Astérisque

PH. SATGÉ

Quelques résultats sur les entiers qui sont somme des cubes de deux rationnels

Astérisque, tome 147-148 (1987), p. 335-341
<http://www.numdam.org/item?id=AST_1987__147-148__335_0>

© Société mathématique de France, 1987, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM
Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Société Mathématique de France
Astérisque 147-148 (1987), p. 335-341.

QUELQUES RÉSULTATS SUR LES ENTIERS QUI SONT SOMME DES CUBES DE DEUX RATIONNELS

Ph. SATGÉ

0. INTRODUCTION

Le problème de la décomposition d'un entier en somme de deux cubes rationnels, c'est-à-dire la recherche des points rationnels de la courbe plane $X^3+Y^3=D$ où D est un entier, est un vieux problème sur lequel beaucoup de travail reste à faire. Par exemple, la célèbre conjecture de Sylvester : "tout nombre premier congru à 4, 7 ou 8 modulo 9 est la somme des cubes de deux rationnels", énoncée à la fin du siècle dernier, est toujours un problème ouvert. L'auteur a récemment obtenu les deux résultats suivants, voisin de la conjecture de Sylvester : " si p est un nombre premier impair congru à 2 modulo 9, alors $2p$ est la somme des cubes de deux rationnels" et "si p est un nombre premier congru à 5 modulo 9, alors $2p^2$ est la somme des cubes de deux rationnels". Il ne semble pas que, à l'heure actuelle, on connaisse d'autres familles infinies d'entiers D (sans cubes) décomposables en la somme des cubes de deux rationnels. Pour démontrer ces résultats nous utilisons une idée introduite par Heegner dans [6] ; essentiellement, en calculant certaines valeurs spéciales de fonctions modulaires, nous prouvons l'existence de points rationnels sur des espaces homogènes obtenus par descente à partir de la courbe $X^3+Y^3=D$ qui nous intéresse, et nous en déduisons que cette courbe possède une infinité de points rationnels.

Ce papier comprend deux parties. Dans la première partie, nous rappelons l'argument de descente qui permet le calcul des espaces homogènes qui nous intéressent ; nous montrons aussi que cette descente fait apparaître la conjecture de Sylvester, et même certaines généralisations de cette conjecture, comme un cas particulier d'une conjecture de Cassels et Selmer concernant l'ordre du groupe de Tate-Šafarevich. Dans la deuxième partie, nous donnons les grandes lignes de la démonstration des deux résultats énoncés plus haut, résultats prévus par la généralisation de la conjecture de Sylvester discutée dans la première partie. Le détail de ces démonstrations nécessite des développements techniques assez importants et seront publiés prochainement.

I. REMARQUES SUR LA CONJECTURE DE SYLVESTER.

Nous désignons par D un entier rationnel sans cube. La courbe projective plane d'équation projective $X^3+Y^3=DZ^3$ est une courbe de genre 1 définie sur le corps $\mathbb{Q}$ des nombres rationnels. En choisissant le point rationnel $(1,-1,0)$ comme origine, on munit cette courbe d'une structure de variété abélienne de dimension 1 sur $\mathbb{Q}$. La forme de Weirstrass de cette variété abélienne est la courbe elliptique E_D d'équation projective $Y^2Z=X^3-27(4D)^2Z^3$. Ainsi un entier D est la somme des cubes de deux rationnels si et seulement si le groupe $E_D(\mathbb{Q})$ des points de E_D rationnels sur $\mathbb{Q}$ est non trivial. Nagell [9] a démontré que le groupe $E_D(\mathbb{Q})$ est sans torsion si $D\neq 1,2$. Un entier $D\neq 1,2$ est donc la somme des cubes de deux rationnels si et seulement si le groupe $E_D(\mathbb{Q})$ est infini. Rappelons que $E_1(\mathbb{Q})$ est le groupe à 3 éléments et que $E_2(\mathbb{Q})$ est le groupe à 2 éléments, donc les solutions évidentes $1^3+0^3=0^3+1^3=1$ et $1^3+1^3=2$ sont les seules décompositions possibles de 1 et 2 en somme des cubes de deux rationnels.

Le quotient de la courbe E_D par son sous-groupe d'ordre 3 engendré par le point $(0,12D\sqrt{-3},1)$ est la courbe E'_D d'équation projective $Y^2Z=X^3+(4D)^2Z^3$, et la projection naturelle de E_D sur E'_D est une isogénie de degré 3 définie sur $\mathbb{Q}$ qui apparaît souvent dans la littérature (par exemple dans le travail de Selmer [12]). Nous notons λ cette isogénie et λ' sa duale. On a :

LEMME 1.1.- Les quotients $E_D(\mathbb{Q})/\lambda'(E'_D(\mathbb{Q}))$ et $E'_D(\mathbb{Q})/\lambda(E_D(\mathbb{Q}))$ sont des espaces vectoriels de dimensions finies sur le corps à 3 éléments ; nous notons respectivement t_D et t'_D leurs dimensions. Si r_D désigne le rang sur $\mathbb{Q}$ de la courbe elliptique E_D, on a l'égalité $r_D=t_D+t'_D-1$ si $D\neq 1$.

Démonstration.- La première assertion est claire. D'autre part, E'_D étant isogène sur $\mathbb{Q}$ à E_D, son rang sur $\mathbb{Q}$ est r_D ; de plus le point de coordonnées projective $(0,4D,1)$ est un point d'ordre 3 de $E'_D(\mathbb{Q})$, donc la dimension de $E'_D(\mathbb{Q})/3E'_D(\mathbb{Q})$ sur le corps à 3 éléments est r_D+1. Ce quotient s'insère naturellement dans la suite exacte

$$0 \longrightarrow \lambda(E_D(\mathbb{Q}))/3E'_D(\mathbb{Q}) \longrightarrow E'_D(\mathbb{Q})/3E'_D(\mathbb{Q}) \longrightarrow E'_D(\mathbb{Q})/\lambda(E_D(\mathbb{Q})) \longrightarrow 0$$

d'espaces vectoriels sur le corps à 3 éléments. On conclut en remarquant que le morphisme surjectif de $E_D(\mathbb{Q})/\lambda'(E'_D(\mathbb{Q}))$ vers $\lambda(E_D(\mathbb{Q}))/3E'_D(\mathbb{Q})$ induit par λ est aussi injectif puisque, comme nous l'avons rappelé plus haut, $E_D(\mathbb{Q})$ ne possède pas de points non triviaux tués par une puissance de 3 si $D\neq 1$.

Désignons par S et S' les groupes de Selmer des isogénies λ et λ', par $Ш$ et $Ш'$ les groupes de Tate-Safarevich de E_D et de E'_D, et par $Ш[\lambda]$ et $Ш'[\lambda']$ les sous-groupes de $Ш$ et $Ш'$ formés des éléments tués par λ et λ'. Les deux suites de descente

$$(1) \qquad 0 \longrightarrow E'_D(\mathbb{Q})/\lambda(E_D(\mathbb{Q})) \longrightarrow S \longrightarrow Ш[\lambda] \longrightarrow 0$$

$$(1') \qquad 0 \longrightarrow E_D(\mathbb{Q})/\lambda'(E'(\mathbb{Q})) \longrightarrow S' \longrightarrow Ш'[\lambda'] \longrightarrow 0$$

sont des suites exactes d'espaces vectoriels sur le corps à 3 éléments. Notons $d(S)$, $d(S')$, $Ш_\lambda$ et $Ш'_{\lambda'}$ les dimensions des espaces S, S', $Ш[\lambda]$, et $Ш'[\lambda']$. Le lemme 1.1 et les suites exactes (1) et (1') donnent immédiatement l'égalité suivante :

$$(2) \qquad r_D = d(S) + d(S') - 1 - Ш_\lambda - Ш'_{\lambda'},$$

La conjecture de Cassels-Selmer affirme que $Ш_\lambda + Ш'_{\lambda'}$ est pair, donc que $r_D \geqslant 0$ si $d(S)+d(S')$ est pair, et donc que D peut s'écrire comme la somme des cubes de deux rationnels dans ces cas. Les groupes de Selmer S et S' ont été calculé explicitement dans [11] (théorème 2.9). Ces calculs montrent que la conjecture de Sylvester est conséquence de la conjecture de Cassels-Selmer, et ils permettent des généralisations aisées. Illustrons ce point en dressant la liste des D divisibles par 1 ou 2 facteurs premiers qui, en accord avec la conjecture de Cassels-Selmer, doivent être la somme des cubes de deux rationnels, c'est-à-dire la liste de ces D pour lesquels $d(S)+d(S')$ est pair. Le théorème 2.9 de [11] donne

<u>Proposition 1.2</u>.- Si $D = p^r$ avec p premier et $r \in \{1,2\}$, alors $d(S)+d(S')$ est pair si et seulement si $p \equiv 4,7,8 \bmod 9$ ou si $D = 9$; dans ces cas on a $d(S) = d(S') = 1$.

<u>Proposition 1.3</u>.- Si $D = p^r q^s$ avec p et q premiers distincts et $r,s \in \{1,2\}$, alors $d(S)+d(S')$ est pair si et seulement si, quitte à intervertir p et q, on est dans l'un des 5 cas suivants :

I) $p \equiv 1 \bmod 3$, $q \equiv -1 \bmod 3$, et $D \equiv \pm 1 \bmod 9$

II) $p \equiv -1 \bmod 3$, $q \equiv -1 \bmod 3$, et $D \not\equiv \pm 1 \bmod 9$

III) $p \equiv 1 \bmod 3$, $q \equiv 1 \bmod 3$, et $D \not\equiv \pm 1 \bmod 9$

IV) $p^r = 3$, et $q \equiv -1 \bmod 3$

V) $p^r = 9$, et $q \equiv 1 \bmod 3$.

De plus, on a $d(S) = 2$ et $d(S') = 0$ dans les cas II) et IV) ; on a $d(S) = d(S') = 1$ dans le cas I) sauf si $p \equiv 1 \bmod 9$ et $q \equiv -1 \bmod 9$, et dans le cas V) sauf si $q \equiv 1 \bmod 9$ et 3 est un cube mod q ; dans tous les cas qui restent, on a $d(S) = d(S') = 2$.

Dans la partie suivante, nous indiquons comment, en s'inspirant des idées de Heegner [6], nous pouvons prouver que $r_D = 1$ lorsque $D = 2p$ et p est un premier congru à 2 modulo 9, et lorsque $D = 2p^2$ et p est un premier congru à 5 modulo 9 ; on remarquera que ces deux cas sont des cas particuliers du cas II) de la proposition 1.3. Les deux familles infinies de courbes elliptiques de rang 1 sur $\mathbb{Q}$ exhibées ici s'ajoutent au petit nombre de familles de courbes elliptiques de rang 1 déjà connues et dont une liste exhaustive semble être contenue dans les travaux de Heegner [6], Birch [1], [2], Birch-Stephens [3], Gross [4], [5] et Mazur [7],[8]. Il serait intéressant d'exhiber d'autres familles de ce type ; le cas IV de la proposition 1.3 semble attaquable par les méthodes décrites au paragraphe suivant.

II. LES GRANDES LIGNES DE LA DÉMONSTRATION.

Nous nous plaçons dans le cas II) de la proposition 1.3, c'est-à-dire dans le cas $D = p^r q^s$, $D \not\equiv \pm 1 \bmod 9$, p et q premiers distincts congrus à $-1 \bmod 3$, et $r, s \in \{1,2\}$. On a $S \simeq (\mathbb{Z}/3\mathbb{Z})^2$ et $S' = \{0\}$. Dans [11], on a associé à chaque élément non trivial de S un corps cubique défini à conjugaison près, deux éléments distincts de S étant associés au même corps si et seulement si l'un de ces éléments est le carré de l'autre. Ainsi il y a 4 corps cubiques associés aux éléments non triviaux de S dans le cas que nous considérons ici ; le théorème 2.6 de [11] montre que ces 4 corps sont les corps purs $\mathbb{Q}(\sqrt[3]{p^a q^b})$ avec a et b entiers rationnels non simultanément divisibles par 3 (un tel corps ne dépend, bien entendu, que de la valeur du couple $\pm(a,b)$ modulo 3). A un tel couple d'entiers (a,b) nous associons la cubique plane $C_{a,b}$ d'équation projective $W^3 = p^\alpha q^\beta U^3 - p^\gamma q^\delta V^3$ où $\alpha, \beta, \gamma, \delta \in \{0,1,2\}$ sont définis par les congruences $\alpha \equiv 2r+a$, $\beta \equiv 2s+b$, $\gamma \equiv 2r+2a$, $\delta \equiv 2s+2b$ modulo 3. Au début du §4 de [11], on donne la caractérisation suivante de l'image de $E'_D(\mathbb{Q})/\lambda(E_D(\mathbb{Q}))$ par l'injection de la suite exacte de descente associée à λ (i.e. la suite (1) du paragraphe précédent) :

Proposition 2.1.- Les deux assertions suivantes sont équivalentes :

I) Les deux éléments de S associés au corps cubique $\mathbb{Q}(\sqrt[3]{p^a q^b})$ appartiennent à l'image de $E'_D(\mathbb{Q})/\lambda(E_D(\mathbb{Q}))$ par l'injection de la suite exacte de descente.

II) La courbe $C_{a,b}$ possède un point rationnel.

Rappelons que le point $(0,4D,1)$ de $E'_D(\mathbb{Q})$ est d'ordre 3 et n'appartient pas à $\lambda(E_D(\mathbb{Q}))$ (puisque $D\neq 1$) ; l'image de la classe de $(0,4D,1)$ modulo $\lambda(E_D(\mathbb{Q}))$ par l'injection de la suite exacte de descente est l'élément de S associé au corps cubique $\mathbb{Q}(\sqrt[3]{D}) = \mathbb{Q}(\sqrt[3]{p^r q^s})$, donc la proposition 2.1 affirme l'existence d'un point rationnel sur la courbe $C_{r,s}$ (on peut remarquer que l'équation de $C_{r,s}$ est $W^3 = U^3 - p^r q^s V^3$ et que cette courbe possède le point rationnel évident $(1,0,1)$). Deux cas sont alors possible : ou bien $C_{r,s}$ est la seule des 4 courbes $C_{a,b}$ à posséder un point rationnel, et l'image de $E'_D(\mathbb{Q})/\lambda(E_D(\mathbb{Q}))$ par l'injection de la suite exacte de descente est isomorphe à $\mathbb{Z}/3\mathbb{Z}$, ou bien l'une au moins des courbes $C_{a,b}$ distinctes de $C_{r,s}$ possède un point rationnel, et l'image de $E'_D(\mathbb{Q})/\lambda(E_D(\mathbb{Q}))$ par l'injection de la suite exacte de descente est isomorphe à $(\mathbb{Z}/3\mathbb{Z})^2$ i.e. est S tout entier, et donc toutes les courbes $C_{a,b}$ possèdent des points rationnels. Dans le premier cas $E'_D(\mathbb{Q})$ est un groupe de torsion et $r_D = 0$, dans le deuxième cas $E'_D(\mathbb{Q})$ est de rang 1 et $r_D = 1$; conjecturalement, on est dans le deuxième cas. Explicitons les deux cas $D = 2p$ et $D = 2p^2$ i.e. les cas $q = 2$, $r = 1,2$, et $s = 1$. Dans le premier de ces cas, les quatre courbes $C_{a,b}$ sont $W^3 = U^3 - 2p\,V^3$, $W^3 = p^2U^3 - 2p^2V^3$, $W^3 = 4U^3 - 4p\,V^3$ et $W^3 = 2U^3 - p\,V^3$; dans le deuxième cas $W^3 = U^3 - 2p^2W^3$, $W^3 = pU^3 - 2pV^3$, $W^3 = p^2U^3 - 2\,V^3$ et $W^3 = 4p^2U^3 - 4V^3$; dans les deux cas on a placé en premier la courbe $C_{r,s}$. Pour démontrer les deux résultats annoncés, il suffit donc de montrer que, dans le premier cas si $p \equiv 2 \bmod 9$, et dans le deuxième cas si $p \equiv 5 \bmod 9$, l'une des 3 dernières courbes possède un point rationnel (il est agréable de remarquer qu'il est clair sur les équations que dès que l'une de ces 3 courbes possède un point rationnel, alors les 3 en possèdent, résultat prévu par la théorie générale). Cela termine la partie géométrique de la démonstration.

Nous devons maintenant introduire quelques fonctions modulaires de niveau 6. Nous désignons par j l'invariant modulaire classique, et par γ_3 la fonction modulaire de niveau 2 caractérisée par $\gamma_3^2 = j - 1728$ et par le fait que le développement à l'infini de $\gamma_3(z)$ commence par $e^{-\pi i z}$; ces notations sont celles de Weber dans [13]. Posons $\rho = e^{\frac{2\pi i}{3}}$; alors $\gamma_3^2(\rho) = -1728$, et on vérifie sans mal que $\gamma_3(\rho) = 24i\sqrt{3}$ et $\gamma_3(-\frac{1}{\rho}) = -24i\sqrt{3}$ où $\sqrt{3}$ est le nombre positif dont le carré vaut 3. Avec un peu plus de travail, on établit la proposition suivante :

<u>Proposition 2.2</u>.- Il existe deux fonctions modulaires ψ_1 et ψ_2 de niveau 6 qui vérifient les équations $\psi_1^3 = \gamma_3 - 24i\sqrt{3}$ et $\psi_2^3 = \gamma_3 + 24i\sqrt{3}$.

On normalise ψ_1 et ψ_2 en imposant que les développements à l'infini de

$\psi_1(z)$ et de $\psi_2(z)$ commencent par $e^{-\frac{2\pi i}{6}z}$; les coefficients de ces développements à l'infini sont dans le corps des racines 6ème de l'unité i.e. $\mathbb{Q}(\sqrt{-3})$; les fonctions ψ_1 et ψ_2 sont liées par l'équation $\psi_1^3 = \psi_2^3 - 48i\sqrt{3}$. Dans la suite, nous posons $f_1 = \psi_1/2i\sqrt{3}$ et $f_2 = \psi_2/2i\sqrt{3}$; les fonctions f_1 et f_2 sont donc deux fonctions modulaires de niveau 6 dont le développement à l'infini est à coefficients dans $\mathbb{Q}(\sqrt{-3})$, et qui sont liées par l'équation $f_1^3 = f_2^3+2$. Notons $R^{(p)}$ le corps des classes de l'ordre quadratique imaginaire de discriminant $-3p^2$; le nombre premier p étant congru à -1 modulo 3, le corps $R^{(p)}$ est une extension abélienne de $\mathbb{Q}(\sqrt{-3})$ de degré $\frac{p+1}{3}$. Par des arguments assez généraux de la théorie de la multiplication complexe, on montre assez facilement que les deux nombres $f_1(p\rho)$ et $f_2(p\rho)$ appartiennent au corps $R^{(p)}(\sqrt[3]{2},\sqrt[3]{p})$, corps abélien sur $\mathbb{Q}(\sqrt{-3})$. La partie la plus délicate de la démonstration consiste à calculer précisément l'action du Frobenius de certains idéaux premiers de $\mathbb{Q}(\sqrt{-3})$ d'une part sur $f_1(p\rho)$ et $f_2(p\rho)$, et d'autre part sur $\sqrt[3]{2}$ et $\sqrt[3]{p}$; de ce calcul on tire la proposition suivante :

Proposition 2.3.-

I) Si $p \equiv 2 \bmod 9$, les quotients $f_1(p\rho)/\sqrt[3]{4}$ et $f_2(p\rho)/\sqrt[3]{2p}$ sont dans le corps $R^{(p)}$.

II) Si $p \equiv 5 \bmod 9$, les quotients $f_1(p\rho)/\sqrt[3]{4}$ et $f_2(p\rho)/\sqrt[3]{2p^2}$ sont dans le corps $R^{(p)}$.

Les fonctions f_1 et f_2 étant liées par l'équation $f_1^3 = f_2^3+2$, on a en particulier l'égalité $f_1^3(p\rho) = f_2^3(p\rho)+2$ que l'on peut réécrire sous les deux formes suivantes :

$$4(f_1(p\rho)/\sqrt[3]{4})^3 = 2p(f_2(p\rho)/\sqrt[3]{2p})^3+2$$

$$4(f_1(p\rho)/\sqrt[3]{4})^3 = 2p^2(f_2(p\rho)/\sqrt[3]{2p^2})^3+2.$$

En multipliant ces deux égalités par 2, on déduit que les points de coordonnées projectives $(1,-f_2(p\rho)/\sqrt[3]{2p},2f_1(p\rho)/\sqrt[3]{4})$ et $(f_2(p\rho)/\sqrt[3]{2p^2},-1,2f_1(p\rho)/\sqrt[3]{4})$ appartiennent respectivement aux courbes $W^3 = 4U^3 - 4pV^3$ et $W^3 = 4p^2U^3 - 4V^3$. Ainsi la proposition 2.3 montre que si $p \equiv 2 \bmod 9$ (resp. $\rho \equiv 5 \bmod 9$) la première (resp. la seconde) de ces courbes possède un point rationnel sur le corps $R^{(p)}$ dont le degré absolu $2\,\frac{p+1}{3}$ est premier à 3. D'autre part, ces deux courbes possèdent clairement des points rationnels sur des corps cubiques. On sait qu'une courbe de genre 1 qui possède des points rationnels sur deux corps de degré absolu premiers

entre eux possède un point rationnel sur $\mathbb{Q}$. Ainsi, si $p \equiv 2 \bmod 9$ (resp. $5 \bmod 9$). la courbe $W^3 = 4U^3 - 4pV^3$ (resp. $W^3 = 4p^2U^3 - 4V^3$) possède un point rationnel sur $\mathbb{Q}$. Comme nous l'avons noté plus haut, cela achève la démonstration des résultats annoncés.

[1] Birch, B.J., Elliptic curves and modular functions, Symp. Math. Inst. Alta Math., 4 (1970), 27-32.

[2] Birch, B.J., Heegner points of elliptic curves, Symp. Math. Inst. Alta Math., 15 (1975), 441-445.

[3] Birch, B.J. et Stephens, N.M., Heegner's construction of points on the curve $y^2 = x^3 - 1728\ e^3$, Séminaire de théorie des nombres, Paris 1981-82, Birkhaüser, 1-19.

[4] Gross, B.H., On the Fermat cubic, Proceeding of a conference et Maryland, A.M.S., (1982).

[5] Gross, B.H., Heegner points on $X_0(11)$, Séminaire de théorie des nombres de Bordeaux, 1981-82, 34.01-34.05.

[6] Heegner, K., Diophantische Analysis und Modulfunktionen, Math. Z., 56 (1952), 227-253.

[7] Mazur, B., Modular curves and the Eissentein ideal, Publ. Math. IHES, 47 (1978), 33-186.

[8] Mazur, B., On the arithmetic of special values of L-functions, Invent. Math., 55 (1979), 207-240.

[9] Nagell, T., Solutions de quelques problèmes dans la théorie arithmétique des cubiques planes du premier genre, Skifter Vid. Akad. Oslo, I, Mat. nat. kl. (1935), 1-25.

[10] Satgé, Ph., Une généralisation du calcul de Selmer, Séminaire de Théorie des Nombres, Paris 1981-82, Birkhaüser, 245-265.

[11] Satgé, Ph., Groupes de Selmer et corps cubiques, J. Number Theory, à paraître.

[12] Selmer, E.,S., The diophantine equation $ax^3+by^3+cz^3 = 0$, Acta Math. 85 (1951), 203-362.

[13] Weber, H., Lehrbuch der Algebra, Dritter Band, Chelsea Publishing Company, N.Y., (1908).

Ph. SATGE
Université de CAEN
Département de Mathématiques
14032 CAEN CEDEX
FRANCE