(a,u)$ :

$$2\lambda a \psi^n(R_0) = (a-u)^2.$$

Soient donc $R, S \in \mathbf{Q}[a,u]$ premiers entre eux, tels que $\psi(R_0) = \frac{R(a,u)}{S(a,u)}$. Il vient

$$2\lambda a R^n(a,u) = (a-u)^2 S^n(a,u).$$

Par conséquent $a$ divise $S(a,u)$, ce qui impose $n=1$ et donc $D_\infty$ définit dans ce cas également un point rationnel de la jacobienne de $(C_{1,l})$ d'ordre $l$, ce qui achève la démonstration du lemme **2.4** et donc du théorème **1.1**. En particulier, la conjecture est établie avec la constante $\kappa = 2$.

**Remarque :** Soit $g \geq 2$ et $l$ tel que $g+1 \leq l \leq 2g+1$. La courbe $(C_{Q,R})$ définit vraisemblablement une famille en les paramètres de $Q$ et $R$, dans un sens convenable, de courbes hyperelliptiques de genre $g$, mais nous n'avons pas de preuve de ce fait en toute généralité.

# 3 Les résultats de Flynn

Considérons les deux suites d'éléments de $\mathbf{Z}[x]$ définies par les relations :

$$\theta_1(x) = \psi_1(x) = 1$$

et, pour $i \geq 1$,

$$\theta_{i+1}(x) = (x+2)\theta_i(x) + 2(x+1)\psi_i(x),$$
$$\psi_{i+1}(x) = 2\theta_i(x) + (x+2)\psi_i(x).$$

Nous montrons dans cette section le théorème **1.2**. Pour ce faire, nous rappelons l'énoncé suivant de Flynn ([F-2], Result 1, p. 435) :

**Théorème 3.1** *Pour tout $g \geq 1$ et tout entier $r$ tel que $1 \leq r \leq \frac{g}{2}$,*
*(a) la classe du diviseur rationnel $D = \{(0,0), (g-1).\infty\}$ dans la jacobienne des courbes hyperelliptiques de genre $g$ de la famille à $(g-2r+2)$ paramètres définies par :*

$$y^2 + (\psi_r(x)y - \theta_r(x)x^g).\sum_{k=0}^{g-2r+1} w_k x^k = x^{2g+1} + x^{2g},$$

*où $w_0 \neq 0$ ou $-4^{2-r}$, est d'ordre $l = 2g + 2r - 1$;*
*(b) la classe du diviseur rationnel $D = \{(0,0), (g-1).\infty\}$ dans la jacobienne des courbes hyperelliptiques de genre $g$ de la famille à $(g-r+1)$ paramètres définies par :*

$$y^2 = (y - x^{g+r})\left(x^{g-r+1} + \sum_{k=0}^{g-r} w_k x^k\right),$$

*où $w_0 \neq 0$, est d'ordre $l = 2g + 2r$.*

Dans son article, Flynn montre que l'ordre de la classe du diviseur $D$ dans la jacobienne des courbes définies ci-dessus est égal à $l$. En revanche, il ne vérifie pas que le genre de ces courbes est égal à $g$, ni que ces courbes sont non constantes. Nous montrons dans cette section que le genre des courbes du théorème **3.1** est bien le genre apparent $g$ et, dans le cas *(b)*, que ces courbes définissent une famille géométrique à un paramètre de courbes hyperelliptiques sur $\mathbf{Q}$. Nous n'avons pu établir ce dernier résultat dans le cas *(a)*.

**Cas (a) :**

Notons $S_{g+1-2r}(x) = \sum_{k=0}^{g+1-2r} w_k x^k$. La courbe considérée est $\mathbf{Q}$-isomorphe à la courbe notée ici $C^{(a)}_{2,S}$, d'équation

$$y^2 = 4x^{2g+1} + 4x^{2g} + 4x^g\theta_r(x)S_{g+1-2r}(x) + \psi_r^2(x)S^2_{g+1-2r}(x). \tag{A}$$

Choisissons $S_{g+1-2r}(x) = ax^{g+1-2r} + t$ ; notons alors $C^{(a)}_{2,r}$ la courbe ainsi obtenue, et $k_{t,a,r}(x)$ le membre de droite de (A).

En considérant le degré en $a$ de $k_{t,a,r}(x)$, il est aisé d'établir le

**Lemme 3.2** *Pour tout $g \geq 1$ et tout entier $r$ tel que $1 \leq r \leq \frac{g}{2}$, le discriminant $\mathcal{D}(k_{t,a,r})$ est non identiquement nul.*

**Cas (b) :**

Notons $R_{g-r}(x) = \sum_{k=0}^{g-r} w_k x^k$. La courbe considérée est $\mathbf{Q}$-isomorphe à la courbe notée ici $C^{(b)}_{2,R}$, d'équation

$$y^2 = -4x^{2g+1} - 4x^{g+r}R_{g-r}(x) + \left(x^{g+1-r} + R_{g-r}(x)\right)^2. \tag{B}$$

Comme $r \leq g - r$, il est licite de choisir $R_{g-r}(x) = ax^r + t$ dans l'équation (B). Notons avec ce choix $C^{(b)}_{2,r}$ la courbe ainsi obtenue, et $h_{t,a,r}(x)$ le membre de droite de (B).

**Lemme 3.3** *Pour tout $g \geq 1$, et tout entier $r$ tel que $1 \leq r \leq \frac{g}{2}$, le discriminant $\mathcal{D}(h_{t,a,r})$ est non identiquement nul.*

Si $r = 1$, on a

$$h_{t,0,1}(x) = -3x^{2g+1} - 4x^{g+1} + 2tx^g + t^2,$$

et, si $g \geq 4$ et $2 \leq r \leq g/2$,

$$h_{t,0,r}(x) = -4^{2g+1} - 4tx^{g+r} + x^{2g+2-2r} + 2tx^{g+1-r} + t^2.$$

Il est alors aisé de montrer, par des techniques similaires à celles de la section **2**, que $\mathcal{D}(h_{t,0,r}) \neq 0$, ce qui établit le lemme **3.3**.

Par ailleurs,

$$h_{0,a,r}(x) = -4x^{2g+1} - 4ax^{g+2r} + x^{2g+2-2r} + 2ax^{g+1} + a^2x^{2r}.$$

Le calcul montre alors :

**Lemme 3.4** *Pour tout $g \geq 1$ et tout entier $r$ tel que $1 \leq r \leq \frac{g}{2}$, l'invariant $\mathcal{A}(h_{0,a,r})$ est égal à*

$$2a^2\left(\binom{2g+2}{2r}^{-1} + 2(-1)^{g+1}\binom{2g+2}{g+1}^{-1}\right) - \begin{cases} 8a^3\binom{2g+2}{2r}^{-1} & \text{si } g+2 = 4r \\ 0 & \text{sinon.} \end{cases}$$

Le lemme **3.3** montre que l'invariant absolu $\gamma(h_{t,a,r}) = \frac{\mathcal{A}^{2g+1}(h_{t,a,r})}{\mathcal{D}(h_{t,a,r})}$ est un élément bien défini de $\mathbf{Q}(t,a)$. On a alors le

**Lemme 3.5** *Pour tout $g \geq 1$ et $r$ tel que $1 \leq r \leq \frac{g}{2}$, la courbe $C^{(b)}_{2,R}$ définit une famille géométrique à un paramètre de courbes hyperelliptiques de genre $g$.*

En effet, d'une part, pour tout entier $r$ tel que $1 \leq r \leq \frac{g}{2}$, 0 est racine multiple de $h_{0,a,r}(x)$, et, d'après le lemme **3.4**, $\mathcal{A}(h_{0,a,r}) \neq 0$, donc

$$\gamma(h_{0,a,r}) = \infty.$$

D'autre part, le lemme **3.3** montre que, pour tout entier $r$ tel que $1 \leq r \leq \frac{g}{2}$, il existe $(t_r, a_r)$ tel que $\mathcal{D}(h_{t_r,a_r,r}) \neq 0$. Par conséquent

$$\gamma(h_{t_r,a_r,r}) \in \mathbf{Q},$$

si bien que $\gamma(h_{t,a,r})$ est non constant, ce qui établit le lemme **3.5**.

Le théorème **1.2** découle immédiatement de la démonstration de [F-2], Result 1, p. 435, et des lemmes **3.2** et **3.5**.

*Remerciements :* L'auteur tient à remercier Don Zagier pour son intérêt et ses remarques.

# Bibliographie

[F-1] Flynn, E. V. : Large rational torsion on abelian varieties, J. Number Theory **36**, 257-265 (1990).

[F-2] Flynn, E. V. : Sequences of rational torsions on abelian varieties, Invent. Math. **106**, 433-442 (1991).

[L-1] Leprévost, F. : Famille de courbes hyperelliptiques de genre $g$ munies d'une classe de diviseurs rationnels d'ordre $2g^2+4g+1$, Séminaire de Théorie des Nombres de Paris, Progress in Math., Birkhäuser, **116**, 107-119 (1991-1992).

[L-2] Leprévost, F. : Sur certains sous-groupes de torsion de jacobiennes de courbes hyperelliptiques de genre $g \geq 1$. Prépublication M.P.I.

[M] Mestre, J.-F. : Construction explicite des courbes de genre 2 à partir de leurs modules. In Effective Methods in Algebraic Geometry, Progress in Math., Birkhäuser, **94**, 313-334 (1991).

# Sur certains sous-groupes de torsion de jacobiennes de courbes hyperelliptiques de genre $g \geq 1$

Franck Leprévost

## Introduction

Soient $g$ et $d$ deux entiers $\geq 1$ et $A$ une variété abélienne de dimension $g$ définie sur un corps de nombres $K$ de degré $d$. La *conjecture forte de la borne de l'ordre de torsion des variétés abéliennes* stipule que $|A(K)_{tors}|$, le cardinal du sous-groupe des éléments d'ordre fini de $A(K)$, est majoré par une borne $B$, ne dépendant que de $g$ et $d$ (dans une version affaiblie, $B$ ne dépend que de $g$ et du corps $K$). Si $g = 1$, cette conjecture a été établie pour $d \leq 14$ sous l'impulsion des travaux de Mazur, Kamienny, Abramovich ([12], [5], [6], [1]) et finalement, pour tout $d \geq 1$ par Merel ([13]). Pour une description des méthodes employées par Kamienny et Mazur, l'on pourra consulter le rapport de Edixhoven ([2]). En revanche, à l'heure actuelle, pour aucun $g \geq 2$ et aucun $d \geq 1$ (resp. aucun corps de nombres), la conjecture de la torsion forte (resp. faible) n'est démontrée ou infirmée. Il est donc naturel de chercher une *minoration* de la borne conjecturale correspondant aux jacobiennes des courbes hyperelliptiques de genre $g$, qui sont les variétés abéliennes généralisant en dimension supérieure de la manière peut-être la plus naturelle les variétés abéliennes de dimension 1 *i.-e.* les courbes elliptiques. Nous considérons ici le cas $d = 1$, et convenons de noter $B(g)$ le majorant conjectural de l'ordre des sous-groupes *cycliques* de torsion des jacobiennes des courbes hyperelliptiques de genre $g$ définies sur $\mathbf{Q}$.

Notons, si $g \geq 1$, $C_{1,t}$ et $C_g$ les courbes d'équations respectives $y^2 = f_{1,t}(x)$ et $y^2 = f_g(x)$, où

$$f_{1,t}(x) = [x((x-1)^g - x^g) + t((x-1)^g + x^g)]^2 + 4tx^{2g+1}$$

et

$$\begin{aligned} f_g(x) \quad = \quad & [2(g+3)(2x-g-3)x^{g+1} - (x-1)^{g-1}(4(g+3)x^3 + 2(g-5)(g+3)x^2 \\ & +(g^2-2g+9)(g+3)x - 8)]^2 - 8(g+3)(g+1)^4 x^{g+2}(x-1)^{g-1}. \end{aligned}$$

Nous montrons dans cet article les résultats suivants :

**Théorème 1** *Pour tout entier $g \geq 1$, la courbe $C_{1,t}$ définit une famille géométrique à un paramètre de courbes hyperelliptiques de genre $g$ définies sur $\mathbf{Q}$, et dont la jacobienne possède un point rationnel d'ordre $2g(2g+1)$.*

**Théorème 2** *Si $g \geq 2$, le genre de $C_g$ est égal à $g$. Si de plus $g$ est pair, sa jacobienne possède un point rationnel d'ordre $l = 2g^2 + 5g + 5$.*

Plus généralement :

**Théorème 3** *Si $g \geq 2$, il existe une courbe $C_{2,w}$ définissant une famille géométrique à un paramètre de courbes hyperelliptiques de genre $g$ dont la jacobienne est munie d'un point rationnel d'ordre divisant $l$. Si $g$ est pair (resp. $g \equiv -1 \bmod 4$, resp. $g \equiv 1 \bmod 4$), cet ordre est égal à $l$ (resp. multiple de $\frac{l}{2}$, resp. multiple de $\frac{l}{4}$).*

Ces théorèmes admettent les corollaires suivants :

**Corollaire 4** *Pour tout entier $g \geq 1$, il existe une infinité de courbes hyperelliptiques définies sur $\mathbf{Q}$, deux-à-deux non $\bar{\mathbf{Q}}$-isomorphes, et dont la jacobienne possède un point rationnel d'ordre $2g(2g+1)$.*

**Corollaire 5** *Pour tout entier pair $g \geq 2$, il existe une infinité de courbes hyperelliptiques définies sur $\mathbf{Q}$, deux-à-deux non $\bar{\mathbf{Q}}$-isomorphes, et dont la jacobienne possède un point rationnel d'ordre $2g^2+5g+5$.*

**Corollaire 6** *Pour tout entier $g \geq 1$, $B(g) \geq 2g(2g+1)$.*

Le corollaire **4** (resp. **5**) s'obtient par spécialisation du paramètre dans le théorème **1** (resp. **3**), et le corollaire 6 en considérant l'une des courbes vérifiant les propriétés du corollaire **4**.

Cet article est structuré de la manière suivante : dans une première partie, nous rappelons brièvement la théorie des invariants de formes binaires (*cf.* [14]), et définissons la notion de *famille géométrique, i.-e, à module non constant, de courbes hyperelliptiques.* Dans la deuxième partie, nous décrivons la méthode de construction de la courbe $C_{1,t}$. Nous calculons dans la troisième partie les invariants de $C_{1,t}$ et démontrons le théorème **1**. Nous décrivons, dans la quatrième partie, la méthode de construction des courbe $C_g$ et $C_{2,w}$, qui est commune jusqu'à un certain point. Nous démontrons le théorème **2** dans la cinquième partie. L'objet de la dernière partie est de donner une équation de $C_{2,w}$, et de montrer le théorème **3**. Terminons cette introduction par les remarques suivantes :

1) A notre connaissance, jusqu'alors, l'ordre le plus élevé au regard du genre d'un sous-groupe de torsion cyclique de la jacobienne d'une courbe (hyperelliptique ou non) de genre $g$ était $2g^2+4g+1$ (*cf.* [8]). Il est également établi, dans [3] et [7], que certains entiers, inférieurs à $2g^2+4g+1$, mais néanmoins quadratiques en le genre $g$, sont ordres de torsion de points rationnels de jacobiennes de certaines courbes hyperelliptiques de genre $g$ définies sur $\mathbf{Q}$. Les courbes données ici, ne provenant en outre d'*aucune* de celles décrites dans ces travaux, sont donc les "meilleures" connues actuellement pour ce type de problème.

2) La courbe $C_{2,w}$ généralise celle obtenue par Ogawa ([15]) en genre 2. En revanche, la courbe $C_g$ ne semble avoir été étudiée auparavant pour *aucun* $g \geq 2$. En particulier, $C_2$, d'équation $y^2 = -3240x^5 + 8865x^4 - 7950x^3 + 4009x^2 - 848x + 64$, fournit un nouvel exemple de courbe de genre 2 dont la jacobienne possède un point rationnel d'ordre 23. En effet, cette courbe n'est pas $\overline{\mathbf{Q}}$-isomorphe à un élément de la famille d'Ogawa ([15]), ni à celle obtenue dans [9] (voir également [10] pour une étude plus détaillée des courbes données dans [9]), comme le montre une étude des invariants d'Igusa ([4]) de ces courbes.

3) Pour aucun $g \geq 2$, on ne sait s'il existe un $l \geq 1$ qui n'est ordre de torsion d'un point rationnel d'*aucune* variété abélienne de dimension $g$ définie sur un corps de nombres. Néanmoins, on peut montrer ([11]) que, pour tout entier $g \geq 1$ et $l < 3g$, il existe une famille géométrique à un paramètre de courbes hyperelliptiques définies sur $\mathbf{Q}$, dont la jacobienne est munie d'un point rationnel d'ordre $l$.

*Remerciements :* l'auteur tient à remercier Michael D. Fried, Jean-François Mestre, Michel Waldschmidt et Don B. Zagier de leur intérêt pour ces questions, ainsi que le Max-Planck-Institut für Mathematik de son hospitalité.

# 1 Invariants de courbes hyperelliptiques

Soit

$$F = a_0X^n + a_1X^{n-1}Y + \cdots + a_nY^n$$

une forme binaire de degré $n$, à coefficients dans un corps $K$ de caractéristique 0. Un *invariant* de $F$ est une expression polynômiale $I(a_0, \ldots, a_n)$ telle que

$$I(a'_0, \ldots, a'_n) = (\det M)^{-k} I(a_0, \ldots, a_n),$$

si l'on fait subir à $F$ une transformation

$$\begin{cases} x &= rx' + sy' \\ y &= tx' + uy' \end{cases}$$

où $M = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$ de $\mathrm{GL}_2(\bar{K})$. Le *degré* de $I$ est le degré total de $I$ relativement à $(a_0, \ldots, a_n)$, et $k$ est l'*indice* de $I$. Un *invariant absolu* de $F$ est un quotient de deux invariants de même degré.

Soit maintenant $y^2 = f(x)$ où $f(x) = a_0x^{2g+2} + a_1x^{2g+1} + \cdots + a_{2g+2}$ est un élément de $K[x]$, de degré $2g+1$ ou $2g+2$, sans racines multiples. On lui associe la forme binaire $F$ définie par

$$F(X,Y) = Y^{2g+2} f(\frac{X}{Y}).$$

Un *invariant* (resp. *invariant absolu*) de $f$ est entendu comme étant celui de la forme binaire $F$ associée. Deux équations non homogènes $y^2 = f(x)$ et $y'^2 = f'(x')$ correspondent à deux courbes $K-$isomorphes si et seulement si l'on déduit l'une de l'autre par une transformation

$$(x', y') = (\frac{ax+b}{cx+d}, \frac{uy}{(cx+d)^{g+1}}),$$

$a, b, c, d, u \in K$, $ad-bc$ et $u$ non nuls. Pour tout invariant $I_s$ de degré $s$ des formes binaires de degré $2g+2$, on a alors $I_s(f) = M^s I_s(f')$ avec $M = (ad-bc)^{g+1}u^{-2}$. Réciproquement, s'il existe $r \in \bar{K}^*$ tel que, pour tout invariant $I_s$ de degré pair $s$ des formes binaires de degré $2g+2$, $I_s(f) = r^s I_s(f')$, les courbes d'équations $y^2 = f(x)$ et $y^2 = f'(x)$ sont $\bar{K}$-isomorphes.

Nous considérons dans cet article exclusivement l'invariant absolu $\gamma(f)$ défini par

$$\gamma(f) = \frac{\mathcal{A}^{2g+1}(f)}{\mathcal{D}(f)},$$

où $\mathcal{D}(f)$ désigne le discriminant de la forme binaire $F$ (lequel est égal, lorsque $a_0 = 0$, à $a_1^2\Delta(f)$, où $\Delta(f)$ est le discriminant de $f$), $\mathcal{A}(f) = \sum_{k=0}^{2g+2} \frac{(-1)^k}{C_{2g+2}^k} a_k a_{2g+2-k}$ (*cf.* [7], p. 305) et $C_n^k$ désigne le nombre de combinaisons à $k$ éléments d'un ensemble à $n$ éléments ($= 0$ si $k > n$ ou si $k < 0$). $\mathcal{D}(f)$ (resp. $\mathcal{A}(f)$) est un invariant de degré $2(2g+1)$ (resp. 2) et d'indice $(2g+2)(2g+1)$ (resp. $2g+2$).

Nous dirons ici qu'une équation $y^2 = f_t(x)$ où $f_t(x)$ est un polynôme de degré $2g+1$ ou $2g+2$, à coefficients dans $\mathbf{Q}(t)$ sans racines multiples, définit une *famille géométrique à un paramètre de courbes hyperelliptiques de genre $g$ sur* $\mathbf{Q}$ si l'image de la courbe dans la variété de modules des courbes de genre $g$ est non constante. C'est le cas si et seulement si l'un au moins de ses invariants absolus, par exemple $\gamma(f_t)$, est une fraction rationnelle non constante. Une telle famille permet, par spécialisation du paramètre en des valeurs rationnelles, d'obtenir une infinité de courbes hyperelliptiques de genre $g$ deux à deux non $\bar{\mathbf{Q}}$-isomorphes.

## 2 Construction de la courbe $C_{1,t}$

Fixons $g$ un entier $\geq 1$, et soient $t \in \mathbf{Q}^*$ et $A$ un élément de degré $\leq g$ de $\mathbf{Q}[x]$ tels que la courbe $C$ d'équation

$$y^2 = f(x) = A^2(x) + 4tx^{2g+1}$$

soit hyperelliptique et de genre $g$. Notons $\infty$ son unique point à l'infini, $P_0 = (0, A(0))$ et $D_0$ le diviseur $(P_0) - (\infty)$.

**Lemme 2.1** *S'il existe un diviseur rationnel $D_1$ tel que $2gD_1 \sim D_0$, alors $D_1$ définit un point rationnel de la jacobienne de $C$ d'ordre divisant $2g(2g+1)$.*

Il est en effet clair sur l'équation définissant $C$ que le diviseur de la fonction $\varphi = y - A(x)$ est

$$(\varphi) = (2g+1)D_0.$$

Par conséquent $D_0$ définit un point rationnel de la jacobienne de $C$ d'ordre divisant $2g+1$. En fait, on montre très aisément que cet ordre est égal à $2g+1$. Considérons alors la fonction $\chi$ de diviseur

$$(\chi) = 2gD_1 - D_0.$$

Il vient alors

$$(\varphi\chi^{2g+1}) = 2g(2g+1)D_1,$$

ce qui termine la preuve de ce lemme. On peut de plus remarquer que l'ordre de la classe de $D_1$ est $\geq 2g+1$.

Notons $P_1 = (1, y_1)$ (le calcul montre que l'on peut supposer l'abscisse de $P_1$ égale à 1, son ordonnée sera fixée ultérieurement). La stratégie adoptée ici consiste à déterminer $C$ de sorte que le diviseur $D_1 = (P_1) - (\infty)$ vérifie les hypothèses du lemme **2.1**, dont nous conservons les notations.

Le diviseur de la fonction $\psi = x\chi$ est

$$(\psi) = 2g(P_1) + (P_0^g) - (2g+1)(\infty),$$

où $\sigma$ désigne l'involution hyperelliptique. En particulier $\psi \in \mathcal{L}((2g+1)(\infty))$. Par le théorème de Riemann-Roch, cet espace vectoriel est engendré par les fonctions $\{1, x, \ldots, x^g, y\}$, si bien qu'il existe un élément $U$ de $\mathbf{Q}[x]$ de degré $\leq g$, tels que $\psi = y - U$. La condition sur le diviseur des zéros nécessite l'équation

$$(A-U)(A+U) = 4tx((x-1)^g - x^g)((x-1)^g + x^g).$$

Comme $\psi(P_0^g) = 0$, il vient le système (on vérifie *a posteriori* que l'on peut procéder à une factorisation de la sorte sans restreindre la généralité du problème)

$$\begin{cases} A-U &= 2t[(x-1)^g + x^g] \\ A+U &= 2x[(x-1)^g - x^g]. \end{cases}$$

D'où

$$\begin{cases} U &= x[(x-1)^g - x^g] - t[(x-1)^g + x^g] \\ A &= x[(x-1)^g - x^g] + t[(x-1)^g + x^g]. \end{cases}$$

Si bien que

$$f_{1,t}(x) = [x((x-1)^g - x^g) + t((x-1)^g + x^g)]^2 + 4tx^{2g+1}.$$

Or $P_1$ est un zéro de $\psi$, ce qui impose $y_1 = -(t+1)$, compte tenu de ce que $U(1) = -1 - t$. Comme $f_{1,t}(1) = (t+1)^2$, il est désormais clair que $D_1 = (P_1) - (\infty)$ définit un point rationnel de la courbe $C_{1,t}$ d'équation $y^2 = f_{1,t}(x)$. Réciproquement, comme on le vérifie aisément, la fonction $\chi$ ainsi obtenue a bien pour diviseur $2gD_1 - D_0$.

# 3 Preuve du théorème 1

**Lemme 3.1** *Le discriminant $\Delta(f_{1,t})$ est un élément de $\mathbf{Q}[t]$ non identiquement nul, et divisible par $t+1$.*

Supposons que $\Delta(f_{1,t})$ soit identiquement nul. Il existe alors $P_1(t,x)$ et $P_2(t,x)$, éléments de $\mathbf{Q}[t,x]$, tels que

$$f_{1,t}(x) = P_1(t,x)P_2(t,x)^2.$$

Comme $d^0(f_{1,t}) = 2$, $(d^0(P_1), d^0(P_2)) = (0,1)$ ou $(2,0)$. Supposons $(d^0(P_1), d^0(P_2)) = (0,1)$. Alors $P_1(x) = P_1(t,x)$ divise tous les coefficients de $t$ dans $f_{1,t}(x)$. Il existe donc $Q_1$ et $Q_2$ éléments de $\mathbf{Q}[x]$, tels que

$$\begin{cases} (x-1)^g + x^g &= P_1(x)Q_1(x) \\ x[(x-1)^g - x^g] &= P_2(x)Q_2(x), \end{cases}$$

Donc $P_1(x) = ax$ pour un $a \in \mathbf{Q}^*$. En particulier $P_1(0) = 0 = f_{1,t}(0)$, ce qui est impossible dès que $t \neq 0$. De façon similaire, on montre que $(d^0(P_1), d^0(P_2)) = (2,0)$ est absurde. La seconde assertion découle de ce que $f_{1,-1}(x) = (x-1)^2[(x-1)^{2g} - 2x^g(x-1)^{g-1}(x+1) + x^{2g}]$, ce qui termine la preuve de ce lemme. Remarquons que $f_{1,0}(x) = [x(x-1)^g - x^{g+1}]^2$, et $t$ divise également $\Delta(f_{1,t})$.

**Lemme 3.2** *Si $g \geq 3$, alors $\mathcal{A}(f_{1,-1}) = 16\frac{(-1)^{g+1}}{C_{2g+2}^{g+1}}$. En particulier, $t+1$ ne divise pas l'invariant $\mathcal{A}(f_{1,t})$.*

On vérifie aisément que tel est le cas si $g = 3$. On suppose $g \geq 4$ dans la suite de la démonstration de ce lemme. Avec les notations de la première partie, on a, si $0 \leq k \leq 2g+2$,

$$a_k = (-1)^k[C_{2g}^k + u_k - 2v_k C_{2g}^{k-1} t + (C_{2g}^{k-2} + w_k)t^2],$$

où $v_1 = 2$ et $v_k = 1$ si $k \neq 1$, et où

$$u_k = \begin{cases} -1 & \text{si} \quad k = 0, \\ -2C_g^k & \text{si} \quad 1 \leq k \leq g, \\ 0 & \text{si} \quad g+1 \leq k \leq 2g+2, \end{cases}$$

$$w_k = \begin{cases} 3 & \text{si} \quad k = 2, \\ 2C_g^{k-2} & \text{si} \quad 3 \leq k \leq g+2, \\ 0 & \text{sinon.} \end{cases}$$

Il vient

$$\begin{aligned} \mathcal{A}(f_{1,t}) &= 2\sum_{k=0}^{g} \frac{(-1)^k}{C_{2g+2}^k} a_k a_{2g+2-k} + \frac{(-1)^{g+1}}{C_{2g+2}^{g+1}} a_{g+1}^2 \\ &= \frac{8(gt-1)}{g+1}t^2 + \frac{2}{(g+1)(2g+1)}[4t^2 - 4gt + g^2][g(2g-1)t^2 - 4gt + 1] \\ &\quad +2\sum_{k=3}^{g-1} \frac{(-1)^k}{C_{2g+2}^k}[C_{2g}^k t^2 - 2C_{2g}^{k-1}t + C_{2g}^{k-2}][(2C_g^{k-2} + C_{2g}^{k-2})t^2 - 2C_{2g}^{k-1}t + C_{2g}^k - 2C_g^k] \\ &\quad +2\frac{(-1)^g}{C_{2g+2}^g}[(C_{2g}^{g+2} + 2C_g^2)t^2 - 2C_{2g}^{g+1}t + C_{2g}^g - 2][(C_{2g}^g + 2)t^2 - 2C_{2g}^{g-1}t + C_{2g}^{g-2}] \\ &\quad \frac{(-1)^{g+1}}{C_{2g+2}^{g+1}}[(2g + C_{2g}^{g+1})t^2 - 2C_{2g}^g t + C_{2g}^{g-1}]^2. \end{aligned}$$

On remarque que

$$\begin{cases} C_{2g}^{g+2} + 2C_g^2 + 2C_{2g}^{g+1} + C_{2g}^g - 2 &= C_{2g+2}^{g+2} + 2C_g^2 - 2, \\ C_{2g}^g + 2 + 2C_{2g}^{g-1} + C_{2g}^{g-2} &= C_{2g+2}^g + 2, \\ 2g + C_{2g}^{g+1} + 2C_{2g}^g + C_{2g}^{g-1} &= C_{2g+1}^{g+1} + 2g \end{cases}$$

et, si $3 \leq k \leq g-1$,

$$\begin{cases} C_{2g}^k + 2C_{2g}^{k-1} + C_{2g}^{k-2} &= C_{2g+2}^k, \\ 2C_g^{k-2} + C_{2g}^{k-2} + 2C_{2g}^{k-1} + C_{2g}^k - 2C_g^k &= 2C_g^{k-2} - 2C_g^k + C_{2g+2}^k. \end{cases}$$

Par conséquent

$$\begin{aligned} \mathcal{A}(f_{1,-1}) &= 2g(g+4) + 2\sum_{k=3}^{g-1}(-1)^k[2C_g^{k-2} - 2C_g^k + C_{2g+2}^k] \\ &\quad +2\frac{(-1)^g}{C_{2g+2}^g}[C_{2g+2}^{g+2} + 2C_g^2 - 2][C_{2g+2}^g + 2] + \frac{(-1)^{g+1}}{C_{2g+2}^{g+1}}[C_{2g+2}^{g+1} + 2g]^2. \end{aligned}$$

Par ailleurs, un calcul aisé montre

$$\begin{cases} 2\sum_{k=3}^{g-1}(-1)^k C_g^{k-2} &= (-1)^g g(3-g) - 2(1 + (-1)^g), \\ 2\sum_{k=3}^{g-1}(-1)^k C_g^k &= (g-1)(2-g) + 2(-1)^{g+1}, \\ 2\sum_{k=3}^{g-1}(-1)^k C_{2g+2}^k &= (-1)^g[C_{2g+2}^{g+1} - 2C_{2g+2}^g] - 2g(2g+1). \end{cases}$$

Donc

$$\begin{aligned}\mathcal{A}(f_{1,-1}) &= 2(-1)^{g+1}g^2+6(-1)^g g+(-1)^g[C_{2g+2}^{g+1}-2C_{2g+2}^g]\\ &\quad +2\frac{(-1)^g}{C_{2g+2}^g}[C_{2g+2}^g+2][C_{2g+2}^{g+2}+2C_g^2-2]+\frac{(-1)^{g+1}}{C_{2g+2}^{g+1}}[C_{2g+2}^{g+1}+2g]^2,\end{aligned}$$

soit encore

$$\begin{aligned}\mathcal{A}(f_{1,-1}) &= 4\frac{(-1)^g}{C_{2g+2}^g}[C_{2g+2}^{g+2}+2C_g^2-2-\frac{g^2(g+1)}{g+2}]-4(-1)^g\\ &= 4\frac{(-1)^{g+1}}{C_{2g+2}^{g+1}}[4\frac{g+1}{g+2}-C_{2g+2}^{g+2}+C_{2g+2}^g],\end{aligned}$$

et donc

$$\mathcal{A}(f_{1,-1})=16\frac{(-1)^{g+1}(g+1)}{(g+2)C_{2g+2}^g}=16\frac{(-1)^{g+1}}{C_{2g+2}^{g+1}},$$

et le lemme est démontré.

**Lemme 3.3** *$D_1$ définit un point rationnel de la jacobienne de $C_{1,t}$ d'ordre $2g(2g+1)$.*

D'après le lemme **2.1**, dont nous reprenons les notations,

$$2g(2g+1)D_1=(L),$$

où $L=\frac{\varphi\psi^{2g+1}}{x^{2g+1}}$. Supposons que l'ordre de la classe de $D_1$ soit l'entier $l$ tel que $lm=2g(2g+1)$ pour un $m\in\mathbf{N}^*$. Il existe alors une fonction $N$ telle que $lD_1=(N)$, et donc un élément $a\in\mathbf{Q}^*$ tel que $L=aN^m$. Evaluons $L$ en les points $P_0=(0,(-1)^g t)$ et $Q=(-t,0)$. Le calcul montre que $L(P_0)=2^{2g+2}t^{2g+1}$ et $L(Q)=-2\frac{(t+1)^g}{t^{g-1}}$. On obtient par conséquent l'identité suivante

$$(I_1)\qquad 2^{2g+1}N^m(Q)t^{3g}=-N^m(P_0)(t+1)^g,$$

dans laquelle on peut supposer $N(P_0)$ et $N(Q)$ éléments de $\mathbf{Z}[t]$. D'une part, la considération de la valuation en $t+1$ des deux membres de $(I_1)$ montre que $m$ divise $g$. D'autre part, une rapide étude de la valuation en 2 du contenu des deux membres de $(I_1)$ impose que $m$ doit également diviser $2g+1$, ce qui est nécessite $m=1$, et termine la démonstration de ce lemme.

Nous sommes en mesure de démontrer le théorème **1**. Nous supposons $g\geq 3$, les cas $g=1$ et $g=2$ se traitant aisément par ordinateur. Le lemme **3.1** montre que $C_{1,t}$ est génériquement de genre $g$, que $\gamma(f_{1,t})$ existe et, joint au lemme **3.2**, que $\gamma(f_{-1})=\infty$. Si l'on considère un $t_0\in\mathbf{Q}$ en dehors de l'ensemble fini des zéros de $\Delta(f_{1,t})$, alors $\gamma(f_{t_0})$ est un élément de $\mathbf{Q}$ (en effet, avec les notations de la première partie, $a_1=4t$, et donc les ensembles des racines de $\Delta(f_{1,t})$ et de $\mathcal{D}(F_{1,t})$ coïncident), en particulier $\gamma(f_{t_0})\neq\infty$ : $\gamma(f_{1,t})$ est donc un élément de $\mathbf{Q}(t)$ non constant. Ceci, joint au lemme **3.3**, termine la preuve du théorème **1**.

# 4 Méthode de construction de $C_g$ et $C_{2,w}$

Dorénavant $g$ désigne un entier $\geq 2$. Soient $t\in\mathbf{Q}^*$ et $A$ un élément de degré $\leq g$ de $\mathbf{Q}[x]$ tels que la courbe $C$ d'équation

$$y^2=f(x)=A^2(x)-4tx^{g+2}(x-1)^{g-1}$$

soit hyperelliptique et de genre $g$. Notons $\infty$ son unique point à l'infini, $P_0=(0,A(0))$, $P_1=(1,A(1))$ et $D_0$ et $D_1$ les diviseurs respectifs $(P_0)-(\infty)$ et $(P_1)-(\infty)$. La démonstration du lemme suivant est similaire à celle du lemme **2.1**.

**Lemme 4.1** *Si $-(g+1)D_0+(g+3)D_1$ est le diviseur d'une fonction $\chi$, alors la jacobienne de $C$ possède un point rationnel d'ordre divisant $2g^2+5g+5$ et différent de 1.*

La stratégie adoptée ici consiste à déterminer $C$ de sorte que les hypothèses du lemme **4.1**, dont nous conservons les notations, soient vérifiées. Remarquons pour ce faire, que le diviseur de la fonction $\psi = x^{g+1}\chi$ est

$$(\psi) = (g+1)(P_0^\sigma) + (g+3)(P_1) - (2g+4)(\infty),$$

où $\sigma$ désigne l'involution hyperelliptique. En particulier $\psi \in \mathcal{L}((2g+4)(\infty))$. Par le théorème de Riemann-Roch, cet espace vectoriel est engendré par les fonctions $\{1, x, \ldots, x^{g+2}, y, xy\}$, si bien qu'il existe des éléments $U$ de degré $\leq 1$ et $V$, dont on peut supposer le coefficient dominant égal à 2, de degré $g+2$ de $\mathbf{Q}[x]$, tels que $\psi = yU - V$. La condition sur le diviseur des zéros nécessite l'équation

$$(E_0) \qquad (AU-V)(AU+V) = 4x^{g+1}(x-1)^{g-1}[txU^2 - (x-1)^4].$$

On montre aisément que $x^{g+1}$ (resp. $(x-1)^{g-1}$) divise $AU+V$ (resp. $AU-V$). Nous construisons dans les parties suivantes des éléments $p$ et $q$ de $\mathbf{Q}[x]$, respectivement de degrés 1 et 3, tels que

$$(\mathrm{E}) \qquad txU^2(x) - (x-1)^4 = p(x)q(x),$$

selon que $U$ est de degré 0 ou 1. L'équation $(E_0)$ admet alors pour solution le système

$$(S) \quad \begin{cases} AU - V &= 2(x-1)^{g-1}q(x), \\ AU + V &= 2x^{g+1}p(x). \end{cases}$$

Réciproquement, si $U$ et $V$ sont solutions de $(S)$, alors le diviseur de $\chi$ est égal à $-(g+1)D_0+(g+3)D_1$.

# 5 Construction de $C_g$ et preuve du théorème 2

Nous supposons dans cette partie que $U$ est de degré nul. Quitte à modifier $t$, on peut supposer $U=1$, et $p(x) = x - v$. Si $t = \frac{(v-1)^4}{v}$, l'équation $(E)$ admet la solution $q(x) = -x^3 + (4-v)x^2 - (v^2-4v+6)x + \frac{1}{v}$. Du système $(S)$, on déduit

$$A = x^{g+1}p(x) + (x-1)^{g-1}q(x) = (g+3-2v)x^{g+1} + a(x),$$

où $a(x)$ est un élément de $\mathbf{Q}[x]$ de degré $\leq g$. Comme le degré de $A$ est $\leq g$, il vient $v = \frac{g+3}{2}$. Nous considérons, dans la suite de cette partie, l'équation de $C_g$ donnée en introduction, laquelle s'obtient aisément à partir des quantités précédentes. Le théorème 2 découle des deux lemmes suivants.

**Lemme 5.1** *Le genre de $C_g$ est égal à $g$.*

Notons $t = 2(g+3)(g+1)^4$ et $A_g(x) = x^{g+1}p(x) + (x-1)^{g-1}q(x)$, où $p$ et $q$ se déduisent de manière évidente de l'équation de $C_g$ donnée dans l'introduction. Il s'agit de montrer que $f_g$ est sans racine multiple. Supposons donc l'existence d'une telle racine multiple, $x_0$, nécessairement différente de 0 et 1 comme le montre un rapide calcul. De $f_g(x_0) = f_g'(x_0) = 0$, nous déduisons l'équation

$$2x_0(x_0-1)A_g'(x_0) = [(2g+1)x_0 - (g+2)]A_g(x_0),$$

soit encore $x_0^{g+1}G(x_0) = (x_0-1)^{g-1}H(x_0)$, où

$$\begin{cases} G &= (g+3)xp - 2(g+1)p + 8(g+3)x(x-1) \\ H &= 3xq - (g+2)q - 2x(x-1)q'. \end{cases}$$

L'unique racine entière positive du résultant de $G$ et $H$ par rapport à $x$ est $g=1$. Par conséquent, $G$ et $H$ sont sans racines communes (car $g \geq 2$), et $H(x_0)G(x_0) \neq 0$. Il vient alors $(x_0-1)^{g-1} = \frac{x_0^{g+1}G(x_0)}{H(x_0)}$. Notons $F_1$ et $F_2$ les éléments de $\mathbf{Q}[x]$ définis par

$$(x-1)^2F_1(x) = (Hp+Gq)^2 - 4txGH$$

et

$$\begin{aligned}(x-1)F_2(x) &= (Hp+Gq)[((g-1)q+(x-1)q')xG+((g+1)p+4(g+3)x)(x-1)H] \\ &\quad -2tGHx[(2g+1)x-(g+2)].\end{aligned}$$

Le calcul montre que les équations $f_g(x_0) = f'_g(x_0) = 0$ équivalent à $F_1(x_0) = F_2(x_0) = 0$. Le lemme découle de ce que le résultant de $F_1$ et $F_2$ par rapport à $x$ est un polynôme en $g$, n'admettant pour racine aucun entier positif.

**Lemme 5.2** *Si $g \geq 2$ est pair, l'ordre de la classe de $D_0$ est égal à $2g^2+5g+5$.*

Le diviseur de $L = \frac{\varphi^{g+3}x^{(g-1)(g+1)}}{\psi^{g-1}}$ est égal à $lD_0$, où $l = 2g^2+5g+5$ et $\varphi = y - A_g$. Si $l$ est premier, le lemme est trivial. Supposons donc $l = mn$, pour deux entiers $m, n \geq 2$, et l'ordre de la classe de $D_0$ égal à $n$. Par conséquent, il existe une fonction $M$ de diviseur $nD_0$. De manière similaire à la démonstration du lemme **3.2**, on évalue $L$ en $P_0^\sigma = (0, 8(-1)^{g-1})$ et en $P_1^\sigma = (1, -2(g+3)(g+1))$. On obtient ainsi l'égalité suivante, que l'on peut supposer dans $\mathbf{Z}$ :

$$(I_2) \qquad (g+1)^4(g+3)^{g-1}M(P_0^\sigma)^n = 4^{3g+1}M(P_1^\sigma)^n.$$

Supposons $g$ pair. D'une part, $l$ est impair, et donc $m$ et $n$ également. D'autre part, 2 ne divise ni $g+1$, ni $g+3$, et l'étude de la valuation en 2 des deux membres de $(I_2)$ montre que $n$ divise $2(3g+1)$, donc $n$ divise $3g+1$. Le lemme découle de ce que $l$ et $3g+1$ sont premiers entre eux.

# 6 Construction de $C_{2,w}$ et preuve du théorème 3

Nous supposons désormais que $U$ est de degré 1 et, quitte à modifier $t$, on peut supposer $U = x - u$. Si $p = x - v$ et $t = \frac{(v-1)^4}{v(v-u)^2}$, l'équation $(E)$ admet la solution

$$q = -x^3 + \frac{2uv^3+(6-8u-u^2)v^2+4(u^2-1)v+1}{v(v-u)^2}x^2 - \frac{u^2v^3+4(1-u^2)v^2+(6u^2-8u-1)v+2u}{v(v-u)^2}x + \frac{1}{v}.$$

Notons $R = x^{g+1}p + (x-1)^{g-1}q$. Le calcul montre que

$$(u-v)R(u) = u^{g+1}v^2 - 2u^{g+2}v + u^{g+3} - (u-1)^{g+3},$$

et le discriminant réduit par rapport à $v$ du second membre de l'égalité ci-dessus est

$$\delta = u^{g+1}(u-1)^{g+3}.$$

Si $g$ est impair, $\delta = \left[u^{\frac{g+1}{2}}(u-1)^{\frac{g+3}{2}}\right]^2$, et l'on a

$$v = \frac{u^{g+2} \pm u^{\frac{g+1}{2}}(u-1)^{\frac{g+3}{2}}}{u^{g+1}}.$$

Si $g$ est pair, on pose $u = \frac{1}{1-z^2}$, auquel cas $\delta = \left[\frac{z^{g+3}}{(1-z^2)^{g+3}}\right]^2$, et l'on a

$$v = \frac{1 \pm z^{g+3}}{1-z^2}.$$

Il est clair qu'avec ces choix $A = \frac{R}{U}$ est, dans les deux cas, un élément de $\mathbf{Q}[x]$. Nous choisissons dans l'un et l'autre cas, la fraction rationnelle $v$ avec le signe $-$ entre les deux membres du numérateur. Une équation de la courbe $C_{2,w}$ de l'énoncé du théorème **3** est donc $y^2 = f_{2,w}(x) = A^2 - 4tx^{g+2}(x-1)^{g-1}$, où le paramètre $w$ est égal à $u$ si $g$ est impair, et à $z$ si $g$ est pair. Le théorème **3** se déduit du lemme **4.1**, et des trois lemmes suivants.

**Lemme 6.1** *Le genre de $C_{2,w}$ est égal à $g$.*

La démonstration de ce lemme est analogue à celle du lemme **5.1**, en montrant que l'unique racine multiple de $h(x) = f(x)U^2(x)$ est, génériquement, $u$, dont on vérifie qu'elle n'est pas racine multiple de $f$.

Le lemme 6.1 montre, en particulier, que $\gamma(f_{2,w})$ est un élément bien défini de $\mathbf{Q}(w)$.

**Lemme 6.2** *Si $g$ est pair, l'ordre de la classe de $D_0$ dans la jacobienne de $C_{2,w}$ est égal à $l = 2g^2 + 5g + 5$. Si $g \equiv -1$ mod 4, cet ordre est un multiple de $\frac{l}{2}$. Si $g \equiv 1$ mod 4, cet ordre est un multiple de $\frac{l}{4}$.*

Nous conservons les notations et la méthode de la démonstration du lemme **5.2**. Nous supposons $l = mn$, avec $m, n \geq 2$, la classe de $D_0$ d'ordre $m$, et évaluons $L$ en les points $P_0^\sigma$ et $P_1^\sigma$. Il vient alors

$$\frac{L(P_0^\sigma)}{L(P_1^\sigma)} = \frac{(-1)^{g+1}(1-u)^{g+3}}{u^{g+3}v^{2g+2}(1-v)^4}.$$

Si $g$ est impair, on a l'identité suivante dans $\mathbf{Z}[u]$ :

$$(-1)^{g+1}u^{g(g+3)}(1-u)^{g-1}M^n(P_0^\sigma) = [u^{\frac{g+3}{2}} - (u-1)^{\frac{g+3}{2}}]^{2g+2}[u^{\frac{g+1}{2}} - (u-1)^{\frac{g+1}{2}}]^4 M^n(P_1^\sigma).$$

Il est alors clair que $n$ divise 4. Si $g \equiv -1 \bmod 4$, $l$ n'est pas divisible par 4 et donc $n$ divise 2.

Si $g$ est pair, on a l'identité suivante dans $\mathbf{Z}[z]$ :

$$(I_3) \qquad (1-z^2)^{2(g+3)}z^{2(g-1)}M^n(P_0^\sigma) = (1-z^{g+1})^4(1-z^{g+3})^{2g+2}M^n(P_1^\sigma).$$

Les entiers $g+1$ et $g+3$ étant impairs, $z+1$ ne divise ni $z^{g+1}-1$ ni $z^{g+3}-1$. Par conséquent, l'étude de la valuation en $z+1$ des deux membres de $(I_3)$ montre que $n$ divise $2(g+3)$. Soit $p$ un nombre premier divisant $n$. Comme dans ce cas $l$ est impair, $p \neq 2$, et donc $p$ divise $g+3$ et, comme $l = 2g(g+3) - (g-5)$, $p$ divise $g-5$, si bien que $p$ divise $8 = (g+3) - (g-5)$, ce qui est absurde, et le lemme est démontré.

**Lemme 6.3** *La fraction rationnelle $\gamma(f_{2,w})$ est non constante.*

Supposons $g$ impair. Le calcul montre que $f_{2,w}$ tend vers $f_{2,1} = [x^{g+1} - (x-1)^{g+1}]^2$ lorsque $w = u$ tend vers 1. Par conséquent $u-1$ divise $\Delta(f_{2,u})$. Par ailleurs, un calcul similaire à celui du lemme **3.2** montre que

$$\mathcal{A}(f_{2,1}) = 2\left[1 + \frac{2(-1)^{g+1}}{C_{2g+2}^{g+1}}\right].$$

Par conséquent l'invariant $\gamma(f_{2,u})$ est un élément de $\mathbf{Q}$ pour tout $u \in \mathbf{Q}$ sauf un nombre fini, et égal à $\infty$ quand $u = 1$. Donc $\gamma(f_{2,w})$ est non constante dans ce cas. Si $g$ est pair, on se ramène à la situation précédente en faisant tendre $z$ vers 0, ce qui achève la démonstration du lemme, et donc du théorème 3.

# Bibliographie


[1] *D. Abramovich* : Formal finiteness and the uniform boundness conjecture, a footnote to a paper of Kamienny and Mazur, à paraître dans Astérisque.

[2] *B. Edixhoven* : Rational torsion points on elliptic curves over number fields (after Kamienny and Mazur), Séminaire Bourbaki (1993-1994), Exposé $n^0$ 782.

[3] *E. V. Flynn* : Sequences of rational torsions on abelian varieties, Invent. Math. **106** (1991), 433-442.

[4] *J. I. Igusa* : Arithmetic variety of moduli for genus two, Ann. of Math. **72** (1960), 612-649.

[5] *S. Kamienny* : Torsion points on elliptic curves and $q$-coefficients of modular forms, Invent. Math. **109** (1992), 221 – 229.

[6] *S. Kamienny et B. Mazur* : Rational torsion of prime order in elliptic curves over number fields, à paraître dans Astérisque.

[7] *F. Leprévost* : Torsion sur des familles de courbes de genre g, Manus. Math. **75** (1992), 303-326.

[8] *F. Leprévost* : Famille de courbes hyperelliptiques de genre $g$ munies d'une classe de diviseurs rationnels d'ordre $2g^2 + 4g + 1$, Séminaire de Théorie des Nombres de Paris, Progress in Math. Birkhäuser. **116** (1991-1992), 107-119.

[9] *F. Leprévost* : Points rationnels de torsion de jacobiennes de certaines courbes de genre 2, C. R. Acad. Sci. Paris **316**, série I. (1993), 819 – 821.

[10] *F. Leprévost* : Jacobiennes de certaines courbes de genre 2 : torsion et simplicité, à paraître au Journal de Théorie des Nombres de Bordeaux.

[11] *F. Leprévost* : Sur une conjecture sur les points de torsion rationnels des jacobiennes de courbes, soumis pour publication (1995).

[12] *B. Mazur* : Modular curves and the Eisenstein ideal, Publ. Math. Inst. Hautes Etud. Sci. **47** (1978), 33 – 186.

[13] *L. Merel* : Bornes pour la torsion des courbes elliptiques définies sur les corps de nombres, à paraître à Invent. Math.

[14] *J.-F. Mestre* : Construction explicite des courbes de genre 2 à partir de leurs modules. In Effective Methods in Algebraic Geometry, Progress in Math. Birkhäuser. **94** (1991), 313-334.

[15] *H. Ogawa* : Curves of genus 2 with a rational torsion divisor of order 23, Proc. Japan Acad. **70** Ser. A, No. 9 (1994), 295-298.

*Adresse :* Université Paris 7, Département de Mathématiques. Tour 45-55, 5ème étage, 2 Place Jussieu, F-75252 Paris Cedex 05, France. E-mail : leprevot@mathp7.jussieu.fr