SÉMINAIRE N. BOURBAKI

JEAN-PIERRE SERRE

Travaux de Baker

Séminaire N. Bourbaki, 1971, exp. n° 368, p. 73-86

<http://www.numdam.org/item?id=SB_1969-1970__12__73_0>

© Association des collaborateurs de Nicolas Bourbaki, 1971, tous droits réservés.

L'accès aux archives du séminaire Bourbaki (http://www.bourbaki.ens.fr/) 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/

Séminaire BOURBAKI
22e année, 1969/70, n° 368 Novembre 1969

TRAVAUX DE BAKER

par Jean-Pierre SERRE

§ 1. Théorèmes de transcendance.

1.1. Enoncé des résultats.

On note $\bar{\mathbf{Q}}$ la fermeture algébrique de $\mathbf{Q}$ dans $\mathbf{C}$; c'est l'ensemble des "nombres algébriques". On note L l'ensemble des logarithmes des éléments de $\bar{\mathbf{Q}}^*$, autrement dit l'ensemble des nombres complexes z tels que $\exp(z) \in \bar{\mathbf{Q}}$; c'est un $\mathbf{Q}$-sous-espace vectoriel de $\mathbf{C}$.

Si $\ell \in L$ et si $\alpha = \exp(\ell)$, on se permet d'écrire

$$\ell = \log(\alpha) \quad \text{et} \quad \alpha^z = \exp(\ell z) .$$

THÉORÈME 1 ([2], II).- *Soient $\ell_1,\dots,\ell_n$ des éléments de L qui sont linéairement indépendants sur $\mathbf{Q}$. Alors $\ell_1,\dots,\ell_n$ sont linéairement indépendants sur $\bar{\mathbf{Q}}$.*

(L'injection de L dans $\mathbf{C}$ se prolonge en une application $\bar{\mathbf{Q}}$-linéaire ι de $\bar{\mathbf{Q}} \otimes_{\mathbf{Q}} L$ dans $\mathbf{C}$, et le théorème revient à dire que ι est injective.)

COROLLAIRE.- *Soient $\alpha_1,\dots,\alpha_n$, $\beta_1,\dots,\beta_n$ des nombres algébriques. On suppose que $1,\beta_1,\dots,\beta_n$ sont linéairement indépendants sur $\mathbf{Q}$, et que $\alpha_i \neq 0, 1$ pour tout i. Alors $\alpha_1^{\beta_1} \dots \alpha_n^{\beta_n}$ est transcendant.*

En effet, si $\gamma = \alpha_1^{\beta_1} \dots \alpha_n^{\beta_n}$ était algébrique, l'équation

$$\log(\gamma) = \Sigma\, \beta_i \log(\alpha_i) ,$$

jointe à l'hypothèse faite sur les β_i, entraînerait la nullité des $\log(\alpha_i)$.

Remarques

1) Pour $n = 1$, le corollaire ci-dessus redonne la transcendance de α^β pour α algébrique $\neq 0, 1$ et β algébrique irrationnel (théorème de Gelfond-Schneider).

2) L'analogue p-adique du théorème 1 est vrai, cf. [8]. Cela entraîne, d'après Ax, que le "régulateur p-adique" d'un corps de nombres K est non nul si K est abélien sur $\mathbb{Q}$ ou sur un corps quadratique imaginaire.

3) Les hypothèses étant celles du th. 1, on conjecture que les ℓ_i sont algébriquement indépendants sur $\bar{\mathbb{Q}}$ (ou sur $\mathbb{Q}$ - cela revient au même).

THÉORÈME 2 ([2], III).- Tout élément non nul de $\bar{\mathbb{Q}}.L$ est transcendant.

(En d'autres termes, il n'existe aucune relation linéaire

$$\beta_0 = \beta_1 \ell_1 + \cdots + \beta_n \ell_n$$

avec $\beta_i \in \bar{\mathbb{Q}}$, $\ell_i \in L$ et $\beta_0 \neq 0$.)

COROLLAIRE.- Si $\alpha_1, \ldots, \alpha_n, \beta_0, \beta_1, \ldots, \beta_n$ sont des nombres algébriques non nuls, le nombre $e^{\beta_0} \alpha_1^{\beta_1} \cdots \alpha_n^{\beta_n}$ est transcendant.

Exemples

Si $\alpha \in \bar{\mathbb{Q}}^*$, le nombre $\pi + \log(\alpha)$ est transcendant. En effet, on a $i\pi \in L$ et le th. 1 montre que $\pi + \log(\alpha)$ n'est pas nul ; on applique alors le th. 2.

Un argument analogue montre que l'intégrale

$$\int_0^1 \frac{dt}{1 + t^3} = \frac{1}{3}\left(\log(2) + \frac{\pi}{\sqrt{3}}\right)$$

est un nombre transcendant.

Plus généralement, soit X une courbe algébrique sur $\bar{\mathbb{Q}}$ de genre g et soit ω une forme différentielle sur X. Soit $X(\mathbb{C})$ la "surface de Riemann" de X, et soit

c un chemin différentiable sur $X(\mathbb{C})$. On suppose que les extrémités de c appartiennent à $X(\bar{\mathbb{Q}})$ et que c ne passe par aucun pôle de ω , de sorte que l'intégrale $\int_c \omega$ est définie. Lorsque $g = 0$, les théorèmes 1 et 2 ci-dessus montrent que, en dehors de cas "évidents", le nombre $\int_c \omega$ est transcendant. Il serait très intéressant d'étendre ceci au cas $g \geq 1$; pour $g = 1$ et ω de première ou de seconde espèce, Baker a obtenu des résultats qui doivent paraître dans les Gött. Nach. et l'Amer. J. of Maths.

1.2. Démonstrations.

(On se borne à indiquer le principe de la démonstration du th. 1, sans donner les valeurs explicites des majorations $c_1,\ldots,c_{10}$; le lecteur se reportera à [2] et [3] pour plus de détails.)

Soient $\ell_1,\ldots,\ell_n$ des éléments de L linéairement indépendants sur $\mathbb{Q}$, et supposons qu'il existe des nombres algébriques $\beta_1,\ldots,\beta_{n-1}$ tels que

$$\ell_n = \beta_1\ell_1 + \cdots + \beta_{n-1}\ell_{n-1} .$$

Il s'agit de tirer de là une contradiction.

Posons $\alpha_i = \exp(\ell_i)$; nous supposerons, comme dans [2], I, que les α_i sont multiplicativement indépendants, i.e. qu'un monôme $\alpha_1^{m_1}\ldots\alpha_n^{m_n}$ en les α_i n'est égal à 1 que si les m_i sont nuls. C'est là une hypothèse un peu plus forte que l'indépendance des ℓ_i ; nous reviendrons là-dessus plus loin.

L'idée de Baker (qui est une modification de celle de Gelfond [9], chap. III, §§ 4, 5) consiste à utiliser une fonction de la forme

$$\Phi(z_1,\ldots,z_{n-1}) = \sum_{(\lambda)} p(\lambda)\, \alpha_1^{(\lambda_1+\lambda_n\beta_1)z_1} \cdots \alpha_{n-1}^{(\lambda_{n-1}+\lambda_n\beta_{n-1})z_{n-1}}$$

où $\lambda = (\lambda_1,\dots,\lambda_n)$ appartient à $\mathbb{Z}^n$, avec $0 \le \lambda_i \le c_1$, la constante c_1 étant choisie suffisamment grande. Si $m = (m_1,\dots,m_{n-1})$ est un multi-indice, on note Φ_m la dérivée partielle itérée correspondante de Φ. En tenant compte de l'équation

$$\alpha_n = \alpha_1^{\beta_1} \dots \alpha_{n-1}^{\beta_{n-1}} ,$$

on voit que l'on a

$$\Phi_m(z,\dots,z) = \ell_1^{m_1} \dots \ell_{n-1}^{m_{n-1}} Q(m,z) ,$$

avec

$$Q(m,z) = \sum_{(\lambda)} p(\lambda) \prod_{i=1}^{i=n-1} (\lambda_i + \lambda_n\beta_i)^{m_i} \prod_{i=1}^{i=n} \alpha_i^{\lambda_i z} .$$

On choisit alors les coefficients $p(\lambda)$ de telle sorte que

$$Q(m,\ell) = 0 \qquad \text{pour} \quad |m| \le c_2 \quad \text{et} \quad \ell = 0,1,\dots,c_3$$

où c_2 et c_3 sont des entiers (dépendant de c_1) convenablement choisis. C'est là un problème linéaire homogène, à coefficients algébriques de degré d donné, ayant plus de $2d$ fois d'inconnues que d'équations (si les c_i sont bien choisis) ; de plus, on peut facilement en majorer les coefficients. En vertu d'un lemme fondamental (et élémentaire) de Siegel ([11], vol. I, p. 213) on peut donc choisir pour $p(\lambda)$ des entiers non tous nuls de valeur absolue $\le c_4$.

Ceci fait, le point essentiel de la démonstration consiste à prouver que l'on a

$$Q(m,\ell) = 0 \qquad \text{pour} \quad |m| \le c_5 \quad \text{et} \quad \ell = 0,1,\dots,c_6$$

où c_5 est un peu plus petit que c_2, mais c_6 nettement plus grand que c_3. Pour cela, on remarque que la fonction analytique $\Phi_m(z,\dots,z)$ a beaucoup de zéros (les points $z = \ell$, avec $0 \le \ell \le c_3$) avec des ordres de multiplicité élevés dans le disque $|z| \le c_3$. D'autre part, on peut facilement majorer la valeur absolue de cette fonction dans un disque de rayon c_7 très grand. Si l'on choisit alors c_6 intermédiaire entre c_3 et c_7, une variante du lemme de Schwarz montre que

$|\Phi_m(z,\dots,z)|$ est majoré par $1/c_8$ pour $|z| \leq c_6$. Mais, si ℓ est un entier positif $\leq c_6$, $Q(m,\ell)$ est un nombre algébrique dont on peut facilement estimer le dénominateur ainsi que les valeurs absolues des conjugués. Il en résulte que, si ce nombre n'est pas nul, sa valeur absolue est au moins égale à $1/c_9$ (c'est une variante du principe bien connu : un entier non nul est au moins égal à 1 en valeur absolue). Comme $\Phi_m(\ell,\dots,\ell)$ et $Q(m,\ell)$ sont proportionnels, on en déduit une minoration

$$|\Phi_m(\ell,\dots,\ell)| \geq 1/c_{10} \quad \text{si} \quad \Phi_m(\ell,\dots,\ell) \neq 0 \quad \text{et} \quad 0 \leq \ell \leq c_6 .$$

Or, si $|m| \leq c_5$, on peut s'arranger pour que $c_{10} < c_8$. On a donc bien

$$\Phi_m(\ell,\dots,\ell) = 0 \qquad \text{pour} \quad |m| \leq c_5 \quad \text{et} \quad 0 \leq \ell \leq c_6 .$$

En prenant $m = 0$, on obtient en particulier les relations

$$\sum_{0 \leq \lambda_i \leq c_1} p(\lambda)\ (\alpha_1^{\lambda_1} \dots \alpha_n^{\lambda_n})^{\ell} = 0 \qquad \text{pour} \quad 0 \leq \ell < c_6 .$$

Or, si l'on a bien ajusté les c_i , on peut prendre $c_6 = (c_1 + 1)^n$. Le système d'équations linéaires ci-dessus a alors c_6 inconnues (les $p(\lambda)$) et c_6 équations. Comme il a une solution non triviale, son déterminant est nul. Mais ce déterminant n'est autre que le déterminant de Vandermonde formé à partir des monômes $\alpha_1^{\lambda_1} \dots \alpha_n^{\lambda_n}$, où $0 \leq \lambda_i \leq c_1$; on en conclut que deux de ces monômes doivent être égaux, donc qu'il existe deux familles distinctes $(\lambda_1,\dots,\lambda_n)$ et $(\lambda_1',\dots,\lambda_n')$ telles que

$$\alpha_1^{\lambda_1} \dots \alpha_n^{\lambda_n} = \alpha_1^{\lambda_1'} \dots \alpha_n^{\lambda_n'} .$$

Cela contredit l'indépendance multiplicative des α_i , C.Q.F.D.

Remarques

1) Lorsqu'on ne suppose plus les α_i multiplicativement indépendants, l'argument ci-dessus doit être modifié (cf. [2], II) ; on établit une majoration des coefficients de la série de Taylor de $\Phi(z,\dots,z)$ et l'on obtient une contradiction en

utilisant le déterminant de Vandermonde formé à partir des $\lambda_1\ell_1 + \ldots + \lambda_n\ell_n$.

2) La démonstration du th. 2 est analogue à celle du th. 1 : on suppose que l'on a une relation

$$\log(\alpha_n) = \beta_o + \beta_1 \log(\alpha_1) + \ldots + \beta_{n-1} \log(\alpha_n) ,$$

où les α_i et β_i sont algébriques, et $\beta_o \neq 0$, et l'on utilise la fonction

$$\Phi(z_o,\ldots,z_{n-1}) = \sum_{(\lambda)} p(\lambda) z_o^{\lambda_o} e^{\lambda_n\beta_o z_o} \alpha_1^{(\lambda_1+\lambda_n\beta_1)z_1} \ldots \alpha_{n-1}^{(\lambda_{n-1}+\lambda_n\beta_{n-1})z_{n-1}} ,$$

cf. [2], III.

§ 2. Minorations et majorations effectives.

2.1. Formes linéaires en logarithmes.

Soit $x \in \bar{\mathbb{Q}}$; parmi les équations non triviales

$$a_o x^d + \ldots + a_d = 0 \qquad (a_i \in \mathbb{Z})$$

vérifiées par x , il en existe une et une seule (au changement de signe près) qui est de degré minimum et dont les coefficients a_i sont premiers entre eux. L'entier $\sup|a_i|$ est alors appelé la hauteur de x , et noté $h(x)$.

THÉORÈME 1' ([2], III).- Soient n et d des entiers ≥ 1 , soit k un nombre réel $> n$ et soient $\ell_1,\ldots,\ell_n$ des éléments de L , non tous nuls. Il existe alors une constante

$$C = C(n,\ell_1,\ldots,\ell_n,k,d) > 0$$

ayant la propriété suivante :

Si $\beta_1,\ldots,\beta_n$ sont des nombres algébriques non nuls, de degré $\leq d$, et sont linéairement indépendants sur $\mathbb{Q}$ (ou si les ℓ_i sont linéairement indépendants sur $\mathbb{Q}$), on a :

(*) $\quad |\beta_1 \ell_1 + \ldots + \beta_n \ell_n| > C.\exp(-(\log H)^k)$, où $H = \sup.h(\beta_i)$.

De plus (c'est un point essentiel), la constante C est effectivement calculable en fonction de $n, k, d, \ell_1, \ldots, \ell_n$.

L'inégalité (*) entraîne en particulier que $\beta_1 \ell_1 + \ldots + \beta_n \ell_n$ est $\neq 0$; le th. 1' est donc une amélioration "quantitative" du th. 1. Sa démonstration (cf. [2], I, II, III) est très voisine de celle du th. 1. On suppose que l'on a

$$|\ell_n - (\beta_1 \ell_1 + \ldots + \beta_{n-1} \ell_{n-1})| \leq \varepsilon_1 ,$$

avec ε_1 très petit, et l'on doit tirer de là une contradiction. On introduit la même fonction Φ qu'au n° 1.3, et l'on impose ici encore les conditions

$$Q(m,\ell) = 0 \qquad \text{pour } |m| \leq c_2 \text{ et } \ell = 0, 1, \ldots, c_3 ;$$

le point essentiel consiste à montrer que l'on a

$$Q(m,\ell) = 0 \qquad \text{pour } |m| \leq c_5 \text{ et } \ell = 0, 1, \ldots, c_6 .$$

Pour cela, on considère la fonction $\Phi_m(z,\ldots,z)$ et l'on utilise le fait que $\Phi_m(\ell,\ldots,\ell)$ est très voisin de $\ell_1^{m_1} \ldots \ell_{n-1}^{m_{n-1}} Q(m,\ell)$, donc très petit. Le lemme de Schwarz ne s'applique plus, mais Baker le remplace par une intégrale convenable. La fin de la démonstration est essentiellement la même.

Remarque. Le théorème ci-dessus avait été conjecturé par Gelfond, qui en avait démontré le cas particulier $n = 2$ (cf. [9], chap. III) et avait mis en évidence l'intérêt du cas général.

Le th. 2 a également une forme quantitative :

THÉORÈME 2' ([2], III).- Soient $n, d \geq 1$, soit $k > n+1$ et soient $\ell_1, \ldots, \ell_n$ des éléments de L . Il existe une constante $C' > 0$ telle que, si $\beta_0, \ldots, \beta_n$ sont des nombres algébriques de degré $\leq d$, avec $\beta_0 \neq 0$, on ait :

(**) $\quad |\beta_0 + \beta_1 \ell_1 + \ldots + \beta_n \ell_n| > C'.\exp(-(\log H)^k)$, où $H = \sup.h(\beta_i)$.

(Ici encore, la constante C' est effectivement calculable en fonction de $n, k, d, \ell_1, \ldots, \ell_n$.)

On trouvera diverses variantes des ths. 1' et 2' dans [2], IV, dans [3], ainsi que dans des articles récents de N. Feldman, V. Sprindžuk, A. Vinogradov parus aux Doklady, Mat. Zam. et Mat. Sbornik.

2.2. Approximation des nombres algébriques par des nombres rationnels.

Soit α un nombre algébrique de degré $d \geq 3$. Comme l'a remarqué Liouville, il existe une constante $c > 0$, facile à expliciter, telle que

$$|\alpha - \frac{p}{q}| \geq \frac{c}{q^d} \qquad \text{pour } p, q \in \mathbb{Z},\ q \geq 1 .$$

Autrement dit, on ne peut pas approcher α par un nombre rationnel p/q avec une approximation sensiblement meilleure que $1/q^d$.

On sait que ce résultat a été amélioré successivement par Thue, Siegel, Dyson, Roth ; l'énoncé le plus fort, celui de Roth, affirme que

$$|\alpha - \frac{p}{q}| \geq \frac{c(\varepsilon)}{q^{2+\varepsilon}} \qquad \text{pour tout } \varepsilon > 0 .$$

Toutefois, la démonstration de Roth (comme celles de ses prédécesseurs) ne donne aucun moyen de calculer $c(\varepsilon)$, pour α et ε donnés ; elle ne fournit qu'un théorème d'existence.

On doit à Baker la première amélioration effective du théorème de Liouville :

THÉORÈME 3 ([3], I).- Soit α un nombre algébrique de degré $d \geq 3$ et soit $k > d + 1$. Il existe une constante $c = c(\alpha, k) > 0$, effectivement calculable, telle que

$$|\alpha - \frac{p}{q}| \geq c\, q^{-d}\, e^{(\log q)^{1/k}} \qquad \text{pour } p, q \in \mathbb{Z},\ q \geq 1 .$$

Remarques

1) Le th. 3 améliore le théorème de Liouville "seulement" par un facteur $e^{(\log q)^{1/k}}$; à part son côté "effectif", il est moins bon que le théorème de Roth (ou même que celui de Thue).

2) Pour certains α , Baker a obtenu de meilleures estimations, grâce à une méthode toute différente. Ainsi (cf. [1]) :

$$|\sqrt[3]{2} - \frac{p}{q}| > \frac{10^{-6}}{q^{2,955}} \qquad \text{et} \qquad |\sqrt[3]{17} - \frac{p}{q}| > \frac{10^{-9}}{q^{2,4}} \ .$$

Démonstration du théorème 3.

Elle est basée sur une variante du th. 1'. Indiquons-en brièvement le principe (déjà utilisé par Gelfond [9], fin du chap. III, dans le cas où $d = 3$ et où l'un des conjugués de α n'est pas réel).

On peut supposer α entier. Soient $\alpha_1,\dots,\alpha_d$ ses conjugués, avec $\alpha_1 = \alpha$, et posons

$$m = |(q\alpha_1 - p)\dots(q\alpha_d - p)| \ .$$

C'est un entier ≥ 1 , et tout revient à montrer qu'il ne peut pas être trop petit (par rapport à q), i.e. que l'on ne peut pas avoir

$$|m| < c' \, e^{(\log q)^{1/k}} \ .$$

Supposons que ce soit le cas. On montre sans difficulté que l'idéal engendré par $p\alpha - q$ admet un générateur γ dont les conjugués γ_i sont "assez petits" en valeur absolue (de l'ordre de $|m|^{1/d}$). On a donc

$$p\alpha - q = \gamma\varepsilon \ , \qquad \text{où } \varepsilon \text{ est une unité.}$$

De plus, si $\varepsilon(1),\dots,\varepsilon(r)$ est un système fondamental d'unités du corps $\mathbb{Q}(\alpha)$, on peut supposer que l'on a

$$\varepsilon = \varepsilon(1)^{n_1} \dots \varepsilon(r)^{n_r} \ , \quad \text{avec } n_i \in \mathbb{Z} \ .$$

Comme $d \geq 3$, on peut appliquer ceci à trois conjugués de α :

$$p\alpha_1 - q = \gamma_1 \varepsilon_1$$
$$p\alpha_2 - q = \gamma_2 \varepsilon_2$$
$$p\alpha_3 - q = \gamma_3 \varepsilon_3 \quad .$$

Par hypothèse, $p\alpha_1 - q$ est "petit" ; l'un au moins de $p\alpha_i - q$ doit donc être "grand" ; c'est celui que l'on appelle $p\alpha_3 - q$. Eliminons maintenant p et q des trois équations linéaires ci-dessus. On obtient une relation de la forme

$$A_1 \varepsilon_1 + A_2 \varepsilon_2 + A_3 \varepsilon_3 = 0 ,$$

où les rapports mutuels des A_i sont assez petits en valeur absolue. Mais ε_1 est "petit" et ε_3 est "grand". En divisant par ε_2 , on voit que $A_2 + A_3 \varepsilon_3/\varepsilon_2$ est "petit", i.e. que $\log(\varepsilon_3/\varepsilon_2)$ est très voisin de $\log(-A_2/A_3)$. Or, si l'on pose $\eta_i = \varepsilon(i)_3/\varepsilon(i)_2$, on a

$$\log(\varepsilon_3/\varepsilon_2) = n_1 \log(\eta_1) + \ldots + n_r \log(\eta_r) .$$

On obtient ainsi une valeur "très petite" de la forme linéaire

$$n_1 \log(\eta_1) + \ldots + n_r \log(\eta_r) - \log(-A_2/A_3) ;$$

comme on peut en outre majorer explicitement les n_i , on en déduit une inégalité dont on peut montrer qu'elle contredit une variante du th. 1' ([3], I, th. 3).

2.3. Majorations des solutions entières de certaines équations.

a) Equations $f(X,Y) = m$.

Soit $f(X,Y) = \sum_{i=0}^{i=d} a_i X^i Y^{d-i}$ un polynôme homogène de degré $d \geq 3$, irréductible sur $\mathbb{Q}$, et à coefficients entiers. On peut écrire

$$f(X,Y) = a_o \prod_{i=1}^{i=d} (Y - \alpha_i X) ,$$

où les α_i sont les conjugués d'un nombre algébrique α de degré d . Les théorèmes

d'approximation de α par des nombres rationnels se traduisent ainsi en des théorèmes sur les solutions entières de l'équation $f(X,Y) = m$ où m est un entier donné ; c'est par ce procédé que Thue avait démontré qu'une telle équation n'a qu'un nombre fini de solutions (mais sans pouvoir majorer celles-ci). Le th. 3 entraîne immédiatement :

THÉORÈME 4 ([3], II).- Soit $k > d + 1$. Il existe une constante

$$c = c(k, d, a_0, \ldots, a_d) > 0 ,$$

effectivement calculable, telle que, si $f(x,y) = m$, avec $x, y \in \mathbb{Z}$, et $m \geq 1$, on ait

$$\sup(|x|, |y|) \leq c.\exp(\log(m)^k) .$$

(Si $H = \sup(|a_i|)$ et si $r = 32dk^2/(k-d-1)$, on peut prendre $c = \exp(d^{r^2} H^{rd^3})$, cf. [3], II, th. 2.)

b) L'équation $Y^2 - X^3 = D$.

De nombreux cas particuliers de cette équation ont été étudiés depuis le dix-septième siècle (cf. [10], chap. 26). Baker démontre :

THÉORÈME 5 ([3], II).- Si $x, y \in \mathbb{Z}$ sont tels que $y^2 = x^3 + D$, avec $D \neq 0$, on a

$$\sup(|x|, |y|) < \exp(10^{10}|D|^{10^4}) .$$

Autrement dit, si $x^3 \neq y^2$, on a :

$$|x^3 - y^2| > 10^{-10}(\log(x))^{10^{-4}} , \qquad \text{pour tout } x \geq 1 .$$

(Noter que cette minoration n'est intéressante que si le nombre de chiffres de x^3 dépasse 10^{100000} , i.e. si x n'est pas "trop petit" ...)

Ainsi, pour D donné, l'équation $y^2 - x^3 = D$ peut être résolue par un calcul fini, bien qu'un peu long. Il est d'ailleurs certain que les bornes données par Baker peuvent être améliorées. Un premier pas dans cette voie vient d'être fait par Siegel [12].

Démonstration du th. 5.

Elle utilise une méthode de Mordell. Si $y^2 - x^3 = D$, on considère la forme cubique $f(X,Y) = X^3 - 3xXY^2 - 2yY^3$, dont le discriminant Δ est égal à $-108\,D$. La théorie de la réduction, due à Hermite, montre qu'il existe une forme cubique

$$g(X,Y) = a_0X^3 + \ldots + a_3Y^3 \quad , \qquad \text{avec } |a_i| \leq |\Delta|^{\frac{1}{2}} ,$$

et une matrice $s = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ telles que $s(g) = f$. En écrivant que le coefficient de X^3 (resp. X^2Y) dans $s(g)$ est égal à 1 (resp. à 0), on obtient des équations que doivent vérifier les coefficients a, b, c, d de s ; en utilisant le théorème 4, on en déduit des majorations de ces coefficients en fonction de $|\Delta|$; d'où une majoration pour $\sup(|x|, |y|)$, qui est celle du théorème 5.

c) Autres équations.

Dans [4] et [5], Baker donne des bornes explicites pour les solutions entières d'équations de la forme

$$y^m = a_0x^n + \ldots + a_n \quad , \qquad a_i \in \mathbb{Z} \ , \ a_0 \neq 0 \ ,$$

en fonction de $H = \sup(|a_i|)$. Les résultats sont les suivants :

- Si $m = 2$, $n = 3$, et si le polynôme $a_0X^3 + \ldots + a_3$ a trois racines distinctes, on a

$$\sup(|x|, |y|) < \exp((10^6H)^{10^6}) .$$

- Si $m, n \geq 3$, et si le polynôme $a_0X^n + \ldots + a_n$ a au moins deux racines simples, on a

$$\sup(|x|, |y|) < \exp(\exp((5m)^{10}(n^{10n}H)^{n^2})) .$$

- Si $m = 2$, et si le polynôme $a_0X^n + \ldots + a_n$ a au moins trois racines simples, on a

$$\sup(|x|, |y|) < \exp(\exp(\exp((n^{10n}H)^{n^2}))) .$$

Plus généralement, on peut espérer que ces méthodes permettront de rendre effectif le théorème de Siegel disant qu'une courbe de genre ≥ 1 n'a qu'un nombre fini de points à coordonnées entières ; le cas du genre 1 vient d'être traité par Baker et Coates [7].

2.4. Nombres de classes des corps quadratiques imaginaires.

Si d est un entier ≥ 1, sans facteur carré, notons $h(d)$ le nombre de classes du corps $\mathbb{Q}(\sqrt{-d})$. D'après un théorème de Heilbronn, $h(d)$ tend vers l'infini avec d ; ce résultat a été ensuite précisé et généralisé par Siegel et R. Brauer. Cependant, aucun de ces auteurs n'obtient une minoration effective de $h(d)$ et par suite on n'a aucun moyen de déterminer les valeurs de d pour lesquelles $h(d)$ est un entier m donné. C'est ainsi que le cas $m = 1$ n'a été résolu que tout récemment par Stark. Le cas $m = 2$ n'est pas encore tranché ; toutefois Baker a obtenu le résultat suivant :

THÉORÈME 6 ([6]).- *Soit d un entier ≥ 1, sans facteur carré, tel que $d \not\equiv 3 \pmod 8$. Si $h(d) = 2$, on a $d \leq 10^{500}$.*

Remarques

1) En fait, les seules valeurs de d vérifiant ces conditions sont

$$5, 6, 10, 13, 15, 22, 37, 58 ;$$

elles correspondent aux discriminants

$$-20, -24, -40, -52, -15, -88, -148, -232 .$$

Cela vient d'être démontré par P. Weinberger (thèse, Berkeley, 1969) par une méthode analogue à celle suivie par Stark pour $h(d) = 1$. En principe, cela pourrait aussi se déduire du théorème précédent et d'une vérification "finie".

2) Pour $d \equiv 3 \pmod 8$ et $h(d) = 2$, on n'a que des résultats partiels (C. J. Moreno, N.Y.U.).

BIBLIOGRAPHIE

[1] A. BAKER - Rational approximations to $\sqrt[3]{2}$ and other algebraic numbers, Quart. J. of Maths., 15 (1964), p. 375-383.

[2] A. BAKER - Linear forms in the logarithms of algebraic numbers, Mathematika, 13 (1966), p. 204-216 ; II, id., 14 (1967), p. 102-107 ; III, id., 14 (1967), p. 220-228 ; IV, id., 15 (1968), p. 204-216.

[3] A. BAKER - Contributions to the theory of Diophantine equations, Phil. Trans. Roy. Soc. London, 263 (1968), p. 173-208.

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

[5] A. BAKER - Bounds for the solutions of the hyperelliptic equation, Proc. Camb. Phil. Soc., 65 (1969), p. 439-444.

[6] A. BAKER - A remark on the class number of quadratic fields, Bull. London Math. Soc., 1 (1969), p. 98-102.

[7] A. BAKER and J. COATES - Integer points on curves of genus 1 , Proc. Camb. Phil. Soc., à paraître.

[8] A. BRUMER - On the units of algebraic number fields, Mathematika, 14 (1967), p. 121-124.

[9] A. O. GELFOND - Nombres transcendants et algébriques [en russe], Moscou, 1952 [traduction anglaise : Dover Publ., New York, 1960].

[10] L. J. MORDELL - Diophantine equations, Acad. Press, New York, 1969.

[11] C. L. SIEGEL - Gesammelte Abhandlungen, Springer-Verlag, Berlin, 1966.

[12] C. L. SIEGEL - Abschätzung von Einheiten, Gött. Nach., 1969, n° 9, p. 71-86.