120. *Nouvelle démonstration d'une congruence modulo 16 entre les nombres de classes d'idéaux de* $Q(\sqrt{-2p})$ *et* $Q(\sqrt{2p})$ *pour* p *premier* $\equiv 1 \pmod 4$

Par Pierre KAPLAN*)

(Communicated by Shokichi IYANAGA, M. J. A., Dec. 12, 1981)

Soit p un nombre premier congru à 1 modulo 4. On pose $p=8l+1$ ou bien $p=8l+5$. Soient $h(-2p)$ le nombre des classes d'idéaux du corps quadratique $\boldsymbol{Q}(\sqrt{-2p})$ et $h(2p)$ le nombre des classes d'idéaux au sens strict du corps quadratique $\boldsymbol{Q}(\sqrt{2p})$. Soit enfin (R, S) la plus petite solution en entiers rationnels strictement positifs de l'équation

$$R^2-2pS^2=1. \tag{1}$$

La congruence que nous allons démontrer s'écrit

$$h(-2p)\equiv 3h(2p)\frac{S}{2}+8l \pmod{16}. \tag{2}$$

Cette congruence a été découverte par Kaplan et Williams ([3] et [4]). Leur démonstration n'utilise que les formules de Dirichlet donnant le nombre des classes d'idéaux des corps quadratiques, mais est assez longue.

La démonstration que nous présentons ici s'appuie sur la théorie de Lang et Schertz [5]; elle est plus courte que la démonstration exposée dans [3] et [4], mais moins directe; de plus, on ne peut pas, semble-t-il, obtenir par cette méthode les congruences modulo 16 entre les nombres de classes d'idéaux des corps $Q(\sqrt{p})$ et $Q(\sqrt{-p})$ établies dans [6] et [4].

Nous partons du théorème 3.3 de [5], dont la deuxième formule s'écrit, pour $D=8p$ (cf. aussi Hayashi [2], p. 4):

$$3h(-2p)+6h(-p)\equiv h^*(2p)\frac{2}{e_2}\rho(u_2, v_2) \pmod{16} \tag{3}$$

où: $h^*(2p)$ est le nombre de classes *au sens large* de $Q(\sqrt{2p})$;

$e_2=[U: U_2]$; $U=$groupe des unités de l'anneau $\mathcal{O}$ des entiers de $Q(\sqrt{2p})$, d'unité fondamentale ε_{2p};

$U_2=$groupe des unités de l'anneau $\mathcal{O}_2$ de conducteur 2, formé des nombres $X+2Y\sqrt{2p}$, où $X,\ Y\in \boldsymbol{Z}$; enfin $\varepsilon_2=(u_2/2)+2v_2\sqrt{2p}$ est l'unité fondamentale de l'anneau $\mathcal{O}_2$.

L'expression de $\rho(u_2, v_2)$ dépend de la parité de v_2 (cf. [4], (2.15)).

D'après Gauss [1], p. 673, 674, 694, on sait que:

*) U.E.R. de Mathématiques, Université de Nancy, France.

$$(4) \qquad h(-p)\equiv h(-2p)+4l \pmod 8.$$

Comme $h(2p)$ est pair, on déduit de (3) et (4)

$$(5) \qquad h(-2p)+8l\equiv h^*(2p)\frac{2}{e_2}\rho(u_2, v_2) \pmod{16}.$$

Si le nombre premier p est donné, exactement une des trois équations

$$(6) \qquad V^2-2pW^2=E_p, \quad E_p=-2, \quad 2 \text{ ou } -1,$$

a des solutions en entiers rationnels et, si V, W désigne la plus petite solution strictement positive, on a, suivant que $E_p=-2$, 2 ou -1:

$$(7) \quad -2=V^2-2pW^2, \quad R=1+V^2, \quad S=VW, \quad V\equiv S\equiv 0 \pmod 4,$$

$$(8) \quad 2=V^2-2pW^2, \quad R=V^2-1, \quad S=VW, \quad V\equiv S\equiv 2 \pmod 4,$$

$$(9) \quad -1=V^2-2pW^2, \quad R=1+2V^2, \quad S=2VW,$$
$$W\equiv 1 \pmod 4, \quad S\equiv 2 \pmod 4.$$

A) *Cas où* $N(\varepsilon_{2p})=-1$ $(E_p=-1)$:

On a $\varepsilon_{2p}=V+W\sqrt{2p}$, avec $V\equiv 1 \pmod 2$, $W\equiv 1 \pmod 4$ et $\varepsilon_1^2=R+S\sqrt{2p}\in\mathcal{O}_2$, car $S=2VW$ est pair.

Donc $\varepsilon_2=\varepsilon_1^2$, $e_2=2$, $u_2=2R$, $v_2=S/2\equiv 1 \pmod 2$, $h^*(2p)(2/e_2)=h(2p)$.

Comme v_2 est impair, l'expression de $\rho(u_2, v_2)$ est:

$$(10) \qquad \rho(u_2, v_2)=2\left\{\left(\frac{R}{S/2}\right)-1\right\}+\frac{S}{2}(2R-3)$$

avec

$$(11) \qquad R=V^2+2pW^2=2V^2+1=4pW^2-1.$$

Si $p\equiv 1 \pmod 8$, comme $h(2p)\equiv 0 \pmod 4$ et R est impair, on a:

$$(12) \qquad \rho(u_2, v_2)\equiv -\frac{S}{2} \pmod 4.$$

Portant (12) dans (5), on trouve (2).

Si $p\equiv 5 \pmod 8$, comme $h(2p)\equiv 2 \pmod 4$, il faut calculer $\rho(u_2, v_2)$ modulo 8.

On a $R=1+2V^2\equiv 3 \pmod 4$, donc $2R-3\equiv 3 \pmod 8$. Et aussi:

$$\left(\frac{R}{S/2}\right)=\left(\frac{R}{VW}\right)=\left(\frac{1+2V^2}{V}\right)\left(\frac{4pW^2-1}{W}\right)=1,$$

car $W\equiv 1 \pmod 4$.

D'où $\rho(u_2, v_2)\equiv 3(S/2) \pmod 8$; portant dans (5), on trouve (2).

B) *Cas où* $N(\varepsilon_{2p})=+1$ $(E_p=+2 \text{ ou } -2)$:

Alors, nécessairement, $p\equiv 1 \pmod 8$.

Ici $\varepsilon_{2p}=R+S\sqrt{2p}\in\mathcal{O}_2$, car S est pair, donc:

$$e_2=1, \quad u_2=2R, \quad v_2=\frac{S}{2}, \quad h^*(2p)\frac{2}{e_2}=h(2p)\equiv 0 \pmod 4.$$

Si $S/2$ est impair, c'est-à-dire si $E_p=2$, comme R est impair, on a comme plus haut:

$$\rho(u_2, v_2)\equiv -\frac{S}{2} \pmod 4.$$

Si $S/2$ est pair, c'est-à-dire si $E_p=-2$, $R=1+V^2\equiv 1 \pmod 4$ et la formule pour ρ donne:

$$\rho(u_2, v_2)=2\left\{\left(\frac{S/2}{R}\right)-1\right\}+\frac{1}{2}2R\cdot\frac{S}{2}(8p-1)+\frac{3}{2}(2R-2)\equiv -\frac{S}{2} \pmod 4.$$

Donc, dans tous les cas, la formule (2) est vraie.

Références

[1] C. F. Gauss: Arithmetische Untersuchungen. Chelsea (1965).

[2] H. Hayashi: Note on the class numbers of the quadratic number fields $Q(\sqrt{-p})$, $Q(\sqrt{-2p})$ and $Q(\sqrt{2p})$ with a prime number $p\equiv 1 \bmod 2^2$. Memoirs of the Faculty of General Education, Kumamoto University, Series of Natural Sciences, no. 13 (February 1978).

[3] P. Kaplan and K. S. Williams: On the class number of $Q(\sqrt{\pm 2p})$ modulo 16, for $p\equiv 1 \pmod 8$ a prime. Acta Arithmetica (à paraître).

[4] ——: Congruences modulo 16 for the class numbers of the quadratic fields $Q(\sqrt{\pm p})$ and $Q(\sqrt{\pm 2p})$ for p a prime congruent 5 modulo 8. ibid. (à paraître).

[5] H. Lang and R. Schertz: Kongruenzen zwischen Klassenzahlen quadratischer Zahlkörper. J. Number Theory, **8**, 352–356 (1976).

[6] K. S. Williams: On the class numbers of $Q(\sqrt{-p})$ modulo 16 for $p\equiv 1 \pmod 8$ a prime. Acta Arithmetica (à paraître).