ACTA ARITHMETICA
LXXXVII.2 (1998)

Courbes algébriques de genre ≥ 2 possédant de nombreux points rationnels

par

Leopoldo Kulesz (Paris et San Miguel)

Introduction. En 1983, G. Faltings a montré la conjecture de Mordell : si $\mathbb{K}$ est un corps de nombres et $C/\mathbb{K}$ une courbe algébrique de genre $g \geq 2$ alors l'ensemble $C(\mathbb{K})$ de points $\mathbb{K}$-rationnels de C est fini. Il est naturel de se demander si $\#C(\mathbb{K})$ peut être borné en fonction de $\mathbb{K}$ et de g. Dans ce sens, L. Caporaso, J. Harris et B. Mazur ([CHM1], [CHM2]) ont montré que ceci est une conséquence de deux conjectures très générales concernant les points $\mathbb{K}$-rationnels sur les variétés de type général (dues à S. Lang 1986). Plus précisément, ils obtiennent les résultats suivants : si on pose

$$B(g,\mathbb{K}) = \max_C \#C(\mathbb{K}),$$
$$N(g,\mathbb{K}) = \limsup_C \#C(\mathbb{K}) \quad [\leq B(g,\mathbb{K})],$$

et

$$N(g) = \max_{\mathbb{K}} N(g,\mathbb{K}),$$

alors, si les conjectures de Lang sont vérifiées, pour tout $g \geq 2$, $B(g,\mathbb{K})$, $N(g,\mathbb{K})$, et $N(g)$ sont finis ([Elk1]).

La meilleure borne inférieure connue pour $N(g)$ et g quelconque est $16(g+1)$. Elle a été obtenue indépendamment par J.-F. Mestre et A. Brumer, qui ont construit des courbes dont le groupe d'automorphismes est d'ordre $4(g+1)$, passant par $16(g+1)$ points $\mathbb{Q}(\zeta)$-rationnels où ζ est une racine primitive $(g+1)$-ème de l'unité ([CHM2], [Elk1]).

Dans cet article nous nous proposons d'améliorer ce dernier résultat pour g petit ($g = 2, \ldots, 7$ et 11), que ce soit en trouvant des familles infinies de courbes passant par plus de $16(g+1)$ points rationnels ou en ayant recours à un corps de nombres dont le degré est inférieur à $\varphi(g+1)$.

Je remercie mon directeur de thèse Jean-François Mestre dont les idées sont à la source de ce travail; je remercie également Noam Elkies pour l'aide

1991 *Mathematics Subject Classification*: 11G30, 14G05.

considérable qu'il m'a apportée, ainsi que Marc Giusti pour ses conseils très enrichissants.

1. Alignement de points rationnels. Dans ce paragraphe, nous développons une méthode due à J.-F. Mestre.

1.1. *Les résultats*

THÉORÈME 1. $N(2,\mathbb{Q}) \geq 66$.

Plus précisément, nous construisons une famille infinie de courbes de genre 2 sans autre automorphisme que l'involution hyperelliptique passant par 66 points rationnels au moins. On avait pour ce type de courbes $N(2,\mathbb{Q}) \geq 38$ (cf. [Elk2]).

THÉORÈME 2. $N(3,\mathbb{Q}) \geq 37$.

Plus précisément, nous construisons une famille infinie de courbes lisses de genre 3 sans automorphismes passant par 37 points rationnels au moins. On avait pour ce type de courbes $N(3,\mathbb{Q}) \geq 14$.

1.2. *La méthode.* Soit C une quartique de $\mathbb{P}^2$ d'équation $F = 0$ où

$$\begin{aligned} F(x,y,z) = {} & a_0y^4 + y^3(a_1z + a_2x) + y^2(a_3z^2 + a_4xz + a_5x^2) \\ & + y(a_6z^3 + a_7xz^2 + a_8x^2z + a_9x^3) \\ & + a_{10}z^4 + a_{11}xz^3 + a_{12}x^2z^2 + a_{13}x^3z + a_{14}x^4. \end{aligned}$$

Une quartique de $\mathbb{P}^2$ est de genre 3 si elle est lisse et de genre 2 si elle possède un seul point double D. Dans le premier cas, on dispose de 14 paramètres homogènes libres et dans le deuxième, de 11, le point double correspondant aux trois équations linéaires suivantes :

$$\frac{\partial F}{\partial x}(D) = 0, \quad \frac{\partial F}{\partial y}(D) = 0, \quad \frac{\partial F}{\partial z}(D) = 0.$$

Par le théorème de Bézout, toute droite de $\mathbb{P}^2$ qui passe par trois points $\mathbb{K}$-rationnels de C passe par un quatrième point de C qui est aussi $\mathbb{K}$-rationnel. L'idée pour le genre 2 consiste à se donner onze points $\mathbb{Q}$-rationnels $P_1, \ldots, P_{11}$ dans $\mathbb{P}^2$ de manière à avoir le plus possible de droites passant exactement par trois points parmi ces onze et de construire ensuite la quartique passant par un point double D arbitraire et par $P_1, \ldots, P_{11}$. Grâce au théorème de Pappus ([EGH]) nous trouvons une première configuration avec 14 droites (cf. Figure 1). Nous obtenons ainsi des courbes de genre 2 possèdant au moins $(11 + 14) \times 2 = 50$ points $\mathbb{Q}$-rationnels.

N. Elkies m'a indiqué comment améliorer cette méthode en utilisant les points de torsion de courbes elliptiques. Soit une courbe elliptique $E/\mathbb{Q}$ dont le groupe de torsion G est isomorphe à $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Prenons $P_1, \ldots, P_{11}$

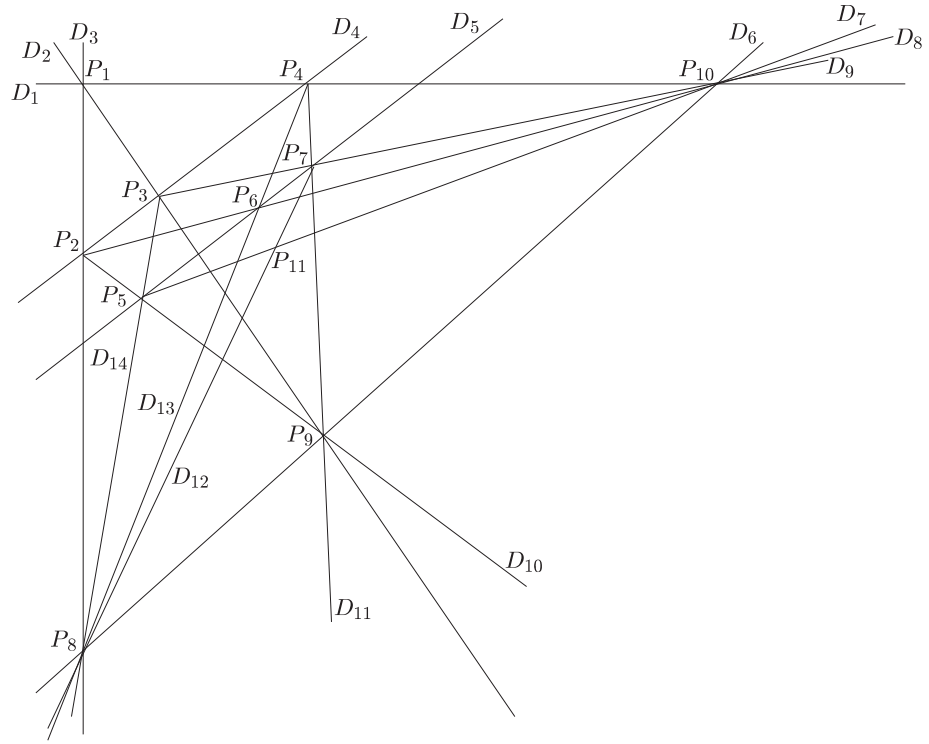

Fig. 1. Configuration de 14 droites $D_1, \ldots, D_{14}$ chacune passant exactement par trois points parmi $P_1, \ldots, P_{11}$

dans G et construisons la courbe C de genre 2 correspondante. Nous savons que $\mathrm{Card}(C \cap E) = 12$ et que $\mathrm{div}(F) = 0$ sur E, donc le 12-ième point de $C \cap E$ est aussi dans G et finalement $C \cap E = G$. Sur E trois points sont alignés si et seulement si leur somme est nulle; en faisant toutes les sommes possibles de trois éléments de G nous trouvons 19 triplets de points alignés de C. On construit ainsi une infinité de courbes de genre 2 ayant au moins $(12 + 19) \times 2 = 62$ points rationnels.

Comme l'a remarqué N. Elkies, si on choisit convenablement le point double D de C il est possible d'améliorer sensiblement ce résultat. En effet, soient $T_1,\ T_2,\ T_3,\ Q_1,\ Q_2,\ R_1$ et R_2 des points différents de G tels qu'aucune somme de trois points de $\{T_1, T_2, T_3, Q_1, Q_2\}$ ou de $\{T_1, T_2, T_3, R_1, R_2\}$ ne soit nulle et qu'aucune somme de trois points de $\{Q_1, Q_2, R_1, R_2\}$ ne soit égale à $-(T_1 + T_2 + T_3)$. Les coniques passant par $\{T_1, T_2, T_3, Q_1, Q_2\}$ et $\{T_1, T_2, T_3, R_1, R_2\}$ se coupent en $T_1,\ T_2,\ T_3$ et en un quatrième point rationnel que l'on choisit comme étant le point double D de la courbe C de genre 2 que nous voulons construire. Par construction, $D \notin E$. On a donc deux coniques qui coupent C doublement en D et simplement en cinq points

rationnels, donc—d'après le théorème de Bézout—en un 8-ème point qui est encore rationnel. Nous avons donc construit une famille infinie de courbes de genre 2—paramétrée par les courbes elliptiques sur $\mathbb{Q}$ dont le groupe de torsion est isomorphe à $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$—passant par $(12 + 19 + 2) \times 2 = 66$ points rationnels au moins, d'où le théorème 1. Nous avons cherché sur ces courbes des points rationnels supplémentaires et notre meilleur résultat est une courbe passant par $76 \times 2 = 152$ points rationnels. Nous rappelons que le meilleur résultat pour des courbes sans automorphisme autre que l'involution hyperelliptique est $B(2, \mathbb{Q}) \geq 366$, obtenu par Colin Stahlke ([Sta]).

Pour le genre 3, nous considérons les quartiques lisses de $\mathbb{P}^2$ et disposons donc de 14 paramètres homogènes libres. En ajoutant convenablement trois points à la configuration de 11 points utilisée pour le genre 2, il est facile d'obtenir trois droites supplémentaires passant chacune par trois points exactement (cf. Figure 2). Nous construisons ainsi une famille infinie de courbes lisses de genre 3 passant par $12 + 19 + 3 + 3 = 37$ points rationnels au moins, d'où le théorème 2.

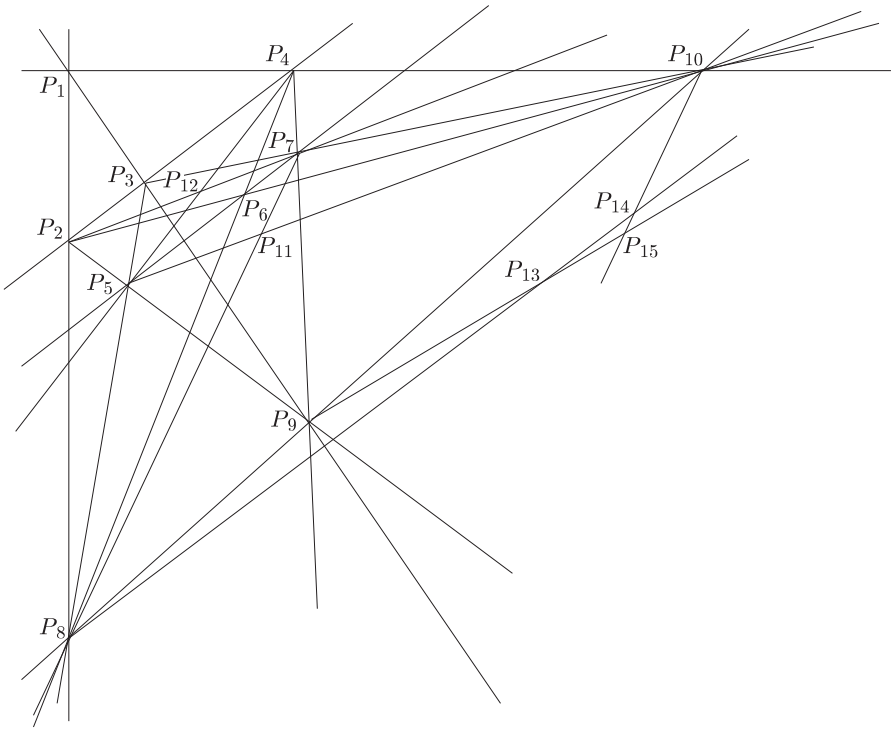

Fig. 2. Mise en évidence du 12-ème point P_{12} et des trois points P_{13}, P_{14}, P_{15} complétant la configuration pour les courbes de genre 3

REMARQUE. La première configuration de N. Elkies et celle de la Figure 1 sont les mêmes. En effet, toutes les quartiques de genre 2 passant par 11 points $\mathbb{Q}$-rationnels $\{P_1, \ldots, P_{11}\}$ pris dans la configuration de la Figure 1 passent aussi par un 12-ième point $\mathbb{Q}$-rationnel P_{12} (cf. Figure 2). Ceci s'explique par le fait que si nous construisons la courbe elliptique E' qui passe par $P_1, \ldots, P_9$ nous remarquons que $C \cap E' = \{P_1, \ldots, P_{12}\} = G'$ où G', groupe de torsion de E', est isomorphe à $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

1.3. *Explicitation de la construction*

1.3.1. *Structure d'un groupe de torsion isomorphe à* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Pour obtenir des courbes elliptiques possédant un sous-groupe de torsion sur $\mathbb{Q}$ isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ nous partons de la forme de Weierstrass :

$$E: \quad y^2 = (x-\alpha)(x-\beta)(x-\gamma) \tag{1}$$

avec α, β et γ dans $\mathbb{Q}$.

Ces courbes possèdent un sous-groupe de torsion T sur $\mathbb{Q}$ isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ donc, pour obtenir un groupe isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ contenant T, il suffit de poser dans (1) $\alpha = -1$, $\beta = -x_1^2$ et $\gamma = -x_2^2$ et de trouver x_1 et x_2 tels que le point $(0, x_1 x_2)$ soit d'ordre 3. Ainsi, après un changement de variables, nous obtenons les courbes d'équation

$$E_t: \quad y^2 = (x+1)(x+t^2)\left(x - \left(\frac{t}{t-1}\right)^2\right), \tag{2}$$

qui possèdent un groupe de torsion $E_t(\mathbb{Q})_{\text{tors}}$ sur $\mathbb{Q}$ isomorphe à $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ engendré par les points

$$P_1 = \left(\frac{2t^2}{-1+t}, \frac{-t^2(t+1)(-1+2t)}{(-1+t)^2}\right), \quad P_2 = (-t^2, t^3),$$

d'ordre six et deux respectivement.

1.3.2. *Courbes de genre* 2. Dans le paragraphe 1.2 nous avons vu comment construire des quartiques avec un seul point double (donc de genre $g = 2$) passant par onze points du plan projectif. Comme nous l'avons indiqué, le fait de choisir ces onze points dans le groupe de torsion d'une courbe elliptique, isomorphe à $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$, et le point double dans l'intersection de deux coniques C_1 et C_2 convenablement construites, impose des conditions fortes d'alignement entre les points.

Soient P_1 et P_2 les deux générateurs de $E_t(\mathbb{Q})_{\text{tors}}$ (cf. 1.3.1) et C_1 et C_2 les coniques passant respectivement par $\{[4]P_1, [4]P_1 + P_2, [2]P_1 + P_2, P_1, [3]P_1\}$ et $\{[4]P_1, [4]P_1+P_2, [2]P_1+P_2, P_1+P_2, [5]P_1\}$. Elles se coupent en $\{[4]P_1, [4]P_1+P_2, [2]P_1+P_2\}$ et en un quatrième point D, défini sur $\mathbb{Q}(t)$.

En suivant la méthode exposée au paragraphe 1.2, nous construisons une

famille de quartiques à partir de onze points du groupe $E_t(\mathbb{Q})_{\mathrm{tors}}$ ayant D comme point double, qui passent par 66 points définis sur $\mathbb{Q}(t)$.

Après avoir effectué le changement de variables qui envoie le point double D à l'infini, les courbes de cette famille ont pour équation

$$y^2 = f_t(x) = a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0,$$

avec

$$\begin{aligned}
a_0 &= 64t^8(2t-1)^2(3t-2)^2(5t^5-21t^4+20t^3+10t^2-16t+4)^2\\
&\quad\times(t^2-5t+2)^2,\\
a_1 &= 64t^6(2t-1)(3t-2)(t^2-5t+2)(72t^{16}-930t^{15}+4086t^{14}-1821t^{13}\\
&\quad-49365t^{12}+210283t^{11}-422225t^{10}+450788t^9-176502t^8\\
&\quad-161824t^7+273318t^6-177036t^5+60700t^4-9496t^3-312t^2\\
&\quad+320t-32),\\
a_2 &= 16t^4(6144t-85216t^2+678496t^3-3425132t^4-186536008t^{13}\\
&\quad+369339203t^{12}-463518704t^{11}+388985444t^{10}-209441512t^9\\
&\quad+53904780t^8+11222328t^5+15327536t^7-17940t^{18}-11503153t^{16}\\
&\quad+9968052t^{15}+44186446t^{14}+3385564t^{17}-22275436t^6-272640t^{19}\\
&\quad+576t^{22}-10944t^{21}+82548t^{20}-192),\\
a_3 &= 32t^2(32-736t+6688t^2-22632t^3-95898t^4+17547032t^{13}\\
&\quad-88067797t^{12}+159150894t^{11}-178295044t^{10}+138385940t^9\\
&\quad-77060520t^8+1494360t^5+30818440t^7-5906476t^{18}-7922635t^{16}\\
&\quad-4023010t^{15}+10851658t^{14}+9993172t^{17}-8573428t^6+2166508t^{19}\\
&\quad+288t^{23}-7176t^{22}+79848t^{21}-519588t^{20}),\\
a_4 &= 4(64-2176t+34528t^2-337664t^3+2264996t^4-320862992t^{13}\\
&\quad+258536999t^{12}-311561452t^{11}+366884652t^{10}-328703472t^9\\
&\quad+217139264t^8-10981480t^5-106874672t^7+135699144t^{18}\\
&\quad+466237595t^{16}-545383880t^{15}+467597218t^{14}-292496220t^{17}\\
&\quad+39528996t^6-46522256t^{19}+576t^{24}-17664t^{23}+246208t^{22}\\
&\quad-2065616t^{21}+11639544t^{20}),\\
a_5 &= -4(2t^2-5t+1)(2t^2-4t+1)(96t^{18}-2296t^{17}+24800t^{16}\\
&\quad-159484t^{15}+678048t^{14}-2001341t^{13}+4187711t^{12}-6212791t^{11}\\
&\quad+6365713t^{10}-4112436t^9+1035518t^8+860368t^7-1137114t^6\\
&\quad+666448t^5-243272t^4+58216t^3-8928t^2+800t-32),\\
a_6 &= (t-2)^2(2t^2-5t+1)^2(2t^2-4t+1)^2\\
&\quad\times(4t^5-29t^4+73t^3-70t^2+28t-4)^2.
\end{aligned}$$

REMARQUE. Nous savons que les automorphismes sur un corps $\Bbbk$ d'une courbe affine de genre 2 d'équation $y^2 = g(x)$ où g est un polynôme de degré six défini sur $\Bbbk$, sont de la forme

$$(x, y) \mapsto \left(\frac{ax+b}{cx+d}, \frac{eY}{(cx+d)^3}\right), \quad \text{avec } a, b, c, d \in \Bbbk,\ ad - bc \neq 0,\ e \in \Bbbk^*$$

(cf. [C-F]). Il est donc aisé de vérifier que les courbes d'équation $y^2 = f_t(x)$ n'ont pas d'automorphisme sur $\mathbb{Q}(t)$ autre que l'hyperelliptique.

1.3.3. *Courbes de genre* 3. Nous avons vu dans le paragraphe 1.2 comment construire des quartiques irréductibles lisses (donc de genre $g = 3$) définies sur $\Bbbk$ et passant par 37 points $\Bbbk$-rationnels au moins. Une quartique irréductible étant univoquement définie par 14 points génériques du plan projectif, nous construisons celle passant par onze points dans $E_t(\mathbb{Q})_{\text{tors}}$, et trois autres points P_1, P_2, P_3 qui vérifient:

- P_1, P_2 et $(0, 0, 1)$ alignés.
- P_1, P_3 et $(-1, -1, 1)$ alignés.
- P_2, P_3 et $(-t^2, t^3, 1)$ alignés.

Nous pouvons donc poser:

$$\begin{aligned} P_1 &= (x_1, y_1, 1), \\ P_2 &= (2t^2x_1, 2y_1t^2, (t-1)(-y_1 + ux_1)), \\ P_3 &= (x_3, y_3, z_3), \end{aligned}$$

avec

$$\begin{aligned} x_3 = & -(-x_1t + x_1 + y_1t - y_1 - 2t^2 - 2t^2x_1)(1 + x_1)(-y_1 + ux_1), \\ y_3 = & -(-2t^2x_1 - 2t^2x_1y_1 + x_1ty_1 - x_1^2tu - x_1y_1 + ux_1^2 - y_1^2t + y_1tux_1 \\ & + y_1^2 - y_1ux_1)(-1 - y_1 + u + ux_1), \\ z_3 = & (t-1)(1 + x_1)(-y_1 + ux_1)(-1 - y_1 + u + ux_1), \end{aligned}$$

où u est la pente de la droite passant par P_2 et P_3.

REMARQUE. Nous savons que les automorphismes sur un corps $\Bbbk$ d'une courbe projective de genre 3 d'équation $f(x, y, z) = 0$ où f est un polynôme de degré quatre défini sur $\Bbbk$, sont de la forme

$$(x, y, z) \mapsto (a_1x + b_1y + c_1z, a_2x + b_2y + c_2z, a_3x + b_3y + c_3z),$$

avec $a_i, b_i, c_i \in \Bbbk$ et

$$a_1b_2c_3 - a_1b_3c_2 - b_1a_2c_3 + b_1a_3c_2 + c_1a_2b_3 - c_1a_3b_2 \neq 0.$$

Il est donc aisé de vérifier sur une équation explicite (qui est trop longue pour figurer ici), que les courbes de genre 3 que nous venons de construire n'ont aucun automorphisme exceptionnel sur $\mathbb{Q}(t, u, x_1, y_1)$.

Exemple. La courbe d'équation

$$a_0y^4+y^3(a_1z+a_2x)+y^2(a_3z^2+a_4xz+a_5x^2)+y(a_6z^3+a_7xz^2+a_8x^2z+a_9x^3) + a_{10}z^4 + a_{11}xz^3 + a_{12}x^2z^2 + a_{13}x^3z + a_{14}x^4 = 0,$$

avec $a_0 = 0$, $a_1 = 260784$, $a_2 = 328725$, $a_3 = -520848$, $a_4 = 1503381$, $a_5 = -2301075$, $a_6 = -465536$, $a_7 = -15081816$, $a_8 = -18831274$, $a_9 = 3318666$, $a_{10} = 0$, $a_{11} = 6233600$, $a_{12} = 16363200$, $a_{13} = 9370624$, $a_{14} = -4035273$, n'a pas d'automorphisme et passe par les 37 points rationnels suivants:

$[520848, -10760728, 4035273]$,
$[-4062445000176, 58494543325296, 40520264995809]$,
$[-1642734417648, 31441391279880, 4751541118809]$,
$[-615816, -5576907, 230931]$,
$[-1204046640400, 5159655216536, 3138917346601]$,
$[-29440858320, 148910730840, 211685859675]$,
$[-58307461200, 106068390392, 119948405547]$,
$[371385817232, -4227794937040, 839134777849]$,
$[-31281150576, 20854100384, 62612142267]$,
$[-4977936, 47397940, 44259843]$, $[-59172, -1496247, 44379]$,
$[-1, -1, 1]$, $[0, 0, 1]$, $[-24, -24, 9]$, $[0, 8, 3]$, $[-72, -192, 27]$,
$[-12, -24, 9]$, $[2, -7, 1]$, $[-255, -165, 225]$,
$[562350271600, 4091150698264, 409480968649]$,
$[12, -8, 3]$, $[-4, -8, 1]$, $[-108, 72, 243]$, $[-36, -24, 27]$,
$[15916, -5783, 3979]$, $[1264, -21251, 6241]$,
$[312184118640, -13108956185780, 9753671109675]$,
$[886492688, 886492688, 1102040809]$, $[0, -3637, 5433]$,
$[-8247248, 28865368, 49857721]$,
$[-524724683824, 4060990334324, 1671153438361]$,
$[-16215384, -36875200, 4414107]$,
$[3626718256, 7253436512, 14490622129]$,
$[-101506440560, 1342684355920, 340571452225]$, $[4, 24, 1]$,
$[-624, 2184, 1521]$, $[-588892, 213971, -147223]$.

1.4. *Invariants projectifs des courbes de genre* 2 *et* 3. Le but de ce paragraphe est de montrer que les familles de courbes de genre 2 et 3 que nous venons de construire ne sont pas isotriviales, c'est-à-dire que chacune contient une infinité de courbes deux à deux non isomorphes sur $\overline{\mathbb{Q}}$. Pour ce faire, nous allons utiliser les résultats de F. Leprévost [Lep] sur les invariants des courbes hyperelliptiques et ceux de J. Dixmier [Dix] sur les invariants des quartiques planes.

1.4.1. *Famille de courbes de genre* 2. Nous dirons que l'équation $y^2 = f(x) = a_0x^{2g+2}+a_1x^{2g+1}+\ldots+a_{2g+2}$, où f est un polynôme de degré $2g+2$ sans racines multiples défini sur $\mathbb{Q}(t)$, définit une *famille géométrique à un*

paramètre de courbes hyperelliptiques de genre g sur $\mathbb{Q}$ 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 t en des valeurs rationnelles, d'obtenir une infinité de courbes hyperelliptiques de genre g deux à deux non isomorphes sur $\overline{\mathbb{Q}}$ (cf. [Lep]).

Soient F et G deux formes binaires de degrés respectifs m et n. Clebsch définit l'opération suivante, souvant désignée sous le nom de *transvectant* :

$$(FG)_k = \frac{(m-k)!(n-k)!}{m!n!}\left(\frac{\partial F}{\partial x}\frac{\partial G}{\partial y} - \frac{\partial F}{\partial y}\frac{\partial G}{\partial x}\right)^k.$$

Il s'agit de notations symboliques, en ce sens que, dans le développement binômial de l'expression ci-dessus, on remplace $(\partial F/\partial x)^l(\partial F/\partial y)^m$ par $(\partial^{l+m}F/\partial x^l\partial y^m)$ (cf. [Mes]).

Si $F(X,Z)$ est la forme binaire associée à $f(x)$, un invariant absolu d'une courbe d'équation $y^2 = f(x)$ est par exemple

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

où $\mathcal{D}(F)$ est le discriminant de F et

$$\mathcal{A}(F) = (FF')_{2g+2} = \sum_{k=0}^{2g+2} \frac{(-1)^k}{C^k_{2g+2}} a_{2g+2-k}a_k \quad \text{(cf. [Lep])}.$$

Dans 1.3.2 nous avons construit la famille de courbes d'équation $y^2 = f_t(x)$. Le calcul de $\gamma(F_t)$ (F_t est la forme binaire associée à f_t) aboutit à une fraction rationnelle non constante de $\mathbb{Q}(t)$ (avec une expression trop longue pour figurer ici), donc la famille de courbes de genre 2 d'équation $y^2 = f_t(x)$ n'est pas isotriviale.

1.4.2. *Famille de courbes de genre* 3. Dans 1.3.3 nous avons construit une famille de quartiques lisses définies sur $\mathbb{Q}(t,u,x_1,y_1)$. Nous allons montrer que l'image de ces courbes dans la variété de modules des courbes de genre 3 est non constante, en exhibant un invariant absolu non constant.

Soit C une quartique plane d'équation $\phi(x,y,z) = 0$ avec

$$\begin{aligned}\phi(x,y,z) = {} & ax^4 + 4bx^3y + 6cx^2y^2 + 4dxy^3 + ey^4 + 4fx^3z + 12gx^2yz \\ & + 12hxy^2z + 4iy^3z + 6jx^2z^2 + 12kxyz^2 + 6ly^2z^2 \\ & + 4mxz^3 + 4nyz^3 + pz^4.\end{aligned}$$

En suivant J. Dixmier [Dix], la courbe C possède les deux invariants

suivants :

$$\begin{aligned} I_3 = {} & aep + 3(al^2 + ej^2 + pc^2) + 4(bim + fdn) - 4(ain + efm + pbd) \\ & + 6cjl + 12(ck^2 + jh^2 + lg^2) - 12ghk \\ & - 12(bkl + fhl + dkj + igj + mhc + ngc) + 12(gdm + hnb + kfi), \end{aligned}$$

et

$$I_6 = \det(M) \quad \text{où} \quad M = \begin{pmatrix} a & c & j & g & f & b \\ c & e & l & i & h & d \\ j & l & p & n & m & k \\ g & i & n & l & k & h \\ f & h & m & k & j & g \\ b & d & k & h & g & c \end{pmatrix}.$$

Ainsi $I(C) = I_3^2/I_6$ est un invariant absolu de C.

Le calcul de $I(C)$ pour la famille de courbes construites en 1.3.3 aboutit à une fraction rationnelle non constante de $\mathbb{Q}(t, u, x_1, y_1)$ (avec une expression trop longue pour figurer ici), il s'agit donc d'une famille de courbes de genre 3 qui n'est pas isotriviale.

2. Courbes dont le groupe d'automorphismes est maximal. Ce paragraphe s'inspire notamment de [Kul] et [K-K] où nous avons construit des courbes hyperelliptiques de genre 2 et 3 à partir d'éléments de $\mathbb{Q}(x)$ invariants par l'action d'un sous-groupe fini de $PGL_2(\mathbb{Q})$.

2.1. *Courbes de genre* 2

2.1.1. *Les résultats*

Théorème 3. $N(2, \mathbb{Q}) \geq 66$.

Plus précisément, nous construisons une famille infinie de courbes de genre 2 dont le groupe d'automorphismes est d'ordre 12 passant par 66 points rationnels au moins. On avait pour ce type de courbes $N(2, \mathbb{Q}) \geq 48$.

2.1.2. *La méthode.* Dans [Kul] et [K-K] nous avons construit une famille infinie de courbes de genre 2 d'équation

$$y^2 = ax^2(x^2 - 9)^2 + b(x^2 - 1)^2, \quad a, b \in \mathbb{Q},$$

passant par 48 points rationnels au moins. Rappelons-en le principe.

On construit d'abord une fonction rationnelle invariante par un groupe d'automorphismes convenablement choisi. Soit G le groupe engendré par les automorphismes $x \mapsto -x$ et $x \mapsto (x + 3)/(x - 1)$. Ce groupe est d'ordre 6, et laisse invariante la fonction rationnelle

$$F(x) = \frac{x^2(x^2 - 9)^2}{(x^2 - 1)^2}.$$

On constate par ailleurs que pour tout $x \in \mathbb{Q} - \{0, 1, -1, 3, -3\}$ on a $\#\{\mathrm{orb}_G(x)\} = 6$. Par la suite, les courbes d'équation $y^2 = aF(x) + b$, où $a, b \in \mathbb{Q}$ sont de genre 2 et ont un groupe d'automorphismes d'ordre 12. Celui-ci est engendré par G et w où w est l'involution hyperelliptique donnée par $w(x, y) = (x, -y)$. La méthode suivante permet d'obtenir une famille de telles courbes, définies sur $\mathbb{Q}$ et possédant au moins $4 \times 12 = 48$ points rationnels.

Soient X, X_1, X_2, X_3, X_4 cinq indéterminées et $\mathbb{K} = \mathbb{Q}(X_1, X_2, X_3, X_4)$. Soit $P \in \mathbb{K}[X]$ le polynôme

$$P(X) = \prod_{i=1}^{4}(X - X_i) = X^4 + c_3X^3 + c_2X^2 + c_1X + c_0.$$

Il s'écrit de manière unique sous la forme $P = Q^2 - R$ avec Q et R dans $\mathbb{K}[X]$ tels que $Q(X) = X^2 + d_1X + d_0$ et $R(X) = aX + b$, où $d_1, d_0, a, b \in \mathbb{Q}$. En effet, on obtient l'égalité en posant $d_1 = c_3/2$, $d_0 = (c_2 - d_1^2)/2$, $a = 2d_1d_0 - c_1$ et $b = d_0^2 - c_0$.

On choisit ensuite des nombres x_1, x_2, x_3, x_4 dans $\mathbb{Q} - \{0, 1, -1, 3, -3\}$ appartenant à des orbites différentes deux à deux sous l'action de G et on pose $X = F(x)$ et $X_i = F(x_i)$ pour $i = 1, 2, 3, 4$. Nous obtenons ainsi une famille infinie

$$(*) \qquad \mathcal{F} = \{\mathcal{C} : y^2 = ax^2(x^2 - 9)^2 + b(x^2 - 1)^2\}$$

de courbes de genre 2 ayant 48 points rationnels (au moins) appartenant aux orbites des points d'abscisse x_1, x_2, x_3, x_4.

Il est possible d'améliorer ce dernier résultat en partant de quartiques $C_{\alpha,\beta} = V(F_{\alpha,\beta})$ où

$$F_{\alpha,\beta}(x, y) = y^2(x + 1)^2 + \alpha y(x^3 - 9x) + \beta(x - 1)^2.$$

Remarquons que le calcul de $\mathrm{Disc}_y(F_{\alpha,\beta}(x, y))$ nous ramène à des courbes de la forme $(*)$ avec 12 automorphismes et qui passent par l'orbite (dégénérée) de l'infini, formée par les points d'abscisse 1, -1 et ∞. Choisissons α et β pour que $C_{\alpha,\beta}$ passe par les points $(x_1, 1)$ et $(x_2, 1)$ avec $x_1, x_2 \in \mathbb{Q}$. Nous trouvons

$$\alpha_0 = \frac{4x_1x_2 - 4}{x_1^2x_2^2 - 2x_2x_1^2 + x_1^2 + 10x_1x_2 - 9 + x_2^2 - 2x_1x_2^2}$$

et

$$\beta_0 = -\frac{x_1^2x_2^2 + 2x_2x_1^2 + x_1^2 + 10x_1x_2 + 2x_1x_2^2 + x_2^2 - 9}{x_1^2x_2^2 - 2x_2x_1^2 + x_1^2 + 10x_1x_2 - 9 + x_2^2 - 2x_1x_2^2}.$$

Or, comme F_{α_0,β_0} est de degré 3 en x, la courbe C_{α_0,β_0} passe par un troisième point $\left(\frac{x_1+x_2}{x_1\,x_2-1}, 1\right)$ et au total par trois orbites plus celle (dégénérée) de l'infini, donc par $3 \times 12 + 6 = 42$ points rationnels. Nous allons améliorer

ce résultat en choisissant convenablement les paramètres rationnels x_1 et x_2. Un des automorphismes de C_{α_0,β_0} est donné par

$$x \mapsto \frac{x-3}{x+1},$$

qui envoie $(x_1, 1)$ en $\left(\frac{x_1-3}{x_1+1}, -2\frac{x_1+1}{(x_1-1)^2}\right)$. Donc $F_{\alpha_0,\beta_0}\left(x, -2\frac{x_1+1}{(x_1-1)^2}\right)$ est un polynôme de degré 3 en x dont $(x_1-3)/(x_1+1)$ est une racine. Une condition suffisante pour qu'il ait ses deux autres racines x_4 et x_5 rationnelles est que x_2 soit abscisse d'un point de la courbe elliptique E_{x_1} d'équation

$$y^2 = c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0$$

avec

$$\begin{aligned}
c_4 &= (x_1+1)^4(x_1-3)^2(x_1-1)^4,\\
c_3 &= 4(x_1+1)^2x_1(x_1^5 - 3x_1^4 + 2x_1^3 + 10x_1^2 - 35x_1 + 89)(x_1-1)^2,\\
c_2 &= 2(x_1+1)(3x_1^9 - 11x_1^8 + 30x_1^7 + 58x_1^6 - 316x_1^5 + 996x_1^4\\
&\quad - 1486x_1^3 + 1686x_1^2 + 233x_1 - 169),\\
c_1 &= 4(x_1+1)x_1(x_1^8 - 6x_1^7 + 6x_1^6 + 2x_1^5 - 104x_1^4 + 366x_1^3\\
&\quad - 934x_1^2 + 1174x_1 - 1529),\\
c_0 &= (x_1+1)(x_1^9 - 11x_1^8 + 32x_1^7 - 8x_1^6 - 70x_1^5 + 314x_1^4\\
&\quad - 920x_1^3 + 1936x_1^2 - 2115x_1 + 2889).
\end{aligned}$$

En spécialisant $x_1 = 2$ nous trouvons

$$E_2 : \quad y^2 = 81x^4 + 4248x^3 + 43494x^2 - 41208x + 9321,$$

qui est de rang ≥ 1. Nous avons ainsi construit une famille infinie de courbes de genre 2 paramétrée par E_2 passant par cinq orbites plus celle de l'infini, d'où le théorème 3.

2.2. *Courbes de genre* 3

2.2.1. *Les résultats*

Théorème 4. $N(3, \mathbb{Q}) \geq 72$.

Plus précisément, nous construisons une famille infinie de courbes de genre 3 dont le groupe d'automorphismes est d'ordre 16 passant par 72 points rationnels au moins. On avait pour ce type de courbes $N(3, \mathbb{Q}) \geq 64$.

2.2.2. *La méthode.* En [K-K] nous avons construit une famille infinie de courbes de genre 3 d'équation

$$(**) \qquad y^2 = a(x^2+1)^4 + bx^2(x^2-1)^2, \quad a, b \in \mathbb{Q},$$

passant par 64 points rationnels au moins. Nous avons appliqué la même méthode que pour le genre 2 ([C-F], [Kul], [K-K]) mais cette fois avec

le groupe d'automorphismes G engendré par $x \mapsto -x$, $x \mapsto 1/x$ et $x \mapsto (x+1)/(x-1)$ qui est d'ordre 8 et laisse invariante la fonction rationnelle

$$F(x) = \frac{(x^2+1)^4}{x^2(x^2-1)^2}.$$

Nous allons améliorer ce dernier résultat en partant de quartiques $C_{\alpha,\beta} = V(F_{\alpha,\beta})$ où

$$F_{\alpha,\beta}(x,y) = y^2x(x+1) + \alpha y(x^2+1)^2 + \beta x(x+1)(x-1)^2.$$

Remarquons que le calcul de $\mathrm{Disc}_y(F_{\alpha,\beta}(x,y))$ nous ramène à des courbes de la forme $(**)$ avec 16 automorphismes et qui passent par l'orbite (dégénérée) de l'infini, formée par les points d'abscisse 0, 1, -1 et ∞. Comme au paragraphe précédent, choisissons α et β pour que $C_{\alpha,\beta}$ passe par les points $(x_1,1)$ et $(x_2,1)$, $x_1, x_2 \in \mathbb{Q}$. Nous trouvons

$$\alpha_0 = -\frac{(x_2^2x_1 + x_2^2 - x_2 + x_2x_1^2 + x_1^2 - 2 - x_1)x_2x_1}{h(x_1,x_2)}$$

et

$$\beta_0 = \frac{x_2^3x_1^2 + x_2^3x_1 + x_2^2x_1^2 + x_1^3x_2^2 - x_2 + 2x_2x_1 + x_1^3x_2 - x_1 - 1}{h(x_1,x_2)}$$

avec

$$\begin{aligned} h(x_1,x_2) = {} & -x_2 - x_1 - x_2^3x_1 + x_2^3x_1^3 + 1 + x_2^2x_1 + 3x_1^3x_2^2 + x_2x_1^2 - 3x_2^2x_1^2 \\ & + 3x_2^3x_1^2 - x_1^3x_2 - 3x_2x_1 - x_2^2 + x_2^3 - x_1^2 + x_1^3. \end{aligned}$$

Le polynôme $F_{\alpha,\beta}(x,1)$ est de degré 4 en x et admet x_1 et x_2 comme racines. Une condition suffisante pour qu'il ait ses deux autres racines x_3 et x_4 rationnelles est que x_2 soit abscisse d'un point de la courbe elliptique E_{x_1} d'équation

$$y^2 = c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0$$

avec

$$\begin{aligned} c_4 &= x_1^4 + 12x_1^3 + 22x_1^2 - 4x_1 + 1, \\ c_3 &= 4(3x_1 - 1)(-x_1 + x_1^3 + 1 + 3x_1^2), \\ c_2 &= 22x_1^4 - 24x_1^3 - 4x_1^2 - 24x_1 - 2, \\ c_1 &= -4(x_1+1)(x_1^3 - 5x_1^2 + 11x_1 - 3), \\ c_0 &= (x_1+1)^2(x_1-3)^2. \end{aligned}$$

En spécialisant $x_1 = 7$ nous trouvons

$$E_7 : \quad y^2 = 7568x^4 + 38720x^3 + 44224x^2 - 5504x + 1024,$$

qui est de rang ≥ 1. Nous avons ainsi construit une famille infinie de courbes de genre 3 paramétrée par E_7 passant par quatre orbites plus celle de l'infini, d'où le théorème 4.

2.3. *Courbes de genre* 5

2.3.1. *Les résultats*

THÉORÈME 5. $N(5,\mathbb{Q}) \geq 96$ *et* $B(5,\mathbb{Q}) \geq 120$.

Plus précisément, nous construisons une famille infinie de courbes de genre 5 dont le groupe d'automorphismes est d'ordre 24, passant par 96 points rationnels au moins. De plus, cette famille contient une courbe passant par 120 points rationnels au moins.

2.3.2. *La méthode.* Nous appliquons la même méthode que pour le genre 2 et 3 ([Kul], [K-K]) mais cette fois avec le groupe d'automorphismes G engendré par $x \mapsto -x$, $x \mapsto 3/x$ et $x \mapsto (x-3)/(x+1)$ qui est d'ordre 12 et laisse invariante la fonction rationnelle

$$F(x) = \frac{(x(x^2-1)(x^2-9))^2}{(x^2+3)^6}.$$

Nous pouvons donc construire la famille infinie

$$\mathcal{F} = \{\mathcal{C} : y^2 = a(x^2+3)^6 + b(x(x^2-1)(x^2-9))^2\}$$

de courbes de genre 5 passant par 96 points rationnels (au moins).

En cherchant sur les courbes de genre 5 ainsi construites d'éventuelles orbites supplémentaires, nous obtenons la courbe d'équation

$$y^2 = 31479198381225(x^2+3)^6 - 4016043759196990(x(x^2-1)(x^2-9))^2$$

qui passe par les 5 orbites des points d'abscisse 2, 4, 11, 21 et 86/17, d'où le théorème 5.

2.4. *Courbes de genre* 7 *et* 11

2.4.1. *Les résultats.* La méthode précédente ne peut malheureusement pas s'appliquer pour des courbes de genre plus grand, en effet, l'ordre maximal des sous-groupes finis de $PGL_2(\mathbb{Q})$ est 12. Cependant, le choix de $\mathbb{Q}(\sqrt{2})$ et de $\mathbb{Q}(\sqrt{3})$ à la place de $\mathbb{Q}$ nous permet d'obtenir les résultats suivants :

THÉORÈME 6. $N(7,\mathbb{Q}(\sqrt{2})) \geq 128$ *et* $N(11,\mathbb{Q}(\sqrt{3})) \geq 192$.

Plus précisément, nous construisons une famille infinie de courbes de genre 7 dont le groupe d'automorphismes est d'ordre 32 passant par 128 points $\mathbb{Q}(\sqrt{2})$-rationnels au moins et une famille infinie de courbes de genre 11 dont le groupe d'automorphismes est d'ordre 48 passant par 192 points $\mathbb{Q}(\sqrt{3})$-rationnels au moins.

2.4.2. *La méthode.* Soit G_1 le groupe d'automorphismes engendré par

$$x \mapsto -x \quad \text{et} \quad x \mapsto \frac{(\sqrt{2}+1)x+1}{-x+\sqrt{2}+1}$$

et soit G_2 celui engendré par

$$x \mapsto -x \quad \text{et} \quad x \mapsto \frac{(\sqrt{3}+2)x+1}{-x+\sqrt{3}+2}.$$

Nous obtenons que G_1 est d'ordre 16 et laisse invariante la fonction rationnelle

$$F_1(x) = \frac{(x^4-4x^3-6x^2+4x+1)^2(x^4+4x^3-6x^2-4x+1)^2}{x^2(-1+x)^2(x+1)^2(x^2-2x-1)^2(x^2+2x-1)^2}$$

et G_2 est d'ordre 24 et laisse invariante la fonction rationnelle

$$F_2(x) = \frac{(x^2-2x-1)^2(x^2+2x-1)^2(x^4-8x^3+2x^2+8x+1)^2(x^4+8x^3+2x^2-8x+1)^2}{x^2(x-1)^2(x+1)^2(3x^2-1)^2(x^2+4x+1)^2(x^2-4x+1)^2(x^2-3)^2}.$$

Soient N_1 et D_1 (resp. N_2 et D_2) le numérateur et dénominateur de $F_1(x)$ (resp. $F_2(x)$).

Nous pouvons donc construire la famille infinie

$$\mathcal{F}_1 = \{\mathcal{C} : y^2 = aN_1 + bD_1\}$$

de courbes de genre 7 passant par 128 points $\mathbb{Q}(\sqrt{2})$-rationnels (au moins), et la famille infinie

$$\mathcal{F}_2 = \{\mathcal{C} : y^2 = aN_2 + bD_2\}$$

de courbes de genre 11 passant par 192 points $\mathbb{Q}(\sqrt{3})$-rationnels (au moins), d'où le théorème 6.

3. Isogénies entre courbes elliptiques. Nous développons ici une méthode due à J.-F. Mestre qui consiste, comme au paragraphe précédent, à construire des courbes de genre ≥ 2 à l'aide de fractions rationnelles sur $\mathbb{Q}$ invariantes par l'action d'un groupe déterminé. Cette fois-ci, on choisit le groupe formé par les points de torsion de courbes elliptiques.

3.1. *Les résultats*

THÉORÈME 7. $N(6, \mathbb{Q}) \geq 96$.

THÉORÈME 8. $N(7, \mathbb{Q}) \geq 128$.

REMARQUE. La meme méthode nous permet aussi d'obtenir $N(2, \mathbb{Q}) \geq 40$, $N(3, \mathbb{Q}) \geq 64$, $N(4, \mathbb{Q}) \geq 64$, et $N(5, \mathbb{Q}) \geq 96$. Cependant, pour $g = 2, 3$ et 5, nous avons obtenu de meilleurs résultats dans les chapitres 1 et 2 de ce travail, et en ce qui concerne le gas $g = 4$, N. Elkies a montré que $N(4, \mathbb{Q}) \geq 126$, à l'aide de courbes de genre 4 (non hyperelliptiques) ayant un groupe d'automorphismes d'ordre 36 et 18 points de base (cf. [Elk1]).

3.2. *La méthode.* Si E est une courbe elliptique définie sur $\mathbb{Q}$, les seuls groupes de torsion possibles de $E(\mathbb{Q})$ sont (cf. [Maz]):

$$\begin{cases} \mathbb{Z}/k\mathbb{Z}, & k = 2, \ldots, 10 \text{ et } 12, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}, & m = 1, 2, 3 \text{ et } 4. \end{cases}$$

D'autre part, l'existence de courbes elliptiques de rang ≥ 1 possédant chacun de ces sous-groupes de torsion a été démontrée par H. Suyama et par A. O. L. Atkin et F. Morain (cf. [Suy], [A-M]).

Soit donc $E/\mathbb{Q}$ une courbe elliptique de groupe de torsion $G = \{P_1, \ldots, P_n\}$. L'isogénie $\varphi : E \to E/G$ est donnée par $\varphi(P) = (X(P), Y(P))$ et il est possible d'exprimer X et Y explicitement en fonction des coordonnées (x, y) de P.

Pour cela, soit G_2 l'ensemble des points d'ordre 2 de $G - \{0\}$, R une partie de $G - \{0\} - G_2$ telle que $G - \{0\} - G_2 = R \cup (-R)$ et $R \cap (-R) = \emptyset$ et enfin $S = G_2 \cup R$. Avec ces notations nous avons

$$X(P) = x + \sum_{Q \in S} \left(\frac{t_Q}{x - x(Q)} + \frac{u_Q}{(x - x(Q))^2} \right)$$

où t_Q et u_Q sont des scalaires qui dépendent de Q, u_Q étant nul si $Q \in G_2$ (cf. [Vel]).

Supposons maintenant que $\text{rang}(E) \geq 1$. Si P est un point d'ordre infini de E il est clair que

$$X(P) = X(P + P_i) \quad \forall i = 1, \ldots, n.$$

D'autre part, nous avons vu que si Z, Z_1, Z_2, Z_3, Z_4 sont cinq indéterminées et $K = Q(Z_1, Z_2, Z_3, Z_4)$, le polynôme

$$U(Z) = \prod_{i=1}^{4} (Z - Z_i) = Z^4 + c_3 Z^3 + c_2 Z^2 + c_1 Z + c_0$$

s'écrit de manière unique sous la forme $U = V^2 - W$ avec V et W dans $K[Z]$ tels que $V(Z) = Z^2 + d_1 Z + d_0$ et $W(Z) = aZ + b$.

Ainsi, en posant $Z_i = X([i] \times P)$ $\forall i = 1, \ldots, 4$ on obtient la famille infinie

$$\mathcal{F}_{a,b} = \{\mathcal{C}_{a,b} : y^2 = aX(P) + b\}$$

de courbes passant par $8 \times n$ points rationnels au moins. Le genre de ces courbes dépend du degré de $X(P)$ par rapport à x et donc du groupe de torsion G.

Considérons trois cas:

1. $G_2 = \{0\}$. On peut écrire $X(x) = f(x)/h(x)^2$ avec f et h dans $\mathbb{Q}[x]$ et $\deg(f) = n$, $\deg(h^2) = n-1$. Les courbes $C_{a,b}$ admettent pour équation $y^2 = af(x) + bh(x)^2$ et sont donc de genre $(n-1)/2$. Nous obtenons $N(2, \mathbb{Q}) \geq 40$ en appliquant cette méthode avec G isomorphe à $\mathbb{Z}/5\mathbb{Z}$.

2. $\mathrm{Card}(G_2 - \{0\}) = 1$. On peut écrire $X(x) = f(x)/h(x)^2$ avec f et h dans $\mathbb{Q}[x]$ et $\deg(f) = n+1$, $\deg(h^2) = n-1$. Les courbes $C_{a,b}$ admettent pour équation $y^2 = af(x) + bh(x)^2$ et sont donc de genre $n/2$. Nous obtenons $N(4, \mathbb{Q}) \geq 64$ et le théorème 7 en appliquant cette méthode avec G isomorphe respectivement à $\mathbb{Z}/8\mathbb{Z}$ et $\mathbb{Z}/12\mathbb{Z}$.

3. $\mathrm{Card}(G_2 - \{0\}) = 3$. Si $P = (x, y) \in E$ et Q_1, Q_2, Q_3 sont les trois points non nuls d'ordre 2, nous avons que

$$y^2 = (x - x(Q_1))(x - x(Q_2))(x - x(Q_3)).$$

Alors, nous pouvons encore écrire

$$X(x) = \frac{f(x)}{h(x)^2(x - x(Q_1))(x - x(Q_2))(x - x(Q_3))}$$

avec f et h dans $\mathbb{Q}[x]$ et $\deg(f) = n$, $\deg(h^2) = n-4$ et les courbes $C_{a,b}$ admettent pour équation $y^2 = af(x)+bh(x)^2(x-x(Q_1))(x-x(Q_2))(x-x(Q_3))$ et sont de genre $(n-2)/2$. Nous obtenons $N(3, \mathbb{Q}) \geq 64$, $N(5, \mathbb{Q}) \geq 96$ et le théorème 8 en appliquant cette méthode avec G isomorphe respectivement à $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Références

[A-M] A. O. L. Atkin and F. Morain, *Finding suitable curves for the Elliptic Curve Method of factorization*, Math. Comp. 60 (1993), 399–405.

[CHM1] L. Caporaso, J. Harris and B. Mazur, *Uniformity of rational points*, J. Amer. Math. Soc. 10 (1997), 1–35.

[CHM2] —, —, —, *How many rational points can a curve have?*, dans: The Moduli Space of Curves (Texel Island, 1994), Progr. Math. 129, Birkhäuser, 1995, 13–31.

[C-F] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus* 2, London Math. Soc. Lecture Note Ser. 230, Cambridge Univ. Press, 1996.

[Dix] J. Dixmier, *On the projective invariant of quartic plane curves*, Adv. Math. 64 (1987), 279–304.

[EGH] D. Eisenbud, M. Green and J. Harris, *Cayley–Bacharach theorems and conjectures*, Bull. Amer. Math. Soc. 33 (1996), 295–324.

[Elk1] N. Elkies, *Curves with many points*, preprint, 1995.

[Elk2] — , Communication personnelle, 1997.

[K-K] W. Keller et L. Kulesz, *Courbes algébriques de genre 2 et 3 possédant de nombreux points rationnels*, C. R. Acad. Sci. Paris Sér. I 321 (1995), 1469–1472.

[Kul] L. Kulesz, *Courbes algébriques de genre 2 possédant de nombreux points rationnels*, ibid., 91–94.

[Lep] F. Leprévost, *Familles de courbes hyperelliptiques*, dans : Séminaire de Théorie des nombres, Paris, 1991–1992, S. David (ed.), Progr. Math. 116, Birkhäuser, 1993, 107–119.

[Maz] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. 44 (1978), 129–169.

[Mes] J.-F. Mestre, *Construction explicite de courbes de genre 2 à partir de leurs modules*, dans : Effective Methods in Algebraic Geometry, Progr. Math. 94, Birkhäuser, 1991, 313–334.

[Sta] C. Stahlke, *Algebraic curves over Q with many rational points and minimal automorphism group*, Internat. Math. Res. Notices 1997, no. 1, 1–4.

[Suy] H. Suyama, Informal preliminary report (8), 1985.

[Vel] J. Vélu, *Isogénies entre courbes elliptiques*, C. R. Acad. Sci. Paris Sér. A 273 (1971), 238–241.

UFR de mathématiques
Université Paris 7
2, pl. Jussieu
F-75251 Paris Cedex 05, France
E-mail: kulesz@math.jussieu.fr

Departamento de Matemáticas
Universidad de General Sarmiento
Roca 850, 1363 San Miguel
Pcia. de Buenos Aires, Argentina
E-mail: lkulesz@ungs.edu.ar

Reçu le 27.10.1997
et révisé le 31.3.1998 (3285)