PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 31, No. 2, February 1972

THE CLASS NUMBER OF $Q(\sqrt{-p})$, FOR $p\equiv 1 \pmod 8$ A PRIME

EZRA BROWN

ABSTRACT. Let $h(-p)$ be the class number of the quadratic field $Q(\sqrt{-p})$, where $p\equiv 1 \pmod 8$ is a prime. Write $p=a^2+b^2=2e^2-d^2$, where $a\equiv e\equiv d\equiv b+1\equiv 1 \pmod 2$ and $e>0$. We prove that $h(-p)\equiv 0$ or $4 \pmod 8$ according as $(e|p)=1$ or -1; using this, we prove that $h(-p)\equiv(p-1)/2+b \pmod 8$. The proofs are elementary, relying on the theory of composition of binary quadratic forms.

1. **Introduction.** Let $h(-d)$ denote the class number of the algebraic number field $Q(\sqrt{-d})$. Recently, Barrucand and Cohn (see [**1**]) and Hasse (see [**2**] and [**3**]) have studied congruence conditions on $h(-p)$ and $h(-2p)$ modulo 8, where p is an odd prime. In this paper we present some new results related to this problem; in particular, we prove the following theorem.

THEOREM 1. *Let $p\equiv 1 \pmod 8$ be a prime, and write $p=a^2+b^2$, where a is odd and b is even. Then $h(-p)\equiv(p-1)/2+b \pmod 8$.*

2. **Preliminary definitions and results.** Our study uses the Gaussian theory of composition of binary quadratic forms; we begin by reviewing some standard definitions and results. For details and proofs, see [**4**].

DEFINITIONS. A binary quadratic form $[a, b, c]=ax^2+bxy+cy^2$ is called *primitive* if $(a, b, c)=1$ and *ambiguous* if $a|b$. An *ambiguous class* of forms is one which contains an ambiguous form. The *principal form* of discriminant d is $f_1=[1, \varepsilon, (\varepsilon-d)/4]$, where $\varepsilon=0$ or $1\equiv d \pmod 4$; the class (genus) containing f_1 is called the *principal class* (*genus*). The primitive classes of discriminant d form a group under Gaussian composition, called the *class group* (if $d<0$, only the positive-definite classes are considered). The symbol $(p|q)_4=1$ or -1 according as p is or is not a biquadratic residue (mod q), and $(p|q)$ is the Legendre quadratic residue symbol.

PROPOSITION. *If A and B are primitive classes of discriminant d, there exist forms $[a_1, b, a_2c]$ in A and $[a_2, b, a_1c]$ in B. The product (composite)*

Received by the editors March 29, 1971.

AMS 1970 *subject classifications*. Primary 12A25, 12A50; Secondary 10A15, 10C05.

Key words and phrases. Class number, quadratic residues, quadratic fields, algebraic number fields, composition of binary quadratic forms.

class AB of A and B is the class containing $[a_1 a_2, b, c]$. The ambiguous classes are precisely those classes A such that $A^2=I$, the principal class; every class in the principal genus is a square, and each genus contains the same number of classes. If $p\equiv 1 \pmod 8$ is a prime, $h(-p)$ is the number of positive-definite classes of discriminant $-4p$ ($=$determinant p).

3. **The main results.** Proof of Theorem 1 uses the following.

THEOREM 2. *Let $p\equiv 1 \pmod 8$ be a prime. Write $p=a^2+b^2=2e^2-d^2$, where $a\equiv d\equiv e\equiv b+1\equiv 1 \pmod 2$ and $e>0$. Then $h(-p)\equiv 0$ or $4 \pmod 8$ according as $(e|p)=1$ or -1.*

PROOF. If $p=2e^2-d^2$, then the form $f=[e, 2d, 2e]$ has determinant p. Denote by A the class of f, by B the class of $g=[2, 2, (p+1)/2]$, and by I the class of $f_1=[1, 0, p]$. The forms of determinant p have generic characters $(m|p)$ and $(-1|m)$, and are divided into two genera: the two ambiguous classes are I and B. Since $(2|p)=(-1|(p+1)/2)=1$, B is in the principal genus.

If $(e|p)=1$, then A is in the principal genus; by the proposition, $A=C^2$ for some class C. Now $A^2=B$, since $[e, 2d, 2e]^2=[e^2, 2d, 2]$, which is equivalent to g. Since A^3 contains $[2, 2d, e^2]\cdot[e, 2d, 2e]=[2e, 2d, e]$, $A^3=A^{-1}$. Hence, A is an element of order 4 in the class group G. Since C^2 has order 4, C has order 8 (this is easy to check). Hence G has an element of order 8, so we have that $h(-p)=\text{ord } G\equiv 0 \pmod 8$.

If $(e|p)=-1$, then f is in the nonprincipal genus, and so A is not the square of any class (for, if $A=C^2$, the generic characters of A would be the squares of those of C, and A would be in the principal genus). By the above, A has order 4. Let D be a class whose order is 2^n. If $n=0$, $D=I$; if $n=1$, $D=B$; if $n=2$, $D^2=B$, so $(DA)^2=B^2=I$, and hence $D=A$ or A^{-1}. If $n\geqq 3$, then either $A=(D^{2^{n-1}})^2$ or $A=((D^{-1})^{2^{n-1}})^2$, contrary to our assumption that A is in the nonprincipal genus, and thus not a square. Hence, the only elements of G of order 2^n are A, A^{-1}, B and I. Let H be the subgroup of G generated by A; we show that G/H has odd order. If there is a class K whose square is in H, then $K^2=A$, A^2, A^3 or I. In these cases, we see that either A is in the principal genus, $K=A$ or A^{-1}, A is in the principal genus, or $A=B$. None of these are possible by previous reasoning; hence G/H has odd order, and we have $h(-p)=\text{ord } G=\text{ord } H\cdot\text{ord } (G/H)=4 \text{ ord } (G/H)\equiv 4 \pmod 8$. Q.E.D.

PROOF OF THEOREM 1. Let $p=a^2+b^2=2e^2-d^2$, where $a\equiv d\equiv e\equiv b+1\equiv 1 \pmod 2$. From the congruences $2e^2\equiv d^2 \pmod p$ and $2e^2\equiv p \pmod d$, we find that $(e|p)=(2|p)_4(d|p)=(2|p)_4(p|d)=(2|p)_4(2|d)$. Since e is odd, $2e^2\equiv 2 \pmod{16}$; hence $p\equiv 2-d^2 \pmod{16}$. Thus, $p\equiv 1$ or $9 \pmod{16}$ according as $(2|d)=1$ or -1. Then $(e|p)=(2|p)_4$ or $-(2|p)_4$ according as $p\equiv 1$ or $9 \pmod{16}$. It is well known (see [5]) that if $p\equiv 1$

(mod 8) is a prime represented by a^2+b^2 with b even, then $(2|p)_4=(-1)^{b/4}$. Now, if $p\equiv 1 \pmod{16}$, then $(e|p)=1$ if and only if $b\equiv 0 \pmod 8$; if $p\equiv 9 \pmod{16}$, then $(e|p)=1$ if and only if $b\equiv 4 \pmod 8$. In each case, $(e|p)=1$ or -1 according as $(p-1)/2+b\equiv 0$ or 4 (mod 8). Hence, by Theorem 2, we have that $h(-p)\equiv(p-1)/2+b \pmod 8$. Q.E.D.

References

1. P. Barrucand and H. Cohn, *Note on primes of type x^2+32y^2, class number, and residuacity*, J. Reine Angew. Math. **238** (1969), 67–70. MR **40** #2641.

2. H. Hasse, *Über die Klassenzahl des Körpers $P(\sqrt{-p})$ mit einer Primzahl $p\equiv 1 \bmod 2^3$*, Aequationes Math. **3** (1969), 165–169. MR **40** #2642.

3. ———, *Über die Klassenzahl des Körpers $P(\sqrt{-2p})$ mit einer Primzahl $p\neq 2$*, J. Number Theory **1** (1969), 231–234. MR **39** #1424.

4. B. W. Jones, *The arithmetic theory of quadratic forms*, Carus Monograph Series, no. 10, Math. Assoc. of America, Buffalo, New York, 1950. MR **12**, 244.

5. A. L. Whiteman, *The sixteenth power residue character of* 2, Canad. J. Math. **6** (1954), 364–373. MR **16**, 14.

Department of Mathematics, Virginia Polytechnic Institute and State University, Blacksburg, Virginia 24061