ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 11, Number 1, Winter 1981

THE CLASS NUMBER OF $Q(\sqrt{-2p})$ MODULO 8, FOR $p \equiv 5 \pmod 8$ A PRIME

KENNETH S. WILLIAMS*

ABSTRACT. Let $p \equiv 5 \pmod 8$ be a prime. Let $h(\pm 2p)$ denote the class number of the quadratic field $Q(\sqrt{\pm 2p})$. Let $T + U\sqrt{2p}$ be the fundamental unit of $Q(\sqrt{2p})$. It is shown that $h(-2p) \equiv h(2p) + 2T + 2 \pmod 8$.

If p is a prime congruent to 5 modulo 8, it is well known that the class number $h(-2p)$ of the imaginary quadratic field $Q(\sqrt{-2p})$ is congruent to 2 modulo 4 (see for example [**2**: p. 413]). In this paper, we determine $h(-2p)$ modulo 8. This is a problem of D.H. Lehmer [**6**: p. 10]. (The corresponding problem for $h(-p)$, $p \equiv 3 \pmod 4$, has been solved by the author in [**9**].)

We let $\varepsilon_{2p} = T + U\sqrt{2p}$ be the fundamental unit of the real quadratic field $Q(\sqrt{2p})$, so that T and U are positive integers. It is a classical theorem of Dirichlet [**5**: p. 226] that ε_{2p} has norm -1, that is,

$$N(\varepsilon_{2p}) = T^2 - 2pU^2 = -1,$$

from which it follows that T and U are both odd. The class number $h(2p)$ of $Q(\sqrt{2p})$ is also congruent to 2 modulo 4 (see for example [**3**: p. 101]). With this notation we prove the following theorem.

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

PROOF. It is assumed throughout that p is a prime congruent to 5 modulo 8. We set $\rho = \exp(2\pi i/p)$. For z a complex variable, we let

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

so that

$$F_+(z)F_-(z) = F(z), \tag{2}$$

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

MOS Subject Classification Numbers: 12A25, 12A50.
Key words and phrases: Quadratic fields, class number, fundamental unit, Dirichlet class number formula.
*Research supported by National Research Council of Canada Grant No. A-7233.
Received by the editors on August 1, 1978.
Copyright © 1981 Rocky Mountain Mathematics Consortium

that is,

$$F(z) = \prod_{j=1}^{p-1} (z - \rho^j) = \frac{z^p - 1}{z - 1} = z^{p-1} + z^{p-2} + \cdots + z + 1. \tag{3}$$

F_+ and F_- are each polynomials in z of degree $(p-1)/2$ with coefficients in the ring of integers of $Q(\sqrt{p})$ (see for example [7: p. 215]). Hence we can write

$$F_+(z) = (Y(z) - Z(z)\sqrt{p})/2, \quad F_-(z) = (Y(z) + Z(z)\sqrt{p})/2, \tag{4}$$

where Y and Z are polynomials with rational integral coefficients. From (2) and (4) we have

$$Y(z)^2 - pZ(z)^2 = 4F(z). \tag{5}$$

It is also known [7: p. 216] that Y and Z have the forms

$$Y(z) = \sum_{n=0}^{(p-5)/4} a_n(z^{(p-1)/2-n} + z^n) + a_{(p-1)/4} z^{(p-1)/4}, \tag{6}$$

$$Z(z) = \sum_{n=0}^{(p-5)/4} b_n(z^{(p-1)/2-n} + z^n) + b_{(p-1)/4} z^{(p-1)/4}, \tag{7}$$

where the a_n and b_n are integers with $a_0 = 2$, $a_1 = 1$, $a_2 = (p+3)/4$, ... and $b_0 = 0$, $b_1 = 1$, $b_2 = 0$, ... For further values of a_n and b_n see, for example, [7: pp. 217–218] or [8: pp. 210–217].

Taking $z = \omega = \exp(2\pi i/8) = (1+i)/\sqrt{2}$ (note $\omega^2 = i$, $\omega^4 = -1$, $\omega^6 = -i$, $\omega^8 = +1$) in (3), (6) and (7) we obtain

$$F(\omega) = \omega + \omega^2 + \omega^3, \tag{8}$$

$$Y(\omega) = \begin{cases} A_5 + B_5\omega + A_5\omega^2, & \text{if } p \equiv 5 \pmod{16}, \\ A_{13} - A_{13}\omega^2 + B_{13}\omega^3, & \text{if } p \equiv 13 \pmod{16}, \end{cases} \tag{9}$$

$$Z(\omega) = \begin{cases} C_5 + D_5\omega + C_5\omega^2, & \text{if } p \equiv 5 \pmod{16}, \\ C_{13} - C_{13}\omega^2 + D_{13}\omega^3, & \text{if } p \equiv 13 \pmod{16}, \end{cases} \tag{10}$$

where A_5, B_5, C_5, D_5, A_{13}, B_{13}, C_{13}, D_{13} are rational integers depending upon the a_n and b_n. Substituting (8), (9) and (10) into (5) with $z = \omega$, we obtain

$$\begin{cases} 2A_5^2 + B_5^2 - 2pC_5^2 - pD_5^2 = 4, \\ A_5B_5 - pC_5D_5 = 2, \end{cases} \quad \text{if } p \equiv 5 \pmod{16}, \tag{11}$$

and

$$\begin{cases} 2A_{13}^2 + B_{13}^2 - 2pC_{13}^2 - pD_{13}^2 = -4, \\ A_{13}B_{13} - pC_{13}D_{13} = 2, \end{cases} \quad \text{if } p \equiv 13 \pmod{16}. \tag{12}$$

Now, from Dirichlet's class number formula (see for example [**1**: p. 343] or [**4**: p. 171], we have

$$h(2p) = \frac{\sqrt{2p}}{\log(T + U\sqrt{2p})} \sum_{n=1}^{\infty} \left(\frac{8p}{n}\right) \frac{1}{n}$$

and

$$h(-2p) = \frac{2\sqrt{2p}}{\pi} \sum_{n=1}^{\infty} \left(\frac{-8p}{n}\right) \frac{1}{n}.$$

As

$$\sum_{n=1}^{\infty} \left(\frac{\pm 8p}{n}\right) \frac{1}{n} = \sum_{n=0}^{\infty} \left(\frac{\pm 2p}{2n+1}\right) \frac{1}{2n+1} = \sum_{n=0}^{\infty} \left(\frac{\pm 2}{2n+1}\right)\left(\frac{2n+1}{p}\right) \frac{1}{2n+1}$$

and

$$\left(\frac{2}{2n+1}\right) = \begin{cases} (-1)^{n/2}, & \text{if } n \text{ even}, \\ (-1)^{(n+1)/2}, & \text{if } n \text{ odd} \end{cases} \qquad \left(\frac{-2}{2n+1}\right) = \begin{cases} (-1)^{n/2}, & \text{if } n \text{ even}, \\ (-1)^{(n-1)/2}, & \text{if } n \text{ odd} \end{cases}$$

we obtain

$$\frac{h(2p)}{2} \log(T + U\sqrt{2p}) = \frac{\sqrt{p}}{\sqrt{2}} \sum_{n=0}^{\infty} \left\{\left(\frac{4n+1}{p}\right)\frac{(-1)^n}{4n+1} - \left(\frac{4n+3}{p}\right)\frac{(-1)^n}{4n+3}\right\} \tag{13}$$

and

$$\frac{\pi h(-2p)}{4} = \frac{\sqrt{p}}{\sqrt{2}} \sum_{n=0}^{\infty} \left\{\left(\frac{4n+1}{p}\right)\frac{(-1)^n}{4n+1} + \left(\frac{4n+3}{p}\right)\frac{(-1)^n}{4n+3}\right\}. \tag{14}$$

Thus, from (13) and (14), we obtain (recalling that $h(2p) \equiv h(-2p) \equiv 2 \pmod 4$)

$$\begin{aligned} & i(-1)^{(h(-2p)-2)/4} (T + U\sqrt{2p})^{h(2p)/2} \\ &= \exp\left\{\frac{h(2p)}{2} \log (T + U\sqrt{2p}) + \frac{\pi i h(-2p)}{4}\right\} \\ &= \exp\left\{\frac{\sqrt{p}}{2} \sum_{n=0}^{\infty} \left\{\left(\frac{4n+1}{p}\right)\frac{\sqrt{2}(1+i)(-1)^n}{4n+1} - \left(\frac{4n+3}{p}\right)\frac{\sqrt{2}(1-i)(-1)^n}{4n+3}\right\}\right\}, \end{aligned}$$

that is,

$$\begin{aligned} & i(-1)^{(h(-2p)-2)/4} (T + U\sqrt{2p})^{h(2p)/2} \\ &\quad = \exp\left\{\frac{\sqrt{p}}{2} \sum_{n=1}^{\infty} \left(\frac{n}{p}\right)(1 - (-1)^n) \frac{\omega^n}{n}\right\}. \end{aligned} \tag{15}$$

Using the familiar Gauss sum (recall $p \equiv 5 \pmod 8$)

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

in (15), and after interchanging the order of the resulting summations, we obtain

$$i(-1)^{(h(-2p)-2)/4}(T + U\sqrt{2p})^{h(2p)/2} = \exp\left\{\tfrac{1}{2}\sum_{j=1}^{p-1}(j/p)(\log(1 + \omega\rho^j) - \log(1 - \omega\rho^j))\right\}, \tag{16}$$

where (here and throughout) log denotes the principal branch of the logarithm. Now

$$\begin{aligned}
&\sum_{j=1}^{p-1}(j/p)(\log(1 + \omega\rho^j) - \log(1 - \omega\rho^j)) \\
&= \left\{-\sum_{\substack{j=1\\(j/p)=-1}}^{p-1} + \sum_{\substack{j=1\\(j/p)=+1}}^{p-1}\right\}(\log(1 + \omega\rho^j) - \log(1 - \omega\rho^j)) \\
&= \left\{-2\sum_{\substack{j=1\\(j/p)=-1}}^{p-1} + \sum_{j=1}^{p-1}\right\}(\log(1 + \omega\rho^j) - \log(1 - \omega\rho^j)),
\end{aligned}$$

so (16) becomes

$$i(-1)^{(h(-2p)-2)/4}(T + U\sqrt{2p})^{h(2p)/2} = \prod_{\substack{j=1\\(j/p)=-1}}^{p-1}\frac{1 - \omega\rho^j}{1 + \omega\rho^j}\cdot\exp\left\{\tfrac{1}{2}\sum_{j=1}^{p-1}(\log(1 + \omega\rho^j) - \log(1 - \omega\rho^j))\right\}. \tag{17}$$

Taking $z = \pm\omega^3$ in (1) we obtain (after a little manipulation) as $p \equiv 5 \pmod 8$

$$\prod_{\substack{j=1\\(j/p)=-1}}^{p-1}\frac{1 - \omega\rho^j}{1 + \omega\rho^j} = \frac{F_-(-\omega^3)}{F_-(\omega^3)}. \tag{18}$$

Next, using (4), (9) (10) with $z = \pm\omega^3$, and making use of (11) and (12), we find, after some manipulation,

$$\frac{F_-(-\omega^3)}{F_-(\omega^3)} = \begin{cases}\dfrac{(A_5^2 - pC_5^2 - 1) + (A_5D_5 - B_5C_5)\sqrt{2p}/2}{1 - \sqrt{2}}, & \text{if } p \equiv 5 \pmod{16},\\[2ex] \dfrac{(A_{13}^2 - pC_{13}^2 + 1) + (B_{13}C_{13} - A_{13}D_{13})\sqrt{2p}/2}{-1 + \sqrt{2}}, & \text{if } p \equiv 13 \pmod{16},\end{cases} \tag{19}$$

From (11) and (12), we see that L and M, defined by

$$L = \begin{cases}A_5^2 - pC_5^2 - 1, & \text{if } p \equiv 5 \pmod{16},\\ A_{13}^2 - pC_{13}^2 + 1, & \text{if } p \equiv 13 \pmod{16},\end{cases} \tag{20}$$

and

$$M = \begin{cases} (A_5D_5 - B_5C_5)/2, & \text{if } p \equiv 5 \pmod{16}, \\ (B_{13}C_{13} - A_{13}D_{13})/2, & \text{if } p \equiv 13 \pmod{16}, \end{cases} \tag{21}$$

are odd integers. Moreover we have

$$L \equiv (-1)^{(p+3)/8} \pmod 4. \tag{22}$$

Putting (17), (18), (19), (20) and (21) together, we obtain

$$\begin{aligned} &i(1 - \sqrt{2})(-1)^{(p-5)/8+(h(-2p)-2)/4}(T + U\sqrt{2p})^{h(2p)/2}(L + M\sqrt{2p})^{-1} \\ &= \exp\left\{\tfrac{1}{2}\sum_{j=1}^{p-1}(\log(1 + \omega\rho^j) - \log(1 - \omega\rho^j))\right\}. \end{aligned} \tag{23}$$

Next we consider

$$\sum_{j=1}^{p-1}\log(1 - i\rho^j) = \sum_{j=1}^{p-1}\log(1 - \omega^2\rho^j).$$

As j runs through $1, 2, \ldots, p-1$ so does $2j \pmod p$, so we have

$$\begin{aligned} &\sum_{j=1}^{p-1}\log(1 - i\rho^j) \\ &= \sum_{j=1}^{p-1}\log(1 - \omega^2\rho^{2j}) \\ &= \sum_{j=1}^{p-1}\log\{(1 + \omega\rho^j)(1 - \omega\rho^j\} \\ &= \sum_{j=1}^{p-1}\{\log(1 + \omega\rho^j) + \log(1 - \omega\rho^j) \\ &\quad + i(\arg((1 + \omega\rho^j)(1 - \omega\rho^j)) - \arg(1 + \omega\rho^j) - \arg(1 - \omega\rho^j))\}, \end{aligned}$$

where $\arg(z)$ denotes the principal value of the argument of z, that is, $\arg(z)$ is restricted to satisfy $-\pi < \arg(z) \leqq \pi$. Hence we have

$$\begin{aligned} &\sum_{j=1}^{p-1}(\log(1 + \omega\rho^j) - \log(1 - \omega\rho^j)) \\ &= -2\sum_{j=1}^{p-1}\log(1 - \omega\rho^j) \\ &\quad + \sum_{j=1}^{p-1}\log(1 - i\rho^j) + i(\arg(1 + \omega\rho^j) + \arg(1 - \omega\rho^j) - \arg(1 - i\rho^{2j}))\} \\ &= -2\sum_{j=1}^{p-1}\log(1 - \omega\rho^j) \\ &\quad + \sum_{j=1}^{p-1}\{\log(1 - i\rho^j) + i(\arg(1 + \omega\rho^j) + \arg(1 - \omega\rho^j) - \arg(1 - i\rho^j))\} \\ &= -2\sum_{j=1}^{p-1}\log(1 - \omega\rho^j) + \log\prod_{j=1}^{p-1}(1 - i\rho^j) \\ &\quad - i\arg\left(\prod_{j=1}^{p-1}(1 - i\rho^j)\right) + i\sum_{j=1}^{p-1}(\arg(1 + \omega\rho^j) + \arg(1 - \omega\rho^j)), \end{aligned}$$

that is

$$\begin{aligned}(24)\quad &\sum_{j=1}^{p-1}(\log(1+\omega\rho^j)-\log(1-\omega\rho^j))\\ &=-2\sum_{j=1}^{p-1}\log(1-\omega\rho^j)+i\sum_{j=1}^{p-1}(\arg(1+\omega\rho^j)+\arg(1-\omega\rho^j)),\end{aligned}$$

where we have again used the fact that as j runs through $1, 2, \ldots, p-1$ so does $2j \pmod p$, and the result

$$\prod_{j=1}^{p-1}(1-i\rho^j)=\frac{1-i^p}{1-i}=\frac{1-i}{1-i}=1.$$

Putting (23) and (24) together, we obtain

$$\begin{aligned}(25)\quad &i(1-\sqrt{2})(-1)^{(p-5)/8+(h(-2p)-2)/4}(T+U\sqrt{2p})^{h(2p)/2}(L+M\sqrt{2p})^{-1}\\ &=\prod_{j=1}^{p-1}(1-\omega\rho^j)^{-1}\cdot\exp\left\{\frac{i}{2}\sum_{j=1}^{p-1}(\arg(1+\omega\rho^j)+\arg(1-\omega\rho^j))\right\}.\end{aligned}$$

As

$$\prod_{j=1}^{p-1}(1-\omega\rho^j)^{-1}=\frac{1-\omega}{1-\omega^p}=\frac{1-\omega}{1+\omega}=\frac{-i}{1+\sqrt{2}},$$

(25) becomes

$$\begin{aligned}(26)\quad &(-1)^{(p-5)/8+(h(-2p)-2)/4}(T+U\sqrt{2p})^{h(2p)/2}(L+M\sqrt{2p})^{-1}\\ &=\exp\left\{\frac{i}{2}\sum_{j=1}^{p-1}(\arg(1+\omega\rho^j)+\arg(1-\omega\rho^j))\right\}.\end{aligned}$$

Now, for $j = 1, 2, \ldots, p-1$, we have

$$1+\omega\rho^j=2\cos(\pi j/p+\pi/8)\,e^{(\pi j/p+\pi/8)i}$$

and

$$1-\omega\rho^j=2\sin(\pi j/p+\pi/8)\,e^{(\pi j/p-3\pi/8)i}.$$

Since

$$\begin{aligned}&\cos(\pi j/p+\pi/8)>0, \quad \text{for } 1\leqq j<3p/8,\\ &\cos(\pi j/p+\pi/8)<0, \quad \text{for } 3p/8<j\leqq p-1,\\ &\sin(\pi j/p+\pi/8)>0, \quad \text{for } 1\leqq j<7p/8,\\ &\sin(\pi j/p+\pi/8)<0, \quad \text{for } 7p/8<j\leqq p-1,\end{aligned}$$

we have

$$\arg(1+\omega\rho^j)=\begin{cases}\pi j/p+\pi/8, & \text{for } 1\leqq j<3p/8,\\ \pi j/p-7\pi/8, & \text{for } 3p/8<j\leqq p-1,\end{cases}$$

and

$$\arg(1 - \omega\rho^j) = \begin{cases} \pi j/p - 3\pi/8, & \text{for } 1 \leqq j < 7p/8, \\ \pi j/p - 11\pi/8, & \text{for } 7p/8 < j \leqq p - 1, \end{cases}$$

so

$$\arg(1 + \omega\rho^j) + \arg(1 - \omega\rho^j) = \begin{cases} 2\pi j/p - \pi/4, & \text{for } 1 \leqq j < 3p/8, \\ 2\pi j/p - 5\pi/4, & \text{for } 3p/8 < j < 7p/8, \\ 2\pi j/p - 9\pi/4, & \text{for } 7p/8 < j \leqq p - 1, \end{cases}$$

giving

$$\begin{aligned} &\sum_{j=1}^{p-1} (\arg(1 + \omega\rho^j) + \arg(1 - \omega\rho^j)) \\ &= \frac{2\pi}{p} \sum_{j=1}^{p-1} j - \frac{\pi}{4} \cdot \frac{3p - 7}{8} - \frac{5\pi}{4} \cdot \frac{p + 1}{2} - \frac{9\pi}{4} \cdot \frac{p - 5}{8} \\ &= \pi(p - 1) - \pi(p - 1) \\ &= 0. \end{aligned}$$

Using this, (26) gives the important result connecting $h(-2p)$ and $h(2p)$, namely,

$$(27) \qquad (T + U\sqrt{2p})^{h(2p)/2} = (-1)^{(p-5)/8 + (h(-2p)-2)/4}(L + M\sqrt{2p}).$$

Expanding the left hand side of (27) by the binomial theorem, and equating rational parts, we obtain

$$\begin{aligned} &T^{h(2p)/2} + \binom{h(2p)/2}{2} T^{(h(2p)-4)/2} U^2 (2p) \\ &\quad + \binom{h(2p)/2}{4} T^{(h(2p)-8)/2} U^4 (2p)^2 \\ &\quad + \cdots = (-1)^{(p-5)/8 + (h(-2p)-2)/4} L. \end{aligned} \tag{28}$$

Reducing (28) modulo 4, we obtain (using (22) and recalling that $h(2p) \equiv 2 \pmod 4$, $T \equiv U \equiv 1 \pmod 2$, $p \equiv 5 \pmod 8$)

$$T + \frac{h(2p)}{2} - 1 \equiv (-1)^{(h(-2p)+2)/4} \pmod 4$$

or

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

This completes the proof of the theorem.

We remark that our proof is purely analytic in nature and that it would be interesting to give an algebraic one. We also note that for those primes p for which $h(2p) = 2$ (a common occurrence) our theorem takes the simple form

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

or

$$\left(\frac{-1}{h(-2p)/2)}\right) = (-1)^{(T+1)/2}.$$

Finally, I would like to thank Mr. Lee-Jeff Bell for computing for me the polynomials $Y(z)$ and $Z(z)$, together with the corresponding values of $A_5, \ldots, D_{13}$, for all primes $p \equiv 5 \pmod 8$ with $p \leq 317$. These values were indispensable in formulating the correct sign in the relation $(Y + U\sqrt{2p})^{h(2p)/2} = \pm (L + M\sqrt{2p})$ (see (27)).

REFERENCES

1. Z.I. Borevich and I.R. Shafarevich, *Number Theory*, Academic Press, New York and London, 1966.

2. E. Brown, *The power of* 2 *dividing the class-number of a binary quadratic discriminant*, J. Number Theory **5** (1973), 413–419.

3. ———, *Class numbers of real quadratic number fields*, Trans. Amer. Math Soc. **190** (1974), 99–107.

4. H. Cohn, *A Second Course in Number Theory*, John Wiley and Sons, Inc., New York and London, 1962.

5. P.G.L. Dirichlet, *Einige neue Sätze über unbestimmte Gleichungen*, Abh. Königlich Preussischen Akad. Wiss. (1834), 649–664. (Reprinted in Ges. Werke, Chelsea (1969), 221–236).

6. D.H. Lehmer, *Problem* 38, *Problems from Western Number Theory Conferences*, edited by David G. Cantor, 9–10.

7. G.B. Mathews, *Theory of Numbers*, republished by Chelsea Publishing Company, New York, 1961.

8. G.K.C. von Staudt, *Über 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.

9. K. S. Williams, *The class number of* $Q(\sqrt{-p})$ *modulo* 4, *for* $p \equiv 3 \pmod 4$ *a prime*, submitted for publication.

DEPARTMENT OF MATHEMATICS, CARLETON UNIVERSITY, OTTAWA, ONTARIO, CANADA K1S 5B6