## Conspectus materiae tomi XXVI, fasciculi 2




La revue est consacrée à la Théorie des Nombres
The journal publishes papers on the Theory of Numbers
Die Zeitschrift veröffentlicht Arbeiten aus der Zahlentheorie
Журнал посвящен теории чисел

| L'adresse de la Rédaction et de l'échange | Address of the Editorial Board and of the exchange | Die Adresse der Schriftleitung und des Austausches | Адрес редакции и книгообмена |
|---|---|---|---|

ACTA ARITHMETICA
ul. Śniadeckich 8, 00-950 Warszawa

Les auteurs sont priés d'envoyer leurs manuscrits en deux exemplaires
The authors are requested to submit papers in two copies
Die Autoren sind gebeten um Zusendung von 2 Exemplaren jeder Arbeit
Рукописи статей редакция просит предлагать в двух экземплярах

PRINTED IN POLAND

WROCŁAWSKA DRUKARNIA NAUKOWA


ACTA ARITHMETICA
XXVI (1974)

# Formulas for some Diophantine approximation constants, II

by

T. W. Cusick (Buffalo, N. Y.)

**1. Introduction.** In the theory of simultaneous Diophantine approximation, there are two well known constants associated with each pair of real numbers $\alpha$, $\beta$. One constant, which I denote by $c_1(\alpha, \beta)$, is defined to be the infimum of those $c > 0$ such that the inequality

$$|x+\alpha y+\beta z|\max(y^2, z^2) < c$$

has infinitely many solutions in integers $x, y, z$ with $y$ and $z$ not both zero. The other constant, which I denote by $c_2(\alpha, \beta)$, is defined to be the infimum of those $c > 0$ such that the inequality

$$\max\left(|x|(\alpha x-y)^2,\ |x|(\beta x-z)^2\right) < c$$

has infinitely many solutions in integers $x, y, z$ with $x \neq 0$.

The constant $c_2(\alpha, \beta)$ is a measure of how well one can simultaneously approximate to $\alpha$ and $\beta$ with rational numbers having the same denominator. It is a well known unsolved problem to evaluate $C = \sup c_2(\alpha, \beta)$, where the supremum is taken over all pairs of real numbers $\alpha$, $\beta$. Davenport [5] showed that $C$ is equal to the dual constant $\sup c_1(\alpha, \beta)$, where the supremum is taken over all pairs of real numbers $\alpha$, $\beta$.

In an earlier paper, I gave explicit formulas for the constants $c_1(\alpha, \beta)$ and $c_2(\alpha, \beta)$, where $1, \alpha, \beta$ is an integral basis for a real cubic number field ([4], Theorem 1). If the field is totally real, these formulas are not valid in general; an extra hypothesis (see Theorem 3 below) is required. A similar modification is necessary in the totally real case in Theorem 2 of [4].

In the present paper I give corrected versions of the formulas for $c_1(\alpha, \beta)$ and $c_2(\alpha, \beta)$. The results apply whenever $1, \alpha, \beta$ is a basis for a real cubic field, so the restriction in [4] to the case where $\alpha$, $\beta$ are algebraic integers is removed.

Throughout this paper, if $\delta$ is an element of a real cubic field, then $\delta, \delta', \delta''$ are the conjugates of $\delta$. The norm $\delta\delta'\delta''$ of $\delta$ is denoted by $N(\delta)$.

## 2. Nontotally real cubic fields

THEOREM 1. *Suppose* $1, \alpha, \beta$ *is a basis for a nontotally real cubic number field* $F$. *Let* $M$ *denote the module with basis* $1, \alpha, \beta$ *and let* $D_M$ *denote the discriminant of* $M$. *Define*

$$\varkappa = \min\{|N(\delta)|:\ \delta \neq 0 \text{ in } M\} \tag{1}$$

*and define the binary quadratic form* $f(x, y)$ *by*

$$f(x, y) = \big((\beta'' - \beta)x + (\alpha - \alpha'')y\big)\big((\beta - \beta')x + (\alpha' - \alpha)y\big). \tag{2}$$

*Define* $c_1^*(\alpha, \beta)$ *by*

$$\frac{1}{c_1^*(\alpha, \beta)} = \max\big(|f(1, 1)|, |f(1, -1)|\big). \tag{3}$$

*Then*

$$c_1(\alpha, \beta) = \varkappa c_1^*(\alpha, \beta). \tag{4}$$

*Let* $M^*$ *denote the dual module of* $M$ *and define*

$$\tau = \min\{|D_M N(\delta)|:\ \delta \neq 0 \text{ in } M^*\}. \tag{5}$$

*Then*

$$c_2(\alpha, \beta) = \tau c_1^*(\alpha, \beta). \tag{6}$$

The proof of Theorem 1 follows the same general lines as the proof of Theorem 1 of [4], but the details are more complicated. We first observe that if $x + \alpha y + \beta z$ is small, then

$$\begin{aligned} \varkappa &\leqslant |(x + \alpha y + \beta z)(x + \alpha' y + \beta' z)(x + \alpha'' y + \beta'' z)| \\ &\approx \big|(x + \alpha y + \beta z)\big((\alpha' - \alpha)y + (\beta' - \beta)z\big)\big((\alpha'' - \alpha)y + (\beta'' - \beta)z\big)\big| \\ &= |(x + \alpha y + \beta z) f(z, -y)| \\ &\leqslant \max\big(\max_{|\mu| \leqslant 1} |f(\mu, 1)|, \max_{|\nu| \leqslant 1} |f(1, \nu)|\big)\, |x + \alpha y + \beta z| \max(y^2, z^2). \end{aligned} \tag{7}$$

The second inequality in (7) is obtained by taking $\mu = z/y$ if $\max(y^2, z^2) = y^2$ and $\nu = y/z$ if $\max(y^2, z^2) = z^2$.

Define $\mu_0$ and $\nu_0$ by

$$|f(\mu_0, 1)| = \max_{|\mu| \leqslant 1} |f(\mu, 1)|, \qquad |f(1, \nu_0)| = \max_{|\nu| \leqslant 1} |f(1, \nu)|.$$

Since the first inequality in (7) is an equality if and only if $|N(x + \alpha y + \beta z)| = \varkappa$, formula (4) follows from (7) *provided* that there exist numbers $x + \alpha y + \beta z$ in $M$ having arbitrarily small absolute value and norm $\pm\varkappa$, and having the property that the appropriate one of the following conditions holds: either $z/y$ is arbitrarily close to $-\mu_0$, or $y/z$ is arbitrarily close to $-\nu_0$. The following lemmas establish the existence of the desired numbers in $M$.



LEMMA 1. *Suppose* $1, \alpha, \beta$ *is a basis for a real cubic number field* $F$, *and let* $M$ *denote the module with basis* $1, \alpha, \beta$. *Let* $\varkappa$ *be defined by* (1). *There is a finite set* $\mu_1, \ldots, \mu_k$ *of elements of* $M$ *with norm* $\pm\varkappa$ *such that every solution* $\eta$ *in* $M$ *of one of the equations* $N(\eta) = \pm\varkappa$ *has the form*

$$\eta = \pm\mu_i \theta^m \tag{8}$$

*if* $F$ *is nontotally real, where* $1 \leqslant i \leqslant k$, $\theta$ *is a unit in the coefficient ring of* $M$ *and* $m$ *is an integer; or has the form*

$$\eta = \pm\mu_i \theta^m \varphi^n \tag{9}$$

*if* $F$ *is totally real, where* $1 \leqslant i \leqslant k$, $\theta$ *and* $\varphi$ *are multiplicatively independent units in the coefficient ring of* $M$ *and* $m, n$ *are integers. Conversely, every number* $\eta$ *of the appropriate form* (8) *or* (9) *is in* $M$ *and satisfies* $N(\eta) = \pm\varkappa$.

Proof. This is a special case of a well known general theorem about norm forms (see [2], Theorem 1, p. 118).

LEMMA 2. *Suppose* $1, \alpha, \beta$ *is a basis for a nontotally real cubic field, and let* $M$ *denote the module with basis* $1, \alpha, \beta$. *Let* $\varkappa$ *be defined by* (1). *Then given any* $\varepsilon > 0$, *both* $+1$ *and* $-1$ *are limit points of the set* $\{z/y:\ x + \alpha y + \beta z$ *is a number in* $M$ *with norm* $\pm\varkappa$ *and* $|x + \alpha y + \beta z| < \varepsilon\}$.

Proof. By (8) of Lemma 1, we can find a number $\mu$ in $M$ with norm $\pm\varkappa$ and a unit $\theta > 1$ in $M$ such that $\mu\theta^m$ is in $M$ and $N(\mu\theta^m) = \pm\varkappa$ for all integers $m$. Define for each integer $m$

$$\theta^m = a_m + \alpha b_m + \beta c_m \tag{10}$$

and

$$\mu\theta^m = x_m + \alpha y_m + \beta z_m.$$

We shall show that the set $\{z_m/y_m:\ m < 0\}$ has both $+1$ and $-1$ as limit points, which will prove the lemma since $|\mu\theta^m| \to 0$ as $m \to -\infty$.

If the matrix $A$ is defined by

$$A = \begin{bmatrix} \alpha' - \alpha & \beta' - \beta \\ \alpha'' - \alpha & \beta'' - \beta \end{bmatrix}, \tag{11}$$

then the matrix identity

$$\begin{bmatrix} b_m \\ c_m \end{bmatrix} = A^{-1} \begin{bmatrix} \theta'^m - \theta^m \\ \theta''^m - \theta^m \end{bmatrix} \tag{12}$$

holds. Expanding (12) gives (note $\det A = \pm D_M^{1/2}$, where $D_M$ is the discriminant of $M$)

$$\begin{aligned} \pm D_M^{1/2} b_m &= (\beta' - \beta'')\theta^m + (\beta'' - \beta)\theta'^m + (\beta - \beta')\theta''^m, \\ \pm D_M^{1/2} c_m &= (\alpha'' - \alpha')\theta^m + (\alpha - \alpha'')\theta'^m + (\alpha' - \alpha)\theta''^m. \end{aligned} \tag{13}$$

For brevity, we introduce new symbols $r_i$ and $s_i$ for the coefficients in (13), so we have

$$(14)\qquad \begin{aligned} b_m &= r_1\theta^m + r_2\theta'^m + r_3\theta''^m,\\ c_m &= s_1\theta^m + s_2\theta'^m + s_3\theta''^m. \end{aligned}$$

Now let $Q(\mu) = (q_{ij})$ $(1 \leqslant i, j \leqslant 3)$ denote the matrix with the property

$$(15)\qquad \begin{bmatrix} 1 & \alpha & \beta \\ 1 & \alpha' & \beta' \\ 1 & \alpha'' & \beta'' \end{bmatrix} \begin{bmatrix} q_{11} & q_{12} & q_{13} \\ q_{21} & q_{22} & q_{23} \\ q_{31} & q_{32} & q_{33} \end{bmatrix} = \begin{bmatrix} \mu & \mu\alpha & \mu\beta \\ \mu' & \mu'\alpha' & \mu'\beta' \\ \mu'' & \mu''\alpha'' & \mu''\beta'' \end{bmatrix}.$$

It follows immediately from (15) that the determinant of $Q(\mu)$ satisfies

$$(16)\qquad \det Q(\mu) = N(\mu) \neq 0.$$

We also clearly have

$$(17)\qquad \begin{bmatrix} x_m \\ y_m \\ z_m \end{bmatrix} = Q(\mu) \begin{bmatrix} a_m \\ b_m \\ c_m \end{bmatrix}$$

for each integer $m$. It follows from (10), (14) and (17) that

$$(18)\qquad \frac{z_m}{y_m} = \frac{S_1\theta^m + S_2\theta'^m + S_3\theta''^m}{R_1\theta^m + R_2\theta'^m + R_3\theta''^m}$$

where

$$(19)\qquad \begin{aligned} R_1 &= q_{21} + (q_{22} - \alpha q_{21})r_1 + (q_{23} - \beta q_{21})s_1,\\ S_1 &= q_{31} + (q_{32} - \alpha q_{31})r_1 + (q_{33} - \beta q_{31})s_1,\\ R_2 &= (q_{22} - \alpha q_{21})r_2 + (q_{23} - \beta q_{21})s_2,\\ S_2 &= (q_{32} - \alpha q_{31})r_2 + (q_{33} - \beta q_{31})s_2,\\ R_3 &= (q_{22} - \alpha q_{21})r_3 + (q_{23} - \beta q_{21})s_3,\\ S_3 &= (q_{32} - \alpha q_{31})r_3 + (q_{33} - \beta q_{31})s_3. \end{aligned}$$

Now (18) implies that

$$(20)\qquad \frac{z_m}{y_m} - \frac{(\theta'/\theta'')^m S_2 + S_3}{(\theta'/\theta'')^m R_2 + R_3} \to 0$$

as $m \to -\infty$, since $\theta > 1$ and $|\theta'| = |\theta''| < 1$. We have

$$(21)\qquad \det\begin{bmatrix} S_2 & S_3 \\ R_2 & R_3 \end{bmatrix} = \det\begin{bmatrix} q_{33} - \beta q_{31} & q_{32} - \alpha q_{31} \\ q_{23} - \beta q_{21} & q_{22} - \alpha q_{21} \end{bmatrix} \det\begin{bmatrix} s_2 & s_3 \\ r_2 & r_3 \end{bmatrix}.$$

A calculation shows that the second determinant on the right of (21) is equal to $\pm D_M^{-1/2}$, where $D_M$ is the discriminant of $M$ and so is not zero.



If the first determinant on the right of (21) were zero, then its first row would be a multiple of its second row, so that the third row of the matrix $Q(\mu)$ would be a multiple of its second row, contradicting (16). Hence $S_2R_3 - S_3R_2 \neq 0$.

A little calculation shows that the complex numbers $z$ which satisfy $(S_2 z + S_3)/(R_2 z + R_3) = \pm 1$ must also satisfy $|z| = 1$. The number $\theta'/\theta''$ has absolute value 1 and obviously cannot be a root of unity, so the numbers $(\theta'/\theta'')^m$, $m$ a negative integer, are dense on the circle $|z| = 1$ in the complex plane. These facts in conjunction with (20) and the fact that $S_2R_3 - S_3R_2 \neq 0$ prove Lemma 2.

Lemma 2 proves formula (4), because $f(x, y)$ is a definite form if and only if $F$ is nontotally real (for it is easily seen that the discriminant of $f(x, y)$ is equal to the discriminant $D_M$ of $M$), and for such forms $f(x, y)$ we have $\mu_0 = \pm 1$ and $\nu_0 = \pm 1$.

We need some more notation for the proof of (6). A basis $\delta_0, \delta_1, \delta_2$ for the dual module $M^*$ is defined by

$$(22)\qquad \delta_0 + \delta_1\alpha + \delta_2\beta = 1,\ \delta_0 + \delta_1\alpha' + \delta_2\beta' = 0,\ \delta_0 + \delta_1\alpha'' + \delta_2\beta'' = 0,$$

so we have

$$(23)\qquad \delta_0 = \frac{\alpha'\beta'' - \alpha''\beta'}{\det A},\qquad \delta_1 = \frac{\beta' - \beta''}{\det A},\qquad \delta_2 = \frac{\alpha'' - \alpha'}{\det A}$$

where $A$ is defined by (11). For each positive real number $r$, define the open square $B_r$ in the $x-y$ plane by

$$B_r = \{(x, y)\colon \max(|x|, |y|) < r\}.$$

The proof of (6) depends on the following lemma.

Lemma 3. *Suppose $1, \alpha, \beta$ is a basis for a real cubic number field $F$. Let $M$ denote the module with basis $1, \alpha, \beta$ and let $M^*$ denote its dual module. Let $D_M$ denote the discriminant of $M$. Then $c_2(\alpha, \beta) = \inf\{r^2$: for some $\delta \neq 0$ in $M^*$, the curve $D_M^{-1}f(x, y) = N(\delta)$ intersects $B_r\}$.*

Proof. This is a theorem of Adams ([1], Proposition 3, p. 10). The basis whose existence is asserted in [1] (Lemma 1, pp. 8–9) is here taken to be the dual basis, so $\varkappa_0$ in that lemma is 1. This gives our lemma as stated; note that it follows from (23) that the form $Z(x, y)$ defined by Adams ([1], p. 9) is the same as $D_M^{-1}f(x, y)$, where $f(x, y)$ is defined by (2).

The curves $f(x, y) = D_M N(\delta)$, $\delta$ in $M^*$, form a discrete set of nonintersecting curves, which are all ellipses if $F$ is nontotally real. Since for any real number $s$, $f(sx, sy) = s^2 f(x, y)$, it is clear that

$$\inf\{r^2\colon f(x, y) = \pm s \text{ intersects } B_r\} = s\inf\{r^2\colon f(x, y) = \pm 1 \text{ intersects } B_r\}.$$

In particular, this holds if $s = \tau$, where $\tau$ is defined by (5). Therefore it follows from (3) and Lemma 3 that (6) holds if we can show:

LEMMA 4. *Let $g(x, y)$ denote any binary quadratic form. Then*

(24) $$\inf\{r^2: g(x,y) = \pm 1 \text{ intersects } B_r\} = 1/\max\left(\max_{|x|\leqslant 1}|g(x,1)|, \max_{|y|\leqslant 1}|g(1,y)|\right).$$

Proof. Suppose that the infimum on the left hand side of (24) occurs for $r = r_0$, and suppose that $|g(x_0, y_0)| = 1$, $\max(|x_0|, |y_0|) = r_0$.

Now let

$$M_1 = \max_{|x|\leqslant 1}|g(x,1)|, \quad M_2 = \max_{|y|\leqslant 1}|g(1,y)|$$

and suppose that the maxima occur for $x = x_1$ and $y = y_1$, respectively. Then $1 = |g(x_1M_1^{-1/2}, M_1^{-1/2})|$ and $1 = |g(M_2^{-1/2}, y_1M_2^{-1/2})|$, so we must have $r_0^2 \leqslant \min(M_1^{-1}, M_2^{-1})$. In fact, equality must hold; for if $|x_0| = r_0$, then $|g(1, y_0x_0^{-1})| = r_0^{-2} \leqslant M_2$, and similarly if $|y_0| = r_0$, then $r_0^{-2} \leqslant M_1$. This proves (24).

Now (6) is proved by taking $g(x, y) = f(x, y)$ in Lemma 4. This completes the proof of Theorem 1. Note that if $1, \alpha, \beta$ is an *integral* basis for $F$, then $\varkappa = 1$ and Theorem 1 is the same as the nontotally real case of [4], Theorem 1.

**3. Totally real cubic fields.** We shall require the following notation. Let $\alpha_0, \alpha_1, \alpha_2$ be a basis for a totally real cubic number field, and let $M$ be the module with basis $\alpha_0, \alpha_1, \alpha_2$. Define

$$m_+(M) = \inf_{\substack{\xi \text{ in } M, \xi>0 \\ N(\xi)>0}} N(\xi) \quad \text{and} \quad m_-(M) = \inf_{\substack{\xi \text{ in } M, \xi>0 \\ N(\xi)<0}} |N(\xi)|$$

(these definitions were introduced by Adams [1], p. 1), and define $m_+(M^*)$ and $m_-(M^*)$ analogously for the dual module $M^*$ of $M$.

If $1, \alpha, \beta$ is a basis for a totally real cubic number field, define the binary quadratic form $f(x, y)$ by (2). Define the sets $U, U^{-1}, V, V^{-1}$ by

$$U = \{x: |x| \leqslant 1 \text{ and } f(x,1) \geqslant 0\}, \quad U^{-1} = \{y: |y| \leqslant 1 \text{ and } f(1,y) \geqslant 0\}$$

and

$$V = \{x: |x| \leqslant 1 \text{ and } f(x,1) \leqslant 0\}, \quad V^{-1} = \{y: |y| \leqslant 1 \text{ and } f(1,y) \leqslant 0\}.$$

Define the numbers $f_U$ and $f_V$ by

$$f_U = \max\left(\max_{\substack{|x|\leqslant 1\\ x \text{ in } U}} f(x,1), \max_{\substack{|y|\leqslant 1\\ y \text{ in } U^{-1}}} f(1,y)\right)$$

and

$$f_V = \max\left(\max_{\substack{|x|\leqslant 1\\ x \text{ in } V}} |f(x,1)|, \max_{\substack{|y|\leqslant 1\\ y \text{ in } V^{-1}}} |f(1,y)|\right).$$

Now the result for totally real cubic fields can be stated as follows:

THEOREM 2. *Suppose $1, \alpha, \beta$ is a basis for a totally real cubic number field $F$. Let $M$ denote the module with basis $1, \alpha, \beta$ and let $D_M$ denote the discriminant of $M$. Define the binary quadratic form $f(x, y)$ by (2). Then*

(25) $$c_1(\alpha, \beta) = \min\left(\frac{m_+(M)}{f_V}, \frac{m_-(M)}{f_U}\right)$$

*and*

(26) $$c_2(\alpha, \beta) = \min\left(\frac{D_M m_+(M^*)}{f_U}, \frac{D_M m_-(M^*)}{f_V}\right).$$



We begin the proof of Theorem 2 with (7); the reasoning that led to (7) in the nontotally real case still applies in the totally real case if $x + \alpha y + \beta z$ is small. However, the equality

(27) $$\sup_{y,z} \frac{|f(z, -y)|}{\max(y^2, z^2)} = \frac{1}{c_1^*(\alpha, \beta)},$$

where the supremum is taken over all pairs $y, z$ such that $x + \alpha y + \beta z$ in $M$ has absolute value less than any preassigned arbitrarily small positive number and $N(x + \alpha y + \beta z) = \pm\varkappa$ ($\varkappa$ defined by (1)), does not hold in the totally real case, in general; hence formula (4) is not valid for the totally real case. Formula (27) (which in the nontotally real case is essentially another way of stating Lemma 2) has to be replaced by the following result:

LEMMA 5. *Suppose $1, \alpha, \beta$ is a basis for a totally real cubic number field $F$. Let $M$ denote the module with basis $1, \alpha, \beta$. Define the binary quadratic form $f(x, y)$ by (2). If $m_+(M) = m_-(M)$, then (27) holds. If $m_+(M) \neq m_-(M)$, then*

(28) $$\sup_{f(z,-y)>0} \frac{f(z, -y)}{\max(y^2, z^2)} = f_U$$

*and*

(29) $$\sup_{f(z,-y)<0} \frac{|f(z, -y)|}{\max(y^2, z^2)} = f_V,$$

*where the suprema in (28) and (29) are taken over all pairs $y, z$ such that $f(z, -y) > 0$ or $f(z, -y) < 0$, respectively, and such that $x + \alpha y + \beta z > 0$ in $M$ has value less than any preassigned arbitrarily small positive number and $N(x + \alpha y + \beta z)$ is $m_+(M)$ or $-m_-(M)$, respectively.*

Proof. We shall require some auxiliary results from my earlier paper [3]. Firstly, by (9) of Lemma 1 we can find a number $\mu > 0$ in $M$ with norm $m_+(M)$ and multiplicatively independent units $\theta, \varphi$ in the coefficient ring of $M$ such that $\mu\theta^m\varphi^n$ is in $M$ and $N(\mu\theta^m\varphi^n) = \pm m_+(M)$ for all integers $m$ and $n$. Furthermore, by [3], Lemma 9, p. 176, we may assume without loss of generality that $\varphi > 0$ and

(30) $$N(\theta) = 1, \quad \theta > 1, \quad |\theta'| < 1, \quad |\theta''| > \theta.$$

Define for each integer pair $m, n$

$$\theta^m\varphi^n = a_{mn}+\alpha b_{mn}+\beta c_{mn} \tag{31}$$

and

$$\mu\theta^m\varphi^n = x_{mn}+\alpha y_{mn}+\beta z_{mn}.$$

We note that $\mu\theta^m\varphi^n > 0$ for all $m, n$.

If the matrix $A$ is defined by (11), then the matrix identity

$$\begin{bmatrix} b_{mn} \\ c_{mn} \end{bmatrix} = A^{-1}\begin{bmatrix} \theta'^m\varphi'^n - \theta^m\varphi^n \\ \theta''^m\varphi''^n - \theta^m\varphi^n \end{bmatrix}$$

holds. Expanding this identity gives

$$\begin{aligned} b_{mn} &= r_1\theta^m\varphi^n + r_2\theta'^m\varphi'^n + r_3\theta''^m\varphi''^n, \\ c_{mn} &= s_1\theta^m\varphi^n + s_2\theta'^m\varphi'^n + s_3\theta''^m\varphi''^n, \end{aligned} \tag{32}$$

where the numbers $r_i$ and $s_i$ are defined by (13) and (14). We also have

$$\begin{bmatrix} x_{mn} \\ y_{mn} \\ z_{mn} \end{bmatrix} = Q(\mu)\begin{bmatrix} a_{mn} \\ b_{mn} \\ c_{mn} \end{bmatrix} \tag{33}$$

for each integer pair $m, n$, where the matrix $Q(\mu)$ is defined by (15), and (16) holds as before.

For any integer $n$, define $u(n)$ to be that value of $m$ satisfying

$$\big||\theta'^{u(n)}\varphi'^n/\theta''^{u(n)}\varphi''^n|-1\big| \leqslant \big||\theta'^m\varphi'^n/\theta''^m\varphi''^n|-1\big| \quad \text{for all integers } m;$$

that is, $u(n)$ is the value of $m$ for which $|\theta'^m\varphi'^n/\theta''^m\varphi''^n|$ is nearest to 1. Let $E(n)$ denote $\theta'^{u(n)}\varphi'^n/\theta''^{u(n)}\varphi''^n$. Note that if $N(\varphi) = +1$, then $E(n) = (\theta\theta'^2)^{u(n)}(\varphi\varphi'^2)^n$ is *positive for all integers* $n$, but if $N(\varphi) = -1$ then $E(n)$ is *positive if and only if $n$ is even*. Also, if $m_+(M) \neq m_-(M)$, then $N(\varphi) = +1$; for if $N(\varphi) = -1$, then $\varphi$ is a positive unit with negative norm, and the existence of such a unit in the coefficient ring of $M$ of course implies $m_+(M) = m_-(M)$.

We first consider the case $m_+(M) \neq m_-(M)$, so $N(\varphi) = +1$ and $E(n) > 0$ for all $n$. We now take $m = u(n)+j$, where $j$ is a fixed integer to be chosen later. It follows from (31), (32) and (33) that

$$\frac{z_{u(n)+j,n}}{y_{u(n)+j,n}} = \frac{S_1(\theta/\theta'')^{u(n)+j}(\varphi/\varphi'')^n + S_2E(n)(\theta'/\theta'')^j + S_3}{R_1(\theta/\theta'')^{u(n)+j}(\varphi/\varphi'')^n + R_2E(n)(\theta'/\theta'')^j + R_3} \tag{34}$$

where the numbers $R_i$ and $S_i$ are defined by (19). It was proved in [3] (Lemma 5 Corollary, p. 171), using (30), that

$$\lim_{n\to\pm\infty} u(n)/n = -\log|\varphi\varphi'^2|/\log\theta\theta'^2.$$



Therefore if we let $n\to+\infty$ or $n\to-\infty$ with the sign chosen in such a way that $u(n)\log\theta+n\log|\varphi|\to-\infty$, then $\theta^{u(n)+j}\varphi^n\to 0$. It follows from (34) that for any choice of $j$

$$\frac{z_{u(n)+j,n}}{y_{u(n)+j,n}} - \frac{S_2E(n)(\theta'/\theta'')^j+S_3}{R_2E(n)(\theta'/\theta'')^j+R_3} \to 0 \tag{35}$$

as $|n|\to\infty$ in the appropriate (positive or negative) direction.

We know $S_2R_3-S_3R_2 \neq 0$ from the proof of Lemma 2. It is easily seen that $E(n)$ satisfies

$$\frac{2}{1+\theta\theta'^2} > E(n) > \frac{2\theta\theta'^2}{1+\theta\theta'^2} \tag{36}$$

for every $n$ (see [3], formula (17), p. 170). Using the facts that $\theta'/\theta'' = \theta\theta'^2$ and that $E(n)$ is dense in the interval defined by (36) (which follows easily from Kronecker's Diophantine approximation theorem), we see that for a suitable choice of $j$ and $n$ we can make $E(n)(\theta'/\theta'')^j$ arbitrarily near to any positive real number. Thus (35) implies that as $j$ and $n$ vary, the set of limit points of the values of $-z_{u(n)+j,n}/y_{u(n)+j,n}$ is just the set $S$ defined by

$$S = \{-(S_2x+S_3)/(R_2x+R_3)\colon\ x \geqslant 0\}.$$

Thus in order to prove (29) it suffices to show that the set $S$ is the same as the set $\{x\colon f(x,1)\leqslant 0\}$ (note that in (7) we have

$$\big((\alpha'-\alpha)y+(\beta'-\beta)z\big)\big((\alpha''-\alpha)y+(\beta''-\beta)z\big) = -f(z,-y);$$

thus we must have $f(z,-y) < 0$ in order to have $N(x+\alpha y+\beta z) = m_+(M)$ and $x+\alpha y+\beta z > 0$). The first step in showing this is the observation that

$$\frac{S_2}{R_2} = \frac{s_2}{r_2} \quad\text{and}\quad \frac{S_3}{R_3} = \frac{s_3}{r_3} \tag{37}$$

(the numbers $r_i$ and $s_i$ are defined by (13) and (14)). A simple calculation shows that (21) and (37) hold if and only if the equalities

$$\frac{q_{32}-\alpha q_{31}}{q_{23}-\beta q_{21}} = -\frac{s_2s_3}{r_2r_3} \quad\text{and}\quad \frac{q_{33}-\beta q_{31}-q_{22}+\alpha q_{21}}{q_{23}-\beta q_{21}} = \frac{s_2}{r_2}+\frac{s_3}{r_3} \tag{38}$$

are true, whatever the choice of the $q_{ij}$.

One way to prove (38) is as follows: Elementary row and column manipulations applied to (15) give

$$\begin{bmatrix} 0 & s_2 & -r_2 \\ 0 & s_3 & -r_3 \\ 1 & \alpha'' & \beta'' \end{bmatrix}\begin{bmatrix} q_{11} & q_{12}-\alpha q_{11} & q_{13}-\beta q_{11} \\ q_{21} & q_{22}-\alpha q_{21} & q_{23}-\beta q_{21} \\ q_{31} & q_{32}-\alpha q_{31} & q_{33}-\beta q_{31} \end{bmatrix} = \begin{bmatrix} \mu-\mu'' & s_2\mu'' & -r_2\mu'' \\ \mu'-\mu & s_3\mu' & -r_3\mu' \\ \mu'' & -s_2\mu'' & r_2\mu'' \end{bmatrix} \tag{39}$$

and this matrix equality implies

$$
(40)\qquad \begin{aligned} s_3(q_{22}-\alpha q_{21})-r_3(q_{32}-\alpha q_{31}) &= s_3\mu', \\ s_2(q_{23}-\beta q_{21})-r_2(q_{33}-\beta q_{31}) &= -r_2\mu'', \\ s_3(q_{23}-\beta q_{21})-r_3(q_{33}-\beta q_{31}) &= -r_3\mu'. \end{aligned}
$$

Using the first and second equations in (40), we see that the first equality in (38) holds if and only if

$$
(41)\qquad q_{22}+q_{33} = \mu'+\mu''+\alpha q_{21}+\beta q_{31}.
$$

Similarly, using the second and third equations in (40), we see that the second equality in (38) holds if and only if (41) is true. Now $\mu = q_{11}+ +\alpha q_{21}+\beta q_{31}$ by (15), so (41) reduces to $q_{11}+q_{22}+q_{33} = \mu+\mu'+\mu''$, which is true since $\mu$ is an eigenvalue of $Q(\mu)$ by (15). This proves (37).

Let $I$ denote the half-open interval with endpoints $-S_2/R_2$ and $-S_3/R_3$, the latter being in $I$ but the former not. Then the definition of $S$ implies

$$
(42)\qquad S = \begin{cases} (-\infty, +\infty) \text{ except } I & \text{if } R_2R_3 < 0, \\ I & \text{if } R_2R_3 > 0. \end{cases}
$$

Now (39) gives

$$
\det\begin{bmatrix} s_2 & -r_2 \\ s_3 & -r_3 \end{bmatrix} = \det\begin{bmatrix} q_{22}-\alpha q_{21} & q_{23}-\beta q_{21} \\ q_{32}-\alpha q_{31} & q_{33}-\beta q_{31} \end{bmatrix} \det\begin{bmatrix} s_3\mu' & -r_3\mu' \\ -s_2\mu'' & r_2\mu'' \end{bmatrix}
$$

so the middle determinant in (21) is equal to $1/\mu'\mu'' > 0$. Hence (21) and (37) imply that $R_2R_3$ and $r_2r_3$ have the same sign. Since $-s_2/r_2$ and $-s_3/r_3$ are the roots of

$$
f(x, 1) = (r_2x+s_2)(r_3x+s_3) = 0,
$$

it follows from (37) and (42) that $S = \{x\colon f(x,1) \leqslant 0\}$. This proves (29).

A proof analogous to the above, but beginning with a number $\mu > 0$ in $M$ with norm $-m_-(M)$, establishes (28).

Now we consider the case $m_+(M) = m_-(M)$; thus there is a positive unit with norm $-1$ in $M$. If such a unit belongs to the coefficient ring of $M$, then by (9) of Lemma 1 we can find a number $\mu$ in $M$ with norm $m_+(M)$ and multiplicatively independent units $\theta, \varphi$ in the coefficient ring of $M$ such that (30) holds, $\varphi > 0$, $N(\varphi) = -1$, and $\mu\theta^m\varphi^n$ is in $M$ with $N(\mu\theta^m\varphi^n) = \pm m_+(M)$ for all integers $m$ and $n$. Now (35) is derived as before, and we find that both $E(n)$ and $-E(n)$ are dense in the interval defined by (36). Hence as $j$ and $n$ vary, the set of limit points of the values of $-z_{u(n)+j,n}/y_{u(n)+j,n}$ is $(-\infty, +\infty)$; therefore (27) holds. Even if there is no positive unit with norm $-1$ in the coefficient ring of $M$, (27) still



holds because $\max(f_U, f_V) = 1/c_1^*(\alpha, \beta)$. This completes the proof of Lemma 5.

Now (25) follows immediately from Lemma 5 and (7) (with $\varkappa$ replaced in turn by $m_+(M)$ and $m_-(M)$). The proof of (26) depends on the following lemma, which is very similar to Lemma 4:

LEMMA 6. *Let $g(x, y)$ denote any indefinite binary quadratic form. Then*

$$
\inf\{r^2\colon g(x,y) = +1 \text{ intersects } B_r\} = f_U^{-1}
$$

*and*

$$
\inf\{r^2\colon g(x,y) = -1 \text{ intersects } B_r\} = f_V^{-1}.
$$

Proof. The proof exactly parallels that of Lemma 4.

Now (26) follows at once from Lemmas 3 and 6. This completes the proof of Theorem 2.

The following special case of Theorem 2 is of particular interest.

THEOREM 3. *Suppose $1, \alpha, \beta$ is an integral basis for a totally real cubic number field $F$. Let $M$ denote the module with basis $1, \alpha, \beta$ and let $D$ denote the discriminant of $M$ and $F$. Suppose $m_+(M) = m_-(M) = 1$. Define the binary quadratic form $f(x, y)$ by (2) and define $c_1^*(\alpha, \beta)$ by (3). Then*

$$
c_1(\alpha, \beta) = c_1^*(\alpha, \beta).
$$

*Let $M^*$ denote the dual module of $M$ and let*

$$
\tau = \min\{|DN(\delta)|\colon \delta \neq 0 \text{ in } M^*\}.
$$

*Then*

$$
c_2(\alpha, \beta) = \tau c_1^*(\alpha, \beta).
$$

Proof. The theorem is an immediate corollary of Theorem 2 if $m_+(M^*) = m_-(M^*)$. But the hypothesis $m_+(M) = m_-(M) = 1$ implies $m_+(M^*) = m_-(M^*)$, for $M$ is the set of all algebraic integers in $F$ and so $M$ is equal to its coefficient ring. Since $M$ and $M^*$ have the same coefficient ring ([2], Exercise 14, p. 94), there is a positive unit of norm $-1$ in $M^*$, and this implies $m_+(M^*) = m_-(M^*)$.

Theorem 3 is just the totally real case of [4], Theorem 1, with the needed extra hypothesis $m_+(M) = m_-(M)$. Under this extra hypothesis for the totally real case, the corollaries of [4], p. 187, are also valid.

## References


[1] W. W. Adams, *Simultaneous diophantine approximations and cubic irrationals*, Pac. J. Math. 30 (1969), pp. 1–14.

[2] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, New York 1966.

[3] T. W. Cusick, *Diophantine approximation of ternary linear forms*, Math. Comp. 25 (1971), pp. 163–180.
[4] — *Formulas for some Diophantine approximation constants*, Math. Ann. 197 (1972), pp. 182–188.
[5] H. Davenport, *On a theorem of Furtwängler*, J. London Math. Soc. 30 (1955), pp. 186–195.

DEPARTMENT OF MATHEMATICS
STATE UNIVERSITY OF NEW YORK AT BUFFALO
Buffalo, New York

*Received on 15. 2. 1973* (386)

ACTA ARITHMETICA
XXVI (1974)

# Multiplication par un entier d'une fraction continue périodique

par

Henri Cohen (Talence)

**§ 1. Introduction et notations.** Soit $x$ un nombre rationnel. Il possède deux développements en fraction continue:

$$x = [a_0, \ldots, a_n] = [a_0, \ldots, a_n - 1, 1],$$

où $a_i \geqslant 1$ pour $i \geqslant 1$ et $a_n \geqslant 2$.

Nous poserons $\Psi(x) = n$; soit $L(x)$ le nombre de termes de la fraction continue représentant $x$ de longueur impaire, et soit $[[x]]$ cette fraction continue. On a donc $L(x) = \Psi(x) + 1 + \varepsilon(\Psi(x))$ où $\varepsilon(n) = (1-(-1)^n)/2$. Remarquons pour la suite que $\Psi$ et $L$ sont des fonctions définies sur $\boldsymbol{Q}/\boldsymbol{Z}$.

Soit maintenant $x$ un nombre quadratique, c'est-à-dire une racine réelle non rationnelle d'une équation du second degré à coefficients entiers. Le développement en fraction continue de $x$ est périodique, et on écrira:

$$x = [b_0, b_1, \ldots, b_m, \overline{a_1, \ldots, a_n}] \quad \text{avec } a_i, b_i \geqslant 1 \text{ pour } i \geqslant 1$$

$(b_0, \ldots, b_m)$ est la partie non périodique et $(a_1, \ldots, a_n)$ la période.

Nous poserons $P(x) = n$; si on écrit

$$[a_1, \ldots, a_n] = \alpha/\gamma, \quad [a_1, \ldots, a_{n-1}] = \beta/\delta$$

avec $(\alpha, \gamma) = (\beta, \delta) = 1$; $\gamma, \delta \geqslant 0$, on a $\alpha\delta - \beta\gamma = (-1)^n$ et la matrice $M = \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} \in \mathrm{GL}_2(\boldsymbol{Z})$ sera appelée la matrice du nombre quadratique $x$, ou encore la matrice de la période $(a_1, \ldots, a_n)$ ou de la fraction continue $[a_1, \ldots, a_n]$.

Soit $N > 1$ un entier. Dans [4] M. Mendès France démontre que:

$$\sup_{x\in\boldsymbol{Q}} \big(\Psi(Nx)/\Psi(x)\big) = \sup_{0\leqslant i<N} L(i/N)$$

et il trouve même plus précisément la valeur de $\sup\limits_{\Psi(x)=n} \Psi(Nx)$.