PACIFIC JOURNAL OF MATHEMATICS
Vol. 83, No. 2, 1979

THE CLASS NUMBER OF $Q(\sqrt{-p})$ MODULO 4, FOR $p\equiv 3$ (MOD 4) A PRIME

KENNETH S. WILLIAMS

If p is a prime congruent to 3 modulo 4, it is well-known that the class number $h(-p)$ of the imaginary quadratic field $Q(\sqrt{-p})$ is odd. In this paper we determine $h(-p)$ modulo 4.

The class number of $Q(\sqrt{-p})$ is odd, if p is a prime congruent to 3 modulo 4 (see for example [3: p. 413]. D.H. Lehmer [4: p. 9] has posed the problem of determining the Jacobi symbol $(-1/h(-p))=(-1)^{(h(-p)-1)/2}$, that is, of determining $h(-p)$ modulo 4. In this paper we evaluate $h(-p)$ modulo 4 in terms of the class number $h(p)$ and the fundamental unit $\varepsilon_p = T + U\sqrt{p}$ of the corresponding real quadratic field $Q(\sqrt{p})$. It is known that T and U are positive integers which satisfy $T\equiv 0 \pmod 2$, $U\equiv 1 \pmod 2$, $N(\varepsilon_p) = T^2 - pU^2 = +1$. We prove

THEOREM. *If $p > 3$ is a prime congruent to 3 modulo 4 then*

$$h(-p) \equiv h(p) + U + 1 (\mathrm{mod}\ 4) . \tag{1}$$

It is easily checked that (1) does not hold for $p = 3$ ($h(-3)=h(3) = U = 1$). ($p = 3$ is a special case as this is the only value of $p\equiv 3 (\mathrm{mod}\ 4)$ for which the ring of integers of $Q(\sqrt{-p})$ has more than 2 units.) The method of proof is purely analytic in nature, it uses Dirichlet's class number formula (in various forms) for both real and imaginary quadratic fields and also some results from cyclotomy. It would be of interest to give a purely algebraic proof.

Proof. Let $p > 3$ be a prime congruent to 3 modulo 4 and set $\rho = \exp(2\pi i/p)$. For z a complex variable, we let

$$F_+(z) = \prod_{\substack{j=1\\(j/p)=+1}}^{p-1} (z-\rho^j),\ F_-(z) = \prod_{\substack{j=1\\(j/p)=-1}}^{p-1} (z-\rho^j) , \tag{2}$$

so that

$$F_+(z)F_-(z) = F(z) , \tag{3}$$

where $F(z)$ is the cyclotomic polynomial of index p, that is,

$$F(z) = \prod_{j=1}^{p-1} (z - \rho^j) = \frac{z^p - 1}{z - 1} = z^{p-1} + z^{p-2} + \cdots + z + 1 . \tag{4}$$

F_+ and F_- are polynomials in z of degree $(p-1)/2$ with coefficients in the ring of integers of $Q(\sqrt{-p})$ (see for example [6: p. 215]). Hence we can write

$$F_+(z) = \frac{1}{2}(Y(z) - Z(z)\sqrt{-p}) , \quad F_-(z) = \frac{1}{2}(Y(z) + Z(z)\sqrt{-p}) , \tag{5}$$

where Y and Z are polynomials with rational integral coefficients. From (3) and (5) we have

$$Y(z)^2 + pZ(z)^2 = 4F(z) . \tag{6}$$

It is also known [6: p.216] or [7: p. 209] that Y and Z have the symmetry properties expressed by

$$Y(z) = \sum_{n=0}^{(p-3)/4} a_n(z^{(p-1)/2-n} - z^n) , \quad Z(z) = \sum_{n=0}^{(p-3)/4} b_n(z^{(p-1)/2-n} + z^n) , \tag{7}$$

where the a_n and b_n are integers with

$$a_0 = 2, a_1 = 1, a_2 = (3 - p)/4 , \cdots$$

and

$$b_0 = 0, b_1 = 1, b_2 = \frac{1}{2}\left(1 + \left(\frac{2}{p}\right)\right) , \cdots$$

(see [7] for further values of a_n and b_n: see [6] for a table of values of Y and Z for $p \leqq 29$).

Differentiating the expressions in (7) and (6) with respect to z, we obtain respectively

$$\begin{aligned} Y'(z) &= \sum_{n=0}^{(p-3)/4} a_n \left(\left(\frac{p-1}{2} - n\right)z^{(p-3)/2-n} - nz^{n-1}\right) , \\ Z'(z) &= \sum_{n=0}^{(p-3)/4} b_n \left(\left(\frac{p-1}{2} - n\right) z^{(p-3)/2-n} + nz^{n-1}\right) , \end{aligned} \tag{8}$$

and

$$Y(z)Y'(z) + pZ(z)Z'(z) = 2F'(z) . \tag{9}$$

Taking $z = i$ in (7) and (8) we obtain

$$\begin{aligned} Y(i) &= \begin{cases} A_3(1 - i), \text{ if } p \equiv 3 \pmod 8 , \\ A_7(1 + i), \text{ if } p \equiv 7 \pmod 8 , \end{cases} \\ Z(i) &= \begin{cases} -B_3(1 + i), \text{ if } p \equiv 3 \pmod 8 , \\ B_7(1 - i), \text{ if } p \equiv 7 \pmod 8 , \end{cases} \end{aligned} \tag{10}$$

and

$$(11)\qquad Y'(i) = \begin{cases} C_3 + 2D_3 i, \text{ if } p \equiv 3 \pmod 8, \\ C_7 + 2D_7 i, \text{ if } p \equiv 7 \pmod 8, \end{cases} \quad Z'(i) = \begin{cases} E_3 + 2F_3 i, \text{ if } p \equiv 3 \pmod 8, \\ E_7 + 2F_7 i, \text{ if } p \equiv 7 \pmod 8, \end{cases}$$

where $A_3, \cdots, F_7$ are rational integers (given in terms of the a_n and b_n). Using (10) and (11) in (6) and (9) with $z = i$, we obtain

$$(12)\qquad \begin{cases} A_3^2 - pB_3^2 = -2, \text{ if } p \equiv 3 \pmod 8, \\ A_7^2 - pB_7^2 = +2, \text{ if } p \equiv 7 \pmod 8, \end{cases}$$

and

$$(13)\qquad \begin{cases} A_3C_3 + 2pB_3F_3 = -1,\ 2A_3D_3 - pB_3E_3 = p, \text{ if } p \equiv 3 \pmod 8, \\ A_7C_7 + 2pB_7F_7 = p,\ 2A_7D_7 - pB_7E_7 = 1, \text{ if } p \equiv 7 \pmod 8. \end{cases}$$

Clearly from (12) and (13) we see that A_3, B_3, C_3, E_3, A_7, B_7, C_7 and E_7 are all odd. Now Liouville [5: p. 415] has shown that

$$(14)\qquad Z(z)Y'(z) - Z'(z)Y(z) = \frac{2}{z-1}\sum_{j=1}^{p-1}\left(\frac{j}{p}\right)z^{p-1-j}.$$

Taking $z = i$ in (14) we obtain

$$(15)\qquad Z(i)Y'(i) - Z'(i)Y(i) = (L + M) + i(L - M),$$

where

$$L = \sum_{j=0}^{(p-1)/2}(-1)^j\left(\frac{2j}{p}\right), \quad M = \sum_{j=0}^{(p-1)/2}(-1)^j\left(\frac{2j+1}{p}\right).$$

Applying the transformation $j \to (p-1)/2 - j$ to L or M we obtain $L = M$. Also we have

$$\begin{aligned} L &= \sum_{j=1}^{(p-3)/4}\left(\frac{4j}{p}\right) - \sum_{j=0}^{(p-3)/4}\left(\frac{4j+2}{p}\right) \\ &= \sum_{j=1}^{(p-3)/4}\left(\frac{j}{p}\right) - \sum_{j=(p+1)/4}^{(p-1)/2}\left(\frac{4((p-1)/2 - j) + 2}{p}\right) \\ &= \sum_{j=1}^{(p-3)4}\left(\frac{j}{p}\right) + \sum_{j=(p+1)/4}^{(p-1)/2}\left(\frac{j}{p}\right) = \sum_{j=1}^{(p-1)/2}\left(\frac{j}{p}\right), \end{aligned}$$

so, by Dirichlet's class number formula (as $p \equiv 3 \pmod 4$, $p < 3$) see for example [2: p. 346], we have

$$(16)\qquad L = M = \left\{2 - \left(\frac{2}{p}\right)\right\}h(-p).$$

Hence from (15) and (16) we have

$$Z(i)Y'(i) - Z'(i)Y(i) = 2\left\{2 - \left(\frac{2}{p}\right)\right\}h(-p)\ . \tag{17}$$

Using (10) and (11) in (17), after equating real and imaginary parts, we obtain

$$\begin{cases} 3h(-p) = 2B_3D_3 - A_3E_3\ , & \text{if } p \equiv 3 \pmod 8\ , \\ h(-p) = 2B_7D_7 - A_7E_7\ , & \text{if } p \equiv 7 \pmod 8\ . \end{cases} \tag{18}$$

Now from (13) we have

$$\begin{cases} E_3 \equiv -2A_3B_3D_3 - B_3 \pmod 8, \text{ if } p \equiv 3 \pmod 8\ , \\ E_7 \equiv -2A_7B_7D_7 + B_7 \pmod 8, \text{ if } p \equiv 7 \pmod 8\ . \end{cases} \tag{19}$$

Using (19) in (18) we have

$$h(-p) \equiv \begin{cases} -A_3B_3 \pmod 4, \text{ if } p \equiv 3 \pmod 8\ , \\ -A_7B_7 \pmod 4, \text{ if } p \equiv 7 \pmod 8\ . \end{cases} \tag{20}$$

From (4) we have $F(i) = i$, and so taking $z = i$ in (2) and (3) we obtain

$$\begin{aligned} -i\{F_-(i)\}^2 = \frac{F_-(i)}{F_+(i)} &= \prod_{j=1}^{p-1}(1 + i\rho^j)^{-(j/p)} \\ &= \exp\left(-\sum_{j=1}^{p-1}\left(\frac{j}{p}\right)\log(1 + i\rho^j)\right) \\ &= \exp\left(\sum_{n=1}^{\infty}\frac{(-i)^n}{n}\sum_{j=1}^{p-1}\left(\frac{j}{p}\right)\rho^{nj}\right) \\ &= \exp\left(i\sqrt{p}\sum_{n=1}^{\infty}\left(\frac{n}{p}\right)\frac{(-i)^n}{n}\right) \\ &= \exp\left(\sqrt{p}\sum_{m=0}^{\infty}\left(\frac{2m+1}{p}\right)\frac{(-1)^m}{2m+1} + \frac{i\sqrt{p}}{2}\left(\frac{2}{p}\right)\sum_{m=1}^{\infty}\left(\frac{m}{p}\right)\frac{(-1)^m}{m}\right) \\ &= \exp\left(h(p)\log(T + U\sqrt{p}) + \frac{\pi i}{2}\left(1 - \left(\frac{2}{p}\right)\right)h(-p)\right) \\ &= (T + U\sqrt{p})^{h(p)}i^{(1-(2/p))h(-p)} \\ &= (-1)^{(p+1)/4}(T + U\sqrt{p})^{h(p)}\ , \end{aligned}$$

where we have made use of the Gauss sum

$$\sum_{j=1}^{p-1}\left(\frac{j}{p}\right)\rho^{nj} = \left(\frac{n}{p}\right)i\sqrt{p}\ ,$$

and the two results

$$\sum_{m=1}^{\infty}\left(\frac{m}{p}\right)\frac{(-1)^m}{m} = \frac{\pi}{\sqrt{p}}\left(\left(\frac{2}{p}\right)-1\right)h(-p)$$

and

$$\sum_{m=0}^{\infty}\left(\frac{2m+1}{p}\right)\frac{(-1)^m}{2m+1} = \frac{h(p)}{\sqrt{p}}\log(T+U\sqrt{p})\ ,$$

which follow easily by standard arguments from Dirichlet's class number formula (see for example [2: p. 343]). Hence we have (using (10))

$$\begin{aligned}(T+U\sqrt{p})^{h(p)} &= (-1)^{(p-3)/4}iF_{-}(i)^2\\ &= (-1)^{(p-3)/4}i\left\{\frac{1}{2}(Y(i)+Z(i)i\sqrt{p})\right\}^2\\ &= \begin{cases}\frac{1}{2}(A_3+B_3\sqrt{p})^2, \text{ if } p\equiv 3 \pmod 8\ ,\\ \frac{1}{2}(A_7+B_7\sqrt{p})^2, \text{ if } p\equiv 7 \pmod 8\ .\end{cases}\end{aligned}$$

This is essentially a result of Arndt [1].

Expanding $(T+U\sqrt{p})^{h(p)}$ by the binomial theorem and equating coefficients of $\sqrt{p}$, we have as $h(p)\equiv 1 \pmod 2$,

$$U^{h(p)}p^{(h(p)-1)/2}+\binom{h(p)}{2}U^{h(p)-2}T^2p^{(h(p)-3)/2}+\cdots = \begin{cases}A_3B_3, \text{ if } p\equiv 3 \pmod 8\ ,\\ A_7B_7, \text{ if } p\equiv 7 \pmod 8\ .\end{cases}$$

As $T\equiv 0 \pmod 2$, $U\equiv 1 \pmod 2$, this gives

$$U(-1)^{(h(p)-1)/2}\equiv\begin{cases}A_3B_3 \pmod 4, \text{ if } p\equiv 3 \pmod 8\ ,\\ A_7B_7 \pmod 4, \text{ if } p\equiv 7 \pmod 8\ ,\end{cases}$$

so that

$$h(p)\equiv\begin{cases}A_3B_3-U+1 \pmod 4, \text{ if } p\equiv 3 \pmod 8\ ,\\ A_7B_7-U+1 \pmod 4, \text{ if } p\equiv 7 \pmod 8\ .\end{cases}\tag{21}$$

Putting (20) and (21) together, we obtain (1) as required.

From (1) we have $(-1/h(-p)) = (-1)^{(h(-p)-1)/2} = (-1)^{(h(p)+U)/2}$. In particular whenever $h(p)=1$ (a common occurrence) we have $(-1/h(-p)) = (-1)^{(U+1)/2}$.

In [8] the author has treated, in a similar way, Lehmer's question [4: p. 10] regarding $h(-2p)$ modulo 8, when p is a prime congruent to 5 modulo 8.

References

1. F. Arndt, *Bemerkung zu den Formeln von Dirichlet, durch welche die Klassenzahl bei positiver Determinante ausgedrückt wird*, J. Reine Angew. Math., **56** (1859), 100.
2. Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, New York and London, 1966.
3. Ezra Brown, *The power of* 2 *dividing the class-number of a binary quadratic discriminant*, J. Number Theory, **5** (1973), 413-419.
4. D. H. Lehmer, *Problem* 38, Problems from Western Number Theory Conferences, edited by David G. Cantor, 16 pp.
5. J. Liouville, *Un point de la théorie des équations binomes*, J. Math. Pures Appl., **2** (1857), 413-423.
6. G. B. Mathews, *Theory of Numbers*, reprinted by Chelsea Publishing Co., New York.
7. G. K. C. von Staudt, *Ueber die Functionen* Y *und* Z, *welche der Gleichung* $4(x^p-1)/(x-1)=Y^2\mp pZ^2$ *Genüge leisten, wo* p *eine Primzahl der Form* $4k\pm 1$ *ist*, J. Reine Angew. Math., **67** (1867), 205-217.
8. Kenneth S. Williams, *The class number of* $Q(\sqrt{-2p})$ *modulo* 8, *for* $p\equiv 5 \pmod 8$ *a prime*, submitted for publication.

Received July 12, 1978. Research supported by National Research Council of Canada Grant No. A-7233.

CARLETON UNIVERSITY
OTTAWA, CANADA K1S 5B6