Zeitschrift: L'Enseignement Mathématique

Herausgeber: Commission Internationale de l'Enseignement Mathématique

Band: 47 (2001)

Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: UNE QUINTIQUE DE GENRE 1 QUI CONTREDIT LE PRINCIPE DE HASSE

Autor: WUTHRICH, Christian

DOI: https://doi.org/10.5169/seals-65433

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 14.07.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

L'Enseignement Mathématique, t. 47 (2001), p. 161–172

UNE QUINTIQUE DE GENRE 1 QUI CONTREDIT LE PRINCIPE DE HASSE

par Christian WUTHRICH

1. INTRODUCTION

Le sujet de ce travail est de construire un contre-exemple au principe de Hasse (voir par exemple [CCS]) pour la famille des quintiques de genre 1.

THÉORÈME 1.1. *La courbe projective plane $C/\mathbf{Q}$, de genre géométrique* 1, *ayant cinq points doubles et donnée par l'équation*

$$\begin{aligned}(1.1)\qquad & x^5 + y(-6x^4 + 10x^3y - x^2y^2 - 6xy^3 + y^4) \\ & + z(4x^4 + 2x^3z - 5x^2z^2 - 2xz^3 + z^4) \\ & + \frac{1}{16}yz(-224x^3 + 108x^2y + 116xy^2 + 10y^3 + 68x^2z \\ & \qquad - 166xyz - 80y^2z + 160xz^2 + 81yz^2 - 56z^3) = 0,\end{aligned}$$

possède des points lisses dans tous les complétés de $\mathbf{Q}$, *mais aucun point rationnel.*

Dans les années 40, Lind [Li] et Reichardt [Re] ont montré par des contre-exemples que le principe ne s'applique pas aux courbes de genre 1. La cubique diagonale découverte par Selmer [Se], $3x^3 + 4y^3 + 5z^3 = 0$, est le contre-exemple le plus connu. Aujourd'hui, on connaît même des familles algébriques dont toutes les courbes sont de genre 1 et contredisent le principe de Hasse (voir [CP]).

Après avoir trouvé cette courbe et sa jacobienne, j'ai pris connaissance des travaux de T. A. Fisher, qui dans sa thèse [Fi] construit d'autres exemples de quintiques qui contredisent le principe de Hasse par une méthode différente de celle utilisée ici. Il obtient ses exemples comme torseurs de courbes elliptiques,

mais il doit apparemment se restreindre à des courbes elliptiques avec 5-torsion sur $\mathbf{Q}$.

La première partie de cet article décrit la méthode pour construire les courbes qui satisfont la condition géométrique, en utilisant des surfaces de Del Pezzo de degré 4. Après la construction du contre-exemple, la démonstration du théorème est expliquée en détail. J'aimerais attirer l'attention sur la démonstration du cas global qui contient des éléments originaux, comme l'examen simultané – *pour une même équation* – de deux éléments qui sont des normes : voir (4.1) et (4.2). Entièrement programmée sur ordinateur, elle a été appliquée à des familles de courbes pour tamiser un contre-exemple. La fin de l'article est réservée au calcul de la jacobienne E associée à cette quintique qui nous sert de contre-exemple. La normalisée de C représente alors un élément d'ordre 5 dans le groupe de Tate-Shafarevich $Ш(E/\mathbf{Q})$.

2. Quintiques planes de genre 1

Soit ω un nombre algébrique de polynôme minimal

$$p(X) = g_0 + g_1 X + g_2 X^2 + g_3 X^3 + g_4 X^4 + X^5$$

sur $\mathbf{Q}$. Soit $P_1 = (1 : \omega : \omega^2) \in \mathbf{P}^2(\mathbf{Q}(\omega))$ et soient P_2, P_3, P_4 et P_5 ses conjugués sur $\mathbf{Q}$. On introduit la notation B pour la conique $xz - y^2 = 0$ qui est définie par les P_i. Nous allons chercher toutes les quintiques $C/\mathbf{Q}$ du plan ayant des points doubles en P_1, P_2, P_3, P_4, P_5. Pour cela nous considérons le système linéaire complet des cubiques passant par les points P_i. Prenons comme base les cubiques $A_i/\mathbf{Q}$ suivantes :

$$A_0 : \ x(xz - y^2) = 0, \qquad A_1 : \ y(xz - y^2) = 0, \qquad A_2 : \ z(xz - y^2) = 0,$$
$$A_3 : \ g_0 x^3 + g_1 x^2 y + g_2 x^2 z + g_3 xyz + g_4 xz^2 + yz^2 = 0,$$
$$A_4 : \ g_0 x^2 y + g_1 x^2 z + g_2 xyz + g_3 xz^2 + g_4 yz^2 + z^3 = 0.$$

Ceci donne une application birationnelle j de $\mathbf{P}^2_{\mathbf{Q}}$ dans une surface S de Del Pezzo de degré 4 dans $\mathbf{P}^4_{\mathbf{Q}}$, isomorphe au plan éclaté en les cinq points P_i, voir [Be].

Un petit calcul de syzygies montre que S est égale à l'intersection complète des deux quadriques

$$\mathcal{Q}_0 : \ x_0 x_4 - x_1 x_3 = g_1 x_0^2 + g_3 x_0 x_2 + x_2^2$$
$$\mathcal{Q}_1 : \ x_2 x_3 - x_1 x_4 = g_0 x_0^2 + g_2 x_0 x_2 + g_4 x_2^2$$

définies sur $\mathbf{Q}$.

L'intersection de S avec une quadrique $\mathcal{Q}$ qui ne contient pas la surface se contracte sur $\mathbf{P}^2$ en une sextique ayant des points doubles dans les cinq points P_i. On prend une droite du plan, par exemple $x = 0$, paramétrée par $(s : t) \mapsto (0 : s : t)$. Son image sur la surface S est une cubique gauche h paramétrée par

$$(s : t) \mapsto (0 : -s^3 : -s^2 t : st^2 : g_4 st^2 + t^3)\,.$$

On cherche toutes les quadriques de $\mathbf{P}^4$ qui contiennent cette cubique gauche h sans contenir toute la surface S. Une telle quadrique coupe la surface le long de h et d'une courbe dont la contraction sur le plan est une quintique ayant un point double en chacun des points P_i. On n'a pas de peine à trouver déjà cinq quadriques dégénérées de la forme $x_0 x_i = 0$ pour $0 \leq i \leq 4$. Les quintiques correspondantes s'écrivent comme

$$C_i = A_i + B \qquad \text{pour} \quad 0 \leq i \leq 4\,.$$

De plus, on trouve trois cônes quadratiques de sommet $(1 : 0 : 0 : 0 : 0)$, au-dessus de trois quadriques dans l'hyperplan donné par l'équation $x_0 = 0$:

$$x_1 x_3 + x_2^2 = 0\,, \quad x_1 x_4 - x_2 x_3 - g_4\, x_1 x_3 = 0\,, \quad x_2 x_4 + x_3^2 - g_4\, x_2 x_3 = 0\,.$$

Voici les quintiques associées :

$$C_5 : \ (xz - y^2)(g_0\, x^2 y + g_1\, xy^2 + g_2\, xyz + g_3\, y^2 z + g_4\, yz^2 + z^3) = 0\,,$$

$$\begin{aligned} C_6 : \ & (xz - y^2)(-g_0 g_4 x^2 y - g_0\, x^2 z + (g_0 - g_1 g_4)\, xy^2 - g_2 g_4\ xyz \\ & - g_2\, xz^2 + (g_2 - g_3 g_4)\, y^2 z - g_4^2\, yz^2 - g_4\, z^3) = 0\,, \end{aligned}$$

$$\begin{aligned} C_7 : \ & g_0^2\, x^5 + 2 g_0 g_1\, x^4 y + 2 g_0 g_2\, x^4 z + g_1^2\, x^3 y^2 + 2(g_1 g_2 + g_0 g_3)\, x^3 yz \\ & + (g_2^2 + g_0 g_4)\, x^3 z^2 + (2 g_1 g_3 + g_0 g_4)\, x^2 y^2 z \\ & + (3 g_0 + 2 g_2 g_3 + g_1 g_4)\, x^2 yz^2 + (g_1 + g_2 g_4)\, x^2 z^3 + (-g_0 + g_1 g_4)\, xy^3 z \\ & + (g_1 + g_3^2 + g_2 g_4)\, xy^2 z^2 + (3 g_2 + g_3 g_4)\, xyz^3 + g_3\, xz^4 \\ & + (-g_2 + g_3 g_4)\, y^3 z^2 + (g_3 + g_4^2) y^2 z^3 + 2 g_4\, yz^4 + z^5 = 0\,. \end{aligned}$$

On voit que les équations de C_5 et C_6 sont des combinaisons linéaires des équations de C_0, C_2 et C_4. Les quintiques $\{C_0, C_1, C_2, C_3, C_4, C_7\}$ forment une base du système des quintiques du plan ayant des points doubles en $P_1, \ldots, P_5$; on vérifie qu'elles sont indépendantes et que la dimension du système est égale à $\binom{5+2}{2} - 3 \cdot 5 = 6$, car les conditions imposées par les points P_i sont indépendantes.

REMARQUE. D'après le théorème de Riemann-Roch, tout diviseur de degré 1 est linéairement équivalent à un diviseur effectif, c-à-d. à un point rationnel. Pour éviter d'avoir de tels points sur notre courbe, il faut que l'application deg: $\mathrm{Div}(C/\mathbf{Q}) \to \mathbf{Z}$ ait $5\mathbf{Z}$ comme image.

Nous avons utilisé cela pour tamiser une certaine famille de quintiques pour trouver notre exemple: on prend une quintique dont on a vérifié qu'elle a des points locaux. On choisit quelques droites au hasard. L'intersection de la quintique avec chacune des droites doit être un diviseur irréductible sur $\mathbf{Q}$. Sinon la quintique possède des points rationnels. Pour la courbe

$$324x^5 - 36x^4y + x^3y^2 + 45x^2yz^2 - x^2z^3 - xy^2z^2 - 9y^5 + z^5 = 0,$$

par exemple, on ne trouve pas tout de suite un point rationnel. Mais quand on coupe par la droite $3x - y + z = 0$, on trouve un polynôme qui se factorise:

$$9(2y^2 + 3yz - 3z^2)(109y^3 - 96y^2z + 99yz^2 - 4z^3),$$

ce qui montre qu'il y a un point rationnel quelque part.

3. UN CORPS DE NOMBRES

Soit ζ une racine primitive $11^{\text{ème}}$ de l'unité. On considère le corps cyclotomique $\mathbf{Q}(\zeta)$. Pour tous les résultats de ce paragraphe, je me réfère à [CF], chap. 3. L'anneau des entiers $\mathcal{O}_{\mathbf{Q}(\zeta)}$ est égal à $\mathbf{Z}[\zeta]$ et le discriminant vaut $\mathrm{disc}(\mathbf{Q}(\zeta)) = -11^9$. Le premier 11 est totalement ramifié: $11\mathcal{O}_{\mathbf{Q}(\zeta)} = (1-\zeta)^{10}$. Un premier rationnel $p \neq 11$ se décompose en dix idéaux premiers si $p \equiv 1 \pmod{11}$, en cinq si $p \equiv -1 \pmod{11}$; autrement il reste premier si $p^5 \equiv -1 \pmod{11}$ et dans les autres cas il se factorise en deux idéaux premiers.

Dans $\mathbf{Q}(\zeta)$ il y a un sous-corps réel de degré 5, $K = \mathbf{Q}(\zeta + \bar{\zeta})$, qui est le corps fixe sous l'action de l'élément σ d'ordre 2 dans $\mathrm{Gal}(\mathbf{Q}(\zeta):\mathbf{Q})$. Comme l'extension $\mathbf{Q}(\zeta):\mathbf{Q}$ est abélienne, $K:\mathbf{Q}$ est galoisienne. Le discriminant $\mathrm{disc}(K)$ doit diviser celui de $\mathbf{Q}(\zeta)$, ce qui entraîne que 11 est le seul premier ramifié dans K; il est aussi totalement ramifié. On trouve un générateur de l'idéal au-dessus de $11\mathbf{Z}$ en prenant $\theta = N_{\mathbf{Q}(\zeta):K}(1-\zeta) = 2 - \zeta - \bar{\zeta} \in \mathcal{O}_K$. Il est facile de calculer le polynôme minimal de θ:

$$\theta^5 - 11\theta^4 + 44\theta^3 - 77\theta^2 + 55\theta - 11 = 0.$$

De plus, l'anneau des entiers $\mathcal{O}_K$ de K est égal à $\mathbf{Z}[\theta]$. Il est principal; un fait que nous n'utiliserons pas. On a $11\mathcal{O}_K = (\theta)^5$. On peut déduire de l'action de σ sur les idéaux que les premiers rationnels $p \equiv \pm 1 \pmod{11}$ se factorisent

en cinq idéaux premiers distincts dans $\mathcal{O}_K$ tandis que les $p \not\equiv \pm 1 \pmod{11}$ différents de 11 restent premiers. *PARI-GP*® trouve une base des unités modulo torsion, à savoir : $\{\theta - 2,\ \theta - 3,\ \theta^2 - 5\theta + 5,\ \theta^4 - 8\,\theta^3 + 21\,\theta^2 - 20\,\theta + 5\}$.

PROPOSITION 3.1. *Pour tout $\xi \in \mathcal{O}_K$ avec $\xi \notin (\theta)$ on a*

$$N(\xi) = N_{K:\mathbf{Q}}(\xi) \equiv \pm 1 \pmod{11}.$$

Preuve. Puisque $|N(\xi)| = N((\xi))$ et que (ξ) se factorise en idéaux premiers, il suffit de montrer que $N(\mathfrak{p}) \equiv \pm 1 \pmod{11}$ pour tout idéal premier $\mathfrak{p} \neq (\theta)$. Soit $\mathfrak{p}$ est au-dessus d'un premier rationnel $p \equiv \pm 1 \pmod{11}$ et alors sa norme est égal à $\pm p$, soit $\mathfrak{p}$ est de la forme $p\mathcal{O}_K$ et dans ce cas $N(\mathfrak{p}) = p^5 \equiv \pm 1 \pmod{11}$. $\square$

REMARQUE. Dans l'appendice de [Co], Daniel Coray utilise cette extension $K:\mathbf{Q}$ pour construire une quintique qui contredit le principe de Hasse. Mais elle est lisse et donc de genre 6. L'équation s'écrit

$$N(x + \theta y) = z(z^2 + xz + x^2)(2z^2 + xz + x^2).$$

Par ailleurs, le premier contre-exemple qui est une courbe plane lisse de degré 5 a été construit par Fujiwara dans [Fu].

4. CHOIX DE LA COURBE

La quintique C qui nous servira de contre-exemple au principe de Hasse sera une combinaison linéaire

$$C = C_7 + \lambda_0 C_0 + \lambda_1 C_1 + \lambda_2 C_2 + \lambda_3 C_3 + \lambda_4 C_4.$$

On choisit les coefficients g_i et λ_i tels que les termes sans z s'écrivent comme $N(x - \varepsilon y) = N_{K:\mathbf{Q}}(x - \varepsilon y)$ et que les termes sans y s'écrivent comme $N(x - \eta z)$ pour certains ε et $\eta \in K$. J'ai essayé avec un millier de choix différents de (ε, η) pour lesquels il existe des coefficients g_i et λ_i. Parmi ceux auxquels ma méthode de démonstration s'applique, j'ai choisi le plus simple :

$$\varepsilon = -1 + 4\theta - \theta^2 \in \mathcal{O}_K^* \quad \text{et} \quad \eta = -3 + \theta \in \mathcal{O}_K^*,$$

dont les normes sont

$$N(x - \varepsilon y) = x^5 - 6x^4y + 10x^3y^2 - x^2y^3 - 6xy^4 + y^5$$

$$N(x - \eta z) = x^5 + 4x^4z + 2x^3z^2 - 5x^2z^3 - 2xz^4 + z^5,$$

et les coefficients

$$g_0 = 1\,, \qquad g_1 = -3\,, \qquad g_2 = \tfrac{5}{2}\,, \qquad g_3 = 0\,, \qquad g_4 = -\tfrac{7}{4}\,,$$
$$\lambda_0 = -6\,, \qquad \lambda_1 = 1\,, \qquad \lambda_2 = \tfrac{5}{8}\,, \qquad \lambda_3 = -1\,, \qquad \lambda_4 = -2\,.$$

Cela nous donne la courbe C donnée par (1.1) dans le théorème principal. Le polynôme minimal de ω est $p(X) = 4 - 12X + 10X^2 - 7X^4 + 4X^5$, qui est irréductible sur $\mathbf{Q}$. Dans la suite on pose $r := -16N(x - \varepsilon y)$ et $s := -16N(x - \eta z)$. Puis on constate que l'équation (1.1) peut être réécrite sous chacune des deux formes suivantes:

$$r = -16N(x - \varepsilon y) = z \cdot f\,, \tag{4.1}$$

$$s = -16N(x - \eta z) = y \cdot g\,, \tag{4.2}$$

où f et g sont des polynômes homogènes de degré 4 sur $\mathbf{Z}$.

5. Démonstration du cas local

Proposition 5.1. *La courbe C donnée par* (1.1) *possède des points lisses dans tous les complétés de* $\mathbf{Q}$.

Preuve. Comme le degré de C est impair, il est clair que $C/\mathbf{R}$ possède un point lisse. On commence petit à petit par les premiers nombres premiers p.

Pour $p = 2$: lorsque l'on remplace z par $8z$ dans l'équation (1.1), on obtient une courbe dont la réduction modulo 2 est égale à

$$x^5 + x^2y^3 + y^5 + y^4z = 0\,.$$

Elle a un point lisse $(0 : 1 : 1)$ sur $\mathbf{F}_2$. Ensuite, on trouve facilement des points lisses de la réduction de C modulo p pour $2 < p < 19$: $(1 : 1 : 2)$ pour $\mathbf{F}_3$, $(0 : 1 : 3)$ pour $\mathbf{F}_5$, $(0 : 1 : 5)$ pour $\mathbf{F}_7$, $(1 : 0 : 7)$ pour $\mathbf{F}_{11}$, $(0 : 1 : 1)$ pour $\mathbf{F}_{13}$ et $(0 : 1 : -2)$ pour $\mathbf{F}_{17}$.

Lemme 5.2. *Soit $p \geq 19$, soit $\widehat{C}$ la réduction de C modulo p. On suppose que $\widehat{C}$ n'est pas une composante de sa Hessienne H. Alors $\widehat{C}(\mathbf{F}_p)$ contient un point lisse.*

Preuve. On suppose d'abord que $\widehat{C}$ est irréductible. Soit $\hat{c}$ la normalisée de $\widehat{C}$. Si elle est une courbe de genre 1, alors par le théorème de Hasse-Weil pour la courbe lisse projective $\hat{c}$, on a

$$\#\hat{c}(\mathbf{F}_p) > p + 1 - 2\sqrt{p} \geq (\sqrt{19} - 1)^2 > 11\,.$$

La contraction sur $\widehat{C}$ peut écraser 10 de nos points lisses, mais il reste au moins un point lisse sur $\widehat{C}(\mathbf{F}_p)$

Si $\widehat{C}/\mathbf{F}_p$ est de genre 0, ou si elle se décompose sur $\overline{\mathbf{F}}_p$ en ayant une composante simple définie sur $\mathbf{F}_p$, le même argument montre qu'elle a toujours suffisamment de points pour en avoir qui soient lisses. Le seul cas où il faut s'inquiéter c'est quand elle se décompose sur $\overline{\mathbf{F}}_p$ en cinq droites. Mais ce cas est exclu par notre hypothèse, car cela voudrait dire que chaque point de $\widehat{C}$ serait un point d'inflexion, et se trouverait donc sur la Hessienne H. $\square$

Pour terminer la démonstration de la proposition, il suffit donc de calculer la résultante de H avec $\widehat{C}$, en éliminant z, ce qui donne la réduction de

$$2^{44} \cdot (4x^5 - 12x^4y + 10x^3y^2 - 7xy^4 + 4y^5)^6 \cdot q(x : y)\,,$$

où $q(x : y)$ est un polynôme homogène, primitif, de degré 15. Ce n'est jamais 0 modulo un premier $p > 2$. $\square$

6. Démonstration du cas global

Proposition 6.1. *La courbe C donnée par* (1.1) *n'a pas de point rationnel.*

Preuve. On suppose que $(x : y : z)$ est une solution rationnelle de (1.1). On peut supposer que x, y et z sont des entiers et qu'ils n'ont pas de facteur en commun.

Soit p un premier rationnel différent de 2 et de 11, avec $p \not\equiv \pm 1 \pmod{11}$. Alors p ne divise pas r dans la formule (4.1) : sinon $x - \varepsilon y = x + y - 4\theta y + \theta^2 y$ serait dans $p\mathcal{O}_K$. Le fait que $\{1, \theta, \theta^2, \theta^3, \theta^4\}$ est une $\mathbf{Z}$-base de $\mathcal{O}_K$ montre alors que p diviserait y et $x + y$. Puisque p ne peut pas être facteur des trois coordonnées, on aurait donc $p \nmid z$, d'où $p \mid f$. Mais $f \equiv 16z^4 \not\equiv 0 \pmod{p}$.

De la même manière, on montre que p ne divise pas s. Donc r et s sont composés de facteurs premiers 2, 11 et de premiers de la forme $p \equiv \pm 1 \pmod{11}$. La même conclusion est vraie pour leurs facteurs y, z, f et g. Considérons $p = 2$ de plus près : rappelons-nous que $2\mathcal{O}_K$ est un idéal premier. On dénote par β la valuation de y en $2\mathbf{Z}$, et par γ celle de z.

On suppose dans un premier temps que β, $\gamma > 0$. Alors $2 \nmid x$, ce qui dit que $x - \varepsilon y \notin 2\mathcal{O}_K$. Ceci implique que $2^4 \parallel r$, autrement dit que $0 < \gamma \leq 4$ et que $2^{4-\gamma} \parallel f$. (On a utilisé la notation $\parallel$ pour dire «divise exactement»). Calculons f modulo 16:

$$f \equiv 4y^2 \cdot 3x^2 + 4y^3 \cdot x + 2y^4 \cdot 5 + 4yz \cdot x^2 + 2y^2z \cdot 5x + y^2z^2 + 8yz^3 \pmod{16}.$$

Par hypothèse, y et z sont au moins une fois divisibles par 2, le terme à droite est donc égal à 0 modulo 16, ce qui n'est pas possible car $16 \nmid f$.

Occupons-nous à présent du cas $\beta = 0$ et $\gamma > 0$: on a $x - \varepsilon y = x + y - 4\theta y + \theta^2 y \notin 2\mathcal{O}_K$, alors comme avant $2^{4-\gamma} \parallel f$. Cette fois-ci on regarde f modulo 4:

$$f \equiv 2 \cdot y^4 + 2xz \cdot y^2 + z^2 \cdot y^2 \equiv 2 \pmod 4,$$

puisque $2 \nmid y$. Cela veut dire que $2 \parallel f$ et donc $\gamma = 3$. (On a vu dans 5.1 que derrière cela «se cache» une solution 2-adique. On ne pourrait pas l'éliminer en considérant $p = 2$.)

Comme dernière possibilité, on considère $\beta \geq 0$ et $\gamma = 0$: on voit que $x - \eta z = x + 3z - \theta z \notin 2\mathcal{O}_K$ (car $2 \nmid z$), alors $2^{4-\beta} \parallel g$ et $0 \leq \beta \leq 4$. On a

$$g \equiv 12x^2yz + 4xy^2z + 10y^3z + 4x^2z^2 + 10xyz^2 + yz^3 + 8z^4 \pmod{16}.$$

Si $\beta < 2$, alors

$$\frac{1}{4} > \frac{1}{2^{4-\beta}} = |g|_2 = |yz^3|_2 = \frac{1}{2^\beta} > \frac{1}{4}.$$

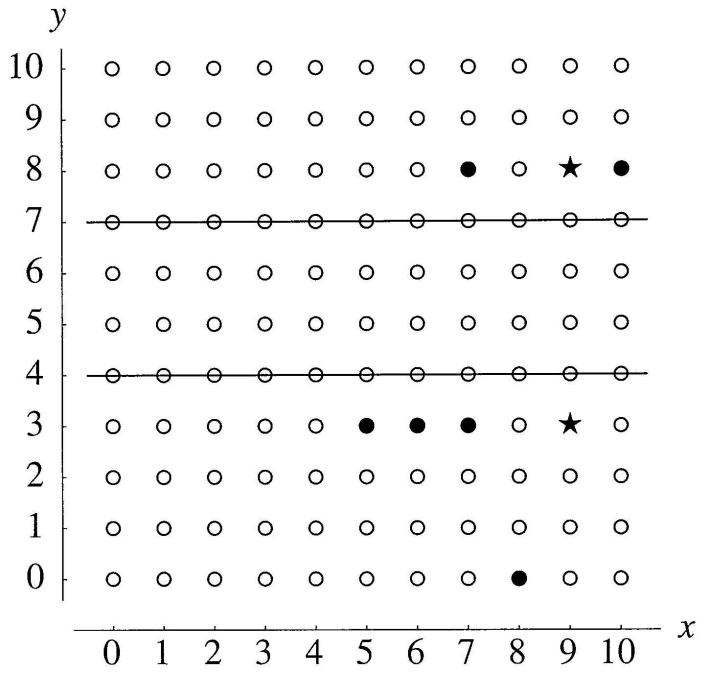
Si $\beta > 2$, alors $4 \mid g$, c-à-d.

$$\frac{1}{4} < \frac{1}{2^{4-\beta}} = |g|_2 \leq \frac{1}{4}.$$

Autrement dit, $\beta = 2$.

En résumé, il y a deux cas possibles pour (β, γ): soit $(0,3)$ soit $(2,0)$. Pour la fin de la démonstration, on se penche sur le premier $p = 11$:

PREMIER CAS: *y et z ne sont pas divisibles par* 11. On sait qu'ils sont composés de facteurs 2 et $p \equiv \pm 1 \pmod{11}$. Si $(\beta, \gamma) = (0,3)$, alors $y \equiv \pm 1 \pmod{11}$ et $z \equiv \pm 2^3 \equiv \pm 8 \pmod{11}$. Leurs réductions se trouvent sur une des deux droites $l_1 : y = 4z$ ou $l_2 : y = 7z$ définies sur $\mathbf{F}_{11}$. Si $(\beta, \gamma) = (2,0)$, on a $y \equiv \pm 4 \pmod{11}$ et $z \equiv \pm 1 \pmod{11}$. Leurs réductions se trouvent sur les même droites. Mais ces deux droites ne coupent la courbe $\widehat{C}/\mathbf{F}_{11}$ en



FIGURE

La réduction de la courbe C dans le plan affine $z = 1$ sur $\mathbf{F}_{11}$

aucun point rationnel sur $\mathbf{F}_{11}$. La figure ci-dessus présente une «image» de la courbe dans la carte affine $z = 1$ sur $\mathbf{F}_{11}$. Les points noirs sont des points lisses et les étoiles des points singuliers de $\widehat{C}$.

DEUXIÈME CAS : *z est divisible par* 11. Alors $11 \mid zf = -16N(x - \varepsilon y)$, autrement dit, $x - \varepsilon y = x + y - 4\theta y + \theta^2 y \in (\theta)$. Pour cela il faut que $x + y \in 11\mathbf{Z}$, c-à-d. $x \equiv -y \not\equiv 0 \pmod{11}$. On calcule f modulo 11, sachant que $z \equiv 0 \pmod{11}$:

$$f \equiv 64x^4 - 224x^3y + 108x^2y^2 + 116xy^3 + 10y^4 \equiv 4y^4 \pmod{11}.$$

Dans le cas $(\beta, \gamma) = (0, 3)$, il faut que $y \equiv \pm 1 \pmod{11}$ puisqu'il n'est pas divisible par 11. D'autre part, $f \equiv 4 \pmod{11}$ devrait être le produit de $2^1 \equiv 2 \pmod{11}$ et de facteurs $p \equiv \pm 1 \pmod{11}$. Dans le cas $(\beta, \gamma) = (2, 0)$, on a aussi une contradiction : $y \equiv \pm 4$, $f \equiv 4 \cdot 4^4 \equiv 1 \pmod{11}$ et $f \equiv 2^4 \cdot (\pm 1) \equiv \pm 5 \pmod{11}$.

TROISIÈME CAS : *y est divisible par* 11. Alors $11 \mid yg = -16N(x - \eta z)$. Pour cela il faut que $x + 3z \in 11\mathbf{Z}$. Cette fois-ci on considère g modulo 11, sachant que $y \equiv 0 \pmod{11}$ et $x \equiv -3z \pmod{11}$:

$$g \equiv -96x^4 - 224x^3z + 68x^2z^2 + 160xz^3 - 56z^4 \equiv 9z^4 \pmod{11}.$$

Comme avant, dans le cas $(\beta,\gamma) = (0,3)$: $z \equiv \pm 8$ et $g \equiv 2^4 \cdot (\pm 1) \equiv \pm 5 \not\equiv 9 \cdot 8^4 \equiv 3 \pmod{11}$. Et dans le cas $(\beta,\gamma) = (2,0)$: $z \equiv \pm 1$ et $g \equiv 2^2 \cdot (\pm 1) \not\equiv 9 \pmod{11}$. $\square$

7. La jacobienne de C

Il est certainement intéressant de connaître la jacobienne associée à la courbe. Nous allons construire une application birationnelle

$$\vartheta\colon C \dashrightarrow \mathrm{Jac}(C) = E$$

définie sur $\mathbf{Q}(\omega)$ à l'aide d'une transformation de Cremona de degré 3 du plan.

L'image de la conique B par l'application j est la droite

$$b = \overline{j(B)} = \{x_0 = x_1 = x_2 = 0\} \subset S \subset \mathbf{P}^4_{\mathbf{Q}}\,.$$

Prenons le point $R = (0:0:0:1:\omega) \in b(\mathbf{Q}(\omega))$ et calculons le plan tangent à S en R :

$$T_R S = T_R \mathcal{Q}_0 \cap T_R \mathcal{Q}_1 : \ \{-\omega x_0 + x_1 = 0\,, \quad \omega x_1 - x_2 = 0\}\,.$$

L'intersection de S avec $T_R S$ se décompose en deux droites b et e_1, où la seconde, qui correspond au diviseur exceptionnel de j au-dessus du point P_1, est décrite par les équations suivantes :

$$x_1 - \omega x_0 = 0\,, \qquad x_2 - \omega x_1 = 0\,, \qquad x_4 - \omega x_3 - (g_1 + g_3\omega^2 + \omega^4)\,x_0 = 0\,.$$

A ces trois équations correspondent trois cubiques du plan, passant par les point P_i et ayant un point double en P_1 :

$$A_0' : (y - \omega x)(xz - y^2) = 0\,, \qquad A_1' : (z - \omega y)(xz - y^2) = 0\,,$$

$$\begin{aligned} A_2' : \ & -g_0\omega\, x^3 + (g_0 - g_1\omega)\,x^2 y + (-g_2\omega - g_3\omega^2 - \omega^4)\,x^2 z \\ & + (g_1 + g_3\omega^2 + \omega^4)\,xy^2 + (g_2 - g_3\omega)\,xyz \\ & + (g_3 - g_4\omega)\,xz^2 + (g_4 - \omega)yz^2 + z^3 = 0\,. \end{aligned}$$

Les trois cubiques $\{A_0', A_1', A_2'\}$ constituent une base du système linéaire de telles cubiques définies sur $\mathbf{Q}(\omega)$. On peut constater que l'application associée $\vartheta' : \mathbf{P}^2_{\mathbf{Q}(\omega)} \dashrightarrow \mathbf{P}^2_{\mathbf{Q}(\omega)}$ est birationnelle car deux telles cubiques n'ont qu'un point d'intersection hors des points P_i. Elle contracte les quatre droites P_1P_j en des points $Q_j \in \mathbf{P}^2(\mathbf{Q}(\omega))$ et elle contracte la conique B en un point $Q_1 = (0:0:1)$. D'autre part, elle éclate les points P_i. Le diviseur

exceptionnel au-dessus de P_1 est la conique B' définie par les Q_i et les diviseurs exceptionnels au-dessus des autres points P_j sont des droites.

Sous cette transformation ϑ', la quintique C se simplifie en une cubique lisse $E'/\mathbf{Q}(\omega)$ passant par les quatre points Q_j pour $1 < j \leq 5$, d'équation du style

$$0 = (-5632 + 8448\omega + 640\omega^2 + 5184\omega^4)\,x^3 + \cdots + 1024\,z^3\,.$$

En reliant les deux autres intersections de E' avec B', on trouve un point T de E' défini sur $\mathbf{Q}(\omega)$ qui peut servir pour transformer E' en une forme de Weierstrass E (voir [Ca]), sans être obligé de monter dans un corps encore plus grand. Là, le miracle prédit par la théorie: E est définie sur $\mathbf{Q}$ (puisqu'elle est la jacobienne de C, une courbe définie sur $\mathbf{Q}$). Sans donner les détails du calcul, je présente les résultats: l'*invariant*

$$j = \frac{3443566663693729}{1289106508910} = \frac{151009^3}{2 \cdot 5 \cdot 11 \cdot 421 \cdot 27836461} = 2671,2817\ldots\,,$$

la *forme canonique*

$$Y^2 = X^3 + AX + B$$

avec

$$\begin{aligned} A &= -45223323296172470380044301516426 8 \\ B &= -21996454706369000130454317982498938892946059949 28\,, \end{aligned}$$

la *forme minimale globale* de E

$$Y^2 = X^3 + X^2 + a_4 X + a_6$$

avec

$$\begin{aligned} a_4 &= -5583126332860798812351148335361 \\ a_6 &= -3017346324604802976330769113064479136657958145 \end{aligned}$$

et le *conducteur arithmétique*

$$\begin{aligned} N &= 1143864722620401428256678161374838265280 \\ &= 2^6 \cdot 5 \cdot 11 \cdot 13^2 \cdot 37^2 \cdot 421 \cdot 72497^2 \cdot 151009^2 \cdot 27836461\,. \end{aligned}$$

Grâce à quelques réductions, on montre que *le groupe de torsion de* $E(\mathbf{Q})$ *est trivial.* Par construction, (C, ϑ) représente un élément d'ordre 5 du groupe de Tate-Shafarevich $Ш(E/\mathbf{Q})$. Si ce groupe est fini, son ordre est divisible par 25.

REMERCIEMENTS. Je tiens à exprimer mes plus vifs remerciements à Sylvia Guibert, à Christian Liedtke, aux frères Bartholdi et surtout aux professeurs Dino Lorenzini et Daniel Coray.

Les calculs monstrueux avec des milliers de polynômes ont été faits par *Mathematica*® et *PARI-GP*®.

RÉFÉRENCES

[Be] BEAUVILLE, A. *Surfaces algébriques complexes.* Astérisque 54, 1978.

[Ca] CASSELS, J. W. S. *Lectures on Elliptic Curves.* Cambridge Univ. Press, 1991.

[CF] CASSELS, J. W. S. et A. FRÖHLICH. *Algebraic Number Theory.* Academic Press, London, 1967.

[CCS] COLLIOT-THÉLÈNE, J.-L., D. CORAY et J.-J. SANSUC. Descente et principe de Hasse pour certaines variétés rationnelles. *J. reine angew. Math. 320* (1980), 150–191.

[CP] COLLIOT-THÉLÈNE, J.-L. et B. POONEN. Algebraic families of nonzero elements of the Shafarevich-Tate group. *J. Amer. Math. Soc. 13* (2000), 83–99.

[Co] CORAY, D. F. Arithmetic on Cubic Surfaces. PhD thesis. University of Cambridge, 1974.

[Fi] FISHER, T. A. On 5 and 7 Descents for Elliptic Curves. PhD thesis. University of Cambridge, 2000.

[Fu] FUJIWARA, M. Hasse principle in algebraic equations. *Acta Arith. 22* (1972/73), 267–276.

[Li] LIND, C.-E. Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven vom Geschlecht Eins. PhD thesis. University of Uppsala, 1940.

[Re] REICHARDT, H. Einige im Kleinen überall lösbare, im Großen unlösbare diophantische Gleichungen. *J. reine angew. Math. 184* (1942), 12–18.

[Se] SELMER, E. The diophantine equation $aX^3 + bY^3 + cZ^3 = 0$. *Acta Math. 85* (1951), 203–362.

(Reçu le 22 janvier 2001)

Christian Wuthrich

Section de Mathématiques
Case postale 240
CH-1211 Genève 24
Suisse
e-mail: christian.wuthrich@math.unige.ch