

THEORIE DES NOMBRES

Année 1978 - 1979

BESANCON

APPLICATIONS DE LA THEORIE DE KUMMER A DES
PROBLEMES DIOPHANTIENS

Michel WALDSCHMIDT

APPLICATIONS DE LA THEORIE DE KUMMER

A DES PROBLEMES DIOPHANTIENS

par

Michel WALDSCHMIDT

Les méthodes actuelles de détermination des points entiers sur une courbe de genre ≥ 1 ramènent cette recherche à un problème de transcendance : soit au théorème de Thue - Siegel - Roth (méthode de Siegel), soit à une minoration de formes linéaires de logarithmes usuels (méthode de Gel'fond - Baker), soit à une minoration de formes linéaires de logarithmes elliptiques (méthode de Lang - Masser). Ces deux dernières méthodes utilisent la théorie de Kummer.

§ 1 - Géométrie diophantienne

Soit $f \in \mathbb{Z}[X, Y]$ un polynôme irréductible tel que la courbe $f(x, y) = 0$ ait un genre ≥ 1 . En 1929, C.L. Siegel a démontré qu'il n'y a qu'un nombre fini de points entiers $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ sur une telle courbe. Sa démonstration utilise le théorème de Thue - Siegel - Roth ; elle permet de majorer le nombre de solutions dans $\mathbb{Z} \times \mathbb{Z}$ de l'équation $f(x, y) = 0$, mais ne permet pas de majorer les solutions elles-mêmes, c'est-à-dire de majorer $\max(|x|, |y|)$. Elle n'est donc pas effective.

Avant de nous limiter au genre 1, mentionnons la conjecture de Mordell : sur une courbe de genre ≥ 2 , il n'y a qu'un nombre fini de points rationnels. L'exemple de la courbe de Fermat $x^n + y^n - 1 = 0$ pour $n \geq 5$ montre la difficulté de cette conjecture.

Sur une courbe de genre 1 définie sur \mathbb{Q} les points rationnels forment un groupe abélien de type fini (théorème de Mordell, généralisé par Weil aux variétés abéliennes sur un corps de nombres). Il n'y a pas pour l'instant d'algorithme général pour déterminer une base du groupe de Mordell - Weil (modulo la torsion), mais la conjecture de Birch et Swinnerton - Dyer contient une majoration de la hauteur des points d'une base.

La détermination effective des points entiers sur une courbe de genre 1 a été obtenue en 1970 par Baker et Coates : si $f \in \mathbb{Z}[X, Y]$ est un polynôme irréductible sur le corps $\bar{\mathbb{Q}}$ des nombres algébriques, tel que la courbe $f(x, y) = 0$ ait un genre égal à 1, et si $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ satisfait $f(x, y) = 0$, alors

$$\max \{ |x|, |y| \} \leq \exp \exp \exp \{ (2H)^{10n^{10}} \}$$

où n est le degré de f et H sa hauteur (maximum des valeurs absolues des coefficients). En utilisant une construction explicite, due à J. Coates, d'une fonction rationnelle sur la courbe ayant des zéros et des pôles donnés (l'existence d'une telle fonction étant assurée par le théorème de Riemann - Roch), on se ramène à une courbe

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

auquel cas on dispose d'une majoration plus fine, due à Baker (1968) :

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

Dans le cas plus particulier de la courbe $y^2 = x^3 + k$, ($k \in \mathbb{Z}$, $k \neq 0$), H. M. Stark (1973) a démontré

$$\max \{ |x|, |y| \} < \exp (C_\epsilon |k|^{1+\epsilon})$$

où $C_\epsilon > 0$ est effectivement calculable en fonction de $\epsilon > 0$.

Les démonstrations se font en trois étapes. D'abord une méthode due à Siegel permet de ramener le problème à une équation $au + a'u' = 1$, où les coefficients a, a' sont dans un corps de nombres K , et les inconnues u, u' sont des unités de K . Voici schématiquement comment procède Siegel : écrivons

$$y^2 = a(x - e_1)(x - e_2)(x - e_3),$$

où e_1, e_2, e_3 appartiennent à un corps de nombres K_1 . En écrivant la décomposition en idéaux dans K_1 , on obtient pour $i = 1, 2, 3$

$$x - e_i = (z_i t_i)^2,$$

où t_1, t_2, t_3 appartiennent à un sous-ensemble fini connu d'un corps de nombres K_2 (extension finie de K_1), et z_1, z_2, z_3 appartiennent à K_2 .

Des équations

$$e_i - e_j = (z_i t_i - z_j t_j)(z_i t_i + z_j t_j), \quad 1 \leq i < j \leq 3,$$

on déduit

$$z_1 t_1 - z_2 t_2 = \beta_3 u_3$$

$$z_2 t_2 - z_3 t_3 = \beta_1 u_1$$

$$z_3 t_3 - z_1 t_1 = \beta_2 u_2,$$

où $\beta_1, \beta_2, \beta_3$ appartiennent à un sous-ensemble fini connu de K_2 , et u_1, u_2, u_3 sont des unités de K_2 . En divisant par $-\beta_3 u_3$ l'égalité $\beta_1 u_1 + \beta_2 u_2 + \beta_3 u_3 = 0$, on obtient l'équation $au + a'u' = 1$.

La deuxième étape a été décrite par Gell'fond. Considérons un système fondamental $\epsilon_1, \dots, \epsilon_r$ d'unités de K . On écrit les inconnues u, u' dans cette base :

$$u = \epsilon_1^{h_1} \dots \epsilon_r^{h_r} \zeta, \quad u' = \epsilon_1^{h'_1} \dots \epsilon_r^{h'_r} \zeta'.$$

On considère un plongement de K dans \mathbb{C} tel que $|u|$ soit le maximum des valeurs absolues des conjugués de u . Soit $H = \max \{|h_1|, \dots, |h_r|\}$. En considérant le plongement logarithmique du groupe des unités de K et en écrivant que deux normes sur un espace de dimension finie sont équivalentes, on obtient une constante $C_1 = C_1(K) > 0$ telle que

$$H \leq C_1 \log |u|.$$

De la propriété suivante de la détermination principale du logarithme :

$$|\log(1+z)| \leq \frac{3}{2} |z| \quad \text{pour } |z| \leq \frac{1}{3}$$

avec $z = -1 - \frac{a'u'}{au}$ on déduit

$$0 < \left| (h_1 - h_1') \log \epsilon_1 + \dots + (h_r - h_r') \log \epsilon_r + \log \zeta'' - \log \frac{a'}{a} \right| \leq \frac{1}{|a|} e^{-C_1^{-1} H}.$$

Ecrivons cette double inégalité sous la forme

$$0 < |b_1 \log \alpha_1 + \dots + b_n \log \alpha_n| \leq C_2^{-B},$$

où b_1, \dots, b_n sont des entiers rationnels, $\alpha_1, \dots, \alpha_n$ des éléments de K^* (l'un d'eux étant -1 , et son logarithme est $i\pi$), $B = \max(|b_1|, \dots, |b_n|)$, et C_2 ne dépend que de $K, n, \alpha_1, \dots, \alpha_n$. Il suffit que l'on minore la forme linéaire de logarithmes par $e^{-g(B)}$ pour en déduire une majoration de B (ce qui conduit à la finitude du nombre de solutions de l'équation $au + a'u' = 1$, et par voie de conséquence à la finitude du nombre de solutions de l'équation initiale $y^2 = ax^3 + bx^2 + cx + d$).

Gelfond savait minorer de manière effective une forme linéaire en 2 logarithmes, mais pour n logarithmes il n'avait qu'une minoration non effective, qui reposait sur le théorème de Thue-Siegel-Roth. Notons que l'inégalité de Liouville

$$|b_1 \log \alpha_1 + \dots + b_n \log \alpha_n| > 2^{-n-1} \exp \left\{ - \sum_{j=1}^n |b_j| \log A_j \right\}$$

où

$$A_j = H_K(\alpha_j) = \prod_v \max \{ 1, |\alpha_j|_v^{n_v} \}$$

(v décrivant les valeurs absolues de K et n_v étant le degré local en v) n'est pas suffisante.

La troisième étape de la démonstration (minoration non triviale d'une forme linéaire de logarithmes) a été accomplie par Baker en 1966. Sa minoration a été raffinée par de nombreux auteurs. En ce qui concerne la dépendance en $B = \max \{|b_1|, \dots, |b_n|\}$, le meilleur résultat possible a été obtenu par N. I. Feldman dès 1968 :

$$|b_1 \log \alpha_1 + \dots + b_n \log \alpha_n| > B^{-C_3},$$

où C_3 est un nombre positif qui peut être explicité en fonction de

$\log \alpha_1, \dots, \log \alpha_n$ et n .

Une autre voie pour l'étude des points entiers sur les courbes elliptiques a été décrite par S. Lang en 1964. Elle consiste à travailler directement sur une fonction elliptique \wp (dans un modèle de Weierstrass) de manière analogue à ce que faisait Gel'fond sur le groupe multiplicatif. Au lieu d'utiliser le théorème de Minkowski sur les unités, on écrit les points dans une base du groupe de Mordell - Weil. On arrive à une forme linéaire

$$\Lambda = b_1 u_1 + \dots + b_n u_n$$

où b_1, \dots, b_n sont des entiers rationnels et les nombres $\wp(u_1), \dots, \wp(u_n)$ sont algébriques. En écrivant que la fonction \wp a un pôle double à l'origine, et en utilisant la quadraticité de la hauteur de Néron Tate, on trouve une période ω de \wp telle que $\Lambda' = \Lambda - \omega$ vérifie

$$0 < |\Lambda'| < C_4^{-1} B^2.$$

Il suffit de minorer $|\Lambda|$ par $e^{-g(B^2)}$ pour conclure. Pour $n = 2$ une minoration effective a été obtenue par N. I. Feldman en 1968. Pour $n \geq 2$ une minoration non effective a été obtenue par J. Coates à partir du théorème de Thue - Siegel - Roth (analogue elliptique d'un résultat de Gel'fond). L'inégalité de Liouville donne seulement

$$|\Lambda'| > C_5^{-1} B^2,$$

où C_5 est facilement calculable en fonction de $g_2, g_3, \wp(u_1), \dots, \wp(u_n)$ et n . En 1975, D. W. Masser a traité de manière effective le cas $n \geq 2$ en supposant que \wp admet des multiplications complexes. (Le cas où \wp n'a pas de multiplication complexe n'est toujours pas résolu ; c'est un des problèmes ouverts les plus importants de la théorie). La minoration de Masser

$$|\Lambda'| > C_6(\epsilon)^{-1} B^\epsilon$$

a été raffinée par Coates et Lang en

$$|\Lambda'| > \exp \{ - (\log B)^{C_7} \},$$

grâce au théorème de Bashmakov, puis par Anderson :

$$|\Lambda'| > \exp \{ -C_8(\epsilon)(\log B)(\log \log B)^{n+1+\epsilon} \}.$$

On espère arriver à

$$|\Lambda'| > B^{-C_9},$$

ce qui serait le meilleur résultat possible.

Pour appliquer ces minoration à la détermination des points entiers sur la courbe elliptique, il faut connaître une base du groupe de Mordell Weil. Une solution consiste à supposer que la conjecture de Birch et Swinnerton-Dyer est vérifiée. Il faut ensuite dans les minoration préciser la dépendance en $\wp(u_1), \dots, \wp(u_n)$, mais aussi en g_2 et g_3 . Cela a été fait par H. Groscot qui en déduit par exemple que si k est une puissance d'un nombre premier et $y^2 = x^3 + k$ avec $(x, y) \in \mathbb{Z} \times \mathbb{Z}$, alors

$$\max \{ |x|, |y| \} < \exp \{ C_e |k|^{\frac{1}{2}+\epsilon} \},$$

ce qui améliore dans ce cas l'énoncé de Stark, mais suppose vérifiée la conjecture de Birch et Swinnerton-Dyer. D'autres résultats dans cette direction ont été annoncés sans démonstration par G. V. Chudnovsky.

Il semble qu'à long terme, cette méthode de Lang porte plus d'espérance que la méthode de Gel'fond.

Toutes les démonstrations récentes de minoration de formes linéaires de logarithmes (usuels ou elliptiques) font usage de la théorie de Kummer. Les méthodes transcendantes font intervenir une fonction auxiliaire

$$F(z) = P(\alpha_1^z, \dots, \alpha_n^z)$$

pour le cas multiplicatif, et

$$F(z) = P(\wp(u_1 z), \dots, \wp(u_n z))$$

pour le cas elliptique, où $P \in \mathbb{Z}[X_1, \dots, X_n]$ est un polynôme non nul à coefficients dans \mathbb{Z} . Les nombres $\alpha_1, \dots, \alpha_n$ (resp. $\wp(u_1), \dots, \wp(u_n)$ et g_2, g_3) sont dans un corps de nombres K . Sachant que F n'est pas la fonction nulle, on voudrait trouver un point où elle ne s'annule pas.

L'idée, due à J. Coates, consiste à chercher ce point sous la forme $1/\ell$, où ℓ est un nombre premier suffisamment grand. Il suffit pour cela de minorer le degré sur K du corps

$$K(\alpha_1^{1/\ell}, \dots, \alpha_n^{1/\ell}),$$

respectivement

$$K\left(\wp\left(\frac{u_1}{\ell}\right), \dots, \wp\left(\frac{u_n}{\ell}\right)\right).$$

La méthode de Kummer usuelle résout le cas multiplicatif,

Lemme 1. Soient $\log \alpha_1, \dots, \log \alpha_r$ des logarithmes \mathbb{Q} -linéairement indépendants de nombres algébriques. Il existe un entier positif L_0 tel que si $P \in \mathbb{Z}[X_1, \dots, X_r]$ est un polynôme non nul de degré au plus L en X_i , $(1 \leq i \leq r)$, avec $L \geq L_0$, alors pour tout nombre pre- mier $\ell > L$ on a

$$P(\alpha_1^{1/\ell}, \dots, \alpha_r^{1/\ell}) \neq 0$$

où $\alpha_j^{1/\ell} = \exp\left(\frac{1}{\ell} \log \alpha_j\right)$, $(1 \leq j \leq r)$.

Dans le cas elliptique, on remplace la théorie de Kummer par un théorème de Bashmakov (généralisé par Ribet aux variétés abéliennes) qui conduit au lemme suivant.

Lemme 2. Soient \wp une fonction elliptique de Weierstrass d'invariants g_2, g_3 algébriques, k le corps des endomorphismes de \wp , et u_1, \dots, u_r des nombres complexes k -linéairement indépendants tels que les nombres $\wp(u_j)$ soient algébriques $(1 \leq j \leq r)$. Il existe un entier positif L_0 tel que si $P \in \mathbb{Z}[X_1, \dots, X_r]$ est un polynôme non nul de degré au plus L en X_i , $(1 \leq i \leq r)$ avec $L \geq L_0$, alors pour tout nombre premier ℓ avec $\ell^2 > L$ on a

$$P\left(\wp\left(\frac{u_1}{\ell}\right), \dots, \wp\left(\frac{u_r}{\ell}\right)\right) \neq 0.$$

Grâce à une remarque de Cassels, on peut calculer L_0 effectivement en fonction de u_1, \dots, u_r , et aussi de g_2, g_3 dans le cas de multiplication complexe. Pour plus de détails sur ce sujet, voir l'exposé du 27 Avril 1979 au séminaire de théorie des nombres de Bordeaux.

Dans le cas multiplicatif, cette méthode est remplacée maintenant par de nouveaux arguments qui font intervenir la théorie de Kummer de manière différente. Dans la partie principale de la démonstration, on suppose

$$[K(\sqrt{\alpha_1}, \dots, \sqrt{\alpha_n}) : K] = 2^n.$$

(Les procédés qu'on utilise alors n'ont pas encore été étendus au cas elliptique). Il reste ensuite à montrer que cette hypothèse n'est pas restrictive. Nous allons indiquer comment on y parvient.

§ 2 - La descente finale dans le cas multiplicatif

Nous commençons par un résultat simple que nous préciserons ensuite.

Lemme 3. Soient K un corps de nombres, et ℓ_1, \dots, ℓ_r des nombres complexes \mathbb{Q} -linéairement indépendants tels que

$$\alpha_j = e^{\ell_j} \in K, \quad (1 \leq j \leq r).$$

Il existe des nombres complexes ℓ'_1, \dots, ℓ'_r , qui engendrent le même \mathbb{Q} -espace vectoriel que ℓ_1, \dots, ℓ_r , tels que

$$\alpha'_j = e^{\ell'_j} \in K, \quad (1 \leq j \leq r),$$

et tels que pour tout nombre premier q pour lequel les racines q -ièmes de l'unité sont dans K , on ait

$$[K((\alpha'_1)^{1/q}, \dots, (\alpha'_r)^{1/q}) : K] = q^r$$

où

$$(\alpha'_j)^{1/q} = e^{\ell'_j/q}, \quad (1 \leq j \leq r).$$

Démonstration.

Soit M le \mathbb{Z} -module engendré par ℓ_1, \dots, ℓ_r , et soit M' l'ensemble des $\ell \in \mathbb{C}$ tels que $e^\ell \in K$ et que $\ell, \ell_1, \dots, \ell_r$ soient \mathbb{Q} -linéairement dépendants. Alors M' est un \mathbb{Z} -module de type fini et sans torsion. Soit ℓ'_1, \dots, ℓ'_r une base de M' . Soit q un nombre premier tel que K contienne les racines q -ièmes de l'unité. Supposons que les nombres $(\alpha'_j)^{1/q}$, ($1 \leq j \leq r$) engendrent une extension L de K de degré inférieur à q^r . Nous allons en déduire une contradiction.

D'après la théorie de Kummer le degré de L sur K est égal à l'indice de K^{*q} dans $\Gamma' K^{*q}$, où Γ' est le sous-groupe de K^* engendré par $\alpha'_1, \dots, \alpha'_r$. Donc le groupe quotient $\Gamma' K^{*q}/K^{*q}$ a un ordre inférieur à q^r , ce qui montre l'existence d'entiers rationnels positifs ou nuls a_1, \dots, a_r , avec $1 \leq \max a_j \leq q-1$, et d'un élément $\eta \in K^*$, tels que

$$(\alpha'_1)^{a_1}, \dots, (\alpha'_r)^{a_r} = \eta^q.$$

Soit $\log \eta$ une détermination du logarithme de η ; il existe un entier rationnel a_0 tel que

$$\sum_{j=1}^r a_j \ell'_j = q \log \eta + 2i\pi a_0.$$

Soit $\ell = \log \eta + 2i\pi \frac{a_0}{q}$. Alors $q\ell \in M'$, donc $\ell \in M'$, et il existe des entiers b_1, \dots, b_r dans \mathbb{Z} tels que

$$\ell = b_1 \ell'_1 + \dots + b_r \ell'_r.$$

De la relation

$$\sum_{j=1}^r (a_j - b_j q) \ell'_j = 0$$

on déduit $a_j = b_j q$, ($1 \leq j \leq r$), ce qui est incompatible avec $1 \leq \max a_j \leq q-1$.

L'argument précédent revient à écrire que $\Gamma'^q = \Gamma' \cap K^{*q}$ et à utiliser l'isomorphisme

$$\Gamma' / (\Gamma' \cap K^{*q}) \simeq (\Gamma' K^{*q}) / K^{*q}$$

avec le fait que Γ'^q est d'indice q^r dans Γ' .

Pour utiliser le lemme 3, il faut construire explicitement une base $\ell_1^1, \dots, \ell_r^1$ de M^1 . Pour cela soit u l'indice de M dans M^1 . Pour $1 \leq s \leq r$, soient $k_{s,1}, \dots, k_{s,s}$ des entiers rationnels tels que

$$\sum_{j=1}^s k_{s,j} \ell_j \in u M^1,$$

avec $k_{s,s} > 0$ minimal (donc $1 \leq k_{s,s} \leq u$) et $0 \leq k_{s,j} \leq u-1$, ($1 \leq j \leq s-1$).

On définit $\ell_1^1, \dots, \ell_r^1$ par

$$u \ell_s^1 = \sum_{j=1}^s k_{s,j} \ell_j, \quad (1 \leq s \leq r).$$

Montrons que $\ell_1^1, \dots, \ell_r^1$ engendrent M^1 . Pour $1 \leq s \leq r$, soit M_s le \mathbb{Z} -module engendré par ℓ_1, \dots, ℓ_s , et M_s^1 l'ensemble des $\ell \in \mathbb{C}$ tels que $e^\ell \in K$ et que $\ell, \ell_1, \dots, \ell_s$ soient \mathbb{Q} -linéairement dépendants (ainsi $M = M_r$, $M^1 = M_r^1$). Montrons que $\ell_1^1, \dots, \ell_s^1$ engendrent M_s^1 . On remarque que $u M_s^1 \subset M_s$ et on procède par récurrence sur s . Pour $s = 1$, soit $\ell \in M_1^1$; alors $u \ell \in M_1$; on écrit $u \ell = a \ell_1$ et on divise a par $k_{1,1}$. Comme $k_{1,1}$ a été choisi minimal, on obtient $a = k_{1,1} b$, $b \in \mathbb{Z}$, et $\ell = b \ell_1^1$. Quand on sait que $\ell_1^1, \dots, \ell_{s-1}^1$ engendrent M_{s-1}^1 , ($2 \leq s \leq r$), on choisit $\ell \in M_s^1$, on écrit $u \ell = a_1 \ell_1 + \dots + a_s \ell_s$, on divise a_s par $k_{s,s}$, on obtient $a_s = k_{s,s} b_s$, $b_s \in \mathbb{Z}$, d'où $u(\ell - b_s \ell_s^1) \in M_{s-1}$, et $\ell - b_s \ell_s^1 \in M_{s-1}^1$, ce qui permet de conclure.

Comme $M \subset M^1$, les espaces vectoriels engendrés sur \mathbb{Q} par ℓ_1, \dots, ℓ_r d'une part et $\ell_1^1, \dots, \ell_r^1$ d'autre part ont même dimension (donc coïncident), et $\ell_1^1, \dots, \ell_r^1$ sont donc \mathbb{Q} -linéairement indépendants.

(Il est avantageux de travailler additivement avec les logarithmes plutôt que multiplicativement, à cause de la torsion de K^*).

On peut alors préciser le lemme 3.

Lemme 4. On reprend les notations du lemme 3. Soient $D = [K : \mathbb{Q}]$, et $V_1 \leq V_2 \leq \dots \leq V_r$ des nombres réels tels que

$$V_s \geq \max \{ \log H_K(\alpha_s), |\ell_s| \}, \quad (1 \leq s \leq r).$$

Alors

$$\max \{ \log H_K(\alpha'_s), |\ell'_s| \} \leq V_1 + \dots + V_s, \quad (1 \leq s \leq r).$$

De plus, il existe des entiers rationnels $m_{s,j}$, $(1 \leq s \leq r, 0 \leq j \leq s)$, avec $m_{s,0} > 0$, tels que

$$m_{s,0} \ell'_s = \sum_{j=1}^s m_{s,j} \ell'_j, \quad (1 \leq s \leq r),$$

et

$$\max_{0 \leq j \leq s} |m_{s,j}| \leq (9sD^2)^s s! \max(1, V_s^s), \quad (1 \leq s \leq r).$$

Par conséquent, quand on veut minorer une forme linéaire de logarithmes

$$\Lambda = b_1 \log \alpha_1 + \dots + b_r \log \alpha_r$$

où $\log \alpha_1, \dots, \log \alpha_r$ sont \mathbb{Q} -linéairement indépendants, on l'écrit

$$\Lambda = b'_1 \log \alpha'_1 + \dots + b'_r \log \alpha'_r$$

où

$$b'_j = \sum_{s=j}^r b_s m_{s,j} / m_{s,0},$$

et $\sqrt{\alpha'_1}, \dots, \sqrt{\alpha'_r}$ engendrent une extension de $\mathbb{Q}(\alpha'_1, \dots, \alpha'_r)$ de degré 2^r .

Référence

Serge LANG : Elliptic curves diophantine analysis, Grund. der math. Wiss. , 231 , Springer Verlag 1978.

Michel WALDSCHMIDT
Institut Henri Poincaré
11, Rue P. et M. Curie
75231 PARIS CEDEX 05