Séminaire Delange-Pisot-Poitou.
Théorie des nombres

JACQUELINE SAUVAGEOT

Algorithmes d'Euclide dans certains corps biquadratiques

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 14, n° 1 (1972-1973), exp. n° 15, p. 1-3

<http://www.numdam.org/item?id=SDPP_1972-1973__14_1_A13_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
14e année, 1972/73, n° 15, 3 p.

26 février 1973

ALGORITHMES D'EUCLIDE DANS CERTAINS CORPS BIQUADRATIQUES

par Jacqueline SAUVAGEOT

Soient K un corps de nombres, algébrique sur $\mathbb{Q}$, et $\mathcal{O}_K$ l'anneau des entiers de K ; on dit que K admet un algorithme d'Euclide si l'énoncé suivant est vrai $\xi \in K$; $e \in \mathcal{O}_K$; $N_{K/\mathbb{Q}}$ est la norme de l'extension

$$\forall\, \xi\,,\ \exists\, e\,,\ |N_{K/\mathbb{Q}}(\xi - e)| < 1\ .$$

On sait quels corps quadratiques sont euclidiens. La question reste ouverte pour les corps biquadratiques. Elle devrait être bientôt (?) résolue pour ceux d'entre eux qui sont bicycliques imaginaires, c'est-à-dire pour les extensions K de $\mathbb{Q}$ de la forme

$$\mathbb{Q}(\sqrt{a_1\, a_2}\ ,\ i\sqrt{a_1\, b}\ ,\ i\sqrt{a_2\, b})$$

avec a_1 , a_2 et b entiers naturels non nuls, sans facteur carré et deux à deux premiers entre eux.

I

En effet, R. B. LAKEIN dans [1] a publié un catalogue de trente corps biquadratiques euclidiens, extensions quadratiques des corps $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-3})$ ou $\mathbb{Q}(\sqrt{-7})$, sans se limiter au cas des extensions bicycliques puisqu'il établit une condition suffisante sur la norme du discriminant relatif. Parmi eux, huit corps sont bicycliques

$\mathbb{Q}(i\ ;\sqrt{3})$; $\mathbb{Q}(i\ ,\sqrt{5})$; $\mathbb{Q}(i\ ;\sqrt{7})$

$\mathbb{Q}(i\sqrt{3}\ ,\sqrt{5})$; $\mathbb{Q}(i\sqrt{3}\ ,\ i\sqrt{7})$; $\mathbb{Q}(i\sqrt{3}\ ,\sqrt{2})$; $\mathbb{Q}(i\sqrt{3}\ ,\ i\sqrt{2})$; $\mathbb{Q}(i\sqrt{3}\ ,\ i\sqrt{11})$.

II

On peut d'autre part établir qu'un grand nombre de corps K de ce type ne sont pas euclidiens en mettant en évidence un élément ξ_0 de K tel que

$$\forall\, e \in \mathcal{O}_K\ ,\ |N_{K/\mathbb{Q}}(\xi_0 - e)| \geqslant 1\ .$$

La norme, toujours positive puisque le corps K est imaginaire, d'un élément ξ de K tel que

$$\xi = x + y\sqrt{a_1\, a_2} + iz\sqrt{a_1\, b} + it\sqrt{a_2\, b}\ ,\qquad x\ ,\ y\ ,\ z\ ,\ t \in \mathbb{Q}$$

peut s'écrire sous une des trois formes équivalentes suivantes :

(I) $N(\xi) = (x^2 - a_1\, bz^2 - a_1\, a_2\, y^2 + a_2\, bt^2)^2 + 4a_1\, b(xz - a_2\, yt)^2$

(I bis) $N(\xi) = (x^2 - a_2\, bt^2 - a_1\, a_2\, y^2 + a_1\, bz^2)^2 + 4a_2\, b(xt - a_1\, yz)^2$

(II) $N(\xi) = b^2(x_1\, z^2 - a_2\, t^2)^2 + 2a_1\, b(xz - a_2\, yt)^2 + 2a_2\, b(xt - a_1\, yz)^2 + (x^2 - a_1\, a_2\, y^2)^2$.

La base du $\underset{\sim}{Z}$-module $\mathcal{O}_K$ dépend, comme dans le cas quadratique, des classes modulo 4 des entiers a_1, a_2 et b, ce qui amène à distinguer trois catégories de corps, dans le cas où a_1, a_2 et b sont tous impairs (le cas où un des nombres est pair ne sera pas examiné ici).

1°) $a_1 a_2 \equiv +1 \ (4)$; $-a_1 b \equiv -a_2 b \equiv -1 \ (4)$.

Alors les entiers e de K sont de la forme

$$(1) \qquad \frac{X + Y\sqrt{a_1 a_2} + iZ\sqrt{a_1 b} + iT\sqrt{a_2 b}}{2} \quad \text{avec} \quad \begin{cases} X \equiv Y \ (2) \\ Z \equiv T \ (2) \end{cases}$$

N. B. - Ici, comme dans toute la suite, les lettres X, Y, Z, T désigneront des entiers relatifs.

Soit ξ_0 le nombre $(1 + i\sqrt{a_1 b})/2$; les nombres $(\xi - e)$, avec $e \in \mathcal{O}_K$, sont de la forme (1) mais avec $X \not\equiv Y \ (2)$ et $Z \not\equiv T \ (2)$, un des nombres, $XZ - a_2 YT$ ou $XT - a_1 YZ$, est impair, et la norme de $\xi_0 - e$ vaut au moins $4a_1 b(\frac{1}{4})^2$ ou $4a_2 b(\frac{1}{4})^2$ (formes I). Pour que K soit euclidien, il faut donc qu'un des deux nombres, $a_1 b$ ou $a_2 b$, soit inférieur à 4. Puisqu'on a $a_i b \equiv 1 \ (4)$, il faut donc

$$a_1 b = 1 \quad \text{ou} \quad a_2 b = 1 .$$

Soit ξ_1 le nombre $(\varepsilon + \sqrt{a_1 a_2} + i\sqrt{a_1 b} + i\sqrt{a_2 b})/4$, avec $\varepsilon = \pm 1$; les nombres $(\xi_1 - e)$ sont de la forme $(X + Y\sqrt{a_1 a_2} + iZ\sqrt{a_1 b} + iT\sqrt{a_2 b})/4$, avec X, Y, Z, T tous impairs, et

$$XZ - a_2 YT \equiv \varepsilon - a_2 \ (4) .$$

On peut choisir $\varepsilon \not\equiv a_2 \ (4)$, d'où $|XZ - a_2 YT| \geqslant 2$. Dès lors, la norme de $(\xi_1 - e)$ ne peut être inférieure à 1 que si la condition suivante est vérifiée (forme I)

$$4a_1 b(\frac{2}{16})^2 < 1 \quad \text{ou} \quad a_1 b < 16 .$$

Même démonstration pour $a_2 b$. Même condition

$$a_2 b < 16 .$$

Les seuls corps de cette catégorie qui vérifient ces conditions sont $\underset{\sim}{Q}(i , i\sqrt{5})$ qui est euclidien, et $\underset{\sim}{Q}(i , i\sqrt{13})$ dont je ne sais rien.

2°) $a_1 b \equiv 1 \ (4)$; $a_1 a_2 \equiv -1 \equiv -a_2 b \ (4)$.

Les mêmes procédés élémentaires permettent d'établir que les seuls corps éventuellement euclidiens de cette famille sont $\underset{\sim}{Q}(i , i\sqrt{7})$ et $\underset{\sim}{Q}(i , i\sqrt{3})$ qui le sont en effet, et $\underset{\sim}{Q}(i , i\sqrt{11})$ dont on peut montrer qu'il ne l'est pas.

3°) $-a_1 b \equiv 1 \equiv -a_2 b \equiv a_1 a_2 \ (4)$.

C'est le cas le plus compliqué, les entiers en effet sont de la forme

$$(2) \qquad \frac{X + Y\sqrt{a_1 a_2} + Zi\sqrt{a_1 b} + Ti\sqrt{a_2 b}}{4}$$

avec $X \equiv Y \equiv Z \equiv T \pmod 2$ (et une autre condition sur leur somme).

Soit ξ_0 le nombre $(1 + i\sqrt{a_1 b})/4$; les nombres $\xi_0 - e$ sont de la forme (2), mais avec $X \equiv Z \not\equiv Y \equiv T \pmod 2$, et le nombre $XZ - a_2 YT$ est impair, d'où la condition (forme I)

$$4a_1 b(\tfrac{1}{16})^2 < 1 \quad \text{ou} \quad a_1 b < 64$$

on établit également la condition nécessaire

$$a_2 b < 64 .$$

Si, de plus, a_1 est supérieur à 16, le nombre $XT - a_1 YZ$, qui est pair, ne peut pas être nul car si X (ou T) divise a_1, $X^2 - a_1 a_2 Y^2$ (ou $a_1 Z^2 - a_2 T^2$) est un multiple impair de a_1 et vaut au moins 16, la norme de $\xi_0 - e$ (forme II) ne peut être inférieure à 1.

La condition $|XT - a_1 YZ| \geq 2$, portée dans la forme (I bis) de la norme donne alors

$$4a_2 b(\tfrac{2}{16})^2 < 1 \quad \text{ou} \quad a_2 b < 16$$

et, portée dans la forme II, où les trois autres carrés sont impairs, elle donne également la condition

$$b^2 + 2a_1 b + 8a_2 b + 1 < 256 .$$

Il reste un assez grand nombre de corps qui vérifient ces conditions, mais pour être euclidiens ils doivent être de classe 1. La question est dès lors presque résolue, les seuls survivants de ces éliminatoires sont

$$\underset{\sim}{Q}(i\sqrt{3}, i\sqrt{7}) \; ; \quad \underset{\sim}{Q}(i\sqrt{3}, i\sqrt{11}) \; ; \quad \underset{\sim}{Q}(i\sqrt{3}, \sqrt{5})$$

dont LAKEIN a montré qu'ils sont euclidiens.

$$\underset{\sim}{Q}(i\sqrt{3}, i\sqrt{19}) \; ; \quad \underset{\sim}{Q}(i\sqrt{3}, \sqrt{17})$$

dont j'espère montrer qu'ils le sont.

$$\underset{\sim}{Q}(i\sqrt{3}, i\sqrt{43}) ,$$

que je crois non-euclidien et

$$\underset{\sim}{Q}(i\sqrt{7}, \sqrt{5})$$

dont je ne sais rien.

Les mots "j'espère" et "je crois" sont conséquence d'explorations du problème sur ordinateurs que j'exposerai... si elles aboutissent.

BIBLIOGRAPHIE

[1] LAKEIN (Richard B.). - Euclid's algorithm in complex quartic fields, Acta Arithmetica, Warszawa, t. 20, 1972, p. 393-400.

(Texte reçu le 28 mai 1973)

Jacqueline SAUVAGEOT
6 rue Oudinot
75007 PARIS