Représentation des nombres entiers par des formes binaires

Par K. GYŐRY (Debrecen)

1. Sur la résolution en entiers rationnels des équations (1) et (5)

Considérons l'équation diophantienne

$$(1) \qquad F(x, y) = a_0 x^n + a_1 x^{n-1} y + \ldots + a_n y^n = m,$$

où $F(x, y) \in \mathbf{Z}[x, y]$ et $0 \neq m \in Z$. On peut supposer que $F(x, y)$ soit irréductible sur le corps $\mathbf{Q}$ des nombres rationnels. D'après un théorème bien connu de A. THUE [37] (1) n'admet qu'un nombre fini de solutions en entiers rationnels x, y, à condition que $n \geqq 3$. De plus, d'après un célèbre résultat de A. BAKER [4], on a

$$\max(|x|, |y|) < \exp\{n^{\nu^2} \cdot \|F\|^{\nu n^3} + (\log |m|)^{n+2}\}$$

pour toute solution $(x, y) \in \mathbf{Z}^2$, où $\nu = 32n(n+2)^2$ et $\|F\| = \max\limits_{0 \leqq j \leqq n} (|a_j|)$. Plus tard N. I. FELDMAN [15] a obtenu une majoration de la forme

$$(2) \qquad \max(|x|, |y|) < c_1 |m|^{c_2}$$

avec des constantes c_1 et c_2 effectivement calculables qui ne dépendent que de n et $\|F\|$.*) Voir encore A. BAKER [6]. Récemment, certaines variantes des majorations antérieures ont été substantiellement améliorées par G. V. SPRINDZUCK [33], H. M. STARK [34], [35] et A. BAKER [7]. Tous ces résultats reposent sur les minorations effectives des formes linéaires de logarithmes de nombres algébriques.

En cas de certaines formes $F(x, y)$ particulières on peut obtenir de meilleures majorations pour $\max(|x|, |y|)$ que celles mentionnées plus haut. Antérieurement, pour certaines formes particulières $F(x, y)$ de la forme $ax^n + by^n$, (2) a été démontré par A. BAKER [1], [2], [3] avec des constantes c_1, c_2 calculées explicitement. Voir encore les travaux [13], [14] de N. I. FELDMAN, où, pour des formes particulières $F(x, y)$, les valeurs de c_2 sont également explicitées. (Nous remarquons que dans [1], [3], [13] et [14] ces résultats s'obtiennent des estimations concernant des équations plus générales que (1)).

---

*) *Note ajoutée aux épreuves.* Dans notre travail "Effective estimates for the integer solutions of norm form and discriminant form equations" (à paraître), fait en commun avec Z. Z. PAPP, Corollary 1.2 fournit (2) aves des constantes c_1, c_2 calculées explicitement.

Si la forme $F(x, y)$ est définie, on peut facilement déduire (2) avec les constantes

$$c_1 = 2\{n\|F\| \max(|a_0|, |a_n|)\}^{\frac{n-1}{2}-\frac{1}{n}} \cdot \{\max(|a_0|, |a_n|)\}^{1-\frac{1}{n}}, c_2 = 1/n$$

(cf L. J. MORDELL [22], p. 186, Theorem 2). Pour cela on n'a pas besoin de la méthode de Baker. Ici $c_2 = 1/n$ est déjà la meilleure possible, vu que $(0, m^{1/n})$ est solution de (1) lorsque $a_n = 1$ et $m = m_1^n$, $m_1 \in \mathbf{Z}$.

Soit en particulier $F(x, y)$ *une forme construite sur* une extension quadratique totalement imaginaire d'un corps de nombres algébriques totalement réel (c'est-à-dire que le corps des racines de $F(x, 1)$ soit un corps de nombres ayant cette propriété). Dans ce cas, en utilisant une inégalité de norme (voir [19], Théorème 3 ou [18]) obtenue originairement (sous une forme moins générale) en collaboration avec L. LOVÁSZ [16], la constante c_1 ci-dessus peut être améliorée davantage.

Théorème 1. *Soit* $F(x, y) = a_0x^n + a_1x^{n-1}y + \ldots + a_ny^n \in \mathbf{Z}[x, y]$ *produit de* $l \geqq 1$ *formes irréductibles à coefficients entiers qui sont toutes construites sur extensions quadratiques totalement imaginaires des corps de nombres totalement réels. Soit* $m \neq 0$ *un nombre entier. Alors toute solution* $(x, y) \in \mathbf{Z}^2$ *de* (1) *vérifie*[1)]

$$|x| \leqq 2|a_n|^{1-\frac{2l-1}{n}} \cdot |m|^{\frac{1}{n}}; |y| \leqq 2|a_0|^{1-\frac{2l-1}{n}} \cdot |m|^{\frac{1}{n}}. \tag{3}$$

Le cas où $F(x, 1)$ est le produit des polynômes cyclotomiques semble particulièrement intéressant.

L'équation (10_2) montre que la majoration (3) est la meilleure possible. De plus, notre résultat n'est pas vrai en général, pour des formes d'autre type. Si par exemple $F(x, y) = x(x-b_2y)\ldots(x-b_ny)+y^n$ avec des entiers $0 = b_1 < b_2 < \ldots < b_n$ et $m = m_1^n$, $m_1 \in \mathbf{Z}$, alors (m_1b_j, m_1) $(j = 1, \ldots, n)$ sont les solutions de (1).

Comme il est bien connu, à partir d'une solution (x_0, y_0) de (1), on peut transformer (1) par une transformation unimodulaire dans une équation $F'(x', y') = m$ avec $F'(1, 0) = m$, où $|y'| \leqq 2|m|$ pour toute solution entière x', y'.

Corollaire 1. *Soit* $F(x, y) \in \mathbf{Z}[x, y]$ *une forme de degré n avec la propriété indiquée dans le Théorème* 1. *Alors on a*

$$|F(x, y)| \geqq c_3\{\max(|x|, |y|)\}^n \tag{4}$$

pour tout $(x, y) \in \mathbf{Z}^2$, *où* $c_3 = 2^{-n}\{\max(|a_0|, |a_n|)\}^{-n+(2l-1)}$.

Si un polynôme $f(x) \in \mathbf{Z}[x]$ de degré n possède l facteurs irréductibles dont les corps des racines sont des extensions quadratiques totalement imaginaires des corps de nombres totalement réels, alors du Théorème 1 il résulte que $|f(x)| \geqq c_3'|x|^n$ pour tout $x \in \mathbf{Z}$ avec $c_3' = 2^{-n}|f(0)|^{-n+(2l-1)}$. Le Théorème 2 fournit une conséquence de type similaire.

Considérons ensuite l'équation plus générale

$$F(x, y) = G(x, y), \tag{5}$$

[1)] Evidemment le cas $l \geqq 1$ se ramène au cas $l = 1$. Cependant cet énoncé nous permet d'établir le Corrollaire 2 avec $l \geqq 1$.

où $F(x, y) \in \mathbf{Z}[x, y]$ est une forme de degré $n \geqq 2$ et $G(x, y) \in \mathbf{Z}[x, y]$ est un polynôme de degré $k < n$. Si $F(x, y)$ n'est pas puissance d'une forme irréductible, alors, d'après un théorème de C. RUNGE [26], (5) n'admet qu'un nombre fini de solutions en entiers rationnels x, y et les solutions eventuelles peuvent être determinées. De plus, A. SCHINZEL [27] a démontré qu'ici il suffit de supposer que $F(x, y)$ ne soit pas la puissance, à un facteur constant près, d'une forme linéaire ou quadratique indéfinie, mais sa démonstration n'est pas effective. Dans le cas de certaines formes $F(x, y)$ de la forme $ax^n + by^n$, $n \geqq 3$, A. BAKER [1] a majoré explicitement les solutions entières de (5), à condition que $k \leqq n-3$.

Désignons par $L(G)$ la longueur de $G(x, y)$, c'est-à-dire la somme des valeurs absolues de ses coefficients. Comme $|G(x, y)| \leqq L(G)\{\max(|x|, |y|)\}^k$ pour tout $(x, y) \in \mathbf{Z}^2$, le Corollaire 1 implique le suivant.

Corollaire 2. *Soit $F(x, y) \in \mathbf{Z}[x, y]$ une forme de degré n avec la même propriété que dans le Théorème 1 et soit $G(x, y) \in \mathbf{Z}[x, y]$ un polynôme de degré $k < n$. Alors on a*

$$\max(|x|, |y|) \leqq [2^n L(G)]^{\frac{1}{n-k}} \cdot \{\max(|a_0|, |a_n|)\}^{\frac{n-(2l-1)}{n-k}} \tag{6}$$

pour toute solution $(x, y) \in \mathbf{Z}^2$ de (5).

2. Sur la résolution en entiers algébriques totalement réels de l'équation (7)

Soit $\mathbf{K}$ un corps de nombres algébriques de degré k et désignons par $\mathbf{Z_K}$ l'anneau des entiers de $\mathbf{K}$. Soient $\alpha_1, \ldots, \alpha_n \in \mathbf{Z_K}$ $n \geqq 3$ nombres distincts et $0 \neq \beta \in \mathbf{Z_K}$. D'un théorème général de C. L. SIEGEL [29] (voir encore W. J. LEVEQUE [38]) il résulte que le nombre de solutions de l'équation

$$(x-\alpha_1 y) \ldots (x-\alpha_n y) = \beta \tag{7}$$

en $x, y \in \mathbf{Z_K}$ est fini, et, d'après un résultat de A. BAKER [4], [5] (voir encore A. BAKER et J. COATES [8]), toute solution $(x, y) \in \mathbf{Z}_{\mathbf{K}}^2$ vérifie[2)]

$$\max(h(x), h(y)) < \exp\{(kH)^{(10k)^5}\}, \tag{8}$$

où H désigne le maximum des hauteurs de $\alpha_1, \ldots, \alpha_n, \beta$ et d'un certain entier de $\mathbf{K}$ qui engendrent $\mathbf{K}$. Les minorations récentes des formes linéaires de logarithmes de nombres algébriques permettent évidemment d'améliorer (8).

Nous démontrerons le théorème suivant sans utiliser la méthode de Baker.

Théorème 2. *Soit $\mathbf{K}$ une extension quadratique totalement imaginaire d'un corps de nombres algébriques totalement réel avec degré $[\mathbf{K}:\mathbf{Q}] = k$. Soient $\alpha_1, \ldots, \alpha_n \in \mathbf{Z_K}$, $n \geqq 1$, des nombres non tous réels et soit $0 \neq \beta \in \mathbf{Z_K}$ tels que $\max_{1 \leqq j \leqq n} h(\alpha_j) \leqq A$, $h(\beta) \leqq B$ et $N_{\mathbf{K}/\mathbf{Q}}(\beta) \leqq N$. Désignons par t, $1 \leqq t \leqq n$, le nombre des éléments non réels de $\{\alpha_1, \ldots, \alpha_n\}$. Alors on a*

$$h(x) \leqq c_4 A B^{1/n}, \quad h(y) \leqq c_4 B^{1/n} \tag{9}$$

pour toute solution de (7) en entiers réels x, y de $\mathbf{K}$, où $c_4 = 2(2^{2-t/n}A)^{k-1} N^{k(1-t/n)}$.

2) $h(\alpha)$ signifie le maximum des valeurs absolues des conjugués d'un nombre algébrique α.

(9) est le meilleur possible en B. Dans (9) on peut évidemment choisir $N=B^k$. De plus, en ce qui concerne le corps $\mathbf{K}$, les majorations (9) ne dépendent que du degré de $\mathbf{K}$. Comme $H(x)\leqq(2h(x))^k$ et $H(y)\leqq(2h(y))^k$,[3] une conséquence immédiate du Théorème 2 est la suivante.

Corollaire. *Soit $k'\geqq 1$ un nombre entier. Sous les hypothèses du Théorème 2 l'équation (7) n'admet qu'un nombre fini de solutions en entiers algébriques totalement réels x, y de degré $\leqq k'$, et toutes les solutions x, y peuvent être déterminées.*

Soit dans (7) $[\mathbf{Q}(\alpha_1, \dots, \alpha_n, \beta)\colon \mathbf{Q}]=k_0$. Si $n\leqq k'/k_0$, ce corollaire ne reste pas vrai en général, car (7) possède une infinité de solutions en entiers algébriques x, y de degré $\leqq k'$. Si $\alpha_1, \dots, \alpha_n$ sont deux à deux distincts et $n>k'^4\left(\frac{nk_0}{s+1}+s\right)$[4] avec $s=\left[\frac{1}{2}\sqrt{4nk_0+1}-1\right]$, ce corollaire, sous une forme non effective, résulte d'un théorème plus général de C. L. Siegel [29].

Pour illustrer le Théorème 2 considérons un polynôme cyclotomique $\Phi(x)$ et supposons que $\mathbf{K}$ contient le corps cyclotomique correspondant. Alors nous avons $h(x), h(y)\leqq 2^k$ pour toute solution réelle $(x, y)\in\mathbf{Z}_{\mathbf{K}}^2$ de l'équation $F(x, y)=1$, où $F(x, y)=y^n\Phi\left(\frac{x}{y}\right)$ et $n=\deg\Phi$.

Le Théorème 2 a des conséquences du même type que le Théorème 1 (voir les Corollaires 1 et 2).

3. Sur la résolution de l'équation (1) lorsque $m=1$

Lagrange a ramené le problème de la résolution de l'équation (1) en entiers rationnels x, y à celui de la résolution de plusieurs équations de la forme (1) dans lesquelles $m=1$ (voir par ex. [23], [32] ou [22]). De plus, si (1) satisfait à l'hypothèse du Théorème 1, alors les équations réduites également satisfont à cette hypothèse. Comme le Théorème 3 ci-dessous le montre, dans le cas $m=1$, $l=1$, sous les autres hypothèses du Théorème 1, le Théorème 1 peut être précisé.

Dans le cas $m=1$ et sous certaines restrictions relatives à (1), de nombreux résultats sont connus qui montrent que (1) n'admet que peu de solutions en entiers rationnels x, y. Pour $n=3$ et 4 entre autres B. N. Delone (Delaunay), T. Nagell, C. L. Siegel, D. K. Faddeev, W. Ljunggren, V. A. Demjanenko ([12]) et pour $n>4$ Th. Skolem, Y. Domar, A. Ekenstam, S. Hyyrö (voir par ex. les livres [23], [32], [11] et [22]) et V. A. Tartakovskiĭ [36] ont obtenu des résultats de ce type. Évidemment, les théorèmes généraux de K. Mahler [21], C. L. Siegel [30], [31], H. Davenport et K. F. Roth [10], D. J. Lewis et K. Mahler [20] et G. V. Čudnovskiĭ [9] sont également applicables au cas particulier $m=1$.

Notre Théorème 3 se rattache à certains résultats de T. Nagell [24], [25]. Soit $m=1$ dans (1) et désignons par M le nombre de solutions entières de (1). T. Nagell

[3] $H(\alpha)$ signifie la hauteur d'un nombre algébrique α, c'est-à-dire le maximum des valeurs absolues des coefficients du polynôme minimal de α sur $\mathbf{Z}$.

[4] En utilisant un récent théorème d'approximation de W. M. Schmidt [28], ici il suffit de supposer $n>k'^2(k'^2+1)$.

a démontré que $M \leqq 8$ pour les polynômes cyclotomiques $F(x, 1)$ ([24], voir encore [25], Théorème 13), et $M \leqq 6$ pour les polynômes $F(x, 1)$ qui engendrent des p^α-ièmes corps cyclotomiques ($p \geqq 3$ nombre premier) ([25], Théorème 14). De plus, il a déterminé, pour tout M donné, toutes les formes $F(x, y)$ de ce type pour lesquelles (1) possède exactement M solutions.

Deux formes à coefficients entiers seront brièvement dites *équivalentes* quand elles sont unimodulairement équivalentes.

Théorème 3. *Soit $F(x, y) \in \mathbf{Z}[x, y]$ une forme irréductible construite sur une extension quadratique totalement imaginaire d'un corps de nombres algébriques totalement réel. Le nombre M de solutions de l'équation*

$$F(x, y) = 1 \tag{10}$$

en entiers rationnels x, y est pair et $M \leqq 8$. De plus:

1° *Pour que* (10) *soit soluble, il faut et il suffit que $F(x, y)$ soit équivalent à une forme $N_{\mathbf{K}/\mathbf{Q}}(x+\alpha y)$, où $\mathbf{K}=\mathbf{Q}(\gamma)$, $F(\gamma, 1)=0$, lorsque*[5]

$$N_{\mathbf{K}/\mathbf{Q}}(x+\alpha y) = 1 \tag{10_1}$$

admet les solutions $(\pm 1, 0)$. Dans (10_1) *$M>2$ si et seulement si $\alpha-\varepsilon \in \mathbf{Z}$ avec une unité non réelle ε (quand* (10_1) *est équivalent à* (10_3)*) ou bien $2\alpha \pm 1 = \eta$ avec une unité imaginaire pure η (quand* (10_1) *est équivalent à* (10_2)*).*

2° *Etant donnée une unité imaginaire pure η telle que $\frac{\eta-1}{2} \in \mathbf{Z}_\mathbf{K}$,*

$$N_{\mathbf{K}/\mathbf{Q}}\left(x+\frac{\eta-1}{2}y\right) = 1 \tag{10_2}$$

possède les solutions $(\pm 1, 0)$, $(1, 2)$, $(-1, -2)$. Dans (10_2) *$M>4$ si et seulement si $\eta = \pm\frac{1-\zeta}{1+\zeta}$ avec une racine de l'unité ζ ayant la propriété indiquée dans 5° quand* (10_2) *est équivalent à* (10_5).

3° *Etant donnée une unité non réelle $\varepsilon \in \mathbf{Z}_\mathbf{K}$, l'équation*

$$N_{\mathbf{K}/\mathbf{Q}}(x+\varepsilon y) = 1 \tag{10_3}$$

admet les solutions $(\pm 1, 0)$ $(0, \pm 1)$. Ici $M>4$ si et seulement si $\varepsilon = \pm\frac{1-\zeta_1}{\zeta_1-\zeta_2}$ avec des racines de l'unité ζ_1, ζ_2 ayant la propriété donnée dans 4° quand (10_3) *est équivalent à* (10_4).

4° *Soit $\vartheta = \frac{1-\zeta_1}{\zeta_1-\zeta_2} \in Z_K$, ζ où chacun des ζ_1, $\zeta_2 (\neq \zeta_1)$, ζ_1/ζ_2 est une racine primitive p^α-ième de l'unité avec le même p^α (p nombre premier) ou bien aucun d'eux n'est racine primitive q^β-ième de l'unité (q nombre premier).* $(\pm 1, 0)$, $(0, \pm 1)$, $(1, 1)$, $(-1, -1)$ *sont solutions de*

$$N_{\mathbf{K}/\mathbf{Q}}(x+\vartheta y) = 1. \tag{10_4}$$

---

[5] **K** est aussi une extension quadratique totalement imaginaire d'un corps de nombres totalement réel.

$M>6$ si et seulement si $\vartheta=\pm(1+\zeta)^{-1}$, ζ ou $\zeta\pm1$, ζ étant une racine de l'unité avec la propriété indiquée dans 5° quand (10_4) est équivalent à (10_5).

5° *Si $\zeta\in\mathbf{K}$ est une racine primitive t-ième de l'unité et $t\neq p^\alpha, 2p^\alpha$, p nombre premier, alors toutes les solutions de l'équation*

$$(10_5) \qquad N_{\mathbf{K}/\mathbf{Q}}(x+\zeta y)=1$$

sont $(\pm1, 0)$, $(0, \pm1)$, $(\pm1, \pm1)$.

Donc, pour qu'on ait $M>4$ il faut que $F(x, y)$ soit construit sur un t-ième corps cyclotomique avec $t\neq 2^\alpha$. Le Théorème 3 est donc une généralisation des résultats mentionnés plus haut de T. NAGELL [24], [25]. L'une des conséquences de notre théorème est la suivante.

Corollaire (T. NAGELL, [24], [25]). *Désignons par M le nombre de solutions de l'équation*

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

en nombres entiers x, y où $F_n(x, y)$ désigne la n-ième forme cyclotomique[6] *avec $n\geqq3$. Alors, on a*

1° *pour $n=p^\alpha$ et $2p^\alpha$, p nombre premier, $\alpha\geqq1$, $M=6$;*
2° *pour $n=2^\beta$, $\beta\geqq2$, $M=4$;*
3° *dans tous les autres cas $M=8$.*[*]

Dans [25] NAGELL a démontré que $M\leqq8$ pour toutes les formes biquadratiques définies $F(x, y)$, à condition que $\mathbf{K}=\mathbf{Q}(\alpha)$, où $F(\alpha, 1)=0$, ait au moins un sous-corps quadratique. Il a déterminé toutes les formes pour lesquelles $M=8$ et $M=6$. Notre Théorème 3 implique ce résultat de Nagell dans le cas particulier où $\mathbf{K}$ possède un sous-corps quadratique réel.

Le Théorème 3 ne reste pas vrai en général (pour cela voir l'exemple qui suit le Théorème 1).

En appliquant le procédé de Lagrange et le Théorème 3, on peut explicitement majorer, sous les hypothèses du Théorème 1, le nombre de solutions primitives de (1) par une borne ne dépendant que de n et du nombre des facteurs premiers distincts de m.

4. Démonstrations des théorèmes

La démonstration du Théorème 1 sera basée sur le lemme suivant.

Lemme 1. *Soit $\mathbf{K}$ une extension quadratique totalement imaginaire d'un corps de nombres totalement réel avec $k=[\mathbf{K}:\mathbf{Q}]$. Si $\alpha\in\mathbf{K}$, alors* $\mathrm{Re}\,\alpha$, $i\,\mathrm{Im}\,\alpha\in\mathbf{K}$,

$$(11) \qquad \{N_{\mathbf{K}/\mathbf{Q}}(\alpha)\}^{2/k}\geqq\{N_{\mathbf{K}/\mathbf{Q}}(\mathrm{Re}\,\alpha)\}^{2/k}+\{N_{\mathbf{K}/\mathbf{Q}}(i\,\mathrm{Im}\,\alpha)\}^{2/k},$$

et l'égalité a lieu si et seulement si $\mathrm{Re}\,\alpha=0$, $i\,\mathrm{Im}\,\alpha=0$ *ou* $\left(\frac{\mathrm{Re}\,\alpha}{i\,\mathrm{Im}\,\alpha}\right)^2\in\mathbf{Q}$.

---

[6] Autrement dit, $F_n(x, 1)$ est le n-ième polynôme cyclotomique.

[*] *Note ajoutée aux épreuves.* Monsieur le Professeur C. L. STEWART a bien voulu attirer mon attention à un résultat de G. D. BIRKHOFF et H. S. VANDIVER (*Annals of Math.* (2), **5** (1904), pp. 173—180; *Theorem V*) qui implique $\max(|x|, |y|)\leqq1$ pour tout $(x, y)\in\mathbf{Z}^2$ satisfaisant à $F_n(x, y)=1$.

Ce lemme est un cas particulier de notre Théorème 3 dans [19] (voir encore [18]). Comme nous l'avons mentionné, (11) a été obtenu (sous une forme moins générale) en collaboration avec L. LOVÁSZ [16].

DÉMONSTRATION DU THÉORÈME 1. Par hypothèse $a_0 a_n \neq 0$. Considérons la décomposition

$$F(x, y) = \prod_{j=1}^{l} F_j(x, y) \tag{12}$$

en facteurs irréductibles $F_j(x, y) \in \mathbf{Z}[x, y]$.

Soit $(x, y) \in \mathbf{Z}^2$ une solution de (1). Posons

$$\begin{aligned} F_j(x, y) &= a_{0j} x^{n_j} + a_{1j} x^{n_j - 1} y + \ldots + a_{n_j j} y^{n_j} = a_{0j} \prod_{s=1}^{n_j} (x - \alpha_{j_s} y) = \\ &= a_{0j} N_{\mathbf{K}_j/\mathbf{Q}}(x - \alpha_{j_1} y), \end{aligned} \tag{13}$$

où les corps $\mathbf{K}_j = \mathbf{Q}(\alpha_{j_1})$ $(j = 1, \ldots, l)$ sont des extensions quadratiques totalement imaginaires des corps de nombres totalement réels. En vertu du Lemme 1 il résulte de (1) et (13) que

$$|m| = |F(x, y)| = \left| \prod_{j=1}^{l} a_{0j} N_{\mathbf{K}_j/\mathbf{Q}}(x - \alpha_{j_1} y) \right| \geqq$$

$$\geqq \left| \prod_{j=1}^{l} a_{0j} N_{\mathbf{K}_j/\mathbf{Q}}(i \operatorname{Im} \alpha_{j_1} y) \right| = |y|^n \cdot \left| \prod_{j=1}^{l} a_{0j} N_{\mathbf{K}_j/\mathbf{Q}}(i \operatorname{Im} \alpha_{j_1}) \right|.$$

Comme $2a_{0j} \cdot i \operatorname{Im} \alpha_{j_1} = a_{0j}(\alpha_{j_1} - \bar{\alpha}_{j_1})$ est entier, on a

$$|a_{0j}| N_{\mathbf{K}_j/\mathbf{Q}}(i \operatorname{Im} \alpha_{j_1}) = \frac{N_{\mathbf{K}_j/\mathbf{Q}}(2a_{0j} \cdot i \operatorname{Im} \alpha_{j_1})}{2^{n_j} \cdot |a_0|^{n_j - 1}} \geqq 2^{-n_j} \cdot |a_{0j}|^{-(n_j - 1)}.$$

Vu que $n_j \geqq 2$ pour tout $1 \leqq l \leqq j$, on obtient

$$\prod_{j=1}^{l} |a_{0j}|^{n_j - 1} \leqq |a_0|^{n - (2l - 1)},$$

ce qui implique

$$|y| \leqq 2 |a_0|^{1 - \frac{2l-1}{n}} \cdot |m|^{\frac{1}{n}}.$$

Le majoration pour $|x|$ s'obtient de la même façon.

DÉMONSTRATION DU THÉORÈME 2. Considérons une solution réelle $(x, y) \in \mathbf{Z}_{\mathbf{K}}^2$ de (7). Le cas $xy = 0$ étant trivial, nous supposons $xy \neq 0$.

Posons

$$x - \alpha_j y = \beta_j, \quad j = 1, \ldots, n, \tag{14}$$

où $\beta_j | \beta$ pour tout j. Désignons par J l'ensemble des indices j pour lesquels les α_j ne sont pas réels. Avec la notation $\bar{\beta}_j = \varrho_j \beta_j$, (14) entraîne

$$x - \bar{\alpha}_j y = \varrho_j \beta_j, \quad j \in J. \tag{15}$$

(14) et (15) impliquent

$$y=\frac{\beta_j(1-\varrho_j)}{(\bar{\alpha}_j-\alpha_j)},\quad j\in J \tag{16}$$

et

$$x=\frac{y(\bar{\alpha}_j-\alpha_j\varrho_j)}{1-\varrho_j},\quad j\in J. \tag{17}$$

Soit $j_0\in J$ un indice fixé. Si $t<n$, de (14) et (17) on obtient

$$\beta_j=x-\alpha_j y=y\frac{(\bar{\alpha}_{j_0}-\alpha_j)+\varrho_{j_0}(\alpha_j-\alpha_{j_0})}{1-\varrho_{j_0}} \tag{18}$$

pour tout $j\notin J$. Ainsi, de (7), (16) et (18) on déduit

(19)

$$y^n=\beta(1-\varrho_{j_0})^{n-t}\prod_{j\in J}(1-\varrho_j)\{\prod_{j\in J}(\bar{\alpha}_j-\alpha_j)\}^{-1}\cdot\{\prod_{j\notin J}[(\bar{\alpha}_{j_0}-\alpha_j)+\varrho_{j_0}(\alpha_j-\alpha_{j_0})]\}^{-1}.$$

Comme $(\bar{\beta}_j)^{(s)}=\overline{\beta_j^{(s)}}$ pour tout conjugué $(\bar{\beta}_j)^{(s)}$ de $\bar{\beta}_j$, on a $|\varrho_j^{(s)}|=|\overline{\beta_j^{(s)}}/\beta_j^{(s)}|=1$ pour tout conjugué $\varrho_j^{(s)}$ de ϱ_j, $1\leqq s\leqq k$, $j\in J$. Désignons par b_j le coefficient dominant du polynôme minimal de ϱ_j sur Z, $j\in J$. Vu que

$$N_{\mathbf{K}/\mathbf{Q}}(\beta_j)\prod_{s=1}^{k}(x-\varrho_j^{(s)})\in Z[x]$$

et $\beta_j|\beta$, on obtient

$$b_j\leqq N_{\mathbf{K}/\mathbf{Q}}(\beta_j)\leqq N_{\mathbf{K}/\mathbf{Q}}(\beta)\leqq N.$$

$\sigma_j=b_{j_0}(\bar{\alpha}_{j_0}-\alpha_j)+b_{j_0}\varrho_{j_0}(\alpha_j-\alpha_{j_0})\in Z_{\mathbf{K}}$ pour tout $j\notin J$, d'où

$$h\left(\frac{1}{\sigma_j}\right)\leqq h^{k-1}(\sigma_j)\leqq(4AN)^{k-1},\quad j\notin J.$$

De plus, on a

$$h\left(\frac{1}{\bar{\alpha}_j-\alpha_j}\right)\leqq h^{k-1}(\bar{\alpha}_j-\alpha_j)\leqq(2A)^{k-1},\quad j\in J.$$

Donc, (19) entraîne

$$h(y)\leqq c_4B^{1/n}$$

avec $c_4=2(2^{2-t/n}A)^{k-1}N^{k(1-t/n)}$.

De (14), (15) et (17) on obtient de la même manière que

$$x^n=\beta(\bar{\alpha}_{j_0}-\alpha_{j_0}\varrho_{j_0})^{n-t}\prod_{j\in J}(\bar{\alpha}_j-\alpha_j\varrho_j)\{\prod_{j\in J}(\bar{\alpha}_j-\alpha_j)\}^{-1}\times$$
$$\times\{\prod_{j\notin J}[(\bar{\alpha}_{j_0}-\alpha_j)+\varrho_{j_0}(\alpha_j-\alpha_{j_0})]\}^{-1},$$

d'où

$$h(x)\leqq c_4AB^{1/n}.$$

Pour démontrer le Théorème 3 nous aurons encore besoin de deux lemmes.

Lemme 2. *Les unités non réelles $\varepsilon_1, \varepsilon_2$ d'une extension quadratique totalement imaginaire d'un corps de nombres totalement réel satisfont à l'équation*

$$\varepsilon_1+\varepsilon_2 = 1$$

si et seulement si

$$\varepsilon_1 = \frac{1-\zeta_2}{\zeta_1-\zeta_2}, \quad \varepsilon_2 = \frac{\zeta_1-1}{\zeta_1-\zeta_2},$$

où chacun des $\zeta_1, \zeta_2\,(\neq\zeta_1), \zeta_1/\zeta_2$ est une racine primitive p^α-ième de l'unité avec le même p^α (p nombre premier) ou bien aucun d'eux n'est racine primitive q^β-ième de l'unité (q nombre premier).

DÉMONSTRATION: voir [17] ou [18].

Lemme 3. *Pour que les unités non réelles $\varepsilon_1, \varepsilon_2$ d'une extension quadratique totalement imaginaire d'un corps de nombres totalement réel soient solutions de l'équation*

$$\varepsilon_1+\varepsilon_2 = 2,$$

il faut et il suffit qu'on ait

$$\varepsilon_1 = 1-\zeta, \quad \varepsilon_2 = 1+\zeta,$$

où ζ est une racine primitive t-ième de l'unité telle que $t\neq p^\alpha, 2p^\alpha$ (p nombre premier).

DÉMONSTRATION: voir [17] ou [18].

DÉMONSTRATION DU THÉORÈME 3. Soit γ l'une des racines de $F(x, 1)=0$. D'après l'hypothèse $\mathbf{K}=\mathbf{Q}(\gamma)$ est une extension quadratique totalement imaginaire d'un corps de nombres totalement réel.

Supposons que (10) est soluble en entiers rationnels x, y et soit x_0, y_0 une solution de (10). Il existe des entiers rationnels k et l tels que $x_0l-y_0k=1$. La transformation unimodulaire

$$x = x_0x'+ky', \quad y = y_0x'+ly'$$

entraîne

$$F(x, y) = F(x_0x'+ky', y_0x'+ly') = F^*(x', y'),$$

où $F^*(1, 0)=F(x_0, y_0)=1$, et ainsi $F^*(x', y')=N_{\mathbf{K}/\mathbf{Q}}(x'+\alpha y')$ avec un entier non réel $\alpha\in\mathbf{K}$.

Donc, pour que M soit positif il faut et il suffit que (10) soit équivalent à une équation de la forme (10_1) qui admet toujours les solutions triviales $(\pm 1, 0)$. M est évidemment pair.

Supposons $M>2$, c'est-à-dire que (10_1) possède une solution x_1, y_1 telle que $y_1\neq 0$. Alors, d'après le Théorème 1 on a $|y_1|\leqq 2$. On peut supposer que $y_1>0$.

Considérons d'abord le cas où $y_1=1$. $x_1+\alpha=\varepsilon$ est une unité non réelle dans $\mathbf{K}$. Par la transformation unimodulaire

$$x' = x-x_1y, \quad y' = y$$

l'équation (10_1) sera transformée en une équation de la forme (10_3), qui possède les solutions $(\pm 1, 0)$, $(0, \pm 1)$.

Supposons que (10_3) a une autre solution x_2, y_2 avec $x_2 \neq 0$ lorsque $M > 4$. Alors, du Théorème 1 on déduit $|x_2| \leqq 2$ et $y_2 = 1$ ou 2. Soit d'abord $y_2 = 1$, lorsque

(20) $$x_2 + \varepsilon = \varepsilon'$$

avec une unité non réelle $\varepsilon' \in \mathbf{K}$. Si $x_2 = 1$, du Lemme 2 il résulte que $\varepsilon = \frac{1-\zeta_1}{\zeta_1 - \zeta_2}$, ζ_1, ζ_2 étant des racines de l'unité avec la propriété indiquée dans le Lemme 2. Par conséquent, nous sommes parvenu à l'équation (10_4) qui admet les six solutions figurant dans le théorème. Si $x_2 = -1$, on a, d'une manière analogue, $\varepsilon = -\frac{1-\zeta_1}{\zeta_1 - \zeta_2}$ et (10_3) est équivalent à (10_4).

Soit ensuite $y_2 = 1$ et $x_2 = 2$ ou -2. Dans ce cas (20) et le Lemme 3 impliquent

$$\varepsilon = \zeta \pm 1 = \mp \frac{1-(\pm\zeta)^{-2}}{(\pm\zeta)^{-2} - (\pm\zeta)^{-1}}$$

avec une racine de l'unité ζ ayant la propriété donnée dans le Lemme 3. Donc, (10_3) est également équivalent à (10_4) (voire à (10)).

Enfin, soit dans (10_3) $y_2 = 2$, lorsque on a nécessairement $x_2 = 1$ où -1. D'après le Lemme 1 on obtient

$$1 \geqq \{N_{\mathbf{K}/\mathbf{Q}}(\pm 1 + 2\,\mathrm{Re}\,\varepsilon)\}^{2/n} + \{N_{\mathbf{K}/\mathbf{Q}}(2\,i\,\mathrm{Im}\,\varepsilon)\}^{2/n}, \quad n = [\mathbf{K}:\mathbf{Q}],$$

d'où, $2i\,\mathrm{Im}\,\varepsilon \neq 0$ étant un entier dans $\mathbf{K}$, il résulte que

$$\varepsilon + \bar{\varepsilon} = 2\,\mathrm{Re}\,\varepsilon = \mp 1.$$

En appliquant de nouveau le Lemme 2, on en conclut $\varepsilon = \pm \frac{1-\zeta_1}{\zeta_1 - \zeta_2}$ avec des racines de l'unité ζ_1, ζ_2 ayant la même propriété que plus haut et ainsi (10_3) est équivalent à (10_4). Dans ce cas on peut aisément voir que $\varepsilon = \pm \frac{1}{1+\zeta_2}$, ζ_2 étant une racine de l'unité avec la propriété indiquée dans 5°.

Supposons maintenant que dans (10_4) $M > 6$. Soit x_3, y_3 une solution autre que les six solutions données dans le théorème. Comme nous l'avons prouvé plus haut, $y_3 = \pm 2$ implique $\vartheta = \pm \frac{1}{1+\zeta_2}$ avec le ζ_2 précédent et ainsi (10_4) est équivalent à (10_5). Si $(x_3, y_3) = (1, -1)$ ou $(-1, 1)$, alors

$$-1 + \vartheta \quad \text{et} \quad 1 + \vartheta$$

sont des unités non réelles. Ainsi, en conséquence du Lemme 3, $\vartheta = \zeta$ avec une racine de l'unité ζ ayant la propriété indiquée dans le Lemme 3. Dans ce cas (10_4) est également équivalent à (10_5). Si $(x_3, y_3) = (2, 1)$ ou $(-2, -1)$, $2 + \vartheta$ et ϑ étant des unités non réelles, on obtient $\vartheta = \zeta - 1$ avec une racine de l'unité ζ figurant dans le Lemme 3 et (10_4) est équivalent à (10_5). Enfin, si $(x_3, y_3) = (2, -1)$ ou $(-2, 1)$, on obtient de la même façon que $\vartheta = \zeta + 1$.

Considérons ensuite l'équation (10_5) qui possède évidemment les solutions $(\pm 1, 0), (0, \pm 1), (\pm 1, \pm 1)$. On peut aisément voir que (10_5) a exactement ces huit solutions. En effet, en supposant que x_4, y_4 est une solution avec $\max(|x_4|, |y_4|) \geqq 2$, d'après le Théorème 1 nous avons $\max(|x_4|, |y_4|) = 2$. Il suffit de considérer le cas où $y_4=2$ et $x_4=\pm 1$. Mais, comme nous l'avons vu plus haut (dans le cas de l'équation (10_3)), il en résulte que $\zeta=\pm\frac{1}{1+\zeta_2}$ avec une racine de l'unité ζ_2 ayant la même propriété que plus haut, ce qui entraîne une contradiction.

Il nous faut encore tenir compte de la possibilité quand dans (10_1) $y_1=2$ et $x_1=1$ ou -1. On obtient de (10_1), par la même raisonnement que plus haut dans le cas de (10_3), que $x_1+2\operatorname{Re}\alpha=0$, c'est-à-dire $x_1+2\alpha=\eta$ est une unité imaginaire pure. Donc, dans ce cas (10_1) est équivalent à (10_2) qui admet évidemment les solutions $(\pm 1, 0)$, $(1, 2)$ et $(-1, -2)$.

Si (10_2) a une solution x_5, y_5 différente de celles ci-dessus, on obtient nécessairement $y_5=\pm 1$ ou $(x_5, y_5)=(0, \pm 2)$. Si $x_5=0$, $y_5=2$ ou -2, alors $\eta-1$ et η sont des unités non réelles. Ainsi, d'après le Lemme 2, $\eta=\frac{\zeta_1-1}{\zeta_1-\zeta_2}$ avec des racines de l'unité ζ_1, ζ_2 qui possèdent la propriété indiquée dans le Lemme 2. On a $\bar{\eta}=\zeta_2\eta$ et $\bar{\eta}=-\eta$, d'où $\zeta_2=-1$, $\eta=\frac{\zeta_1-1}{\zeta_1+1}$ et $\frac{\eta-1}{2}=-\frac{1}{1+\zeta_1}$, ζ_1 étant une racine primitive t-ième de l'unité avec $t\neq p^\alpha, 2p^\alpha$, p nombre premier. Dans ce cas (10_2) est équivalent à (10_5).

Supposons ensuite que $y_5=1$, lorsque

$$x_5+\frac{\eta-1}{2}=\varepsilon'' \tag{21}$$

avec une unité non réelle $\varepsilon''\in\mathbf{K}$. Dans ce cas, de (21) il résulte

$$x_5+\frac{-\eta-1}{2}=\zeta\varepsilon''$$

avec une racine de l'unité $\zeta=\overline{\varepsilon''}/\varepsilon''$. On en déduit

$$2x_5-1=\varepsilon''(1+\zeta) \quad \text{et} \quad \eta=\varepsilon''(1-\zeta). \tag{22}$$

Si $|2x_5-1|\geqq 3$, alors

$$3^n\leqq N_{\mathbf{K}/\mathbf{Q}}(2x_5-1)=N_{\mathbf{K}/\mathbf{Q}}(1+\zeta)\leqq 2^n,$$

ce qui est impossible. Par conséquent $2x_5-1=\pm 1$, et, d'après (22), $\frac{\eta-1}{2}=-\frac{\zeta}{1+\zeta}$ ou $-\frac{1}{1+\zeta}$ avec une racine de l'unité ζ qui possède la propriété donnée dans 5°. (10_2) est équivalent dans les deux cas à (10_5).

Bibliographie

[1] A. Baker, Rational approximations to certain algebraic numbers, *Proc. London Math. Soc.* (3) **14** (1964), 385—398.

[2] A. Baker, Rational approximations to $\sqrt[3]{2}$ and other algebraic numbers, *Quart. J. Math. Oxford*, **15** (1964), 375—383.

[3] A. Baker, Simultaneous rational approximations to certain algebraic numbers, *Proc. Camb. Phil. Soc.* **63** (1967), 693—702.

[4] A. BAKER, Contributions to the theory of diophantine equations, *Philos. Trans. Roy. Soc. London, Ser. A.*, **263** (1968), 173—208.

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

[6] A. BAKER, A sharpening of the bounds for linear forms in logarithms II, *Acta Arith.*, **24** (1973), 33—36.

[7] A. BAKER, A sharpening of the bounds for linear forms in logarithms III, *Acta Arith.*, **27** (1975), 247—252.

[8] A. BAKER and J. COATES, Integer points on curves of genus 1, *Proc. Camb. Phil. Soc.* **67** (1970), 595—602.

[9] G. V. ČUDNOVSKIĬ, The Gelfond-Baker method in problems of diophantine approximation, *Coll. Math. Soc. János Bolyai*, **13**. *Topics in Number Theory* (*Ed. by* P. TURÁN), *Debrecen*, 1974, pp. 19—30. North Holland Publ. Comp., 1976.

[10] H. DAVENPORT and K. F. ROTH, Rational approximations to algebraic numbers, *Mathematika*, **2** (1955), 160—167.

[11] B. N. DELONE and D. K. FADDEEV, The theory of irrationalities of the third degree, (*Moscow*, 1940; *American Math. Soc., Transl. Math. Monographs*, **10**, 1964).

[12] V. A. DEMJANENKO, Tate height, and the representation of numbers by binary forms *(in Russian)*, *Izv. Akad. Nauk SSSR Ser. Mat.* **38** (1974), 459—470.

[13] N. I. FELDMAN, Effective bounds for the size of the solutions of certain diophantine equations *(in Russian)*, *Mat. Zametki* **8** (1970), 361—371.

[14] N. I. FELDMAN, Diophantine equations with a finite number of solutions *(in Russian)*, *Vestnik Moskov. Univ. Ser. I, Mat. Meh.* **26** (1971), 52—58.

[15] N. I. FELDMAN, An effective refinement of the exponent in Liouville's theorem *(in Russian)*, *Izv. Akad. Nauk SSSR* **35** (1971), 973—990.

[16] K. GYŐRY and L. LOVÁSZ, Representation of integers by norm-forms, II, *Publ. Math. (Debrecen)* **17** (1970), 173—181.

[17] K. GYŐRY, Sur l'irréductibilité d'une classe des polynômes I, *Publ. Math. (Debrecen)* **18** (1971), 289—307.

[18] K. GYŐRY, Investigations diophantiennes dans la théorie des polynômes irréductibles *(en hongrois)*, *Thèse, Debrecen*, 1972, pp. 172.

[19] K. GYŐRY, Sur une classe des corps de nombres algébriques et ses applications, *Publ. Math. (Debrecen)* **22** (1975), 151—175.

[20] D. J. LEWIS and K. MAHLER, On the representation of integers by binary forms, *Acta Arith.* **6** (1961), 333—363.

[21] K. MAHLER, Zur Approximation algebraischer Zahlen, III, Über die mittlere Anzahl der Darstellung grosser Zahlen durch binäre Formen, *Acta Math.* **62** (1933), 91—166.

[22] L. J. MORDELL, Diophantine equations, *London and New York*, 1969.

[23] T. NAGELL, L'analyse indéterminée de degré supérieur, *Mém. Sci. Math., Fasc.* **39**, *Paris*, 1929.

[24] T. NAGELL, Contributions à la théorie des corps et des polynômes cyclotomiques, *Arkiv för Mat.* **5** (1963), 153—192.

[25] T. NAGELL, Sur les représentations de l'unité par les formes binaires biquadratiques du premier rang, *Arkiv för Mat.* **5** (1965), 477—521.

[26] C. RUNGE, Über ganzzahlige Lösungen von Gleichungen zwischen zwei Veränderlichen, *J. Reine Angew. Math.* **100** (1887), 425—435.

[27] A. SCHINZEL, An improvement of Runge's theorem on diophantine equations, *Commentarii Pontif. Acad. Sci.*, **2**, No. **20** (1968), 1—9.

[28] W. M. SCHMIDT, Simultaneous approximation to algebraic numbers by rationals, *Acta Math.* **125** (1970), 189—201.

[29] C. L. SIEGEL, Approximation algebraischer Zahlen *Math. Z.* **10** (1921), 173—213. Voir encore: *Gesammelte Abhandlungen, I* (1966).

[30] C. L. SIEGEL, Die Gleichung $ax^n - by^n = c$, *Math Ann.*, **144** (1937), 57—68. Voir encore: *Gesammelte Abhandlungen, II* (1966).

[31] C. L. SIEGEL, Einige Erläuterungen zu Thues Untersuchungen über Annäherungswerte algebraischer Zahlen und diophantische Gleichungen, *Nachr. Akad. d. Wiss. Göttingen, Math. Phys. Kl., Nr.* **8**, 1970.

[32] TH. SKOLEM, Diophantische Gleichungen, *Berlin*, 1938.

[33] V. G. SPRINDŽUK, On an estimate for solutions of Thue's equation *(in Russian)*, *Izv. Akad. Nauk SSSR* **36** (1972), 712—741.

[34] H. M. Stark, Further advances in the theory of linear forms in logarithms, Diophantine approximations and its applications, pp. 255—294, *New York and London,* 1973.

[35] H. M. Stark, Effective estimates of solutions of some diophantine equations, *Acta Arith.* **24** (1973), 251—259.

[36] V. A. Tartakovskiĭ, Uniform bound for the number of representations of the unity by binary form of degree $n \geqq 3$ *(in Russian), Dokl. Akad. Nauk SSSR,* **193** (1970), 764.

[37] A. Thue, Über Annäherungswerte algebraischer Zahlen, J. *Reine Angew. Math.* **135** (1909), 284—305.

[38] W. J. LeVeque, Topics in number theory, *Reading, Massachusetts,* 1956.

(Reçu le 10 septembre 1975, modifié le 21 décembre 1976)