131. *Sur le nombre de classes de sous-corps cubique cyclique de* $Q^{(p)}, p \equiv 1 \bmod 3$

Par Marie-Nicole MONTOUCHET*)

(Comm. by Kunihiko KODAIRA, M. J. A., June 12, 1971)

Soit p un nombre premier congru à 1 modulo 3. Soit $\zeta_p = e^{2\pi i/p}$ et soit $Q^{(p)} = Q(\zeta_p)$ le p-ième corps cyclotomique. Il existe un sous-corps cubique cyclique et un seul K de $Q^{(p)}$. Nous allons donner un critère permettant de déterminer la parité du nombre de classes de K ainsi que des résultats numériques.

1. Notations et rappels.

Tout nombre premier $p, p \equiv 1 \bmod 3$, se met de manière unique sous la forme $p = (a^2 + 27b^2)/4 = \varphi\bar{\varphi}$, avec $\varphi = (a + 3ib\sqrt{3})/2$, $a \equiv 1 \bmod 3$.

Soit χ un caractère modulo p de K; soit $\tau = \sum_{x \bmod p} \zeta^x \chi(x)$. Tout élèment z de K se met de manière unique sous la forme $z = (x + y\tau + \bar{y}\bar{\tau})/3 = [x, y]$, $x \in Q$, $y \in Q(i\sqrt{3})$.

Les coordonnées (x, y) de l'unité fondamentale ε de K sont la solution (x, y), y déterminé à une racine cubique de l'unité près, de l'equation $x^3 - 3pxy\bar{y} + p(\varphi y^3 + \bar{\varphi}\bar{y}^3) = 27$ pour laquelle $x^2 + 2py\bar{y}$ est minimum avec $y \neq 0$ ([3]).

Soit $\zeta_{2p} = e^{i\pi/p}$ et soit g une racine primitive modulo p. Soit $\eta = -\prod_{n=1}^{(p-1)/6} (\zeta_{2p}^{g^{3n+1}} - \zeta_{2p}^{-g^{3n+1}})/(\zeta_{2p}^{g^{3n}} - \zeta_{2p}^{-g^{3n}})$ l'unité cyclotomique de K. On rappelle que l'indice dans le groupe des unités de K du sous-groupe engendré par les unités cyclotomiques de K est égal à h ([4]).

2. Etude de la parité du nombre de classes de K.

Théorème. *4 divise h si et seulement si l'unité cyclotomique η de K est totalement positive.*

La démonstration de ce théorème résulte du théorème V de J. V. Armitage et A. Fröhlich ([2]) et du fait qu'une condition nécessaire et suffisante pour que 4 divise h est que η soit un carré dans K.

Une généralisation de ce théorème est donné par N. Adachi dans [1].

Proposition. *Soit g une racine primitive modulo p. On désigne par $[g^m]$ la valeur de g^m modulo p comprise entre 1 et $p-1$. Pour i variant de 0 à 2 soit M_i le nombre d'entiers $n, 1 \leq n \leq (p-1)/6$ tels que $[g^{3n+i}]$ soit pair. 4 divise h si et seulement si $M_0 + M_1$ et $M_1 + M_2$ sont impairs.*

---

*) Institut de Mathématiques Pures, Université Scientifique et Médicale de Grenoble, B.P. 116, 38—St. Martin d'Hères, France.

En effet, $\eta=-\prod_{n=1}^{(p-1)/6}[\sin(\pi g^{3n+1}/p)/\sin(\pi g^{3n}/p)]$ et le signe de $\sin(\pi g^m/p)$ se détermine en fonction de la parité de $[g^m]$.

La méthode se programme facilement.

3. Résultats numériques.

Il y a 661 nombres premiers congrus à 1 modulo 3 et inférieurs à 10 000; parmi eux, il y en a 70 pour lesquels 4 divise le nombre de classes du sous-corps cubique cyclique de $Q^{(p)}$; ce sont: $p=163, 277, 349$ 397, 547, 607, 709, 853, 937, 1009, 1399, 1699, 1777, 1789, 1879, 1951, 2131 2311, 2689, 2797, 2803, 3037, 3271, 3517, 3727, 4099, 4219, 4261, 4297, 4357 4561, 4567, 4639, 4789, 4801, 5197, 5479, 5659, 5779, 5953, 6037, 6079, 6163 6247, 6553, 6637, 6709, 7027, 7297, 7489, 7639, 7687, 7867, 7879, 8011, 8191 8209, 8629, 8647, 8731, 8887, 9109, 9283, 9319, 9337, 9391, 9421, 9601, 9649 et 9721.

La détermination explicite de η et de ε permet le calcul de h. Nous avons obtenu les résultats suivants:

$p=163$	$\varepsilon=[11,1]$	$\eta=[174,-6+7i\sqrt{3}]$	$h=4$
$p=277$	$\varepsilon=[71,-5-i\sqrt{3}]$	$\eta=[6851,124+220i\sqrt{3}]$	$h=4$
$p=349$	$\varepsilon=[17,1]$	$\eta=[366,-9+10i\sqrt{3}]$	$h=4$
$p=397$	$\varepsilon=[-105,3+i\sqrt{3}]$	$\eta=[6851,-68+164i\sqrt{3}]$	$h=4$
$p=547$	$\varepsilon=[120,3i\sqrt{3}]$	$\eta=[14\,646,-540-183i\sqrt{3}]$	$h=4$
$p=607$	$\varepsilon=[23,1]$	$\eta=[581,-11-12i\sqrt{3}]$	$h=4$.

Il existe des sous-corps cubiques cycliques de $Q^{(p)}$, $p\equiv 1 \bmod 3$ dont l'unité fondamentale est totalement positive.

En effet, pour $p=1009$, $\varepsilon=[893,-20-11i\sqrt{3}]$ est une unité totalement positive et qui n'est pas un carré.

Remarque. Ces résultats ne sont pas en accord avec le théorème 2 de [1] dont la démonstration s'appuie semble-t-il sur une interprétation erronée d'un résultat de [4].

Références

[1] N. Adachi: On the class number of an absolutely cyclic number field of prime degree. Proc. Japan Acad., **45**, 647–650 (1969).

[2] J. V. Armitage and A. Fröhlich: Classnumbers and unit signatures. Mathematika, **14**, 94–98 (1967).

[3] H. Hasse: Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkörpern. Abhandlungen der Deutschen Akademie der Wissenschaften zu Berlin. Année 1948, n°2.

[4] ——: Über die Klassenzahl abelscher Zahlkörper. Chapitre I et II. Berlin (1952).