

JEAN-RENÉ JOLY

Séries L des cubiques $X^3 + Y^3 = \mathcal{D}$ et décomposition d'un nombre rationnel en somme de deux cubes (démonstration d'une conjecture de Stephens)

Séminaire de théorie des nombres de Grenoble, tome 6 (1977-1978), exp. n° 1, p. 1-9

http://www.numdam.org/item?id=STNG_1977-1978__6__A1_0

© Institut Fourier – Université de Grenoble, 1977-1978, tous droits réservés.

L'accès aux archives du séminaire de théorie des nombres de Grenoble 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/>

Grenoble

SERIES L DES CUBIQUES $X^3 + Y^3 = D$, ET DECOMPOSITION D'UN
NOMBRE RATIONNEL EN SOMME DE DEUX CUBES (démonstration d'une
conjecture de Stephens)

par

Jean-René JOLY (Grenoble)

On démontre une conjecture de Stephens relative à la parité de
l'ordre en $s=1$ des séries L des cubiques $X^3 + Y^3 = D$. On
en déduit que, si ces courbes vérifient une conjecture de Birch
et Swinnerton-Dyer, alors 50% au moins des nombres rationnels
positifs sont représentables comme somme de deux cubes ration-
nels positifs.

1. INTRODUCTION, RAPPELS (d'après Birch et Stephens, [2], [6], [7],
dont nous conservons les notations).

Soit $D \geq 1$ un entier sans facteur cubique. Notons Γ_D la courbe
elliptique $X^3 + Y^3 = D$ (définie sur le corps $\mathbb{Q}$ des rationnels), $\zeta_D(s)$
la fonction zêta globale de Γ_D , et $L_D(s)$ la série L de Γ_D , telle
que $\zeta_D(s) = \zeta(s)\zeta(s-1)/L_D(s)$. Un calcul classique de nombre de points
d'une courbe sur un corps fini (voir par exemple [4], pp. 59-62) montre
que $L_D(s)$ est une série L de Hecke, prolongeable analytiquement à $\mathbb{C}$
tout entier ([6], pp. 123-126), munie d'une équation fonctionnelle de la
forme $L_D(2-s) = \Delta(s)L_D(s)$, et dont l'ordre $\gamma(D)$ en $s=1$ vérifie une
relation de la forme

$$(1) \quad (-1)^{\gamma(D)} = W(D) \text{ .}$$

$W(D)$ désigne ici une certaine somme de caractères ([6], p. 125) dont
la valeur peut se calculer de la manière suivante (voir [2]) : on pose

$$(2) \quad \Delta(D) = \text{le produit des nombres premiers } \neq 3 \text{ et divisant } D \text{ ;}$$

(3) $\delta(D) = \pm 1$ = la classe de $\Delta(D)$ modulo 3 ;

on a alors

$$(4) \quad W(D) = \begin{cases} \delta(D) & \text{si } D \equiv \pm 1, \pm 3 \pmod{9} ; \\ -\delta(D) & \text{si } D \equiv 0, \pm 2, \pm 4 \pmod{9} . \end{cases}$$

Dans [7] , Stephens introduit la somme

$$(5) \quad R(x) = \sum'_{D \leq x} W(D)$$

(où $x \geq 1$ est une variable réelle, et où l'accent rappelle que la sommation est restreinte aux entiers sans facteur cubique). Il en donne une majoration

$$|R(x)| \leq \frac{39}{72}x \quad \left(\text{\AA comparer avec } \sum'_{D \leq x} 1 \sim \frac{1}{\zeta(3)}x \right) \text{ et ajoute (p. 148, § 3) :}$$

"... une étude plus détaillée du comportement de $R(x)$ pourrait montrer que $R(x) = o(x)$; car il semble que $W(D)$ prenne les valeurs ± 1 avec une égale probabilité."

Nous nous proposons ici de vérifier cette conjecture, et plus précisément de démontrer le théorème suivant :

THEOREME 1. - Avec les définitions ci-dessus, on a

$$(6) \quad R(x) = O(x^{3/4} \log x) = o(x) .$$

Ce théorème sera démontré aux §§ 2-3. La démonstration consiste à utiliser (2)-(4) pour ramener $R(x)$ à des sommes $S(x; \chi_\delta)$, qui sont à peu de choses près des sommes de caractères non principaux modulo 9 étendues aux entiers sans facteurs cubiques (voir § 2), puis à transformer ces sommes $S(x; \chi_\delta)$ par des considérations élémentaires pour en donner une estimation en $O(x^{3/4} \log x)$ (voir § 3) .

L'estimation (6) admet une conséquence intéressante (voir d'ailleurs [7] , § 2). Notons A (resp. B, C) l'ensemble des $D \geq 1$ tels que $\chi(D)$ soit pair (resp. impair, supérieur ou égal à 1). On a évidemment

$$(7) \quad R(x) = \sum'_{\substack{D \leq x \\ D \in A}} 1 - \sum'_{\substack{D \leq x \\ D \in B}} 1 .$$

Il est bien connu d'autre part que

$$(8) \quad \sum'_{D \leq x} 1 = \sum'_{\substack{D \leq x \\ D \in A}} 1 + \sum'_{\substack{D \leq x \\ D \in B}} 1 \sim \frac{x}{\zeta(3)} .$$

L'estimation (8), combinée avec (7) et (8), implique donc

$$(9) \quad \sum'_{\substack{D \leq x \\ D \in A}} 1 \sim \sum'_{\substack{D \leq x \\ D \in B}} 1 \sim \frac{x}{2 \zeta(3)} .$$

Comme $B \subset C$, la deuxième équivalence (9) entraîne

$$(10) \quad \lim_{\substack{D \leq x \\ D \in C}} \left(\sum'_{D \leq x} 1 / \sum'_{D \leq x} 1 \right) \geq \frac{1}{2} ;$$

en d'autres termes :

$$(11) \quad 50 \% \text{ au moins des cubiques } \Gamma_D \text{ ont une série } L \text{ dont l'ordre en } s = 1 \text{ vérifie } \gamma(D) \geq 1 .$$

Soit maintenant $g(D)$ le rang de $\Gamma_D(\mathbb{Q})$, groupe (abélien, de type fini) des points $\mathbb{Q}$ -rationnels de Γ_D . Admettons la conjecture suivante (conjecture de Birch et Swinnerton-Dyer pour les cubiques $X^3 + Y^3 = D$: voir [3], [6]) :

$$(12) \quad \text{quel que soit } D, \quad g(D) = \gamma(D) .$$

La propriété (11) se réécrit alors

$$(13) \quad 50 \% \text{ au moins des cubiques } \Gamma_D \text{ ont un rang } g(D) \geq 1 .$$

On sait enfin (voir [3]) que, pour $D \geq 3$ et sans facteur cubique, le groupe $\Gamma_D(\mathbb{Q})$ est sans torsion : il est facile d'en déduire que les trois conditions suivantes sont alors équivalentes :

- (i) $g(D) \geq 1$; (ii) Γ_D admet un point $\mathbb{Q}$ -rationnel "à distance finie" ;
- (iii) Γ_D admet un point $\mathbb{Q}$ -rationnel (x, y) tel que $x \geq 0, y \geq 0$.

(Noter par exemple que $\Gamma_D(\mathbb{R})$ est connexe, donc isomorphe au tore de dimension 1, et que par conséquent, si $\Gamma_D(\mathbb{Q}) \subset \Gamma_D(\mathbb{R})$ est sans torsion et non trivial, il est partout dense dans $\Gamma_D(\mathbb{R})$.)

La combinaison de (13) et de l'équivalence ci-dessus donne ainsi la conséquence annoncée :

THEOREME (conditionnel) 2. - Si les cubiques Γ_D vérifient la conjecture (12), alors 50 % au moins des entiers positifs sans facteur cubique sont représentables comme somme de deux cubes rationnels positifs (non entiers en général : le nombre d'entiers positifs $\leq x$ et représentables comme somme de deux cubes entiers positifs est $O(x^{2/3})$).

2. REDUCTION DE LA SOMME $R(x)$ A DES SOMMES $S(y; \chi_j^\delta)$.

Cette réduction va s'effectuer en plusieurs temps.

1er temps. - A la manière de Stephens ([7], p. 147), mais en utilisant le module 9 au lieu du module 4, on peut écrire

$$(14) \quad R(x) = R_1(x) + R_2(x) + R_3(x) ,$$

avec

$$(15) \quad R_1(x) = \sum_{\substack{n \leq x \\ (n,3)=1}}' W(n) ,$$

$$(16) \quad R_2(x) = \sum_{\substack{3n \leq x \\ (n,3)=1}}' W(3n) ,$$

$$(17) \quad R_3(x) = \sum_{\substack{9n \leq x \\ (n,3)=1}}' W(9n) ,$$

l'accent indiquant toujours que la sommation est restreinte aux entiers sans facteur cubique.

2ème temps. - Pour toute fonction arithmétique $\alpha : \mathbb{N} \rightarrow \mathbb{C}$, posons

$$(18) \quad S(y; \alpha) = \sum_{\substack{n \leq y \\ (n,3)=1}}' \alpha(n) .$$

On peut transformer les sommes R en sommes S de la façon suivante :

Somme $R_2(x)$: si $(n,3) = 1$, on a $3n \equiv \pm 3 \pmod{9}$, donc, d'après (2) - (4), $W(3n) = \delta(3n) = \delta(n)$, et par conséquent

$$(19) \quad R_2(x) = \sum'_{\substack{n \leq x/3 \\ (n,3)=1}} \delta(n) = S(x/3; \delta) .$$

Somme $R_3(x)$: si $(n,3) = 1$, on a $9n \equiv 0 \pmod{9}$, donc, d'après (2) - (4), $W(9n) = -\delta(9n) = -\delta(n)$, et par conséquent

$$(20) \quad R_3(x) = - \sum'_{\substack{n \leq x/9 \\ (n,3)=1}} \delta(n) = -S(x/9; \delta) .$$

Somme $R_1(x)$: si $(n,3) = 1$, on a ou bien $n \equiv \pm 1 \pmod{9}$, auquel cas $W(n) = \delta(n)$; ou bien $n \equiv \pm 2, \pm 4 \pmod{9}$, auquel cas $W(n) = -\delta(n)$ (voir toujours (2) - (4)) . D'où

$$(21) \quad R_1(x) = \sum'_{\substack{n \leq x \\ n \equiv \pm 1(9)}} \delta(n) - \sum'_{\substack{n \leq x \\ n \equiv \pm 2, \pm 4}} \delta(n) .$$

Les six valeurs $\pm 1, \pm 2, \pm 4 \pmod{9}$ sont les éléments du groupe $(\mathbb{Z}/9\mathbb{Z})^*$, cyclique d'ordre 6. Soit X le dual de ce groupe, soit χ_1 un caractère de Dirichlet générateur de X , et posons $\chi_j = \chi_1^j$. On vérifie sans peine que $\chi_2(n) + \chi_4(n)$ vaut 2 si $n \equiv \pm 1 \pmod{9}$, et vaut -1 si $n \equiv \pm 2, \pm 4 \pmod{9}$: d'où

$$(22) \quad R_1(x) = \sum'_{\substack{n \leq x \\ (n,3)=1}} (\chi_2 \delta)(n) + \sum'_{\substack{n \leq x \\ (n,3)=1}} (\chi_4 \delta)(n) - \sum'_{\substack{n \leq x \\ n \equiv \pm 1(9)}} \delta(n) .$$

Un argument classique donne d'autre part, pour $a = \pm 1$,

$$(23) \quad \sum'_{\substack{n \leq x \\ n \equiv a(9)}} \delta(n) = \sum'_{n \leq x} \left(\frac{1}{6} \sum_{j=0}^5 \overline{\chi}_j(a) \chi_j(n) \right) \delta(n) = \frac{1}{6} \sum_{j=0}^5 \overline{\chi}_j(a) \sum'_{n \leq x} (\chi_j \delta)(n) ,$$

d'où

$$(24) \quad \sum'_{\substack{n \leq x \\ n \equiv \pm 1(9)}} \delta(n) = \frac{1}{6} \sum_{j=0}^5 [\overline{\chi}_j(1) + \overline{\chi}_j(-1)] \sum'_{n \leq x} (\chi_j \delta)(n) .$$

Mais $\chi_j(-1) = (-1)^j$: le terme entre crochets vaut donc 0 si $j = 1, 3, 5$, et vaut 2 si $j = 0, 2, 4$. Compte tenu de cette remarque, et du fait que les seuls termes figurant explicitement à droite de (24) correspondent à des n tels que $(n,3) = 1$, la combinaison de (22) et (24) donne fina-

lement (avec la notation (18))

$$(25) \quad R_1(x) = \frac{2}{3} S(x; \chi_2 \delta) + \frac{2}{3} S(x; \chi_4 \delta) - \frac{1}{3} S(x; \chi_0 \delta) .$$

3ème temps. - On combine (14), (15), (16), (17), et (19), (20), (25).

On arrive ainsi au résultat suivant :

LEMME 1. - La somme $R(x)$ s'exprime à l'aide de sommes $S(y; \chi_j \delta)$ par la formule

$$(26) \quad R(x) = S(x/3; \delta) - S(x/9; \delta) + \frac{2}{3} S(x; \chi_2 \delta) + \frac{2}{3} S(x; \chi_4 \delta) - \frac{1}{3} S(x; \chi_0 \delta) .$$

Le lemme 1, la définition (18) et le fait que $\chi_0(n) = 0$ si $(n, 3) \neq 1$ réduisent alors la démonstration du théorème 1 à celle du résultat suivant :

LEMME 2. - Pour $j = 0, 2, 4$, on a

$$(27) \quad S(y; \chi_j \delta) = O(y^{3/4} \log y) .$$

3. ESTIMATION $S(y; \chi_j \delta) = O(y^{3/4} \log y)$ ET FIN DE LA DEMONSTRATION.

Il s'agit de démontrer le lemme 2. Pour simplifier, écrivons χ et x au lieu de χ_j et y . On a par définition

$$(28) \quad S(x; \chi \delta) = \sum_{\substack{n \leq x \\ (n, 3) = 1}} \chi(n) \delta(n) .$$

Comme tout entier sans facteur cubique se met de façon unique sous la forme mn^2 , avec m et n sans facteur carré et premiers entre eux,

(28) peut se réécrire (avec pour n une nouvelle signification)

$$(29) \quad S(x; \chi \delta) = \sum_{\substack{mn^2 \leq x \\ (m, n) = 1 \\ (m, 3) = (n, 3) = 1}} \mu^2(m) \mu^2(n) \chi(mn^2) \delta(mn^2) .$$

μ désigne ici la fonction de Möbius, et on a utilisé le fait que μ^2 est égale à la fonction caractéristique des entiers sans facteur carré.

Pour les entiers m, n apparaissant dans cette dernière somme, on a, d'après (2) - (3),

$$(30) \quad \delta(mn^2) = \prod_{p|mn^2} \left(\frac{p}{3}\right) = \prod_{p|m} \left(\frac{p}{3}\right) \prod_{p|n} \left(\frac{p}{3}\right).$$

Pour m et n sans facteur carré, ce dernier produit est égal à $\left(\frac{m}{3}\right)\left(\frac{n}{3}\right) = \lambda(m)\lambda(n)$, λ désignant le caractère de Legendre $\left(\frac{\cdot}{3}\right)$. Les formules (29) et (30) mènent donc à

$$(31) \quad S(x; \chi\delta) = \sum_{\substack{mn^2 \leq x \\ (m,n)=1}} (\mu^2(n) \chi(n^2) \lambda(n)) (\mu^2(m) (\chi\lambda)(m)).$$

Noter que χ et λ étant des caractères modulo 9 et 3, on a $\chi(n) = \lambda(n) = 0$ si $(n, 3) \neq 1$ (et de même pour m), ce qui permet d'abandonner les conditions $(m, 3) = (n, 3) = 1$ dans la sommation double.

Réécrivons maintenant (31) sous la forme

$$(32) \quad S(x; \chi\delta) = \sum_{n \leq x^{1/2}} \mu^2(n) \chi(n^2) \lambda(n) \sum_{\substack{m \leq x/n^2 \\ (m,n)=1}} \mu^2(m) \psi(m),$$

avec $\psi = \chi\lambda =$ un caractère modulo 9 non principal (puisque, dans le dual X de $(\mathbb{Z}/9\mathbb{Z})^*$, λ est évidemment d'ordre 2, et $\chi = \chi_j$ d'ordre 1 pour $j = 0$, et d'ordre 3 pour $j = 2, 4$). Une estimation de la somme $\sum_m \mu^2(m) \psi(m)$ va résulter du lemme suivant :

LEMME 3. - Soient n et k deux entiers ≥ 1 et ψ un caractère de Dirichlet non principal modulo k . Posons

$$(33) \quad T_n(y; \psi) = \sum_{\substack{m \leq y \\ (m,n)=1}} \mu^2(m) \psi(m).$$

On a alors l'estimation

$$(34) \quad T_n(y; \psi) = O\left(y^{1/2} (nk)^{1/2} \log nk\right).$$

Admettons provisoirement ce lemme et appliquons-le à la somme $\sum_m$ de (32), avec $k = 9$ et $y = x/n^2$: on obtient

$$(35) \quad \sum_{\substack{m \leq x/n^2 \\ (m,n)=1}} \mu^2(m) \psi(m) = O\left(x^{1/2} \frac{\log n}{n^{1/2}}\right).$$

Comme $|\mu^2(n) \chi(n^2) \lambda(n)| \leq 1$ pour tout n , la combinaison de (31) et (35) donne alors

$$(36) \quad S(x; \chi\delta) = O\left(x^{1/2} \sum_{n \leq x^{1/2}} \frac{\log n}{n^{1/2}}\right).$$

Enfin, on a évidemment

$$(37) \quad \sum_{n \leq y} \frac{\log n}{n^{1/2}} \leq (\log y) \sum_{n \leq y} \frac{1}{n^{1/2}}$$

et

$$(38) \quad \sum_{n \leq y} \frac{1}{n^{1/2}} = O\left(\int_1^y \frac{dt}{t^{1/2}}\right) = O(y^{1/2}).$$

Faisant $y = x^{1/2}$ dans (37) - (38) et portant le résultat dans (36), on obtient ainsi

$$(39) \quad S(x; \chi\delta) = O(x^{3/4} \log x),$$

ce qui démontre le lemme 2.

Reste à prouver le lemme 3. Posant $k^* = nk$, et notant ψ^* le caractère modulo k^* induit par ψ , on peut écrire

$$(40) \quad T_n(y; \psi) = \sum_{m \leq y} \mu^2(m) \psi^*(m).$$

Un argument classique ([5], p. 53) montre d'autre part que

$$\mu^2(m) = \sum_{d^2 | m} \mu(d) = \sum_{rd^2=m} \mu(d) \text{ et permet de transformer (40) en}$$

$$(41) \quad T_n(y; \psi) = \sum_{rd^2 \leq y} \mu(d) \psi^*(rd^2) = \sum_{d \leq y^{1/2}} \mu(d) \psi^*(d^2) \sum_{r \leq y/d^2} \psi^*(r).$$

L'inégalité de Pólya-Vinogradov ([1], p. 320) appliquée à ψ^* , caractère non principal modulo k^* , donne

$$(42) \quad \sum_{r \leq y/d^2} \psi^*(r) = O(k^{*1/2} \log k^*).$$

Si alors on remplace k^* par nk et si on porte (42) dans (41) en remar-

quant que $|\mu(d)\psi^*(d^2)| \leq 1$ pour tout d , on obtient l'estimation

$$(43) \quad T_n(y; \psi) = O\left(y^{1/2}(nk)^{1/2} \log(nk)\right).$$

Ceci prouve le lemme 3 et achève donc la démonstration du théorème 1.

BIBLIOGRAPHIE

- [1] AYOUB R. - An Introduction to the Analytic Theory of Numbers. A.M.S. Math. Surveys, 10 (1963).
- [2] BIRCH B.J., STEPHENS N.M. - The parity of the rank of the Mordell-Weil group. Topology, 5 (1966), 295-299.
- [3] BIRCH B.J., SWINNERTON-DYER H.P.F. - Notes on elliptic curves II. J. reine angew. Math., 228 (1966), 79-108.
- [4] JOLY J.R. - Equations et variétés algébriques sur un corps fini. Enseign. Math. 19 (1973), 1-117.
- [5] PRACHAR K. - Primzahlverteilung. Springer (1957).
- [6] STEPHENS N.M. - The diophantine equation $X^3 + Y^3 = D$, and the conjectures of Birch and Swinnerton-Dyer. J. reine angew. Math. 231 (1968), 121-162.
- [7] STEPHENS N.M. - A corollary to a conjecture of Birch and Swinnerton-Dyer. J. London Math. Soc., 43 (1968), 146-148.