Canad. Math. Bull. Vol. **46** (1), 2003 pp. 26–38

Remarques sur les points rationnels des variétés de Fermat

D. Bernardi, E. Halberstadt et A. Kraus

Résumé. Soit K un corps de nombres de degré sur $\mathbb{Q}$ inférieur ou égal à 2. On se propose dans ce travail de faire quelques remarques sur la question de l'existence de deux éléments non nuls a et b de K, et d'un entier $n \geq 4$, tels que l'équation $ax^n + by^n = 1$ possède au moins trois points distincts non triviaux. Cette étude se ramène à la recherche de points rationnels sur K d'une variété projective dans $\mathbb{P}^5$ de dimension 3, ou d'une surface de $\mathbb{P}^3$.

1 Introduction

Étant donnés un corps de nombres K, deux éléments non nuls a et b de K et un entier $n \geq 4$, on notera $C_{a,b}(n)$, la courbe affine d'équation

$$ax^n + by^n = 1. \tag{1}$$

Ce travail concerne l'étude de l'ensemble $C_{a,b}(n)(K)$ des points rationnels sur K des courbes $C_{a,b}(n)$. D'abord, le genre de la compactifiée lisse de $C_{a,b}(n)$ est plus grand que 2, de sorte que, d'après les travaux de Faltings, l'ensemble $C_{a,b}(n)(K)$ est fini. On peut aborder l'étude de $C_{a,b}(n)(K)$ de plusieurs points de vue. On considérera ici la situation où l'entier n est fixé et où les éléments a et b parcourent K^*.

Étant donné un point (x, y) de $C_{a,b}(n)(K)$, nous dirons qu'il est *non trivial* si l'on a

$$xy \neq 0. \tag{2}$$

Deux points (x_1, y_1) et (x_2, y_2) de $C_{a,b}(n)(K)$ seront dits *distincts* si l'on a

$$(x_1^n, y_1^n) \neq (x_2^n, y_2^n). \tag{3}$$

On va s'intéresser à la question suivante :

Question 1 Existe-t-il a et b dans K^* tels que $C_{a,b}(n)(K)$ possède au moins trois points distincts non triviaux ?

Il semble que A. Desboves en 1879 ait été le premier qui se soit intéressé à cette question (*cf.* [De]).

Cette question est optimale au sens où il est facile de trouver a et b dans K^* tels que $C_{a,b}(n)(K)$ possède au moins deux points distincts non triviaux. Il suffit par exemple

Reçu par la rédaction le 2 novembre, 2000.
Classification (AMS) par sujet: 11D41.

de prendre $a = b = 1/(u^n + v^n)$, où u et v sont deux entiers relatifs non nuls tels que $u \neq \pm v$. Les points (u, v) et (v, u) appartiennent alors à $C_{a,b}(n)(\mathbb{Q})$ et sont distincts et non triviaux.

Il est par ailleurs facile de trouver *des* corps de nombres pour lesquels la réponse à la question 1 soit positive. Par exemple, si n est impair, tel est le cas du corps $\mathbb{Q}\big((3)^{1/n}\big)$ (on peut prendre $a = b = 1/2$).

On se limitera dans la suite au cas où le degré de K sur $\mathbb{Q}$ est au plus 2 et où n vaut 4, 5 ou 6. Si l'on a $K = \mathbb{Q}$, A. Granville a explicité une famille infinie à un paramètre d'éléments a et b dans $\mathbb{Q}^*$ tels que $C_{a,b}(4)(\mathbb{Q})$ posssède au moins trois points distincts non triviaux [Gr, th. 2]. Comme on le constatera plus loin, cette famille de couples (a, b) explicitée par Granville est telle que $C_{a,b}(4)(\mathbb{Q})$ posssède au moins *quatre* points distincts non triviaux. Il semble que ce soit le seul résultat publié sur la question 1 si K est le corps $\mathbb{Q}$ ou une extension quadratique de $\mathbb{Q}$. En particulier, la question de savoir s'il existe un couple (a, b) d'éléments de $\mathbb{Q}^*$ et un entier $n \geq 5$ tels que $C_{a,b}(n)(\mathbb{Q})$ possède au moins trois points distincts non triviaux, est ouverte.

Afin d'étudier la question 1, il peut être utile de considérer la surface projective lisse X_n dans $\mathbb{P}^3$ d'équation

$$p^n + q^n = r^n + s^n. \tag{4}$$

Étant donné un point (p, q, r, s) de $X_n(K)$, nous dirons qu'il est *non trivial* si

$$\{p^n, q^n\} \cap \{r^n, s^n\} = \varnothing, \quad pqrs \neq 0 \quad \text{et} \quad p^n + q^n \neq 0. \tag{5}$$

Considérons un point non trivial (p, q, r, s) de $X_n(K)$. Posons

$$a = \frac{p^n}{r^n + s^n} \quad \text{et} \quad b = \frac{q^n}{r^n + s^n}. \tag{6}$$

On a $ab \neq 0$ et $a + b = 1$. Si l'on a de plus $p^n \neq q^n$ et $r^n \neq s^n$, les couples

$$(x, y) \in \left\{ (1, 1), \left(\frac{r}{p}, \frac{s}{q}\right), \left(\frac{s}{p}, \frac{r}{q}\right), \left(\frac{q}{p}, \frac{p}{q}\right) \right\} \tag{7}$$

sont quatre points distincts non triviaux de $C_{a,b}(n)(K)$. On est donc de ce point de vue conduit à l'étude de la question suivante :

Question 2 Existe-t-il un point non trivial de $X_n(K)$?

Rappelons que la surface X_n est de type général si $n \geq 5$, et est de type K3 si $n = 4$ (*cf.* [Be, Chap. X]).

Soit T une indéterminée. Euler a découvert un point non trivial de X_4 rationnel sur le corps $\mathbb{Q}(T)$ (*cf.* [HW, p. 201]). Dans le cas où $n = 5$, en explicitant des plongements de la droite projective dans X_5, nous démontrons principalement les deux résultats suivants :

1. soient d un entier négatif sans facteur carré, non congru à 1 modulo 8, et K le corps $\mathbb{Q}(\sqrt{d})$. Alors, X_5 a un point non trivial sur $K(T)$;

https://doi.org/10.4153/CMB-2003-003-5 Published online by Cambridge University Press

2. si $K = \mathbb{Q}(\sqrt{5})$, X_5 possède un point non trivial sur $K(T)$.

Nous prouvons par ailleurs qu'il existe une infinité de corps quadratiques sur lesquels X_6 possède des points non triviaux. Nous obtenons ce résultat en considérant une courbe de genre 5 sur $\mathbb{Q}$ tracée sur X_6, qui est reliée à la courbe elliptique d'équation

$$y^2 = x^3 - 81,$$

par un morphisme de degré 2 défini sur $\mathbb{Q}$.

La question 2 est ouverte dans les cas suivants :

a) on a $n \geq 7$ et le degré de K sur $\mathbb{Q}$ est 1 ou 2 ;
b) n vaut 5 ou 6 et $K = \mathbb{Q}$.

2 Le théorème de Desboves

Desboves avait remarqué dans son article [De], que la question 1 pouvait être reformulée en termes d'existence de points rationnnels sur K de la variété projective V_n dans l'espace projectif $\mathbb{P}^5$, de dimension 3, d'équation

$$\begin{cases} d^n + e^n + f^n = g^n + h^n + k^n \\ def = ghk. \end{cases} \tag{8}$$

Nous dirons qu'un point (d, e, f, g, h, k) de $V_n(K)$ est *non trivial* si

$$\{d^n, e^n, f^n\} \cap \{g^n, h^n, k^n\} = \varnothing. \tag{9}$$

Le théorème de Desboves peut s'énoncer de la façon suivante :

Théorème 1 *Les deux assertions suivantes sont équivalentes :*

(i) *il existe un point non trivial dans $V_n(K)$;*
(ii) *il existe deux éléments non nuls a et b de K tels que $C_{a,b}(n)(K)$ possède au moins trois points distincts non triviaux.*

Rappelons par commodité la démonstration de cet énoncé.

1) Montrons que (i) implique (ii). Soit (d, e, f, g, h, k) un point non trivial de $V_n(K)$: on a $d^n + e^n + f^n = g^n + h^n + k^n$ et $def = ghk$. Posons

$$a = \frac{d^n - g^n}{k^n - f^n} \quad \text{et} \quad b = \frac{e^n - h^n}{k^n - f^n}. \tag{10}$$

On a

$$ab \neq 0 \quad \text{et} \quad a + b = 1.$$

On constate alors que les couples

$$(x, y) \in \left\{ (1, 1), \left(\frac{ef}{gh}, \frac{f}{h} \right), \left(\frac{hk}{de}, \frac{k}{e} \right) \right\} \tag{11}$$

https://doi.org/10.4153/CMB-2003-003-5 Published online by Cambridge University Press

sont trois points de $C_{a,b}(n)(K)$. Par ailleurs, il résulte directement des définitions que ces points sont distincts et non triviaux. D'où l'implication.

2) Montrons que (ii) implique (i). Soient (x_i, y_i) $(1 \leq i \leq 3)$ trois points non triviaux distincts de $C_{a,b}(n)(K)$. Posons

$$d = x_1y_2, \quad e = x_2y_3, \quad f = x_3y_1, \quad g = y_2x_3, \quad h = x_2y_1, \quad k = x_1y_3.$$

Alors (d, e, f, g, h, k) est un point de $V_n(K)$ non trivial : on vérifie d'abord que l'on a $d^n + e^n + f^n = g^n + h^n + k^n$ et $def = ghk$. Par ailleurs, on a

$$\{d^n, e^n, f^n\} \cap \{g^n, h^n, k^n\} = \varnothing.$$

En effet, supposons par exemple que l'on ait $d^n = g^n$, *i.e.*, que $(x_1y_2)^n = (y_2x_3)^n$. Puisque y_2 est non nul, cela entraîne $x_1^n = x_3^n$. Cela implique l'égalité $(x_1^n, y_1^n) = (x_3^n, y_3^n)$ (on a $ax_i^n + by_i^n = 1$), ce qui conduit à une contradiction. Les autres cas se traitent de façon analogue. D'où l'implication et le théorème.

L'étude de la question 1 peut ainsi se ramener à celle de la question suivante :

Question 3 Existe-t-il un point non trivial dans $V_n(K)$?

Remarques 1) Comme l'a remarqué Granville dans [Gr], on peut déduire du théorème 1 qu'une version généralisée de la conjecture *abc* sur $\mathbb{Q}$ entraîne l'existence d'un entier N_0, tel que pour tout entier $n \geq N_0$, et pour tout couple (a, b) d'éléments de $\mathbb{Q}^*$, l'ensemble $C_{a,b}(n)(\mathbb{Q})$ possède au plus deux points distincts non triviaux. J. Mueller a démontré en 1990 des résultats dans cette direction pour les corps de fonctions [Mu]. Signalons par ailleurs, que Y. Domar en 1954 a prouvé que pour tout entier $n \geq 5$, et tout couple (a, b) d'entiers relatifs non nuls, l'ensemble $C_{a,b}(n)(\mathbb{Q})$ possède au plus deux points entiers distincts non triviaux [Do].

2) Posons $K = \mathbb{Q}(\sqrt{5})$. L'ensemble $V_5(K)$ possède le point de coordonnées :

$$(3 + \sqrt{5}, -3 + \sqrt{5}, -2\sqrt{5}, 1 + \sqrt{5}, -1 + \sqrt{5}, 2\sqrt{5}).$$

Si T est une indéterminée, il peut se déduire de l'identité

$$(T^5 + 75)^5 + (T^5 - 75)^5 + (-50T)^5 = (T^5 + 25)^5 + (T^5 - 25)^5 + (10T^3)^5,$$

obtenue par Sastry en 1934 [Sa]. Il semble que K ait été le premier corps quadratique découvert pour lequel on sache que $V_5(K)$ possède un point non trivial.

3) Par exemple, si K est le corps $\mathbb{Q}(\sqrt{2})$ ou $\mathbb{Q}(\sqrt{3})$, on ne sait pas si $V_5(K)$ possède un point non trivial.

4) Pour tout entier $n \geq 4$, on dispose d'une application rationnelle définie sur $\mathbb{Q}$

$$\varphi\colon X_n \to V_n,$$

qui est définie par

$$\varphi\big((p, q, r, s)\big) = (pr, qr, s^2, ps, qs, r^2). \tag{12}$$

En particulier, la connaissance de $V_n(K)$ permet la détermination de $X_n(K)$.

https://doi.org/10.4153/CMB-2003-003-5 Published online by Cambridge University Press

3 Le cas $n = 4$

Soit T une indéterminée. Euler a explicité un point non trivial de $X_4\big(\mathbb{Q}(T)\big)$: il s'agit du point $P = (p, q, r, s)$, où

$$p = T^7 + T^5 - 2T^3 + 3T^2 + T, \quad q = T^6 - 3T^5 - 2T^4 + T^2 + 1,$$
$$r = T^7 + T^5 - 2T^3 - 3T^2 + T, \quad s = T^6 + 3T^5 - 2T^4 + T^2 + 1.$$

Soient A et B les deux éléments de $\mathbb{Q}(T)$ qui correspondent à P par la formule (6). D'après (7), la courbe $C_{A,B}(4)$ possède quatre points distincts non triviaux sur $\mathbb{Q}(T)$. On vérifie que toute spécialisation de T en un nombre rationnel autre que -1, 0 et 1, conduit à deux éléments a et b non nuls tels que $C_{a,b}(4)(\mathbb{Q})$ ait au moins quatre points distincts non triviaux. En particulier :

Théorème 2 *Il existe une famille infinie à un paramètre d'éléments a et b dans $\mathbb{Q}^*$ tels que $C_{a,b}(4)(\mathbb{Q})$ possède au moins quatre points distincts non triviaux.*

Par exemple, en spécialisant T par 2, on trouve

$$a = \frac{623201296}{635318657} \quad \text{et} \quad b = \frac{12117361}{635318657}.$$

L'ensemble $C_{a,b}(4)(\mathbb{Q})$ possède les quatre points de coordonnées,

$$(1, 1), \quad \left(\frac{67}{79}, \frac{133}{59}\right), \quad \left(\frac{133}{158}, \frac{134}{59}\right), \quad \left(\frac{59}{158}, \frac{158}{59}\right).$$

En existe-t-il un autre ? Plus généralement :

Question 4 Existe-t-il deux nombres rationnels non nuls a et b tels que $C_{a,b}(4)(\mathbb{Q})$ ait au moins cinq points distincts non triviaux ?

Pour tester cette question, il serait intéressant d'obtenir des éléments a et b de $\mathbb{Q}^*$ de petites hauteurs, qui sont associés à des points de $X_4(\mathbb{Q})$ par la formule (6) ou bien à des points de $V_4(\mathbb{Q})$ par la formule (10). Il semble plus facile d'en obtenir par la formule (10). Dans cette direction, nous avons déterminé tous les points non triviaux P de $V_4(\mathbb{Q})$ tels que le maximum en valeur absolue des coordonnées entières de P soit plus petit que 200. Ce sont, aux signes et aux permutations près, les trois points suivants :

$$P_1 = (171, 49, 17, 153, 133, 7), \quad P_2 = (116, 93, 22, 124, 29, 66),$$
$$P_3 = (54, 61, 196, 28, 122, 189).$$

Les éléments a et b correspondant à P_1, donnés par la formule (10), sont

$$a = -\frac{98415}{26} \quad \text{et} \quad b = \frac{98441}{26}.$$

https://doi.org/10.4153/CMB-2003-003-5 Published online by Cambridge University Press

4 Le cas $n = 6$

Pour trouver des points de la surface X_6, on peut partir de l'identité suivante, due à Euler :

$$(3u^2)^6 + (3u - 9u^4)^3 = 1 + (9u^3 - 1)^3.$$

Considérons la courbe C de $\mathbb{A}^3$ définie par les équations :

$$3u - 9u^4 = q^2, \quad 9u^3 - 1 = s^2. \tag{13}$$

La courbe C est lisse et absolument irréductible ; sa compactifiée lisse $\tilde{C}$ est de genre 5, comme on le verra. On a un plongement de C dans X_6, défini sur $\mathbb{Q}$:

$$(u, q, s) \longmapsto [3u^2, q, 1, s].$$

En fait, l'identité d'Euler ne fournit pas de points rationnels sur $\mathbb{Q}$ de X_6, elle permet seulement d'obtenir des points quadratiques de X_6. On a en effet le résultat suivant :

Théorème 3 *Considérons la courbe affine C définie par les équations (13).*

a) *L'ensemble $C(\mathbb{Q})$ est vide ;*
b) *il existe une infinité de corps quadratiques réels (resp. imaginaires) K tels que $C(K)$ soit non vide.*

Démonstration Soit E' la courbe elliptique donnée par l'équation de Weierstrass

$$y^2 = x^3 + x^2 - 2x. \tag{14}$$

C'est la courbe notée 96*A*1 des tables de Cremona [Cr]. Son conducteur est 96. Le groupe de Mordell-Weil $E'(\mathbb{Q})$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$, ses points non triviaux étant $(0, 0), (1, 0), (-2, 0)$. Les formules $x = 1 - 9u^3$, $y = 3uqs$ définissent un morphisme de C dans E', défini sur $\mathbb{Q}$. Par conséquent, si (u, q, s) était un point rationnel de C, uqs serait nul, ce qui est évidemment impossible. Ceci établit l'assertion a).

Pour l'assertion b), partons de la courbe elliptique E donnée par l'équation de Weierstrass

$$y^2 = x^3 - 81. \tag{15}$$

Le conducteur de E est $3888 = 2^4.3^5$; le groupe de Mordell-Weil $E(\mathbb{Q})$ est isomorphe à $\mathbb{Z}$, il est engendré par le point $A = (13, 46)$. Les formules $x = 3/u$, $y = 3q/u^2$ convenablement prolongées fournissent un morphisme φ de degré 2, défini sur $\mathbb{Q}$, de $\tilde{C}$ sur E. Cela étant, si n est un entier non nul, posons $nA = (x_n, y_n)$. La fibre $\varphi^{-1}(nA)$ est formée de deux points P_n, Q_n de $C \subset \tilde{C}$, définis sur un corps quadratique K_n et conjugués l'un de l'autre. On a $P_n = (u_n, q_n, s_n)$, $Q_n = (u_n, q_n, -s_n)$, où

$$u_n = \frac{3}{x_n}, \quad q_n = \frac{3y_n}{x_n^2}, \quad s_n^2 = \frac{243}{x_n^3} - 1.$$

https://doi.org/10.4153/CMB-2003-003-5 Published online by Cambridge University Press

Ainsi $K_n = \mathbb{Q}(\sqrt{d_n})$, en posant $d_n = x_n(243 - x_n^3)$. Lorsque n varie, les points P_n sont deux à deux distincts ; puisque $\tilde{C}$ est de genre 5, pour tout corps de nombres K l'ensemble $C(K)$ est fini. Les corps K_n fournissent donc une infinité de corps quadratiques K tels que $C(K)$ soit non vide. Pour conclure, il suffit de montrer qu'il y a une infinité d'entiers non nuls n tels que d_n soit positif (resp. négatif). C'est une conséquence immédiate du fait que le sous-groupe (infini) engendré par A soit dense dans $E(\mathbb{R})$, ce dernier groupe étant isomorphe, comme groupe de Lie réel, au cercle S^1. Ceci achève la démonstration du théorème.

Corollaire 1 *Il existe une infinité de corps quadratiques réels (resp. imaginaires) K tels que $X_6(K)$ possède des points non triviaux.*

Faisons quelques remarques sur ce qui précède.

1) Pour tout entier $n \neq 0$, on a $K_{-n} = K_n$.

2) On vérifie que $K_1 = \mathbb{Q}(\sqrt{-2 \times 13 \times 977})$ et

$$K_2 = \mathbb{Q}\big(\sqrt{5 \times 13 \times 569 \times 2\,903 \times 33\,328\,572\,289}\big)\ !$$

3) Soit H la courbe affine d'équation

$$y^2 = (9x^3 - 1)(3x - 9x^4),$$

et soit $\tilde{H}$ sa compactifiée lisse, qui est hyperelliptique, de genre 3. Si l'on prolonge convenablement les formules $x = u$, $y = qs$, on obtient un morphisme ψ de degré 2, défini sur $\mathbb{Q}$, de $\tilde{C}$ sur $\tilde{H}$. On voit facilement que ψ est non ramifié, ce qui montre, grâce à la formule de Riemann-Hurwitz, que $\tilde{C}$ est bien de genre 5.

4) Il peut être intéressant de remarquer que la jacobienne $\mathrm{Jac}(\tilde{C})$ de $\tilde{C}$ est isogène sur $\mathbb{Q}$ à un produit de cinq courbes elliptiques E_i, $i = 1, \ldots, 5$. Plus précisément, posons $E_1 = E_2 = E$, $E_3 = E'$, et soient E_4, E_5 les courbes elliptiques données par les équations de Weierstrass suivantes :

$$E_4 : y^2 = x^3 - 81x + 324, \quad E_5 : y^2 = x^3 - 9x - 12.$$

Les courbes E_4, E_5 ont pour conducteur $7776 = 6^5$, et E_5 est tordue quadratique de E_4 par $\mathbb{Q}(\sqrt{-3})$. On obtient pour tout i un morphisme φ_i de $\tilde{C}$ sur E_i, défini sur $\mathbb{Q}$, en prolongeant les formules suivantes :

$$\varphi_1(u,q,s) = \left(\frac{3}{u}, \frac{3q}{u^2}\right), \quad \varphi_2(u,q,s) = (9u, 9s), \quad \varphi_3(u,q,s) = (1 - 9u^3, 3uqs),$$

$$\varphi_4(u,q,s) = \left(-3(3u + 1/u), \frac{3qs}{u^2}\right), \quad \varphi_5(u,q,s) = (x,y), \quad \text{où}$$

$$x = \frac{-(27u^6 + 27u^4 - 48u^3 + 9u^2 + 1)}{3u(3u^2 - 1)^2}, \quad y = \frac{-qs(27u^6 - 81u^4 + 96u^3 - 27u^2 + 1)}{9u^2(3u^2 - 1)^3}.$$

Les degrés des morphismes φ_i sont les suivants :

$$d^\circ(\varphi_1) = d^\circ(\varphi_2) = 2, \quad d^\circ(\varphi_3) = 6, \quad d^\circ(\varphi_4) = d^\circ(\varphi_5) = 4.$$

https://doi.org/10.4153/CMB-2003-003-5 Published online by Cambridge University Press

Pour $i = 1, \ldots, 5$, soit ω_i la différentielle invariante standard sur E_i : ainsi par exemple $\omega_5 = \frac{dx}{2y-3x^2+9}$. Le calcul montre que les différentielles $\varphi_i^*(\omega_i)$, $i = 1, \ldots, 5$ sur $\tilde{C}$ sont linéairement indépendantes (sur $\mathbb{C}$), d'où notre assertion.

5) On peut montrer que les points quadratiques de la courbe C obtenus plus haut (sur les corps K_n) sont essentiellement les seuls. L'idée est la suivante. Tout d'abord, l'involution $[p, q, r, s] \longmapsto [r, s, p, q]$ de X_6 induit une involution θ de $\tilde{C}$, vérifiant :

$$\theta(u, q, s) = \left(\frac{1}{3u}, \frac{s}{3u^2}, \frac{q}{3u^2}\right).$$

On constate que $\varphi_2 = \varphi_1 \circ \theta$. Les morphismes φ_1, φ_2 fournissent donc les mêmes points quadratiques de C, modulo l'involution θ. Par ailleurs, la décomposition de $\mathrm{Jac}(\tilde{C})$ vue en 4) montre que φ_1 et φ_2 sont, à $\mathbb{Q}$-isomorphisme près, les seuls morphismes de degré 2 (définis sur $\mathbb{Q}$) de $\tilde{C}$ sur une courbe elliptique. Puisque $\tilde{C}$ n'est pas hyperelliptique, un résultat de M. Hindry [Hi] montre effectivement que les seuls points quadratiques de C sont, à un nombre fini de points près, les points P_n, Q_n considérés plus haut et leurs images par θ. Ainsi, hormis les corps K_n, il n'y a qu'un nombre fini de corps quadratiques K tels que $C(K)$ soit non vide.

5 Le cas $n = 5$

Ecrivons l'équation de X_5 sous forme plus symétrique :

$$x^5 + y^5 + z^5 + t^5 = 0. \tag{16}$$

Nous ne savons pas si $X_5(\mathbb{Q})$ possède un point non trivial, ni même si $V_5(\mathbb{Q})$ possède un point non trivial. En tous cas, $X_5(\mathbb{Q})$ ne possède pas de point non trivial de coordonnées entières et majorées en valeur absolue par 2000. Par ailleurs, signalons que C. M. Skinner et T. D. Wooley ont démonté l'énoncé suivant [SW] : pour tout réel $x > 0$, soit $\nu_5(x)$ le nombre d'entiers positifs plus petits que x qui s'écrivent de deux façons différentes comme somme de deux puissances cinquièmes positives. Alors, pour tout $\varepsilon > 0$, il existe une constante C_ε telle que l'on ait, pour tout réel $x > 0$:

$$\nu_5(x) < C_\varepsilon x^{\frac{18}{75}+\varepsilon}.$$

On va s'intéresser dans ce qui suit aux corps quadratiques sur lesquels X_5 possède des points non triviaux. Nous démontrerons plus loin qu'il y a une infinité de tels corps quadratiques. En fait, soit K un corps de nombres. Puisque la surface X_5 est de type général, une conjecture de Lang permet de penser que, hormis les points appartenant à un nombre fini de courbes exceptionnelles (courbes de genre 0 ou 1 tracées sur X_5), les points de $X_5(K)$ sont en nombre fini. Dans cette optique, nous allons exhiber certaines de ces courbes exceptionnelles.

Tout d'abord les droites tracées sur X_5 sont la droite d'équation $x+y = z+t = 0$, et celles qui s'en déduisent par les automorphismes évidents de X_5 (sur $\mathbb{C}$). Ces droites sont formées de points triviaux de X_5. Examinons ensuite l'intersection d'un plan Π avec X_5. En général, cette intersection est une courbe irréductible et lisse de genre 6.

https://doi.org/10.4153/CMB-2003-003-5 Published online by Cambridge University Press

Si Π est le plan d'équation $x + y = 0$, on trouve la réunion de cinq droites. Les seuls autres plans présentant un intérêt ici sont, aux automorphismes de X_5 près, les plans Π_k d'équation :

$$(x + y) + k(z + t) = 0,$$

où k est un nombre complexe non nul. Le cas $k = 1$ est simple :

Théorème 4 *L'intersection $\Pi_1 \cap X_5$ est formée des trois droites d'équations*

$$x + y = z + t = 0, \quad x + z = y + t = 0, \quad x + t = y + z = 0$$

et de la conique C d'équation

$$x + y + z + t = 0, \quad x^2 + y^2 + z^2 + xy + yz + zx = 0.$$

Les corps quadratiques sur lesquels C possède des points non triviaux sont exactement les corps quadratiques $\mathbb{Q}(\sqrt{d})$, où d est un entier négatif, sans facteur carré, et non congru à 1 modulo 8.

La première assertion résulte de l'identité suivante :

$$(x + y + z)^5 - (x^5 + y^5 + z^5) = 5(x + y)(y + z)(z + x)(x^2 + y^2 + z^2 + xy + yz + zx).$$

Soit K un corps quadratique. D'après le théorème de Hasse-Minkowski, $C(K)$ est non vide si et seulement si C possède des points sur chaque complété de K. En utilisant le lemme de Hensel, on déduit alors la seconde assertion du théorème.

Corollaire 2 *Soient d un entier négatif, sans facteur carré, tel que $d \not\equiv 1 \mod 8$, et K le corps $\mathbb{Q}(\sqrt{d})$. Il existe des polynômes non constants P, Q, R et S dans $K[T]$ tels que $P^5 + Q^5 = R^5 + S^5$. En particulier, X_5 a une infinité de points non triviaux sur K.*

Supposons maintenant $k \neq 0, 1$. L'intersection $\Pi_k \cap X_5$ est formée d'une droite et d'une courbe irréductible C_k de degré 4. Voici une équation affine de C_k :

$$5kX^4 + 10k^3X^2 + k^5 = 5Y^4 + 10Y^2 + 1, \tag{17}$$

obtenue en posant :

$$z + t = 1, \quad z - t = Y, \quad x + y = -k, \quad x - y = X.$$

On peut mettre l'équation (17) sous la forme suivante :

$$(Y^2 + 1)^2 = kX^4 + 2k^3X^2 + \left(\frac{k^5 + 4}{5}\right).$$

Si k^5 vaut -4 ou $-1/4$, cas qui ne nous intéresse pas ici, la courbe C_k est de genre 1; dans les autres cas, C_k est lisse, donc de genre 3. Supposons désormais $k \neq 0, 1$ rationnel. La jacobienne de C_k est isogène à un produit de trois courbes elliptiques.

https://doi.org/10.4153/CMB-2003-003-5 Published online by Cambridge University Press

L'une de ces courbes, notons la E_k, est la compactifiée lisse de la quartique plane H_k d'équation :

$$v^2 = ku^4 + 2k^3u^2 + \left(\frac{k^5+4}{5}\right).$$

On a un morphisme de degré 2 évident de C_k sur H_k, donné par les formules suivantes (convenablement complétées) :

$$u = X, \quad v = Y^2 + 1.$$

Ainsi, à un point à distance finie $(u, v) \in H_k(\mathbb{Q})$ correspondent en général deux points de $C_k(K)$, où $K = \mathbb{Q}(\sqrt{v-1})$, et donc deux points $(x, y, z, t) \in X_5(K)$:

$$x = u - k, \quad y = -u - k, \quad z = 1 \pm \sqrt{v-1}, \quad t = 1 \mp \sqrt{v-1}. \tag{18}$$

Il est maintenant facile de prouver le résultat suivant :

Théorème 5 *Soit $k \neq 0, 1$ un rationnel. On suppose que $H_k(\mathbb{Q})$ est infini : H_k possède un point rationnel à distance finie, et le groupe de Mordell-Weil $E_k(\mathbb{Q})$ est de rang ≥ 1. Il existe alors une infinité de corps quadratiques K tels que $C_k(K)$ soit non vide. Par exemple, le nombre $k = 1/5$ satisfait l'hypothèse ci-dessus, et en particulier il existe une infinité de corps quadratiques réels K sur lesquels X_5 possède des points non triviaux.*

Soit $M \in H_k(\mathbb{Q})$ un point à distance finie. Il existe un morphisme birationnel θ de E_k sur H_k, défini sur $\mathbb{Q}$, et appliquant O sur M. Soit par ailleurs $A \in E(\mathbb{Q})$ un point d'ordre infini. Pour presque tout entier n, le point $\theta(nA) = (u_n, v_n)$ est à distance finie et, via les formules (18), on obtient deux points de $C_k(K_n)$, où $K_n = \mathbb{Q}(\sqrt{v_n - 1})$. Il est clair que, pour presque tout n, ces deux points de $X_5(K_n)$ sont non triviaux. D'autre part, pour tout corps de nombres K, les résultats de Faltings montrent que $C_k(K)$ est fini. Il y a donc parmi les K_n une infinité de corps quadratiques deux à deux distincts, sur lesquels C_k possède des points non triviaux.

Supposons maintenant que $M = (u, v)$, avec $v > 1$. Quitte à remplacer A par $2A$, on peut supposer que A appartient à la composante neutre G de $E_k(\mathbb{R})$. La fonction $f = v \circ \theta$ est une fonction rationnelle non constante sur E_k, définie sur $\mathbb{Q}$. Le sous-groupe engendré par A étant dense dans G, il existe une infinité de n pour lesquels $v_n = f(nA) > 1$. Ainsi, parmi les K_n, il y a une infinité de corps quadratiques *réels* deux à deux distincts, sur lesquels C_k possède des points non triviaux. On a la même conclusion concernant les corps quadratiques imaginaires, en remplaçant v par $-v$.

Prenons enfin $k = 1/5$. On constate que $M = (1, 126/125)$ appartient à $H_{1/5}$. Les formules de transformation standard donnent pour $E_{1/5}$ le modèle minimal suivant :

$$y^2 = x^3 + x^2 - 15628x - 31252.$$

Le groupe $E_{1/5}(\mathbb{Q})$ est de rang 3, et le point $A = (218, 2640)$ est un point d'ordre infini appartenant à G. Ceci achève la preuve du théorème.

https://doi.org/10.4153/CMB-2003-003-5 Published online by Cambridge University Press

Remarque Voici les "plus petits" corps quadratiques sur lesquels nous ayons obtenu des points non triviaux de X_5, en appliquant le théorème précédent :

$$(25+\sqrt{5},25-\sqrt{5},-30,20),\quad (25+\sqrt{-55},25-\sqrt{-55},10,-20),$$
$$(123+37\sqrt{77},123-37\sqrt{77},20,-446),\quad (-1+3\sqrt{133},-1-3\sqrt{133},27,5),$$

correspondant à $k=5,5,41/71,1/16$ respectivement.

Dans l'étude de X_5, on peut prévoir que le corps $K=\mathbb{Q}(\sqrt{5})$ joue un rôle particulier. C'est effectivement le cas : à automorphismes près, nous allons voir qu'il y a (au moins) deux nouvelles courbes exceptionnelles tracées sur X_5 et définies sur K. La première de ces courbes, notons la Γ_1, est de genre 1; son intérêt pour nous est limité, car $\Gamma_1(K)$ est vide. Nous donnerons donc peu de détails. Pour définir Γ_1, on part de la factorisation

$$x^5+y^5=(x+y)(x^2-axy+y^2)(x^2-bxy+y^2),\quad \text{où}$$
$$a=\frac{1+\sqrt{5}}{2},\quad b=\frac{1-\sqrt{5}}{2},$$

et de la factorisation analogue de z^5+t^5. Considérons alors la quadrique Q d'équation

$$x^2-axy+y^2=z^2-azt+t^2.$$

L'intersection $Q\cap X_5$ a comme composantes six droites et la courbe Γ_1 cherchée, de degré 4. La réunion des quatre premières droites a pour équation :

$$x^2-axy+y^2=z^2-azt+t^2=0,$$

les deux autres droites ont pour équations respectives :

$$x+z=y+t=0\quad\text{et}\quad x+t=y+z=0.$$

La projection $(x,y,z,t)\longmapsto(x,y,z)$ induit un morphisme birationnel de Γ_1 sur une quartique plane Γ_0 ayant deux points doubles ordinaires. Ainsi Γ_0 et Γ_1 sont de genre 1. Pour établir que $\Gamma_1(K)$ est vide, on vérifie que $\Gamma_0(K_2)$ l'est, K_2 étant le complété de K en 2 (2 est inerte dans K).

La deuxième courbe est plus intéressante. On part ici de l'identité suivante :

$$(T\sqrt{5}+1)^5+(T\sqrt{5}-1)^5=5\sqrt{5}T[(1+T)^5+(1-T)^5].$$

Cette identité remarquable fait penser à Euler, mais nous ne l'avons pas trouvée dans la littérature. Voici une autre forme de cette identité :

$$(25T+\sqrt{5})^5+(25T-\sqrt{5})^5=5^5T[(1+5T)^5+(1-5T)^5]. \tag{19}$$

Dans l'identité (19), substituons T^5 à T. On obtient :

$$(25T^5+\sqrt{5})^5+(25T^5-\sqrt{5})^5=[5T(1+5T^5)]^5+[5T(1-5T^5)]^5. \tag{20}$$

https://doi.org/10.4153/CMB-2003-003-5 Published online by Cambridge University Press

Il résulte aussitôt de la dernière identité que les formules homogènes suivantes :

$$x = v(25u^5 + \sqrt{5}v^5), \quad y = v(25u^5 - \sqrt{5}v^5),$$
$$z = -5u(v^5 + 5u^5), \quad t = -5u(v^5 - 5u^5),$$

définissent un plongement π de $\mathbb{P}^1$ dans X_5. La courbe Γ que nous avions en vue est par définition l'image de $\mathbb{P}^1$ par ce plongement.

Théorème 6

a) *La surface X_5 possède une infinité de points non triviaux sur le corps $\mathbb{Q}(\sqrt{5})$.*
b) *L'intersection de X_5 avec la quadrique d'équation*

$$(x + y)(z + t) = \sqrt{5}(x - y)(z - t)$$

est formée de la courbe Γ et de quatre droites d'équations :

$$x + \zeta^h y = z + \zeta^k t = 0,$$

où ζ est une racine primitive 5-ième de l'unité et où (h, k) est l'un des couples $(1, 3)$, $(3, 1)$, $(2, 4)$, $(4, 2)$.

L'assertion a) résulte du fait que π soit défini sur K. La démonstration de l'assertion b) ne présente pas de difficulté ; les couples (h, k) en question sont exactement, modulo 5, ceux qui vérifient l'égalité

$$(1 - \zeta^h)(1 - \zeta^k) = \sqrt{5}(1 + \zeta^h)(1 + \zeta^k).$$

En prenant $u = v = 1$ dans les formules précédant le théorème 6, on obtient le point de $X_5(K)$ indiqué dans la remarque page 11.

Signalons enfin sur $X_5(K)$ un point exotique, *i.e.*, n'appartenant à aucune des courbes exceptionnelles envisagées jusqu'à présent :

$$(80 + 25\sqrt{5}, 80 - 25\sqrt{5}, -25 + 51\sqrt{5}, -25 - 51\sqrt{5}).$$

Références

[Be] A. Beauville, *Surfaces algébriques complexes.* Astérisque **54**, Société Mathématique de France, Paris, 1978.
[Cr] J. E. Cremona, *Algorithms for modular elliptic curves.* Cambridge University Press, 1992.
[De] A. Desboves, *Mémoire sur la résolution en nombres entiers de l'équation $ax^m + by^m = cz^n$.* Nouv. Ann. Math. Sér. II **18**(1879), 481–489.
[Do] Y. Domar, *On the diophantine equation $|Ax^n - By^n| = 1$, $n \geq 5$.* Math. Scand. **2**(1954), 29–32.
[Gr] A. Granville, *On the number of solutions to the generalized Fermat equation.* CMS Conf. Proc. **15**, Amer. Math. Soc., Providence, RI, 1995, 197–207.
[Hi] M. Hindry, *Points quadratiques sur les courbes.* C. R. Acad. Sci. Paris **305**(1987), 219–221.
[HW] G. H. Hardy et E. M. Wright, *An Introduction to the Theory of Numbers.* 5ième édition, Oxford Science Publications, 1979.
[Mu] J. Mueller, *Binomial Thue's equation over function fields.* Compositio Math. **73**(1990), 189–197.

https://doi.org/10.4153/CMB-2003-003-5 Published online by Cambridge University Press

[Sa] S. Sastry, *On sums of powers.* J. London Math. Soc. **9**(1934), 242–246.
[SW] C. M. Skinner et T. D. Wooley, *Sums of two k-th powers.* J. Reine Angew. Math. **462**(1995), 57–68.

Université de Paris VI
Institut de Mathématiques
UMR 7586 du CNRS
Équipe de Théorie des Nombres
175 Rue du Chevaleret
Paris 75013
France
courriel: bernardi@math.jussieu.fr
halberst@math.jussieu.fr
kraus@math.jussieu.fr

https://doi.org/10.4153/CMB-2003-003-5 Published online by Cambridge University Press