Pacific Journal of Mathematics

THE CLASS NUMBER OF $Q(\sqrt{p})$ MODULO 4, FOR $p \equiv 5 \pmod 8$ A PRIME

KENNETH S. WILLIAMS

Vol. 92, No. 1 January 1981

PACIFIC JOURNAL OF MATHEMATICS
Vol. 92, No. 1, 1981

THE CLASS NUMBER OF $Q(\sqrt{p})$ MODULO 4, FOR $p \equiv 5 \pmod 8$ A PRIME

KENNETH S. WILLIAMS

Let $p \equiv 5 \pmod 8$ be a prime. Let $h(p)$ denote the class number of the real quadratic field $Q(\sqrt{p})$. It is well-known that $h(p) \equiv 1 \pmod 2$. In this paper the residue of $h(p)$ modulo 4 is determined.

Let $p \equiv 5 \pmod 8$ be a prime. Let $h = h(p)$ denote the class number of the real quadratic field $Q(\sqrt{p})$. It is well-known (see for example [2; § 3] that

$$h = h(p) \equiv 1 \pmod 2 . \tag{1}$$

In this paper we determine $h(p)$ modulo 4.

The fundamental unit ε_p (> 1) of $Q(\sqrt{p})$ can be written

$$\varepsilon_p = \frac{1}{2}(t + u\sqrt{p}) , \tag{2}$$

where t and u are positive integers satisfying

$$t \equiv u \pmod 2 . \tag{3}$$

The norm of ε_p is -1 so

$$t^2 - pu^2 = -4 . \tag{4}$$

If $t \equiv u \equiv 1 \pmod 2$ then we have (using (4))

$$\left(\frac{-1}{u}\right) = \left(\frac{-4}{u}\right) = \left(\frac{t^2 - pu^2}{u}\right) = \left(\frac{t^2}{u}\right) = +1 ,$$

so

$$u \equiv 1 \pmod 4 . \tag{5}$$

If $t \equiv u \equiv 0 \pmod 2$, we define positive integers t_1 and u_1 by $t = 2t_1$, $u = 2u_1$. Then, from (4), we have

$$t_1^2 = pu_1^2 - 1 \equiv 5u_1^2 - 1 \equiv 7 , \quad 4 \text{ or } 3 \pmod 8$$

according as

$$u_1^2 \equiv 0 , \quad 1 \text{ or } 4 \pmod 8 .$$

Clearly we must have $t_1^2 \equiv 4 \pmod 8$, so that

$$t_1 \equiv 2 \pmod 4 , \qquad u_1 \equiv 1 \pmod 2 . \tag{6}$$

Further, we have

$$\left(\frac{-1}{u_1}\right) = \left(\frac{t_1^2 - pu_1^2}{u_1}\right) = \left(\frac{t_1^2}{u_1}\right) = +1\,,$$

so

(7) $$u_1 \equiv 1 \pmod 4\,.$$

Next we define unique integers a and b by

(8) $$p = a^2 + b^2\,,\quad a \equiv -1 \pmod 4\,,\quad b \equiv -\left(\frac{p-1}{2}\right)!\; a \pmod p\,,$$

and we note that (as $p \equiv 5 \pmod 8$, a odd)

(9) $$b \equiv 2 \pmod 4\,.$$

We prove

THEOREM 1. (a) *If* $t \equiv u \equiv 1 \pmod 2$ *then*

$$h(p) \equiv \frac{1}{2}(-2t + u + b + 1) \pmod 4\,.$$

(b) *If* $t \equiv u \equiv 0 \pmod 2$ *then*

$$h(p) \equiv \frac{1}{2}(t_1 + u_1 + b + 1) \pmod 4\,.$$

The proof depends upon a number of lemmas.

LEMMA 1.

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^{(h+1)/2}\frac{t}{2} \pmod p\,.$$

This is a result of Chowla [3].

LEMMA 2. (a) *If* $t \equiv u \equiv 1 \pmod 2$ *then*

$$t + 2(-1)^{(h+1)/2} i \equiv 0 \pmod{a + bi}\,.$$

(b) *If* $t \equiv u \equiv 0 \pmod 2$ *then*

$$t_1 + (-1)^{(h+1)/2} i \equiv 0 \pmod{a + bi}\,.$$

Proof. From (8) and Lemma 1 we obtain

(10) $$at + 2b(-1)^{(h+1)/2} \equiv 0 \pmod p\,.$$

Then (4) and (10) give

$$t(2a(-1)^{(h+1)/2} - bt) = 2(at + 2b(-1)^{(h+1)/2})(-1)^{(h+1)/2} - bpu^2$$
$$\equiv 0 \pmod{p} .$$

As $t \not\equiv 0 \pmod{p}$, we deduce

(11) $$2a(-1)^{(h+1)/2} - bt \equiv 0 \pmod{p} .$$

Using (10) and (11) one easily verifies that $(t + 2(-1)^{(h+1)/2}i)/(a + bi)$ is a gaussian integer, which completes the proof of (a).

The proof of (b) is similar.

LEMMA 3. (a) *If* $t \equiv u \equiv 1 \pmod 2$ *there are integers* r *and* s *of opposite parity such that*

$$\begin{cases} t = a(r^2 - s^2) - b(2rs) , \quad u = r^2 + s^2 , \\ 2(-1)^{(h+1)/2} = a(2rs) + b(r^2 - s^2) . \end{cases}$$

(b) *If* $t \equiv u \equiv 0 \pmod 2$ *there are integers* r *and* s *of opposite parity such that*

$$\begin{cases} t_1 = -a(2rs) - b(r^2 - s^2) , \quad u_1 = r^2 + s^2 , \\ (-1)^{(h+1)/2} = a(r^2 - s^2) - b(2rs) . \end{cases}$$

Proof. (a) The gaussian integers $(t + 2(-1)^{(h+1)/2}i)/(a + bi)$ and $(t - 2(-1)^{(h+1)/2}i)/(a - bi)$ are coprime and their product is u^2. Hence there exist integers r and s such that

(12) $$\frac{t + 2(-1)^{(h+1)/2}i}{a + bi} = \varepsilon(r + si)^2 ,$$

where $\varepsilon = \pm 1, \pm i$. Multiplying both sides of (12) by $a + bi$ and considering the parities of the coefficients of i on both sides of the resulting equation, we see that $\varepsilon = \pm 1$. Replacing $r + si$ by $-s + ri$, if necessary, we can suppose, without loss of generality, that $\varepsilon = +1$ so

(13) $$t + 2(-1)^{(h+1)/2}i = (a + bi)(r + si)^2 .$$

Equating coefficients we obtain the required expressions for t and $2(-1)^{(h+1)/2}$. Finally, we have

$$\begin{aligned} u^2 &= \frac{t + 2(-1)^{(h+1)/2}i}{a + bi} \cdot \frac{t - 2(-1)^{(h+1)/2}i}{a - bi} \\ &= (r + si)^2(r - si)^2 \\ &= (r^2 + s^2)^2 , \end{aligned}$$

so, as $u > 0$, $r^2 + s^2 > 0$, we obtain

$$u = r^2 + s^2 .$$

Since u is odd this shows that r and s are of opposite parity.

(b) The proof is similar. In this case we obtain

$$t_1 + (-1)^{(h+1)/2} i = i(a+bi)(r+si)^2 . \tag{14}$$

LEMMA 4. (a) *If* $t \equiv u \equiv 1 \pmod 2$ *then*

$$u \equiv a + 2\left(\frac{2}{t}\right) \pmod 8 .$$

(b) *If* $t \equiv u \equiv 0 \pmod 2$ *then*

$$u \equiv a + 2 \pmod 8 .$$

Proof. (a) As $b \equiv 0 \pmod 2$ and one of r and s is even, we have, by Lemma 3(a),

$$t \equiv a(r^2 - s^2) \pmod 8 . \tag{15}$$

In particular, as $a \equiv -1 \pmod 4$, (15) gives

$$t \equiv s^2 - r^2 \pmod 4 ,$$

so that

$$\begin{cases} t \equiv 1 \pmod 4 \Longleftrightarrow r \text{ even, } s \text{ odd ,} \\ t \equiv -1 \pmod 4 \Longleftrightarrow r \text{ odd, } s \text{ even .} \end{cases} \tag{16}$$

Appealing to Lemma 3(a), (15) and (16), we obtain

$$\begin{aligned} u - a &\equiv (r^2 + s^2) - t(r^2 - s^2) \pmod 8 \\ &\equiv (1-t)r^2 + (1+t)s^2 \pmod 8 \\ &\equiv \begin{cases} 1+t \pmod 8 , & \text{if } r \text{ even, } s \text{ odd ,} \\ 1-t \pmod 8 , & \text{if } s \text{ odd, } s \text{ even ,} \end{cases} \\ &\equiv 2\left(\frac{2}{t}\right) \pmod 8 , \end{aligned}$$

as required.

(b) As $b \equiv 0 \pmod 2$ and one of r and s is even, we have by Lemma 3(b),

$$(-1)^{(h+1)/2} \equiv a(r^2 - s^2) \pmod 8 . \tag{17}$$

In particular, as $a \equiv -1 \pmod 4$, (17) gives

$$r^2 - s^2 \equiv (-1)^{(h-1)/2} \pmod 4 ,$$

so that

$$\begin{cases} h \equiv 1 \pmod 4 \Longleftrightarrow r \text{ odd, } s \text{ even ,} \\ h \equiv 3 \pmod 4 \Longleftrightarrow r \text{ even, } s \text{ odd .} \end{cases} \tag{18}$$

Appealing to Lemma 3(b), (17) and (18) we obtain

$$\begin{aligned} u_1 - a &\equiv (r^2 + s^2) - (-1)^{(h+1)/2}(r^2 - s^2) \pmod 8 \\ &\equiv (1 + (-1)^{(h-1)/2})r^2 + (1 + (-1)^{(h+1)/2})s^2 \pmod 8 \\ &\equiv 2 \pmod 8 , \end{aligned}$$

as required.

We are now in a position to prove Theorem 1.

Proof of Theorem 1. (a) As $r + s$ is odd, we have, by Lemma 3(a),

$$2rs = (r + s)^2 - (r^2 + s^2) \equiv 1 - u \pmod 8 . \tag{19}$$

Hence, by Lemma 3(a), (15) and (19), we have

$$2(-1)^{(h+1)/2} \equiv a(1 - u) + abt \pmod 8 ,$$

so, recalling $a \equiv -1 \pmod 4$, $b \equiv 2 \pmod 4$, $t \equiv u \equiv 1 \pmod 2$,

$$\begin{aligned} h &\equiv 2 + (-1)^{(h+1)/2} \pmod 4 \\ &\equiv 2 + a\left(\frac{1-u}{2}\right) + a\left(\frac{b}{2}\right)t \pmod 4 \\ &\equiv 2 + \left(\frac{u-1}{2}\right) - \frac{b}{2}t \pmod 4 \\ &\equiv 2 + \left(\frac{u-1}{2}\right) + \left(\frac{b}{2} - t - 1\right) \pmod 4 \\ &\equiv \frac{1}{2}(-2t + u + b + 1) \pmod 4 , \end{aligned}$$

as required.

(b) As $r + s$ is odd, we have, by Lemma 3(b),

$$2rs = (r + s)^2 - (r^2 + s^2) \equiv 1 - u_1 \pmod 8 . \tag{20}$$

From Lemma 3(b), (17) and (20), we have

$$t_1 \equiv -a(1 - u_1) - ab(-1)^{(h+1)/2} \pmod 8 ,$$

so (as $a \equiv -1 \pmod 4$)

$$\frac{t_1}{2} \equiv \left(\frac{1-u_1}{2}\right) + \left(\frac{b}{2}\right)(-1)^{(h+1)/2} \pmod 4 .$$

As $b \equiv 2 \pmod 4$, multiplying both sides by $b/2 \equiv 1 \pmod 2$, we obtain

$$\frac{b}{2}\cdot\frac{t_1}{2} \equiv \frac{b}{2}\cdot\left(\frac{1-u_1}{2}\right) + (-1)^{(h+1)/2} \pmod 4 ,$$

giving

$$\begin{aligned} h &\equiv 2 + (-1)^{(h+1)/2} \pmod 4 \\ &\equiv 2 + \frac{b}{2}\left(\frac{t_1 + u_1 - 1}{2}\right) \pmod 4 \\ &\equiv 2 + \left(\frac{t_1}{2} - 1\right) + \left(\frac{u_1 - 1}{2}\right) + \frac{b}{2} \pmod 4 \\ &\equiv \frac{1}{2}(t_1 + u_1 + b + 1) \pmod 4 , \end{aligned}$$

as required.

Using Lemma 4 in conjunction with Theorem 1, we obtain

COROLLARY 1. (i) *If* $t \equiv 1$ *or* $3 \pmod 8$ *or* $t_1 \equiv 6 \pmod 8$ *then*

$$h(p) \equiv \frac{1}{2}(a + b + 1) \pmod 4 .$$

(ii) *If* $t \equiv 5$ *or* $7 \pmod 8$ *or* $t_1 \equiv 2 \pmod 8$ *then*

$$h(p) \equiv \frac{1}{2}(a + b - 3) \pmod 4 .$$

Reformulating Theorem 1, we obtain

COROLLARY 2. (a) *If* $t \equiv u \equiv 1 \pmod 2$ *then*

$$h(p) \equiv \begin{cases} -t + \frac{1}{2}(u + 3) \pmod 4 , & \text{if } b \equiv 2 \pmod 8 , \\ t + \frac{1}{2}(u + 3) \pmod 4 , & \text{if } b \equiv 6 \pmod 8 . \end{cases}$$

(b) *If* $t \equiv u \equiv 0 \pmod 2$ *then*

$$h(p) \equiv \begin{cases} \frac{1}{2}(t_1 + u_1 + 3) \pmod 4 , & \text{if } b \equiv 2 \pmod 8 , \\ \frac{1}{2}(t_1 + u_1 - 1) \pmod 4 , & \text{if } b \equiv 6 \pmod 8 . \end{cases}$$

Now Gauss [5] has shown that $h(-p)$ (the class number of the imaginary quadratic field $Q(\sqrt{-p})$, see also [1: p. 828] satisfies.

LEMMA 5. $h(-p) \equiv a + b + 1 \pmod 8$.

Putting together Corollary 1 and Lemma 5 we obtain

COROLLARY 3. (i) *If* $t \equiv 1$ *or* $3 \pmod 8$ *or* $t_1 \equiv 6 \pmod 8$ *then*

$$h(-p) \equiv 2h(p) \pmod 8 .$$

(ii) *If* $t \equiv 5$ *or* 7 (mod 8) *or* $t_1 \equiv 2$ (mod 8) *then*

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

The result corresponding to Corollary 3 for primes $p \equiv 3 \pmod 4$ has been given by the author in [4].

Finally we show that there does not exist a result analogous to Theorem 1 for primes $p \equiv 1 \pmod 8$. It is easily checked that the above arguments fail to yield such a result in this case, as we do not know the exact power of 2 dividing b in the representation $p = a^2 + b^2$, a odd, b even. We prove

THEOREM 2. *Let* $p \equiv 1 \pmod 8$ *be a prime. We define unique integers* a *and* b *by*

$$p = a^2 + b^2 , \quad a \equiv -1 \pmod 4,\ b \equiv -\left(\frac{p-1}{2}\right)!\ a \pmod p ,$$

so that

$$b \equiv 0 \pmod 4 .$$

The fundamental unit (> 1) *of the real quadratic field* $Q(\sqrt{p})$ *is of the form*

$$\varepsilon_p = t_1 + u_1\sqrt{p} ,$$

where t_1 *and* u_1 *are positive integers such that*

$$t_1^2 - pu_1^2 = -1 , \quad t_1 \equiv 0 \pmod 4,\ u_1 \equiv 1 \pmod 4 .$$

Analogous to Lemma 4(b) *we have*

(21) $$u_1 \equiv a + 2 \pmod 8 .$$

Then there do NOT exist integers l_1, l_2, l_3, l_4 *independent of* p, *such that*

(22) $$h(p) \equiv \frac{1}{2}(l_1a + l_2b + l_3t_1 + l_4) \pmod 4 .$$

(*Note*: *We remark that it is unnecessary to include multiples of either* p *or* u_1 *inside the parentheses on the right hand side of* (22) *since* $p \equiv 1 \pmod 8$ *and* u_1 *satisfies* (21).)

Proof. Suppose that a congruence of the form holds. Taking $p = 97$, so that $t_1 = 5604$, $u_1 = 569$, $a = -9$, $b = +4$, $h = 1$; and $p = 257$, so that $t_1 = 16$, $u_1 = 1$, $a = -1$, $b = +16$, $h = 3$; we must have

(23) $$\begin{cases} -9l_1 + 4l_2 + 5604l_3 + l_4 \equiv 2 \pmod 8 , \\ -l_1 + 16l_2 + 16l_3 + l_4 \equiv 6 \pmod 8 . \end{cases}$$

Subtracting the two congruences in (23) we obtain

$$8l_1 + 12l_2 - 5588l_3 \equiv 4 \pmod 8 ,$$

that is

$$4l_2 + 4l_3 \equiv 4 \pmod 8 ,$$

or

(24) $$l_2 + l_3 \equiv 1 \pmod 2 .$$

Next taking $p = 41$, so that $t_1 = 32$, $u_1 = 5$, $a = -5$, $b = +4$, $h = 1$; and $p = 73$, so that $t_1 = 1068$, $u_1 = 125$, $a = 3$, $b = -8$, $h = 1$; we obtain

(25) $$\begin{cases} -5l_1 + 4l_2 + 32l_3 + l_4 \equiv 2 \pmod 8 , \\ 3l_1 + 8l_2 + 1068l_3 + l_4 \equiv 2 \pmod 8 . \end{cases}$$

Subtracting the congruences in (25) we get

$$8l_1 - 12l_2 + 1036l_3 \equiv 0 \pmod 8$$

that is

$$4l_2 + 4l_3 \equiv 0 \pmod 8 ,$$

or

(26) $$l_2 + l_3 \equiv 0 \pmod 2 .$$

(24) and (26) provide the required contradiction.

References

1. Philippe Barkan, *Une propriété de congruence de la longueur de la période d'un développement en fraction continue*, C. R. Acad. Sci. Paris Sér. A, **281** (1975), 825-828.
2. Ezra Brown, *Class numbers of real quadratic number fields*, Trans. Amer. Math. Soc., **190** (1974), 99-107.
3. S. Chowla, *On the class number of real quadratic fields*, Proc. Nat. Acad. Sci. U.S.A., **47** (1961), 878.
4. Kenneth S. Williams, *The class number of $Q(\sqrt{-p})$ modulo 4, for $p \equiv 3 \pmod 4$ a prime*, Pacific J. Math., **83** (1979), 565-570.
5. Carl Friedrich Gauss, Werke, Zweiter Band, Koniglichen Gesellschaft der Wissenschafter, Göttingen (1876), 516-518.

Received May 1, 1979. Research supported by Grant No. A-7233 of the Natural Sciences and Engineering Research Council of Canada.

CARLETON UNIVERSITY
OTTAWA, ONTARIO, CANADA

Printed in Japan by International Academic Printing Co., Ltd., Tokyo, Japan

Pacific Journal of Mathematics

Vol. 92, No. 1 January, 1981

Michael E. Adams and J. Sichler, Lattices with unique complementation 1
Walter Allegretto, Positive solutions and spectral properties of second order elliptic operators 15
Philip J. Boland and Sean Dineen, Holomorphy on spaces of distribution . . . 27
Duncan Alan Buell, Philip A. Leonard and Kenneth S. Williams, Note on the quadratic character of a quadratic unit 35
Herbert Busemann and Bhalchandra B. Phadke, Two theorems on general symmetric spaces 39
Emeric Deutsch, Bounds for the Perron root of a nonnegative irreducible partitioned matrix 49
Charles F. Dunkl, A difference equation and Hahn polynomials in two variables 57
Gustave Adam Efroymson, The Riemann mapping theorem for planar Nash rings 73
John Albert Fridy and Robert Ellis Powell, Tauberian theorems for matrices generated by analytic functions 79
Denton Elwood Hewgill, John Hamilton Reeder and Marvin Shinbrot, Some exact solutions of the nonlinear problem of water waves 87
Bessie Hershberger Kirkwood and Bernard Robert McDonald, The symplectic group over a ring with one in its stable range 111
Esther Portnoy, Transitive groups of isometries on H^n 127
Jerry Ridenhour, On the sign of Green's functions for multipoint boundary value problems 141
Nina M. Roy, An M-ideal characterization of G-spaces 151
Edward Barry Saff and Richard Steven Varga, On incomplete polynomials. II 161
Takeyoshi Satō, The equations $\Delta u = Pu$ $(P \geqq 0)$ on Riemann surfaces and isomorphisms between relative Hardy spaces 173
James Henry Schmerl, Correction to: "Peano models with many generic classes" 195
Charles Madison Stanton, On the closed ideals in $A(W)$ 199
Viakalathur Shankar Sunder, Unitary equivalence to integral operators 211
Pavel G. Todorov, New explicit formulas for the nth derivative of composite functions 217
James Li-Ming Wang, Approximation by rational modules on boundary sets 237
Kenneth S. Williams, The class number of $Q(\sqrt{p})$ modulo 4, for $p \equiv 5$ (mod 8) a prime 241