Kaplan, P. and Williams, K.S.
Osaka J. Math.
21 (1984), 23-29

ON THE STRICT CLASS NUMBER OF $Q(\sqrt{2p})$ MODULO 16, $p\equiv 1 \pmod 8$ PRIME

PIERRE KAPLAN AND KENNETH S. WILLIAMS

(Received August 6, 1982)

Let $p\equiv 1 \pmod 8$ be prime so that there are integers a, b, c, d, e, f with

$$(1)\qquad \begin{cases} p=a^2+b^2=c^2+2d^2=e^2-2f^2 \\ a\equiv 1 \pmod 4,\ b\equiv 0 \pmod 4,\ c\equiv 1 \pmod 4,\ d\equiv 0 \pmod 2, \\ \qquad e\equiv 1 \pmod 4,\ f\equiv 0 \pmod 4. \end{cases}$$

Throughout this note we consider only those primes p for which the strict class number $h^+(8p)$ of the real quadratic field $Q(\sqrt{2p})$ (of discrimanant $8p$) satisfies

$$(2)\qquad h^+(8p)\equiv 0 \pmod 8.$$

These primes have been characterized by Kaplan [4]. Indeed such primes must satisfy [5]

$$(3)\qquad \begin{cases} p\equiv 1 \pmod{16},\ a\equiv 1 \pmod 8,\ b\equiv 0 \pmod 8,\ c\equiv 1 \pmod 8,\ \left(\frac{c}{p}\right)=1, \\ d\equiv 0 \pmod 4,\ e\equiv 1 \pmod 8,\ \left(\frac{e}{p}\right)=+1. \end{cases}$$

In this note we give a new determination of $h^+(8p)$ modulo 16, and compare it with the determination given by Yamamoto in [15].

We begin by introducing some notation. We denote the fundamental unit (>1) of $Q(\sqrt{2p})$ by η_{2p}. As one and only one of the equations $V^2-2pW^2=-1, -2$, or $+2$ is solvable in integers V, W, we define

$$E_p=\begin{cases} -1, & \text{if } V^2-2pW^2=-1 \text{ solvable,} \\ -2, & \text{if } V^2-2pW^2=-2 \text{ solvable,} \\ +2, & \text{if } V^2-2pW^2=+2 \text{ solvable.} \end{cases}$$

Clearly the norm $N(\eta_{2p})$ of η_{2p} satisfies

$$N(\eta_{2p})=\begin{cases} +1, & \text{if } E_p=\pm 2, \\ -1, & \text{if } E_p=-1. \end{cases}$$

Further we let

$$\varepsilon_2 = 1+\sqrt{2}, \ \ \varepsilon_p = T+U\sqrt{p}$$

denote the fundamental units (>1) of $Q(\sqrt{2})$ and $Q(\sqrt{p})$ respectively, and set

$$e_2 = -\sqrt{2}\ \varepsilon_2' = -\sqrt{2}\ (1-\sqrt{2}) = 2-\sqrt{2}\ , \tag{4}$$

$$e_p = -\sqrt{p}\ \varepsilon_p' = -\sqrt{p}\ (T-U\sqrt{p}) = pU-T\sqrt{p}\ . \tag{5}$$

Finally the fundamental unit of $Q(\sqrt{2p})$ of norm $+1$ is denoted by $R+S\sqrt{2p}$ so that

$$R+S\sqrt{2p} = \begin{cases} \eta_{2p}, & \text{if } N(\eta_{2p}) = +1\,, \\ \eta_{2p}^2, & \text{if } N(\eta_{2p}) = -1\,. \end{cases}$$

Our starting point is the following result of Bucher [1: p. 8].

Lemma 1. *If $p\equiv 1$ (mod 8) is a prime such that $h^+(8p)\equiv 0$ (mod 8) then*

$$(-1)^{\lambda(p)}\left(\frac{e_2}{p}\right)_4 \equiv R^{h^+(8p)/8}\ (\text{mod } p)\,, \tag{6}$$

$$(-1)^{\lambda(p)}\left(\frac{e_p}{2}\right)_4 \equiv R^{h^+(8p)/8}\ (\text{mod } 4)\,, \tag{7}$$

where

$$\lambda(p) = \textit{number of quadratic residues of } p \textit{ less than } p/8\,. \tag{8}$$

[In the biquadratic residue symbols e_2 and e_p are to be taken modulo p and 16 respectively.]

It is convenient to set

$$\alpha = (-1)^{\lambda(p)}\left(\frac{e_p}{2}\right)_4, \quad \beta = (-1)^{\lambda(p)}\left(\frac{e_2}{p}\right)_4\,. \tag{9}$$

As (see for example [1: p. 4] or [8])

$$\begin{cases} E_p = -1 \Rightarrow R\equiv -1\ (\text{mod } p),\ R\equiv -1\ (\text{mod } 4)\,, \\ E_p = -2 \Rightarrow R\equiv -1\ (\text{mod } p),\ R\equiv 1\ (\text{mod } 4)\,, \\ E_p = +2 \Rightarrow R\equiv 1\ (\text{mod } p),\ R\equiv -1\ (\text{mod } 4)\,, \end{cases} \tag{10}$$

we note that Lemma 1 together with (10) gives immediately the following supplement to the biquadratic reciprocity law of Scholz type proved in [2].

Corollary 1. *If $p\equiv 1$ (mod 8) is a prime such that $h^+(8p)\equiv 0$ (mod 8) then*

$$\left(\frac{e_2}{p}\right)_4\left(\frac{e_p}{2}\right)_4 = \begin{cases} +1, & \textit{if } N(\eta_{2p}) = -1\,, \\ (-1)^{h^+(8p)/8}, & \textit{if } N(\eta_{2p}) = +1\,. \end{cases}$$

Next we examine each of the three quantities $\lambda(p)$, $\left(\frac{e_2}{p}\right)_4$, $\left(\frac{e_p}{2}\right)_4$, which appear in α and β.
First, from (8), we have

$$\lambda(p)=\frac{1}{2}\sum_{0<x<p/8}\left\{1+\left(\frac{x}{p}\right)\right\},$$

that is

$$\lambda(p)=\frac{1}{16}(p-1)+\frac{1}{2}\sum_{0<x<p/8}\left(\frac{x}{p}\right). \tag{11}$$

Now it is well-known that for primes $p\equiv 1 \pmod 8$ (see for example [3: p. 694])

$$\sum_{0<x<p/8}\left(\frac{x}{p}\right)=\frac{1}{4}\left(h(-4p)+h(-8p)\right), \tag{12}$$

where $h(-4p)$ and $h(-8p)$ are the class numbers of $Q(\sqrt{-p})$ and $Q(\sqrt{-2p})$ respectively. Hence, from (11) and (12), we obtain

$$\lambda(p)=\frac{1}{16}\left(p-1+2h(-4p)+2h(-8p)\right).$$

Then appealing to the easily proved result

$$\frac{p-1}{16}\equiv\frac{a-1}{8} \pmod 2 \tag{13}$$

we have

$$(-1)^{\lambda(p)}=(-1)^{(a-1+h(-4p)+h(-8p))/8}. \tag{14}$$

Secondly, by a theorem of Emma Lehmer [9], we have

$$\left(\frac{\varepsilon_2}{p}\right)_4=(-1)^{d/4},$$

and so by (4) we obtain

$$\left(\frac{e_2}{p}\right)_4=\left(\frac{2}{p}\right)_8(-1)^{d/4}.$$

Now by the Reuschle [11]–Western [12] criterion for 2 to be an eighth power (see also [13]), we haae

$$\left(\frac{2}{p}\right)_8=(-1)^{b/8},$$

so

(15) $$\left(\frac{e_2}{p}\right)_4 = (-1)^{(b+2d)/8}.$$

Thirdly, as $h^+(8p) \equiv 0 \pmod 8$, we have $h(-4p) \equiv 0 \pmod 8$ [4], and so $T \equiv 0 \pmod 8$ [6]. Moreover, as $p \equiv 1 \pmod 8$, $\sqrt{p}$ is defined modulo 16 and is odd, so that $T\sqrt{p} \equiv T \pmod{16}$, and we have from (5), as $p \equiv 1 \pmod{16}$,

$$\left(\frac{e_p}{2}\right)_4 = (-1)^{(pU+T-1)/8} = (-1)^{(T+U-1)/8}.$$

Appealing to (13) and the easily-proved result

$$U \equiv \frac{1}{2}(p+1) \pmod{16},$$

as well as a theorem of Williams [14]

$$h(-4p) \equiv T \pmod{16},$$

we obtain

(16) $$\left(\frac{e_p}{2}\right)_4 = (-1)^{(a-1+h(-4p))/8}.$$

From (9), (14), (15), (16), we see that

(17) $$\alpha = (-1)^{h(-8p)/8}, \quad \beta = (-1)^{(a-1+b+2d+h(-4p)+h(-8p))/8}.$$

Then by Lemma 1 we obtain the following theorem.

Theorem. *If $p \equiv 1$ (mod 8) is a prime such that $h^+(8p) \equiv 0$ (mod 8) and α and β are as given in (17), then*

$$\begin{aligned}
\alpha = \beta = 1 \quad &\Rightarrow h^+(8p) \equiv 0 \pmod{16},\\
\alpha = 1, \beta = -1 &\Rightarrow h^+(8p) \equiv 8 \pmod{16},\ E_p = -2,\\
\alpha = -1, \beta = 1 &\Rightarrow h^+(8p) \equiv 8 \pmod{16},\ E_p = +2,\\
\alpha = \beta = -1 \quad &\Rightarrow h^+(8p) \equiv 8 \pmod{16},\ E_p = -1.
\end{aligned}$$

As an immediate consequence of our Theorem we have the following corollary.

Corollary 2. *If $p \equiv 1$ (mod 8) is a prime such that $h^+(8p) \equiv 0$ (mod 8) then*

(18) $$\begin{cases} h^+(8p) \equiv T+a+b+2d-1 \pmod{16}, \text{ if } N(\eta_{2p}) = +1,\\ 0 \quad \equiv T+a+b+2d-1 \pmod{16}, \text{ if } N(\eta_{2p}) = -1; \end{cases}$$

and

(19) $$\begin{cases} h(-8p) \equiv 0 \pmod{16}, & \textit{if } E_p = -2,\\ h(-8p) \equiv h^+(8p) \pmod{16}, & \textit{if } E_p = -1, +2. \end{cases}$$

We remark that the congruences in (18) appear to be new but that those of (19) are contained in [7], [8].

Finally we compare our Theorem with the following result of Yamamoto [15].

Lemma 2. *If* $p\equiv 1$ *(mod 8) is a prime such that* $h^+(8p)\equiv 0$ *(mod 8) then*

$$\left(\frac{e}{p}\right)_4=\left(\frac{z-2^{h(p)}}{2}\right)_4=1\Rightarrow h^+(8p)\equiv 0 \pmod{16},$$

$$\left(\frac{e}{p}\right)_4=1,\ \left(\frac{z-2^{h(p)}}{2}\right)_4=-1\Rightarrow h^+(8p)\equiv 8 \pmod{16},\ E_p=-2,$$

$$\left(\frac{e}{p}\right)_4=-1,\ \left(\frac{z-2^{h(p)}}{2}\right)_4=1\Rightarrow h^+(8p)\equiv 8 \pmod{16},\ E_p=+2,$$

$$\left(\frac{e}{p}\right)_4=-1,\ \left(\frac{z-2^{h(p)}}{2}\right)_4=-1\Rightarrow h^+(8p)\equiv 8 \pmod{16},\ E_p=-1,$$

where $h(p)$ is the class number of $Q(\sqrt{p})$ and (z, w) is a solution of

$$z^2-pw^2=2^{h(p)+2},\quad z\equiv 2^{h(p)}+1 \pmod 4 .$$

Clearly from our Theorem and Lemma 2 we have the following corollary.

Corollary 3. *If* $p\equiv 1$ *(mod 8) is a prime such that* $h^+(8p)\equiv 0$ *(mod 8) then*

$$(-1)^{h(-8p)/8}=\left(\frac{e}{p}\right)_4 .$$

However corollary 3 is not quite as general as the following result of Leonard and Williams [10: Theorem 2] (since it is possible to have $h(-8p)\equiv 0$ (mod 8) but $h^+(8p)\not\equiv 0$ (mod 8), for example $p=73$):

$$(-1)^{h(-8p)/8}=\left(\frac{e}{p}\right)_4,$$

if p is a prime such that $h(-8p)\equiv 0$ (mod 8) and e is chosen so that $e\equiv 1$ (mod 8). We remark that Yamamoto [15] has shown that $(-1)^{h(-8p)/8}=\left(\frac{2c}{p}\right)_4$, if $p\equiv 1$ (mod 8) is a prime such that $h(-8p)\equiv 0$ (mod 8).

We conclude with a few examples.

EXAMPLE 1. $p=113$

Here $a=-7$, $b=8$, $c=9$, $d=4$, $e=25$, $f=16$,

$$h(-4p)=8,\quad h(-8p)=8,$$

so

$$\alpha=-1, \beta=-1 .$$

Hence, by Theorem, $h^+(8p)\equiv 8 \pmod{16}$ and $E_p=-1$.
Indeed $h^+(8p)=8$ and $15^2-226\cdot 1^2=-1$.

EXAMPLE 2. $p=353$
Here $a=17$, $b=8$, $c=-15$, $d=8$, $e=49$, $f=32$,

$$h(-4p)=16, \quad h(-8p)=24,$$

so

$$\alpha=-1, \beta=+1.$$

Hence, by Theorem, $h^+(8p)\equiv 8 \pmod{16}$ and $E_p=+2$.
Indeed $h^+(8p)=8$ and $186^2-706\cdot 7^2=+2$.

EXAMPLE 3. $p=1217$
Here $a=-31$, $b=16$, $c=33$, $d=8$, $e=97$, $f=64$,

$$h(-4p)=32, \quad h(-8p)=32,$$

so

$$\alpha=+1, \beta=+1.$$

Hence, by Theorem, $h^+(8p)\equiv 0 \pmod{16}$. Indeed $h^+(8p)=16$.

EXAMPLE 4. $p=257$
Here $a=1$, $b=16$, $c=-15$, $d=4$, $e=17$, $f=4$,

$$h(-4p)=16, \quad h(-8p)=16,$$

so

$$\alpha=+1, \beta=-1.$$

Hence, by Theorem 1, $h^+(8p)\equiv 8 \pmod{16}$ and $E_p=-2$.
Indeed $h^+(8p)=8$ and $68^2-514\cdot 3^2=-2$.

References

[1] J. Bucher: *Neues über Pell'sche Gleichung*, Naturforschende Gesellschaft Mitteilungen Luzern **14** (1943), 1–18.

[2] D.A. Buell and K.S. Williams: *An octic reciprocity law of Scholz type*, Proc. Amer. Math. Soc. **77** (1979), 315–318.

[3] C.F. Gauss: Untersuchungen über höhere Arithmetik, Chelsea, 1965.

[4] 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.

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

[6] P. Kaplan: *Unités de norme* -1 *de* $\boldsymbol{Q}(\sqrt{p})$ *et corps de classes de degré* 8 *de* $\boldsymbol{Q}(\sqrt{-p})$ *où* p *est un nombre premier congru à* 1 *modulo* 8, Acta Arith. **32** (1977), 239–243.

[7] P. Kaplan: *Nouvelle démonstration d'un congruence modulo* 16 *entre les nombres de classes d'idéaux de* $Q(\sqrt{-2p})$ *et* $Q(\sqrt{2p})$ *pour* p *premier* $\equiv 1$ (mod 4), Proc. Japan Acad. Ser. A **57** (1981), 507–509.

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

[9] E. Lehmer: *On the quartic character of quadratic units*, J. Reine Angew. Math. **268/269** (1974), 294–301.

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

[11] C.G. Reuschle: Mathematische Abhandlung, enthaltend neue Zahlen-theoretische Tabellen, Programm zum Schlusse des Schuljahres 1855–56 am Königlichen Gymnasium zu Stuttgart (1856), 61pp.

[12] A.E. Western: *Some criteria for the residues of eighth and other powers*, Proc. London Math. Soc. (2) **9** (1911), 244–272.

[13] A.L. Whiteman: *The sixteenth power residue character of* 2, Canad, J. Math. **6** (1954), 364–373.

[14] K.S. Williams: *On the class number of* $\boldsymbol{Q}(\sqrt{-p})$ *modulo* 16, *for* $p\equiv 1$ (*mod* 8) *a prime*, Acta Arith. **39** (1981), 381–398.

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

Pierre Kaplan
U.E.R. de Mathématiques
Université de Nancy
Nancy, France

Kenneth S. Williams
Department of Mathematics
and Statistics
Carleton University
Ottawa, Ontario
Canada K1S 5B6