JOURNAL OF NUMBER THEORY 12, 106–109 (1980)

The Quartic Characters of Certain Quadratic Units

PHILIP A. LEONARD*

Department of Mathematics, Arizona State University, Tempe, Arizona 85281

AND

KENNETH S. WILLIAMS†

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

Received February 16, 1979

DEDICATED TO PROFESSOR S. CHOWLA ON THE OCCASION OF HIS 70TH BIRTHDAY

Criteria are obtained for the quartic residue character of the fundamental unit of the real quadratic field $Q((2q)^{1/2})$, where q is prime and either $q \equiv 7 \pmod 8$, or $q \equiv 1 \pmod 8$ and $X^2 - 2qY^2 = -2$ is solvable in integers X and Y.

1. INTRODUCTION

Let $m > 1$ be a squarefree integer, and let ϵ_m denote the fundamental unit of the real quadratic field $Q(m^{1/2})$. We assume throughout that ϵ_m has norm $+1$, and investigate the quartic residue character of ϵ_m modulo certain prime ideal divisors of the field $Q(m^{1/2})$. Evaluations of the quartic character of ϵ_m have been obtained by Lehmer [2], and by the present authors [3a,b] for certain values of m. If m is a prime q, the requirement that ϵ_q have norm $+1$ forces $q \equiv 3 \pmod 4$, and in this case the quartic character of ϵ_q has been evaluated (cf. [3b, Case 1.2]). In this paper we consider the case $m = 2q$, q prime.

Following Barrucand and Cohn [1], we consider the equations $X^2 - 2qY^2 = E$, q prime, $E = -1, 2$, or -2. For a given value of q exactly one of these three equations is solvable, and we use the terminology "$E = -2$" (for example) to mean that the equation $X^2 - 2qY^2 = -2$ has solutions. Since we are assuming that the norm of ϵ_{2q} is $+1$, we require $E \neq -1$, that is $E = \pm 2$. This excludes all primes $q \equiv 5 \pmod 8$ and

* Research supported by the Faculty Grant-in-Aid Program at Arizona State University.
† Research supported by Grant A-7233 of the National Research Council of Canada.

0022-314X/80/010106-04$02.00/0

certain primes $q \equiv 1 \pmod 8$. When $q \equiv 3 \pmod 8$, we have $E = -2$, and the evaluation of the quartic character of ϵ_{2q} has been carried out [3b, Case 1.5]. We now treat two of the remaining cases, namely,

(a) $q \equiv 7 \pmod 8$, so that $E = 2$, and

(b) $q \equiv 1 \pmod 8$, assuming $E = -2$.

The final case, which is $q \equiv 1 \pmod 8$ assuming $E = 2$, is more complicated. It is hoped to treat it, and some related questions, in a future paper.

Let p denote a rational prime, $\mathfrak{p}$ a prime ideal divisor of p in $Q((2q)^{1/2})$. Also, let h denote the class number of the imaginary quadratic field $Q((-2q)^{1/2})$, and set $l = h/4$. For q a prime satisfying (a) or (b), we prove the following

THEOREM. *Let p be a prime, such that $(-1/p) = (2/p) = (q/p) = 1$. Then ϵ_{2q} is a quartic residue modulo $\mathfrak{p}$ if and only if $p^l = x^2 + 2qy^2$ for coprime integers x and y.*

Our results, and the methods of proof, are similar to those of Parry [4] concerning the *quadratic* character of ϵ_q when $q \equiv 1 \pmod 8$ is prime. In particular, the quartic residue character of ϵ_{2q} is related to the (unramified) quartic extension of $Q((-2q)^{1/2})$ corresponding to the fourth powers in the ideal class group.

2. SOME LEMMAS

In what follows, (a) and (b) refer to the two cases mentioned in Section 1.

LEMMA 1. *Let H denote the ideal class group of $Q((-2q)^{1/2})$. Corresponding to H^2 is the genus field $Q((-2q)^{1/2}, E^{1/2})$, and to H^4 is the field $Q((-2q)^{1/2}, E^{1/2}, \mu^{1/2})$ with μ given as follows:*

(a) $\mu = U + 2V(2)^{1/2}$, *where* $-q = U^2 - 8V^2$, $U \equiv (-1)^V \pmod 4$,

and,

(b) $\mu = C + 2D(-2)^{1/2}$, *where* $q = C^2 + 8D^2$, $C \equiv (-1)^D \pmod 4$.

Proof. The field corresponding to H^2 is easily determined by genus theory. The biquadratic field for (a) is of "classical origin" [1], and that for (b) is similarly derived. The signs of C and of U are chosen so that $Q(E^{1/2}, \mu^{1/2})$ is unramified over $Q(E^{1/2})$, as $x^2 \equiv \mu \pmod 4$ has a solution in $Z[E^{1/2}]$.

LEMMA 2. *There exist integers R, S such that $\epsilon_{2q} = (R2^{1/2} + Sq^{1/2})^2$, and $4R^2 - 2qS^2 = E$.*

Proof. $\epsilon_{2q} = T + U(2q)^{1/2}$ for positive integers T and U, with $T^2 - 2qU^2 = 1$. Thus T is odd, $U = 2U_1$ and $(T+1)/2.(T-1)/2 = 2qU_1^2$. As $(T \pm 1)/2$ are coprime integers, we have either $(T \pm 1)/2 = R^2$ and $(T \mp 1)/2 = 2qS^2$, or, $(T \pm 1)/2 = 2R^2$ and $(T \mp 1)/2 = qS^2$, for integers R and S such that $RS = U_1$. The former implies $R^2 - 2qS^2 = \pm 1$, which is impossible as ϵ_{2q} is fundamental; hence, the latter possibility holds, with choice of signs determined by the value of E.

LEMMA 3. *Let R and S be as in Lemma* 2.

(a) *There are integers U, V, K, L such that $U \equiv (-1)^V \pmod 4$ and*

$$(U + 2V2^{1/2})(K + L2^{1/2})^2 = (-1)^{R/2}(1 + R2^{1/2}).$$

(b) *There are integers C, D, M, N such that $C \equiv (-1)^D \pmod 4$ and*

$$(C + 2D(-2)^{1/2})(M + N(-2)^{1/2})^2 = (-1)^{R/2}(1 - R(-2)^{1/2}).$$

Proof. As $4R^2 - 2qS^2 = E$, we have

(a) $-qS^2 = 1 - 2R^2 = (1 + R2^{1/2})(1 - R2^{1/2})$, and
(b) $qS^2 = 1 + 2R^2 = (1 + R(-2)^{1/2})(1 - R(-2)^{1/2})$.

The lemma follows upon an analysis of these equations in the unique factorization domains $Z[E^{1/2}]$, $E = 2, -2$, respectively. All normalizations are such that both μ and the right-hand member in each equation are congruent (mod 4) to squares in $Z[E^{1/2}]$.

Finally, we note that the identity

$$2(2R + E^{1/2})(2R + S(2q)^{1/2}) = (2R + E + S(2q)^{1/2})^2$$

has the following interpretations.

LEMMA 4. (a) $(2^{1/2})^2(1 + R(2)^{1/2})(R2^{1/2} + Sq^{1/2}) = (R2^{1/2} + 1 + Sq^{1/2})^2$.
(b) $(1 + i)^2(1 - R(-2)^{1/2})(R2^{1/2} + Sq^{1/2}) = (R2^{1/2} + i + Sq^{1/2})^2$.

3. PROOF OF THE THEOREM

Let $k = Q(i, 2^{1/2}, q^{1/2})$ and $K = k(\epsilon^{1/4}) = k((R2^{1/2} + Sq^{1/2})^{1/2})$, where R and S are as in Lemma 2. For p (prime) satisfying $(-1/p) = (2/p) = (q/p) = 1$, let $\mathfrak{p}$, $\mathfrak{P}$ be prime ideal divisors of p in $Q((2q)^{1/2})$ and k, respectively. Now ϵ_{2q} will be a quartic residue modulo $\mathfrak{p}$ precisely if $R2^{1/2} + Sq^{1/2}$ is a quadratic residue modulo $\mathfrak{P}$. From Lemmas 3 and 4 (using the given conditions on p)

we see that this happens if, and only if, (p) splits into prime ideal factors of degree one in the field $Q((-2q)^{1/2}, E^{1/2}, \mu^{1/2})$ of Lemma 1. As this field corresponds to H^4, (p) splits as required if and only if $p^l = x^2 + 2qy^2$. This completes the proof.

REFERENCES

1. P. BARRUCAND AND H. COHN, On some class-fields related to primes of type $x^2 + 32y^2$, *J. Reine Angew. Math.* **262/263** (1973), 400–414.
2. E. LEHMER, On the quartic character of quadratic units, *J. Reine Angew. Math.* **268/269** (1974), 294–301.
3. P. A. LEONARD AND K. S. WILLIAMS, On the quadratic and quartic character of certain quadratic units, (*a*) I, *Pacific J. Math.* **71** (1977), 101–106; (*b*) II, *Rocky Mountain J. Math.* **9** (1979), 683–692.
4. C. J. PARRY, On a conjecture of Brandler, *J. Number Theory* **8** (1976), 492–495.