Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Hervé Moulin

Sur l'équation diophantienne $y^2 = x^3 + k$

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 16, n° 2 (1974-1975), exp. n° G14, p. G1-G8

<http://www.numdam.org/item?id=SDPP_1974-1975__16_2_A13_0>

Séminaire DELANGE-PISOT-POITOU
(Groupe d'étude de Théorie des nombres)
16e année, 1974/75, n° G14, 8 p.

7 avril 1975

SUR L'ÉQUATION DIOPHANTIENNE $y^2 = x^3 + k$

par Hervé MOULIN

(d'après BAKER [3])

Le problème de la représentation d'un nombre entier donné k par la différence d'un carré et d'un cube a intéressé de longue date les mathématiciens. DICKSON relève ce problème dès 1621 dans la littérature ([7], chap. 20).

L'intérêt de cette équation

$$(*) \qquad y^2 = x^3 + k$$

est sans doute qu'elle est "la plus simple des équations diophantiennes difficiles". Bien qu'aucune méthode de résolution systématique de (*) n'ait été trouvée à ce jour, THUE démontra, en 1909, un théorème qui permit à MORDELL, en 1922, de prouver que, pour tout k non nul, l'équation (*) n'a qu'un nombre fini de solutions (cf. THUE [15], MORDELL [11]). Mais cette méthode ne permettait pas un calcul effectif d'une borne de ces solutions : on doit ce calcul à BAKER (cf. BAKER [2]).

1. Méthodes de congruence.

Soit $F(X_1, \ldots, X_n)$ un polynôme à coefficients entiers. Alors, s'il existe des entiers $(x_1, \ldots x_n)$ solutions de $F(x_1, \ldots, x_n) = 0$ la même équation a une solution modulo n (pour tout n). Cette remarque très simple fournit une infinité de conditions nécessaires à l'existence d'une solution. Une autre condition nécessaire est que l'équation ait une solution en nombres réels $(x_1, \ldots, x_n)$.

Le théorème de Hasse-Minkowski (voir par exemple BOREVIČ-SAFAREVIČ [6]) dit que, si F est une forme quadratique, ces conditions sont suffisantes, autrement dit qu'il suffit d'étudier l'équation "modulo p", pour tout p premier, et "dans $\underset{\sim}{R}$". Ce résultat ne s'étend pas aux polynômes de degré 3. De plus, un théorème de Weil (WEIL [16]) montre que l'équation (*) a une solution modulo p pour p premier assez grand (puisque $y^2 - x^3 - k$ est absolument irréductible).

Donc les méthodes de congruence appliquées à (*) permettent seulement de trouver certaines valeurs de k pour lesquelles (*) n'a pas de solution entière. Par exemple, $y^2 = x^3 - 5$ entraîne $x \equiv 1 \pmod 4$, et s'écrit

$$y^2 + 4 = (x - 1)(x^2 + x + 1) .$$

Donc $z = x^2 + x + 1$ est congru à 3 modulo 4 et divise $y^2 + 4$. Or l'étude de l'équation diophantienne $u^2 + v^2 = a$, montre que les nombres qui sont la somme de deux carrés sont les nombres dont tous les facteurs premiers congrus à 3 modulo 4, apparaissent avec une puissance paire. On vérifie que z contient un

facteur premier congru à 3 modulo 4 à une puissance impaire, ce qui prouve que $y^2 = x^3 - 5$ n'a pas de solution entière. (Pour plus de détails sur ces méthodes, cf. MORDELL [12].)

Cette méthode ne donne pas de moyen de résolution de (*). Pour de petites valeurs de k ($|k| \leqslant 100$), l'équation a été complètement résolue (cf. HEMER [8] et ATKIN-BIRCH [1]).

2. Première réduction du problème.

Dans ce paragraphe, nous allons montrer que si on sait majorer le nombre des solutions d'une équation diophantienne $f(x , y) = + 1$, où f est une forme cubique à coefficients entiers, alors on en déduit une majoration du nombre des solutions de (*). Nous suivons pour cela la méthode de BAKER [2]. On suppose démontré le théorème suivant.

THÉORÈME 1. - *Soit $f(X , Y)$ une forme cubique à coefficients entiers irréductible (sur $\mathbb{Q}$) et dont les coefficients sont bornés (en valeur absolue) par A. Alors les solutions en nombres entiers x, y de l'équation $f(x , y) = + 1$, sont en nombre fini.*

On pose $\varphi(A) = \max\{|x| , |y| ; f(x , y) = + 1\}$, où f décrit l'ensemble des formes cubiques irréductibles dont les coefficients sont bornés par A. Le théorème 1 entraîne alors la proposition suivante.

PROPOSITION 1. - *Les solutions en nombres entiers x, y de l'équation*

$$(*) \qquad y^2 = x^3 + k \quad (k \neq 0)$$

sont en nombre fini et vérifient

$$\max(|x| , |y|) \leqslant 10^5 k^2 \max(3.10^{35} |k|^{15} , 2.\varphi(11\sqrt{|k|})) .$$

Soient x, y, k des entiers vérifiant (*). On considère la forme cubique $f(X , Y)$

$$f(X , Y) = X^3 - 3xXY^2 - 2yY^3$$

dont le discriminant $\mathcal{D}$ vaut $-108k$.

(a) *Supposons pour l'instant $k > 0$.* Alors f a une seule racine réelle θ et s'écrit donc

$$(1) \qquad f(X , Y) = (X + \theta Y)(X - \alpha Y)(X - \bar{\alpha} Y) ,$$

où α est un nombre complexe tel que $\mathrm{Im}(\alpha) > 0$. Or le domaine fondamental du groupe modulaire est

$$D = \{z ; \ |\mathrm{Re}(z)| \leqslant \tfrac{1}{2} , \ |z| \geqslant 1\}$$

voir par exemple SERRE [13]) ; autrement dit, il existe des nombres entiers p, q, r, s tels que

$$ps - qr = 1 \ , \ \frac{p\alpha + q}{r\alpha + s} \in D \ .$$

Donc, par le changement de variable

$$\begin{cases} X' = pX + qY \\ Y' = rX + sY \end{cases}$$

la forme (1) devient

$$(2) \qquad f'(X' \ , \ Y') = (X' + \theta' \ Y')(A' \ X'^2 + B' \ X' \ Y' + C' \ Y'^2) \ ,$$

dont l'unique racine complexe de partie imaginaire positive est dans D . Ceci s'exprime :

$$\left| - \frac{B'}{2A'} \right| \leqslant \frac{1}{2} \ ; \quad \left(- \frac{B'}{2A'} \right)^2 + \left(\frac{\sqrt{4A' \ C' - B'^2}}{2A'} \right)^2 \geqslant 1 \ .$$

Il n'y a pas de restriction à supposer $A' \geqslant 0$ et $\theta' \geqslant 0$ (en choisissant éventuellement $ps - qr = -1$). Finalement les coefficients de (2) vérifient :

$$(3) \qquad - A' \leqslant B' \leqslant A' \leqslant C' \ ; \quad \theta' \geqslant 0 \ .$$

Les inégalités (3), jointes à la relation

$$- \mathfrak{D} = (4A' \ C' - B'^2)(A' \ \theta'^2 - B' \ \theta' + C')^2 \ ,$$

permettent aisément de majorer les coefficients de $f'(X' \ , \ Y')$

$$(4) \qquad f'(X' \ , \ Y') = aX'^3 + bX'^2 \ Y' + cX' \ Y'^2 + dY'^3$$

par

$$(5) \qquad \max(|a| \ , \ |b| \ , \ |c| \ , \ |d|) \leqslant \sqrt{|\mathfrak{D}|} \ .$$

(b) Supposons maintenant $k < 0$. Alors f a trois racines réelles et la forme quadratique

$$F(X,Y) = - \frac{1}{4} \ \text{dét}[D^2 \ f] = \frac{1}{4} \left[\left(\frac{\partial^2 f}{\partial X \partial Y} \right)^2 - \left(\frac{\partial^2 f}{\partial X^2} \right) \cdot \left(\frac{\partial^2 f}{\partial Y^2} \right) \right] = 9(xX^2 + 2yXY + x^2 \ Y^2)$$

est définie positive et de discriminant 30). Un argument vu plus haut montre qu'il existe un changement de variable "unimodulaire"

$$\begin{cases} X' = pX + qY \\ Y' = rX + sY \end{cases} \qquad ps - qr = \pm 1 \ , \ p \ , \ q \ , \ r \ , \ s \in \mathbb{Z}$$

qui transforme $F(X \ , \ Y)$ en $F'(X' \ , \ Y')$ tel que

$$(6) \qquad F'(X' \ , \ Y') = A' \ X'^2 + B' \ X' \ Y' + C' \ Y'^2 \ , \quad 0 \leqslant B' \leqslant A' \leqslant C' \ .$$

Mais F est invariant par tout changement de variable de déterminant ± 1 (à coefficients entiers ou non). Autrement dit,

$$(7) \qquad F'(X' \ , \ Y') = \frac{1}{4} \left[\left(\frac{\partial^2 f'}{\partial X' \ \partial Y'} \right)^2 - \left(\frac{\partial^2 f'}{\partial X'^2} \right) \cdot \left(\frac{\partial^2 f'}{\partial^2 \ Y'^2} \right) \right] ,$$

où $f'(X' \ , \ Y')$ est déduite de f par le même changement de variable. Définissant les coefficients de f' comme en (4), la relation (7) donne :

$$A' = b^2 - 3ac \ , \quad B' = bc - 9ad \ , \quad C' = c^2 - 3bd \ ,$$

qui jointe aux inégalités (6) et à

$$4A' C' - B'^2 = 3\mathfrak{Q} > 0 ,$$

permet de montrer aisément la majoration (5).

Nous venons donc de montrer qu'il existe toujours un changement de variable unimodulaire transformant $f(X , Y)$ en $f'(X' , Y')$ dont les coefficients a,b,c,d vérifient (5).

Nous supposons que $f'(X' , Y')$ est irréductible.

Dans la relation

$$f'(pX + qY , rX + sY) = \pm f(X , Y) , \tag{8}$$

l'identification des coefficients de X^3 donne :

$$ap + bp^2 r + cpr^2 + dr^3 = \pm 1$$

qui, d'après le théorème 1 et la relation (5), entraîne

$$\max(|p| , |r|) \leqslant \varphi(\sqrt{|\mathfrak{Q}|}) .$$

Dans la relation

$$f(sX' - qY' , -rX' + pY') = f'(X' , Y') ,$$

on dérive par rapport à X' (resp. Y') , puis on choisit $X' = p$, $Y' = r$. On obtient

$$3s = 3ap^2 + 2bpr + cr^2 \quad (\text{resp. } -3q = bp^2 + 2crp + 3dr^2) .$$

A l'aide de (5) on obtient donc

$$\max(|s| , |q|) \leqslant 2\sqrt{|\mathfrak{Q}|}\, [\varphi(\sqrt{|\mathfrak{Q}|})]^2 .$$

Enfin, dans (8), l'identification des coefficients de XY^2 , puis de Y^3 , permet d'exprimer x , puis y , en fonction de p , q , r , s et a , b , c , d . On obtient ainsi

$$\max(|x| , |y|) \leqslant 2.10^5\, k^2\, \varphi(11\sqrt{|k|}) .$$

Enfin, si f' est réductible, on obtient directement une majoration de $|p|$ et $|r|$ (sans utiliser le théorème 1) :

$$\max(|p| , |r|) \leqslant 6|\mathfrak{Q}|^{5/2} .$$

On termine la démonstration de façon identique, et on obtient

$$\max(|x| , |y|) \leqslant 3.10^{40}.|k|^{17} .$$

Ceci termine la démonstration de la proposition 1.

Remarque. - Un raisonnement analogue (cf. BAKER [3]) permet de déduire une majoration des solutions de l'équation

$$y^2 = ax^3 + bx^2 + cx + d ,$$

d'une majoration des solutions de l'équation

$$f(x , y) = 1 ,$$

où f est une forme irréductible de degré 4 . Donc, si dans notre exemple, on utilise une forme de même degré que l'équation (*), il ne s'agit que d'une coïncidence.

3. La méthode de Skolem.

C'est une première façon de montrer le théorème 1, mais sans obtenir une majoration effective de φ . On considère l'équation

$$f(X , Y) = k . \tag{9}$$

On peut toujours se ramener au cas où le coefficient de X^3 est 1 . Soit α une racine réelle de $f(X , 1)$, et soient σ_1 , σ_2 , σ_3 les trois plongements de $\mathbb{Q}(\alpha)$ dans $\mathbb{C}$ laissant stable $\mathbb{Q}$ ($\sigma_1(\alpha) = \alpha$) . Si $t \in \mathbb{Q}(\alpha)$, alors sa norme $N(t)$ est définie par

$$N(t) = \sigma^1(t)\ \sigma^2(t)\ \sigma^3(t) \in \mathbb{Q} .$$

La norme N est un homomorphisme multiplicatif de $\mathbb{Q}(\alpha)^*$ dans $\mathbb{Q}^*$.

L'équation (9) s'écrit alors

$$N(X - \alpha Y) = \prod_{i=1}^{3} (X - \sigma_i(\alpha)\ Y) = k .$$

Remarquons que, pour X , Y dans $\mathbb{Z}$, $X - \alpha Y$ est un entier de $\mathbb{Q}(\alpha)$ (le coefficient de X^3 étant 1) : ceci nous conduit à étudier les éléments entiers Z de $\mathbb{Q}(\alpha)$ de norme donnée k . Si Z et Z' sont deux tels éléments qui sont en plus congrus dans $\mathbb{O}$ (l'anneau des entiers) modulo k , alors on a :

$$Z - Z' = kT \quad \text{avec} \quad T \in \mathbb{O} .$$

Donc

$$Z/Z' = 1 + N(Z')/Z'\ T.$$

Or Z' est entier, donc $N(Z')/Z'$ aussi (il suffit de remarquer que $N(Z')$ est le terme constant du polynôme caractéristique de Z'). Donc $Z/Z' \in \mathbb{O}$ et de même $Z'/Z \in \mathbb{O}$. Finalement, le quotient Z/Z' est une unité de $\mathbb{Q}(\alpha)$ (un élément inversible de $\mathbb{O}$).

Ainsi, dans une même classe de congruence de $\mathbb{O}$ modulo k , tous les éléments de même norme "diffèrent" d'une unité. Or il n'y a qu'un nombre fini de telles classes (puisque $\mathbb{O}$ est un $\mathbb{Z}$-module de type fini). Par conséquent, s'il existait une infinité de solutions entières (X_i , Y_i) de l'équation (9) ($i \in \mathbb{N}$) , il en existerait un sous-ensemble infini tel que tous les $Z_i = X_i - \alpha Y_i$ correspondants soient dans une même classe de congruence de $\mathbb{O}$ modulo k . Si Z_0 est l'un d'entre eux, tous les autres s'écriraient

$$Z_i = X_i - \alpha Y_i = Z_0\ \varepsilon_i ,$$

où ε_i est une unité de $\mathbb{Q}$.

Or le théorème de Dirichlet montre que, si on suppose par exemple que $f(X , 1)$ a une seule racine réelle, alors les unités de $\mathbb{Q}$ sont toutes les puissances d'une unité fondamentale ε . On aurait donc

$$X_i - \alpha Y_i = Z_0 \varepsilon^i ,$$

où i décrit un sous-ensemble infini de $\underset{\sim}{N}$.

Ecrivons les deux équations "conjuguées" de la précédente

$$X_i - \sigma_2(\alpha)\, Y_i = \sigma_2(Z_0)[\sigma_2(\varepsilon)]^i ,$$
$$X_i - \sigma_3(\alpha)\, Y_i = \sigma_3(Z_0)[\sigma_3(\varepsilon)]^i .$$

En éliminant X_i et Y_i entre ces trois équations, on trouve une relation

$$A\varepsilon^i + B[\sigma_2(\varepsilon)]^i + C[\sigma_3(\varepsilon)]^i = 0 ,$$

où les trois coefficients A , B , C sont non nuls et indépendants de i . Le membre de gauche de cette équation est une fonction de la variable i dont on montre qu'il est possible de la prolonger en une fonction analytique définie sur le corps des nombres p-adiques. Cette fonction analytique est nulle pour une infinité d'entiers naturels et les entiers p-adiques forment un sous-ensemble compact du corps des nombres p-adiques. D'après le théorème d'unicité des fonctions analytiques (cas p-adique), cette fonction est identiquement nulle, d'où une contradiction. Pour plus de détails, voir par exemple BOREVIČ-SAFAREVIČ [6].

Puisqu'on utilise un résultat du type du théorème d'unicité, on ne peut avoir de majoration effective des solutions de l'équation (9).

4. Une méthode effective de résolution.

Cette nouvelle méthode repose sur les minorations de formes linéaires de logarithmes (dues à BAKER). Ces minorations sont à l'origine d'une foule de résultats en théorie des nombres.

(a) Forme ineffective des résultats de BAKER.

Soient $\alpha_1 , \ldots , \alpha_n$ des nombres algébriques tels que $\log(\alpha_1) , \ldots , \log(\alpha_n)$ soient $\mathbb{Q}$-linéairement indépendants. Alors $1 , \log \alpha_1 , \ldots , \log \alpha_n$ sont $\mathbb{Q}$-linéairement indépendants.

Ce résultat est un résultat de transcendance : on en déduit que si α est algébrique non nul e^α est transcendant, donc que π est transcendant (puisque $e^{2i\pi} = 1$) ; on en déduit aussi le théorème de Gel'fond-Schneider : si α est algébrique $(\alpha \neq 0 , 1)$ et si β est algébrique et irrationnel, alors α^β est transcendant. Plus généralement, si $\alpha_1 , \ldots , \alpha_n$ et $\beta_1 , \ldots , \beta_n$ sont des nombres algébriques tels que $1 , \beta_1 , \ldots , \beta_n$ sont linéairement indépendants sur $\mathbb{Q}$,

alors $\alpha_1^{\beta_1}, \ldots, \alpha_n^{\beta_n}$ est transcendant.

(b) Forme effective des résultats de BAKER.

Soit $b \in \overline{\mathbb{Q}}$ un nombre algébrique. On appelle hauteur de b, et on note $h(b)$, le maximum des valeurs absolues des coefficients de son polynôme minimal sur $\mathbb{Z}$.

Soient $\alpha_1, \ldots, \alpha_n$ et $b_1, \ldots, b_n$ des nombres algébriques tels que $\log \alpha_1, \ldots, \log \alpha_n$ soient $\mathbb{Q}$-linéairement indépendants. Alors il existe une constante C positive, effectivement calculable à l'aide de $\alpha_1, \ldots, \alpha_n$, telle que

$$|\Sigma_{i=1}^{n} b_i \log \alpha_i| > C \exp(-(\log H)^{n+1}) \text{ , où } H = \sup_i h(b_i) .$$

Ce résultat est démontré dans l'article de BAKER [4]. Pour notre équation, nous n'utilisons qu'une forme plus faible à l'occasion de laquelle nous allons expliciter la constante. On appelle degré d'un nombre algébrique α le degré de son polynôme minimal. On le note $d(\alpha)$.

Soient $\alpha_1, \ldots, \alpha_n$ des nombres algébriques, et $A = \sup_i(4, h(\alpha_i))$, $d = \sup_i(4, d(\alpha_i))$. Soient $b_1, \ldots, b_n$ des nombres entiers, et $H = \sup_i |b_i|$. Alors on a

$$(0 < |\Sigma_{i=1}^{n} b_i \log \alpha_i| < e^{-H}) \Longrightarrow (H < (4^{n^2} d^{2n} \log A)^{(2n+1)^2}) .$$

Ce résultat est démontré dans l'article de BAKER [5].

La forme effective des résultats de BAKER permet d'améliorer effectivement l'inégalité de Liouville, et aussi (c'est d'ailleurs équivalent, voir MIGNOTTE [10], prop. 1, et LANG [9], p. 671) de majorer effectivement les solutions entières de l'équation $f(x, y) = k$, où f est une forme irréductible de degré supérieur ou égal à 3. On obtient par exemple le théorème 1 et la majoration suivante de φ,

$$\varphi(A) \leqslant \exp(10^{3400} . A^{500}) .$$

Pour voir comment les résultats de BAKER, entraînent cette majoration nous renvoyons à MIGNOTTE [10].

Conclusion. - En appliquant les résultats des §4 et 2, on peut obtenir la majoration suivante (légèrement meilleure que celle de BAKER [2]).

Les solutions entières de $y^2 = x^3 + k$, $(k \neq 0)$ sont majorées par

$$\log \max(|x|, |y|) \leqslant 10^{4000} |k|^{250} .$$

Une version équivalente de ce résultat est la suivante : Pour x et y entiers

$$(y^2 \neq x^3) \Longrightarrow (|y^2 - x^3|^{250} \geqslant 10^{-4000} \log(\max(|x|, |y|))) .$$

Cette dernière relation n'a d'intérêt que pour des nombres tels que

$$\log(\max(|x|, |y|)) > 10^{4000}$$

c'est-à-dire des nombres d'au moins 10^{3999} chiffres !

Remarque. - STARK a récemment montré que, pour tout ε positif, il existait une constante effectivement calculable $C(\varepsilon)$ (mais non calculée) telle que :

$$\log \max(|x| , |y|) < C(\varepsilon)|k|^{1+\varepsilon}$$

(cf. STARK [14]).

BIBLIOGRAPHIE

[1] ATKIN (A. O. L.) and BIRCH (B. J.) [Editors]. - Computers in number theory. Proceedings of the Atlas symposium [2. 1969. Oxford]. - London and New York, Academic Press, 1971.

[2] BAKER (A.). - Contribution to the theory of diophantine equations, Phil. Trans. Royal Soc. London, Series A, t. 263, 1969, p. 173-208.

[3] BAKER (A.). - The diophantine equation $y^2 = ax^3 + bx^2 + cx + d$, J. London math. Soc., t. 43, 1968, p. 1-9.

[4] BAKER (A.). - Linear forms in the logarithm of algebraic numbers, II., Mathematika, London, t. 14, 1967, p. 220-228.

[5] BAKER (A.). - Linear forms in the logarithm of algebraic numbers, IV., Mathematika, London, t. 15, 1968, p. 204-216.

[6] BOREVIČ (Z. I.) and SAFAREVIČ (I. R.). - Number theory. Translated from the russian. - New York, Academic Press, 1966 (Pure and applied Mathematics, Academic Press, 20).

[7] DICKSON (L. E.). - History of the theory of numbers, Vol. 2. - Washington, Carnegie Institution of Washington, 1920.

[8] HEMER (O.). - Notes on the diophantine equation $y^2 - k = x^3$, Arkiv för Mat., t. 3, 1954, p. 67-77.

[9] LANG (S.). - Transcendental numbers and diophantine approximations, Bull. Amer. math. Soc., t. 77, 1971, p. 635-677.

[10] MIGNOTTE (M.). - Amélioration effective du théorème de Liouville, Séminaire Delange-Pisot-Poitou : Théorie des nombres, 15e année, 1973/74, n° G4, 5 p.

[11] MORDELL (L. J.). - Note on the integer solutions of the equation $Ey^2 = Ax^3 + Bx^2 + Cx + D$, Messenger Math., t. 51, 1921, p. 169-171.

[12] MORDELL (L. J.). - Diophantine equations. - London, New York, Academic Press, 1969 (Pure and applied Mathematics, Academic Press, 30).

[13] SERRE (J.-P.). - Cours d'arithmétique. - Paris, Presses Universitaires de France, 1970 (Collection SUP. "Le Mathématicien", 2).

[14] STARK (H. M.). - Effective estimates of solutions of some diophantine equations, Acta Arithm., Warszawa, t. 24, 1973, p. 251-259.

[15] THUE (A.). - Über Annäherungswerte algebraischer Zahlen J. reine und angew. Math., t. 135, 1909, p. 284-305.

[16] WEIL (A.). - Sur les courbes algébriques et les variétés qui s'en déduisent. - Paris, Hermann, 1948 (Act. scient. et Ind., 1041 ; Publ. Inst. Math. Univ. Strasbourg, 7).

(Texte reçu le 28 mars 1975)

Hervé MOULIN
143 boulevard Lefebvre
75015 PARIS