Kaplan, P., Williams, K.S. et Hardy, K.
Osaka J. Math.
23 (1986), 479–489

DIVISIBILITE PAR 16 DU NOMBRE DES CLASSES AU SENS STRICT DES CORPS QUADRATIQUES REELS DONT LE DEUX-GROUPE DES CLASSES EST CYCLIQUE

PIERRE KAPLAN, KENNETH S. WILLIAMS[1]
ET KENNETH HARDY[2]

(Received March 11, 1985)

1. Introduction

Soit $m>1$ un entier sans diviseur carré, tel que le deux-groupe $H_2(m)$ des classes d'idéaux au sens strict de $Q(\sqrt{m})$ soit cyclique d'ordre au moins 8; soit $h(m)\equiv 0 \pmod 8$ le nombre des classes d'idéaux au sens strict de $Q(\sqrt{m})$. Pour un tel nombre m il y a deux possibilités ([1] et [2]):

a) $m=pq$, p et q nombres premiers $\equiv 1 \pmod 4$ tels que

$$\left(\frac{p}{q}\right) = \left(\frac{p}{q}\right)_4 = \left(\frac{q}{p}\right)_4 = 1\,,$$

b) $m=2p$, p nombre premier $\equiv 1 \pmod{16}$ tel que $\left(\frac{2}{p}\right)_4 = 1$.

Rappelons que les facteurs principaux de $Q(\sqrt{m})$ sont les deux diviseurs sans diviseur carré du discriminant de $Q(\sqrt{m})$ représentés par la forme X^2-mY^2.

Nous obtenons les résultats nouveaux suivants:

Théorème 1. *Soit p et q deux nombres premiers tels que $h(pq)\equiv 0 \pmod 8$. Les équations*

$$Z^2 = pX^2 - qY^2\,, \quad Z'^2 = qX'^2 - pY'^2 \tag{1.1}$$

ont des solutions en entiers rationnels X, Y, Z, X', Y', Z' tels que

$$\begin{cases} (X, Y) = (X', Y') = 1\,, \\ \left(\frac{Z}{p}\right) = \left(\frac{Z'}{p}\right) = \left(\frac{Z}{q}\right) = \left(\frac{Z'}{q}\right) = 1\,, \qquad Z>0,\ Z'>0\,, \\ X \equiv \frac{p+1}{2} \pmod 4\,,\ X' \equiv \frac{q+1}{2} \pmod 4\,,\ Z \equiv Z' \equiv 1 \pmod 2\,. \end{cases} \tag{1.2}$$

(1) Recherche effectuée avec le soutien du Natural Sciences and Engineering Research Council Canada Grant n° A-7233.
(2) Recherche effectuée avec le soutien du Natural Sciences and Engineering Research Council Canada Grant n° A-8049.

Alors les nombres $\alpha=\left(\frac{Z}{p}\right)_4\left(\frac{2X}{Z}\right)$ *et* $\beta=\left(\frac{Z'}{q}\right)_4\left(\frac{2X'}{Z'}\right)$ *ne dépendent que de* p *et* q.

De plus $h(pq)\equiv 0 \pmod{16}$ *si, et seulement si,* $\alpha=\beta=1$. *Sinon* p, q *ou* -1 *est facteur principal suivant que* $(\alpha, \beta)=(1, -1), (-1, 1)$ *ou* $(-1, -1)$ *respectivement.*

Si $n\equiv 1 \pmod 8$, on pose $\left(\frac{n}{2}\right)_4=(-1)^{(n-1)/8}$.

Théorème 2. *Soit* p *un nombre premier tel que* $h(2p)\equiv 0 \pmod 8$. *Les équations*

$$Z^2 = pX^2-2Y^2, \quad Z'^2 = 2X'^2-pY'^2 \tag{1.3}$$

ont des solutions en entiers rationnels X, Y, Z, X', Y', Z' *tels que*

$$(X, Y) = 1,\ Z>0,\ Z\equiv\pm 1 \pmod 8,\ \left(\frac{Z}{p}\right) = 1,\quad X\equiv 1 \text{ ou } 3 \pmod 8, \tag{1.4}$$

$$(X', Y') = 1,\ Z'>0,\ Z'\equiv 1 \pmod 8,\ \left(\frac{Z'}{p}\right) = 1. \tag{1.5}$$

Alors les nombres $\alpha=\left(\frac{Z}{p}\right)_4\left(\frac{X}{Z}\right)$ *et* $\beta=\left(\frac{Z'}{2}\right)_4\left(\frac{X'}{Z'}\right)$ *ne dépendent que de* p.

De plus $h(2p)\equiv 0 \pmod{16}$ *si, et seulement si,* $\alpha=\beta=1$. *Sinon* -2, 2 *ou* -1 *est facteur principal suivant que* $(\alpha, \beta)=(1, -1), (-1, 1)$ *ou* $(-1, -1)$ *respectivement.*

Corollaire du théorème 2. *Un nombre premier* p *tel que* $h(2p)\equiv 0 \pmod 8$ *s'écrit*

$$p = u^2+2v^2 = 2e^2-d^2 \text{ avec } \left(\frac{u}{p}\right) = 1 \text{ et } 2v\equiv 0,\ d\equiv 1 \pmod 8. \tag{1.6}$$

Alors

$$\alpha = \left(\frac{u}{p}\right)_4,\ \beta = \left(\frac{d}{2}\right)_4\left(\frac{e}{d}\right). \tag{1.7}$$

Pour démontrer ces théorèmes nous utilisons la théorie des formes quadratiques binaires, et considérons le groupe des classes de formes quadratiques $[A, B, C]=Ax^2+2Bxy+Cy^2$ de discriminant $4m$ pour la composition, groupe dont le deux sous-groupe est isomorphe à $H_2(m)$. Une méthode analogue a été utilisée par Leonard et Williams ([4] et [5]) pour obtenir des critères de divisibilité de $h(m)$ par 16 quand m est négatif.

Notre méthode est élémentaire en ce sens qu'elle n'utilise que la théorie des corps quadratiques (dans le langage des formes quadratiques binaires). En utilisant la théorie du Corps de Classes, Yamamoto [6] a obtenu des critères

différents des nôtres. Nous comparons ses résultats avec les nôtres et avec ceux de Leonard et Williams ([4], [5]) a la fin des §§ 3 et 4 consacrés respectivement aux cas $m=pq$ et $m=2p$.

2. Racines carrée et quatrième d'une forme d'ordre 2

Dans ce paragraphe p et q désignent deux nombres premiers distincts, éventuellement 2, tels que $h(pq)\equiv 0 \pmod 8$.

Parmi les trois formes $\phi_{-1}=[-1, 0, pq]$, $\phi_p=[p, 0, -q]$, $\phi_q=[q, 0, -p]$ exactement une est dans la classe unité, et les deux autres sont dans la classe ambiguë. Comme $h(pq)\equiv 0 \pmod 8$ ces formes sont des puissances quatrièmes; et $h(pq)\equiv 0 \pmod{16}$ si, et seulement si, ϕ_p et ϕ_q sont des puissances huitièmes; si ϕ_p (respectivement ϕ_q) est puissance huitieme mais non ϕ_q (respectivement ϕ_p) alors p (respectivement q) est facteur principal, et si ni ϕ_p ni ϕ_q ne sont puissances huitièmes alors -1 est facteur principal.

Nous allons déterminer une racine carrée de la forme $\phi_p=[p, 0, -q]$. L'équation

$$Z^2 = pX^2-qY^2 \tag{2.1}$$

a donc des solutions où $Z>0$, $(Z, 2pq)=1$, $(X, Y)=1$, et tout Z solution donne la valeur 1 aux caractères génériques, donc

$$\begin{cases} \left(\frac{Z}{p}\right)=\left(\frac{Z}{q}\right)=1 \quad \text{si } p \text{ et } q\neq 2, \quad \left(\frac{Z}{p}\right)=\left(\frac{2}{Z}\right)=1 \quad \text{si} \quad q=2, \\ \left(\frac{2}{Z}\right)=\left(\frac{Z}{q}\right)=1 \quad \text{si} \quad p=2. \end{cases} \tag{2.2}$$

Considérons l'équation (2.1) modulo 4, on voit que

$$\begin{cases} X\equiv 1 \pmod 2, \ Y\equiv 0 \pmod 2 & \text{si} \quad p\neq 2, \\ X\equiv Y\equiv 1 \pmod 2 & \text{si} \quad p=2. \end{cases} \tag{2.3}$$

Soit maintenant λ et μ tels que

$$\lambda X-\mu Y = 1. \tag{2.4}$$

Si $p\neq 2$ alors (2.3) monter que λ est impair. Appliquant la substitution linéaire de matrice $\begin{pmatrix} X & \mu \\ Y & \lambda \end{pmatrix}$ à la forme $[p, 0, -q]$ on obtient l'identité

$$p(X\xi+\mu\eta)^2-q(Y\xi+\lambda\eta)^2 = Z^2\xi^2+2b\xi\eta+c\eta^2 \tag{2.5}$$

avec

$$b = pX\mu-qY\lambda, \quad c = p\mu^2-q\lambda^2. \tag{2.6}$$

Tenant compte de (2.1), (2.4) et (2.6) on obtient

$$bY = \lambda Z^2 - pX . \tag{2.7}$$

L'équation (2.5) signifie que les formes $[p, 0, -q]$ et $[Z^2, b, c]$ sont équivalentes, donc une racine carrée de $[p, 0, -q]$ est la forme

$$f = [Z, b, Zc] .$$

Comme $h(pq) \equiv 0 \pmod 8$ la forme f est dans le genre principal, donc il existe des entiers x, y et r tels que

$$r^2 = Zx^2 + 2bxy + Zcy^2 \tag{2.8}$$

avec

$$(x, y) = (r, 2Zcpq) = 1 . \tag{2.9}$$

Multipliant (2.8) par Z on obtient

$$Zr^2 = Z^2x^2 + 2bxZy + c(Zy)^2 . \tag{2.10}$$

Appliquant l'identité (2.5) à (2.10) avec $\xi = x$, $\eta = Zy$ on obtient

$$Zr^2 = pS^2 - qT^2 \tag{2.11}$$

avec

$$S = Xx + \mu Zy , \quad T = Yx + \lambda Zy . \tag{2.12}$$

Comme, d'après (2.9), on a $(x, Zy) = 1$ et que $\det\begin{pmatrix} X & \mu \\ Y & \lambda \end{pmatrix} = 1$ on voit que

$$(S, T) = (S, qZr) = (T, pZr) = 1 . \tag{2.13}$$

De (2.7) et (2.8) on déduit $1 = \left(\frac{2bxy}{Z}\right) = \left(\frac{-2xyXYp}{Z}\right)$. Mais (2.11) montre que $\left(\frac{p}{Z}\right) = \left(\frac{Z}{p}\right) = \left(\frac{-q}{p}\right) = 1$, donc

$$\left(\frac{Xx}{Z}\right) = \left(\frac{-2yY}{Z}\right) ; \left(\frac{Yx}{Z}\right) = \left(\frac{-2yX}{Z}\right) . \tag{2.14}$$

Le nombre r est le premier coefficient d'une racine quatrième de la forme $[p, 0, -q]$, qui sera donc une puissance huitième si, et seulement si, le nombre r donne la valeur 1 à un caractère générique.

Ceci est vrai ou faux indépendamment du choix des nombres X, Y, Z, λ, μ, x, y et r, donc nous supposerons les signes de x et y choisis de manière que $T = Yx + \lambda Zy > 0$. De plus, X étant impair, on peut, si nécessaire, supposer μ pair en remplaçant éventuellement (λ, μ) par $(\lambda + Y, \mu + X)$.

3. Démonstration du théorème 1 (cas a)

Ici p et q sont deux nombres premiers impairs distincts, tels que $h(pq)\equiv 0 \pmod 8$.

Dans ce cas nous considérons $\varphi_p=[p, 0, -q]$ et nous allons calculer le caractère $\left(\frac{r}{p}\right)$ où r est défini par (2.8). Nous commençons par remarquer que

$$Y\equiv\begin{cases}0 \pmod 4, & \text{si } p\equiv 1 \pmod 8,\\ 2 \pmod 4, & \text{si } p\equiv 5 \pmod 8.\end{cases} \tag{3.1}$$

On déduit de (2.11) que $\left(\frac{r}{p}\right)\left(\frac{Z}{p}\right)_4=\left(\frac{-1}{p}\right)_4\left(\frac{q}{p}\right)_4\left(\frac{T}{p}\right)$. Comme $\left(\frac{q}{p}\right)_4=1$ et $\left(\frac{-1}{p}\right)_4=\left(\frac{2}{p}\right)$, on a

$$\left(\frac{r}{p}\right)=\left(\frac{Z}{p}\right)_4\left(\frac{2T}{p}\right). \tag{3.2}$$

Nous voulons évaluer $\left(\frac{2T}{p}\right)$. L'équation (2.11) montre que

$$\begin{cases}Z\equiv 1 \pmod 4 \Rightarrow S\equiv 1 \pmod 2 \text{ et } T\equiv 0 \pmod 2\\ Z\equiv 3 \pmod 4 \Rightarrow S\equiv 0 \pmod 2 \text{ et } T\equiv 1 \pmod 2.\end{cases} \tag{3.3}$$

Nous distinguerons deux cas, $Z\equiv 1 \pmod 4$ et $Z\equiv 3 \pmod 4$.

a) $Z\equiv 1 \pmod 4$. Alors $T=2^nT_1$, T_1 impair, avec $n=1$ si, et seulement si, $pZ\equiv 5 \pmod 8$.

On a, utilisant la loi de réciprocité quadratique et (2.11),

$$\left(\frac{2T}{p}\right)=\left(\frac{2}{p}\right)^{n+1}\left(\frac{T_1}{p}\right)=\left(\frac{2}{p}\right)^{n+1}\left(\frac{p}{T_1}\right)=\left(\frac{2}{p}\right)^{n+1}\left(\frac{Z}{T_1}\right)$$
$$=\left(\frac{2}{p}\right)^{n+1}\left(\frac{T_1}{Z}\right)=\left(\frac{2}{p}\right)^{n+1}\left(\frac{2}{Z}\right)^{n}\left(\frac{T}{Z}\right).$$

Tenant compte maintenant de (2.12) et (2.14) on obtient

$$\left(\frac{2T}{p}\right)=\left(\frac{2}{p}\right)^{n+1}\left(\frac{2}{Z}\right)^{n}\left(\frac{Yx}{Z}\right)=\left(\frac{2}{p}\right)^{n+1}\left(\frac{2}{Z}\right)^{n+1}\left(\frac{y}{Z}\right)\left(\frac{X}{Z}\right).$$

Pour évaluer $\left(\frac{y}{Z}\right)$ nous posons $y=2^my_1$, $y_1\equiv 1 \pmod 2$; alors

$$\left(\frac{y}{Z}\right)=\left(\frac{2}{Z}\right)^{m}\left(\frac{y_1}{Z}\right)=\left(\frac{2}{Z}\right)^{m}\left(\frac{Z}{|y_1|}\right)=\left(\frac{2}{Z}\right)^{m}$$

d'après (2.8), d'où

$$\left(\frac{2T}{p}\right)=\left(\frac{2}{p}\right)^{n+1}\left(\frac{2}{Z}\right)^{m+n+1}\left(\frac{X}{Z}\right). \tag{3.4}$$

D'après (2.3) et (3.3) Y et T sont pairs, donc d'après (2.12) y pair et x impair, d'où

$$T \equiv Y+y \pmod 4 . \tag{3.5}$$

Si $p \equiv Z \equiv 1 \pmod 8$, l'équation (3.4) s'écrit $\left(\frac{2T}{p}\right)=\left(\frac{2X}{Z}\right)$.

Si $p \equiv 1$, $Z \equiv 5 \pmod 8$, on a $Y \equiv 0$, $T \equiv 2 \pmod 4$, donc $m=n=1$, donc

$$\left(\frac{2T}{p}\right) = \left(\frac{2}{Z}\right)\left(\frac{X}{Z}\right) = \left(\frac{2X}{Z}\right).$$

Si $p \equiv 5$, $Z \equiv 1 \pmod 8$, on a $Y \equiv T \equiv 2 \pmod 4$, donc $n=1$, donc

$$\left(\frac{2T}{p}\right) = \left(\frac{X}{Z}\right) = \left(\frac{2X}{Z}\right).$$

Si $p \equiv Z \equiv 5 \pmod 8$, on a $Y \equiv 2$, $T \equiv 0 \pmod 4$,donc $m=1$, donc

$$\left(\frac{2T}{p}\right) = (-1)^{2(n+1)}\left(\frac{2}{Z}\right)\left(\frac{X}{Z}\right) = \left(\frac{2X}{Z}\right).$$

b) $Z \equiv 3$ (*mod* 4). Comme $T=Yx+\lambda yZ$ est impair et Y pair, y est impair. De plus comme $S=Xx+Z\mu y \equiv 0 \pmod 2$ on a $x \equiv \mu \pmod 2$. On peut supposer μ choisi pair, donc $x \equiv \mu \equiv 0 \pmod 2$. On a alors

$$\begin{aligned}\left(\frac{2T}{p}\right) &= \left(\frac{2}{p}\right)\left(\frac{T}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{p}{T}\right) = \left(\frac{2}{p}\right)\left(\frac{Z}{T}\right) = \left(\frac{2}{p}\right)\left(\frac{-1}{T}\right)\left(\frac{T}{Z}\right) \\ &= \left(\frac{2}{p}\right)\left(\frac{-1}{T}\right)\left(\frac{Yx}{Z}\right).\end{aligned}$$

Utilisant maintenant (2.14) on obtient

$$\begin{aligned}\left(\frac{2T}{p}\right) &= \left(\frac{2}{p}\right)\left(\frac{-1}{T}\right)\left(\frac{-2yX}{Z}\right) = -\left(\frac{2}{p}\right)\left(\frac{-1}{T}\right)\left(\frac{y}{Z}\right)\left(\frac{2X}{Z}\right) \\ &= -\left(\frac{2}{p}\right)\left(\frac{-1}{Ty}\right)\left(\frac{2X}{Z}\right).\end{aligned}$$

On a utilisé, outre la loi de réciprocité quadratique, l'équation (2.8) qui montre que $\left(\frac{y}{Z}\right)=\left(\frac{-1}{y}\right)\left(\frac{Z}{y}\right)=\left(\frac{-1}{y}\right)$.

Comme Y, x et μ sont pairs on a $T \equiv \lambda yZ \equiv -\lambda y$ et $\lambda X \equiv 1 \pmod 4$, donc

$$Ty \equiv -\lambda \equiv -X \pmod 4 .$$

On trouve donc ici

$$\left(\frac{2T}{p}\right)=\left(\frac{2}{p}\right)\left(\frac{-1}{X}\right)\left(\frac{2X}{Z}\right).$$

Choisissons le signe de X de façon que $\left(\frac{2}{p}\right)\left(\frac{-1}{X}\right)=1$, c'est-à-dire $X\equiv\frac{p+1}{2}\pmod 4$. Alors, dans les deux cas $Z\equiv 1$ et $Z\equiv 3 \pmod 4$, on trouve $\left(\frac{2T}{p}\right)=\left(\frac{2X}{Z}\right)$ donc

$$\left(\frac{r}{p}\right)=\left(\frac{Z}{p}\right)_4\left(\frac{2X}{Z}\right).$$

On voit donc que la classe de $[p, 0, -q]$ est une puissance huitième si, et seulement si, $\left(\frac{Z}{p}\right)_4\left(\frac{2X}{Z}\right)=1$, ce qui prouve le théorème 1.

REMARQUE. Yamamoto ([6]) considère l'équation

$$t^2=pr^2+qs^2.$$

Cette équation a d'une part des solutions t', r', $s'=2q^{(h(p)-1)/2}$ et d'autre part des solutions t'', $r''=2p^{(h(q)-1)/2}$, s'', où, de plus, on suppose les signes de t' et t'' choisis de façon que t' (respectivement t'')$\equiv 2, 6, 3, 7 \pmod 8$ suivant que r' (respectivement s'')$\equiv 0, 4, \pm 1, \pm 3 \pmod 8$. Le résultat de Yamamoto ([6], Theorem 5.4) est que $h(pq)\equiv 0 \pmod{16}$ si, et seulement si, $\left(\frac{t'}{p}\right)_4=\left(\frac{t''}{q}\right)_4=1$, et que, sinon, p, q, -1 est facteur principal suivant que $\left(\left(\frac{t'}{p}\right)_4, \left(\frac{t''}{q}\right)_4\right)=(1, -1), (-1, 1)$ ou $(-1, -1)$, autrement dit que $\alpha=\left(\frac{t'}{p}\right)_4$, $\beta=\left(\frac{t''}{q}\right)_4$.

4. Démonstration du théorème 2

Soit p un nombre premier tel que $h(2p)\equiv 0 \pmod 8$, donc $p\equiv 1 \pmod{16}$.

α) Nous considérons d'abord la première équation (1.3).

$$Z^2=pX^2-2Y^2, \quad (X, Y)=1, \qquad Z>0. \tag{4.1}$$

Comme $Z\equiv\pm 1 \pmod 8$ on a

$$\left(\frac{2}{X}\right)=(-1)^{Y/2}. \tag{4.2}$$

L'équation (2.11) avec $q=2$ montre que S est impair et que

$$\begin{cases} Z\equiv 1 \pmod 8 \Rightarrow T \text{ pair}, \\ Z\equiv -1 \pmod 8 \Rightarrow T \text{ impair}. \end{cases} \tag{4.3}$$

Nous allons calculer $\left(\frac{r}{p}\right)$. L'équation (2.11) avec $q=2$ entraîne

$$\left(\frac{r}{p}\right)=\left(\frac{Z}{p}\right)_4\left(\frac{-2}{p}\right)_4\left(\frac{T}{p}\right)=\left(\frac{Z}{p}\right)_4\left(\frac{T}{p}\right). \tag{4.4}$$

Pour calculer $\left(\frac{T}{p}\right)$ nous distinguons les cas $Z\equiv 1$ et $Z\equiv -1 \pmod 8$.

a) $Z\equiv 1$ (*mod* 8). On trouve successivement

$$\left(\frac{T}{p}\right)=\left(\frac{T_1}{p}\right)=\left(\frac{p}{T_1}\right)=\left(\frac{Z}{T_1}\right)=\left(\frac{T_1}{Z}\right)=\left(\frac{T}{Z}\right)=\left(\frac{Yx}{Z}\right)$$
$$=\left(\frac{-2yX}{Z}\right)=\left(\frac{y_1}{Z}\right)\left(\frac{X}{Z}\right)=\left(\frac{Z}{|y_1|}\right)\left(\frac{X}{Z}\right)=\left(\frac{X}{Z}\right)$$

où T_1 et y_1 désignent les parties impaires de T et y et où nous avons utilisé, outre la loi de réciprocité quadratique, les équations (2.8), (2.11), (2.14) et (4.1).

b) $Z\equiv -1$ (*mod* 8). Comme Y est pair et $T=Yx+\lambda Zy$ impair, y est impair. Nous supposons μ choisi pair, donc, comme $S=Xx+\mu Zy$ est impair, x est impair. Comme plus haut on trouve successivement

$$\left(\frac{T}{p}\right)=\left(\frac{p}{T}\right)=\left(\frac{Z}{T}\right)=\left(\frac{-1}{T}\right)\left(\frac{T}{Z}\right)=\left(\frac{-1}{T}\right)\left(\frac{Yx}{Z}\right)=\left(\frac{-1}{T}\right)\left(\frac{-2yX}{Z}\right)$$
$$=-\left(\frac{-1}{T}\right)\left(\frac{y}{Z}\right)\left(\frac{X}{Z}\right)=-\left(\frac{-1}{Ty}\right)\left(\frac{X}{Z}\right)\left(\frac{Z}{|y|}\right)=-\left(\frac{-1}{Ty}\right)\left(\frac{X}{Z}\right).$$

Comme μ et Y sont pairs on a $\lambda X=1+\mu Y\equiv 1 \pmod 4$, donc

$$Ty=Yxy+\lambda Zy^2\equiv Y-\lambda\equiv Y-X \pmod 4,$$

ce qui, tenant compte de (4.2) donne

$$-\left(\frac{-1}{Ty}\right)=\left(\frac{-1}{X}\right)(-1)^{Y/2}=\left(\frac{-2}{X}\right).$$

Supposons le signe de X choisi de façon que $\left(\frac{-2}{X}\right)=1$. On a alors, dans les deux cas $Z\equiv 1$ et $Z\equiv -1 \pmod 8$,

$$\left(\frac{r}{p}\right)=\left(\frac{Z}{p}\right)_4\left(\frac{X}{Z}\right). \tag{4.5}$$

β) Nous considérons maintenant la deuxième équation de (1.3)

$$Z'^2=2X'^2-pY'^2,\quad Z'>0,\quad (X',Y')=1. \tag{4.6}$$

Ici, d'après (2.3), X' et Y' sont impairs. De plus on peut toujours choisir $Z'\equiv 1 \pmod 8$. En effet si (Z',X',Y') est solution on voit, en utilisant l'unité

$3+2\sqrt{2}$ de norme 1 de $Q(\sqrt{2})$, que $(3Z'+4|X'|, 2Z'+3|X'|, Y')$ est aussi solution, et $3Z'+4|X'|\equiv 1 \pmod 8$ si $Z'\equiv -1 \pmod 8$. L'équation (2.11) avec $p=2$, $q=p$ s'écrit

$$Z'r^2 = 2S^2-pT^2 \tag{4.7}$$

et montre que $Z'r^2\equiv 2-T^2\equiv T^2 \pmod{16}$ c'est-à-dire

$$\left(\frac{2}{r}\right)\left(\frac{Z'}{2}\right)_4 = \left(\frac{2}{T}\right). \tag{4.8}$$

D'autre part on déduit de (4.7) successivement, comme plus haut,

$$\left(\frac{2}{T}\right) = \left(\frac{Z'}{T}\right) = \left(\frac{T}{Z'}\right) = \left(\frac{Y'x}{Z'}\right) = \left(\frac{-2yX'}{Z'}\right) = \left(\frac{y_1X'}{Z'}\right)$$
$$= \left(\frac{X'}{Z'}\right)\left(\frac{Z'}{|y_1|}\right) = \left(\frac{X'}{Z'}\right).$$

Donc on a

$$\left(\frac{2}{r}\right) = \left(\frac{Z'}{2}\right)_4\left(\frac{X'}{Z'}\right) \tag{4.9}$$

ce qui, avec (4.5), achève de démontrer le théorème 2.

Pour démontrer le corollaire il suffit de remarquer que les décompositions $p=u^2+2v^2$ et $p=2e^2-d^2$ nous donnent pour solutions des équations (1.3) respectivement

$$(X, Y, Z)=(1, v, u) \quad \text{et} \quad (X', Y', Z') = (e, 1, d).$$

REMARQUES. Si p vérifie $h(2p)\equiv 0 \pmod 8$, on a

$$p = f^2-2g^2 \text{ avec } f\equiv 1 \pmod 8,\ \left(\frac{f}{p}\right) = 1, f \text{ et } g>0. \tag{4.10}$$

1) Yamamoto [6] considère (comme au § 3) l'équation

$$t^2 = pr^2+2s^2.$$

Cette équation a pour solutions particulières $(f, 1, g)$ et aussi $(t, r, 2^{h(p)+1})$ avec $t\equiv 2^{h(p)+1} \pmod 8$. Le résultat de [6] (Theorem 5.5) est que $h(2p)\equiv 0 \pmod{16}$ si, et seulement si, $\left(\frac{f}{p}\right)_4=1$ et $t\equiv 2^{h(p)}+1 \pmod{16}$. Sinon -2, 2, -1 est facteur principal suivant que

$$\left(\left(\frac{f}{p}\right)_4, \left(\frac{t-2^{h(p)}}{2}\right)_4\right) = (1, -1), (-1, 1) \text{ ou } (-1, -1).$$

En particulier, comparant avec le corollaire du théorème 2 on voit que

$$\left(\frac{f}{p}\right)_4 = \left(\frac{u}{p}\right)_4. \tag{4.11}$$

2) La relation (4.11) peut être généralisée à tous les nombres premiers p tels que $h(-2p)\equiv 0 \pmod 8$. Un tel nombre p satisfait à (1.6) et (4.10), mais n'est pas nécessairement $\equiv 1 \pmod{16}$, et alors on a

$$h(-2p)\equiv 0 \pmod{16} \Leftrightarrow \begin{cases} \left(\frac{u}{p}\right)_4 = 1 & \text{(Yamamoto [6], Theorem 5.8]} \\ \left(\frac{f}{p}\right)_4 = 1 & \text{(Leonard et Williams [4], Theorem 2).} \end{cases}$$

3) On retrouve ainsi le fait que, si $h(2p)\equiv 0 \pmod 8$, $h(-2p)\equiv 0 \pmod{16}$ si, et seulement si, $h(2p)\equiv 0 \pmod{16}$ ou -2 est facteur principal, ce qui a été prouvé dans [3] par une méthode utilisant les formules analytiques pour les nombres des classes.

5. Exemples numériques

Théorème 1.

pq	p	q	X	Y	Z	X'	Y'	Z'	α	β	FP	$h(pq)$
505	5	101	−9	2	1	−1	2	9	1	−1	p	8
905	5	181	−13	2	11	−1	6	1	−1	1	q	8
2305	5	461	−21	2	19	−9	86	19	1	1	−1	16
6953	17	409	41	8	49	9	40	77	−1	−1	−1	8
8105	1621	5	−1	18	1	−37	2	19	1	1	p	16
8473	37	229	−5	2	3	−1	2	9	1	1	q	16

Théorème 2.

p	X	Y	Z	X'	Y'	Z'	α	β	FP	$h(2p)$
113	1	4	9	53	7	9	−1	−1	−1	8
257	3	34	1	13	1	9	1	−1	−2	8
337	3	26	41	13	1	1	−1	1	2	8
3089	3	106	73	669	17	49	1	1	−1	16
3361	3	118	49	41	1	1	1	1	2	16
4481	3	142	1	1941	41	49	1	1	−2	16

Bibliographie

[1] P. Kaplan: *Divisibilité par* 8 *du nombre des classes des corps quadratiques dont le* 2-*groupe des classes est cyclique, et réciprocité biquadratique*, J. Math. Soc. Japan **25** (1973), 596–608.

[2] P. Kaplan: *Sur le* 2-*groupe des classes d'idéaux des corps quadratiques*, J. Reine Angew. Math. **283/284** (1976), 313–363.

[3] P. Kaplan and K.S. Williams: *On the class numbers of* $Q(\sqrt{\pm 2p})$ *modulo* 16, *for* $p \equiv 1$ (*mod* 8) *a prime*, Acta Arith. **40** (1982), 289–296.

[4] P.A. Leonard and K.S. Williams: *On the divisibility of the class numbers of* $Q(\sqrt{-p})$ *and* $Q(\sqrt{-2p})$ *by* 16, Canad. Math. Bull. **25** (1982), 200–206.

[5] P.A. Leonard and K.S. Williams: *On the divisibility of* $Q(\sqrt{-pq})$ *by* 16, Proc. Edinburgh Math. Soc. **26** (1983), 221–231.

[6] Y. Yamamoto: *Disvisibility by* 16 *of class numbers of quadratic fields whose* 2-*class groups are cyclic*, Osaka J. Math. **21** (1984), 1–22.

Pierre Kaplan

10, Allée Jacques Offenbach
54420 Saulxures Lès Nancy
France

Kenneth S. Williams et Kenneth Hardy

Department of Mathematics and Statistics
Carleton University
Ottawa, Ontario, Canada
K1S 5B6