PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 93, Number 2, February 1985

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

KENNETH S. WILLIAMS AND CHRISTIAN FRIESEN[1]

ABSTRACT. An explicit congruence modulo 8 is given for the class number of the real quadratic field $Q(\sqrt{2p})$, where p is a prime congruent to 5 modulo 8.

Let Q denote the rational number field. Let $Q(\sqrt{d})$ denote the quadratic extension of Q having discriminant d. The class number of $Q(\sqrt{d})$ is denoted by $h(d)$. If $d > 0$ the fundamental unit (> 1) of $Q(\sqrt{d})$ is denoted by ε_d.

If $d = p$, where $p \equiv 5 \pmod 8$ is a prime, it is a classical result of Gauss that $h(p) \equiv 1 \pmod 2$ (see for example [**4**, §3]) and the author [**10**, Theorem 1] has given an explicit congruence for $h(p)$ modulo 4, namely;

$$(1) \qquad h(p) \equiv \begin{cases} \frac{1}{2}(-2t + u + b + 1) \pmod 4, & \text{if } t \equiv u \equiv 1 \pmod 2, \\ \frac{1}{4}(t + u + 2b + 2) \pmod 4, & \text{if } t \equiv u \equiv 0 \pmod 2, \end{cases}$$

where

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

and a and b are integers given uniquely by

$$(3) \qquad p = a^2 + b^2, \quad a \equiv 1 \pmod 4, \qquad b \equiv \left(\tfrac{1}{2}(p-1)\right)!a \pmod p.$$

In this short note we obtain the corresponding congruence to (1) for $d = 8p$, where $p \equiv 5 \pmod 8$ is prime. In this case $h(8p) \equiv 2 \pmod 4$ (see for example [**4**, Theorem 1(b)]) and we prove

THEOREM. *For $p \equiv 5 \pmod 8$ a prime we have*

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

where $\varepsilon_{8p} = T + U\sqrt{2p}$ is the fundamental unit of $Q(\sqrt{2p})$ (of discriminant $8p$) and b is given by (3).

PROOF. Our starting point is the following congruence given by Gauss [**6**] in 1828:

$$(5) \qquad h(-4p) \equiv -a + b + 1 \pmod 8.$$

Received by the editors October 11, 1983.

1980 *Mathematics Subject Classification*. Primary 12A25, 12A50.

Key words and phrases. Quadratic fields, class number, fundamental unit, Dirichlet class number formula.

[1] The research of the first author was supported by Natural Sciences and Engineering Research Council Canada Grant No. A-7233, while that of the second was supported by a Natural Sciences and Engineering Research Council Canada Undergraduate Summer Research Award.

A proof by Dedekind is given in Volume 2 of the 1876 edition of Gauss's collected works. In recent years the congruence (5) has been reproved by Barkan [**1**, Corollary 2, p. 828 (with a misprint corrected)] and Williams and Currie [**12**, pp. 971–972]. Next we set

$$S_i = \sum_{ip/8 < x < (i+1)p/8} \left(\frac{x}{p}\right), \quad i = 0,1,2,3. \tag{6}$$

Dirichlet [**5**, p. 152] proved in 1840 that

$$h(-8p) = 2(S_0 - S_3), \tag{7}$$

and Holden [**8**, p. 130] proved in 1907 that

$$h(-4p) = -2(S_0 + S_3). \tag{8}$$

Adding (7) and (8) we obtain

$$\begin{aligned} h(-4p) + h(-8p) &= -4S_3 \equiv 4S_3 \pmod 8 \\ &\equiv 4 \sum_{x=(3p+1)/8}^{(p-1)/2} 1 \pmod 8 \\ &\equiv 4\frac{(p+3)}{8} \pmod 8, \end{aligned}$$

that is

$$h(-4p) + h(-8p) \equiv \tfrac{1}{2}(p+3) \pmod 8. \tag{9}$$

The congruence (9) has been rediscovered many times (see for example [**3**, p. 282]; [**7**, p. 188]; [**9**, p. 188]). Appealing to (3), we have, as $b \equiv 2 \pmod 4$,

$$\tfrac{1}{2}(p+3) \equiv a + 3 \pmod 8. \tag{10}$$

Putting (5), (9) and (10) together we obtain

$$h(-8p) \equiv 2a - b + 2 \equiv b \pmod 8. \tag{11}$$

The congruence (11) has been given by Barkan [**1**, Corollary 1, p. 828]. The required congruence (4) now follows from (11) and the congruence

$$h(-8p) \equiv h(8p) + 2T + 2 \pmod 8, \tag{12}$$

which has been established independently by Barkan [**2**, Lemma 2] and Williams [**11**, Theorem p. 19].

EXAMPLE. $p = 2861$. In this case we have $a = -19$, and $b = -50$, as $((p-1)/2)! \equiv 1659 \pmod{2861}$. Also $\varepsilon_{22888} = 15507 + 205\sqrt{5722}$, so $T = 15507$, $U = 205$, and the theorem gives $h(22888) \equiv 2 \cdot 15507 - 50 + 2 \equiv -2 \pmod 8$. Indeed $h(22888) = 6$.

It appears very unlikely that there is a similar result to (4) for primes $p \equiv 1 \pmod 8$ since for the primes 1097 ($\equiv 9 \pmod{16}$) and 1481 ($\equiv 9 \pmod{16}$) we have

$$T \equiv 1 \pmod{16}, \quad U \equiv 4 \pmod{16}, \quad a \equiv 13 \pmod{16}, \quad b \equiv 0 \pmod{16},$$

yet

$$h(8 \cdot 1097) \equiv 2 \pmod 8, \quad h(8 \cdot 1481) \equiv 6 \pmod 8.$$

References

1. Phillipe 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. ______, *Sur des propriétés de congruence* (mod 4) *liées à l'équation de Pell-Fermat*, C. R. Acad. Sci. Paris Sér. A **289** (1979), 303–306.

3. Bruce C. Berndt, *Classical theorems on quadratic residues*, L'Enseignement Math. **22** (1976), 261–304.

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

5. P. G. L. Dirichlet, *Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres*, J. Reine Angew. Math. **21** (1840), 134–155.

6. Carl Friedrich Gauss, Letter to P. G. L. Dirichlet dated 30 May 1828. (Reproduced in P. G. L. Dirichlet's *Werke*, Vol. 2, Chelsea, New York, pp. 378–380.)

7. J. W. L. Glaisher, *On the expressions for the number of classes of a negative determinant, and on the numbers of positives in the octants of P*, Quart. J. Math. **34** (1903), 178–204.

8. H. Holden, *On various expressions for h, the number of properly primitive classes for a negative determinant not containing a square factor* (fifth paper), Messenger Math. **36** (1907), 126–134.

9. A. Pizer, *On the 2-part of the class number of imaginary quadratic number fields*, J. Number Theory **8** (1976), 184–192.

10. Kenneth S. Williams, *The class number of* $Q(\sqrt{p})$ *modulo* 4, *for* $p \equiv 5 \pmod 8$ *a prime*, Pacific J. Math. **92** (1981), 241–248.

11. ______, *The class number of* $Q(\sqrt{-2p})$ *modulo* 8, *for* $p \equiv 5 \pmod 8$ *a prime*, Rocky Mountain J. Math. **11** (1981), 19–26.

12. Kenneth S. Williams and James D. Currie, *Class numbers and biquadratic reciprocity*, Canad. J. Math. **34** (1982), 969–988.

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