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

NOTE ON THE QUADRATIC CHARACTER OF A QUADRATIC UNIT

DUNCAN A. BUELL, PHILIP A. LEONARD AND
KENNETH S. WILLIAMS

Results are obtained concerning evaluations of the quadratic character of real quadratic units of norm -1.

1. Introduction. Let m be a positive squarefree integer, and let ε_m denote the fundamental integral unit of the real quadratic field $Q(\sqrt{m})$, so that $\varepsilon_m = T + U\sqrt{m}$ with positive integers T and U. Throughout, it is assumed that ε_m has norm -1, so that $m \equiv 1, 5$ or $2 \pmod 8$, and all odd primes q dividing m satisfy $q \equiv 1 \pmod 4$. A number of recent papers ([1] – [3], [7], [9]-[12], [14], [16], [17]) have computed the quadratic character of such ε_m modulo a rational prime p, in terms of representations of a power of p by positive-definite binary quadratic forms of a certain discriminant associated with m. In this note we prove a result which, among other things, identifies the correct form-discriminant for evaluations of this type. A number of illustrations will be given in §3 and §4, after the proof in §2 of the following theorem.

THEOREM. *Let $f = 1, 2$ or 4 according as $m \equiv 1, 5$ or $2 \pmod 8$. Let G denote the group of primitive positive-definite binary quadratic forms of discriminant $-4mf^2$. Then G contains a subgroup H such that*

(i) *G/H is cyclic of order 4,*

and

(ii) *the prime p satisfies $(-1/p) = (m/p) = (\varepsilon_m/p) = 1$ if and only if p is represented by a form from a class in H.*

Before proving this result, we note that an analysis of the equation $T^2 + 1 = mU^2$ in the ring of Gaussian integers gives the following result.

LEMMA. *There exist integers A, B, C, D such that $1 + Ti = (A + Bi)(C + Di)^2$, $m = A^2 + B^2$, $A \equiv 1 \pmod 4$, and $B \equiv 0, 2$ or $T \pmod 4$ according as $m \equiv 1, 5$ or $2 \pmod 8$.* (Note: $C - 1 \equiv D \equiv 0 \pmod 2$).

2. Proof of the theorem. The splitting field, over Q, of the polynomial $x^4 - 2Tx^2 - 1$ is $M = Q(i, \sqrt{m}, \sqrt{\varepsilon_m})$, which is dihedral over Q, and cyclic of degree 4 over $K = Q(\sqrt{-m})$. The primes p