

Pacific Journal of Mathematics

NOTE ON THE QUADRATIC CHARACTER OF A QUADRATIC UNIT

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

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

satisfying $(-1/p) = (m/p) = (\varepsilon_m/p) = 1$ are precisely those which split completely in M . It follows (see [4], especially Satz 8, proof of sufficiency) that, for the positive integer f such that (f) is the conductor of the abelian extension M/K , the group G of classes of forms of discriminant $-4mf^2$ has a subgroup H with the properties given in the theorem. It remains to show that $f = 1, 2$ or 4 according as $m \equiv 1, 5$ or $2 \pmod{8}$. Besides M and K , we shall require $L = Q(\sqrt{\varepsilon_m} - \sqrt{\varepsilon'_m})$ and its subfield $k = Q(i)$. For an abelian extension E/F of number fields, we let $d(E/F)$ denote the relative discriminant, $f(E/F)$ denote the finite part of the conductor, and $N_{E/F}(I)$ the relative norm of the ideal I of E . Then from the work of Halter-Koch ([5], Satz 7) $f(M/K) = (f)$ for a positive integer f . Moreover ([5], Satz 24, (2')), we have

$$(2.1) \quad d(L/Q) = d(K/Q)d(k/Q)\{f(M/K)\}^2 = 16mf^2.$$

On the other hand (see, for example, [13], p. 148), we have

$$(2.2) \quad d(L/Q) = \{d(k/Q)\}^2 N_{k/Q}(d(L/k)) = 16N_{k/Q}(d(L/k)).$$

Finally, as $(\sqrt{\varepsilon_m} - \sqrt{\varepsilon'_m})^2 = (1 - i)^2(A + Bi)(C + Di)^2$ by the lemma, we have $L = Q(i, \sqrt{A + Bi})$. Hence, by direct calculation (or see [8], p. 149), we obtain

$$(2.3) \quad d(L/k) = 2^e(A + Bi),$$

where $e = 0, 1$ or 2 according as $m \equiv 1, 5$ or $2 \pmod{8}$. Appealing to (2.1), (2.2), (2.3) we obtain the evaluation of f stated above.

3. A numerical example. We illustrate the theorem by calculating the subgroup H for the case $m = 226$. As $226 \equiv 2 \pmod{8}$, the theorem tells us that the correct discriminant is -128.113 . The group G is of order 32, and its structure is $C(8) \cdot C(4)$. The 32 classes can be represented by computing the primitive reduced forms of this discriminant. In order for p to be represented by a class from H , p must satisfy $(-1/p) = (226/p) = +1$, so by genus theory only 16 of these forms must be examined. By considering primes represented by these forms, and by appealing to the theorem, we find that H is made up of the principal class, together with the classes of the forms [5, ± 4 , 724], [29, ± 6 , 125], [32, 0, 113] and [25, ± 6 , 145]. Since H contains only two ambiguous classes, H is cyclic of order 8, and G/H is cyclic of order 4, as indicated by the theorem.

4. Conclusion. It is difficult to give H explicitly in general. In spite of this, we can make the theorem explicit in several cases, by considering primitive representations of powers of p by ambiguous

classes.

Sometimes this is possible when G has a particular structure. For example, if $m = q_1 q_2 \cdots q_r \equiv 1 \pmod{8}$, $N(\varepsilon_m) = -1$ and the 2-Sylow subgroup of G is of the type $C(2^t) \cdot C(2)^{r-1}$ with $t \geq 2$. G^2 is the principal genus in G , so that $[G:G^2] = 2^r$ and G^2 has a *unique* subgroup of index 2. This subgroup must be $H \cap G^2$, for otherwise $H \cap G^2 = G^2$, implying $G^2 \subseteq H$ which contradicts the fact that G/H is cyclic of order 4. Thus $H \cap G^2$ has order $l = h/2^{r+1}$, where h denotes the class-number of $Q(\sqrt{-m})$, and consists of those classes C in G^2 such that C^l is the principal class. A prime p satisfying $(-1/p) = (q_1/p) = \cdots = (q_r/p) = +1$ is represented by a class from G^2 . This class lies in H if and only if p^l is represented by the principal class. Therefore, by the theorem, $(\varepsilon_m/p) = +1$ if and only if $p^l = x^2 + my^2$. This result is due to Parry [14] when $r = 1$. When $r \geq 2$, a large class of examples is provided by choosing $m = q_1 q_2 \cdots q_r$, where $r = 2$ or r is odd, each $q_i \equiv 1 \pmod{8}$, and $(q_i/q_j) = -1$ when $i \neq j$, since in this situation ε_m has norm -1 [15] and the 2-Sylow subgroup is of the required type [6].

Another example is provided by choosing $m = q_1 q_2 \cdots q_r$, where r is odd, each $q_i \equiv 5 \pmod{8}$ and $(q_i/q_j) = -1$ when $i \neq j$. Again ε_m has norm -1 [15] and the 2-Sylow subgroup of the group of form-classes of discriminant $-4m$ has the structure $C(2)^r$. Thus the 2-Sylow subgroup of G has the structure $C(4) \cdot C(2)^{r-1}$, as going from discriminant $-4m$ to discriminant $-16m$ doubles the number of classes but introduces no new genera. The "principal genus case" then follows exactly as in the previous example. The remaining cases in this example are covered by a result of Kaplan and Williams [7]. With h as in the previous paragraph, we set $l' = h/2^r$, so that l' is odd. If p satisfies $(-1/p) = (m/p) = +1$ then $p^{l'}$ is represented by an ambiguous class, and so $p^{l'} = Qx^2 + Q'y^2$, where $QQ' = m$, $Q \equiv 1 \pmod{8}$ and $Q' \equiv 5 \pmod{8}$. Then [7] $(\varepsilon_m/p) = +1$ if and only if y is even.

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.
2. J. A. Brandler, *Residuacity properties of real quadratic units*, J. Number Theory, **5** (1973), 271-286.
3. ———, *On a theorem of Barrucand*, Boll. Un. Math. Ital., **12** (1975), 50-55.
4. G. Bruckner, *Charakterisierung der galoisschen Zahlkörper, deren zerlegte Primzahlen durch binäre quadratische Formen gegeben sind*, Math. Nachr., **32** (1966), 317-326.
5. F. Halter-Koch, *Arithmetische Theorie der Normalkörper von 2-Potenzgrad mit Die-dergruppe*, J. Number Theory, **3** (1971), 412-443.
6. P. Kaplan, *Sur le 2-groupe des classes d'ideaux des corps quadratiques*, J. reine angew. Math., **283/284** (1976), 313-363.
7. P. Kaplan and K. S. Williams, *Quadratic character of quadratic units and representa-*

tions of primes by binary quadratic forms, in preparation.

8. S. Kuroda, *Über die Zerlegung rationaler Primzahlen in gewissen nicht-abelschen galoisschen Körpern*, J. Math. Soc. Japan, **3** (1951), 148-156.
9. E. Lehmer, *On the quadratic character of the Fibonacci root*, Fibonacci Quart., **5** (1967), 135-138.
10. ———, *On the quadratic character of some quadratic surds*, J. reine angew. Math., **250** (1971), 42-48.
11. ———, *On some special quartic reciprocity laws*, Acta Arith., **21** (1972), 367-377.
12. P. A. Leonard and K. S. Williams, *The quadratic and quartic character of certain quadratic units*, I, Pacific J. Math., **71** (1977), 101-106; II, Rocky Mountain J. Math., **9** (1979), 683-692.
13. W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Warsaw, 1974.
14. C. J. Parry, *On a conjecture of Brandler*, J. Number Theory, **8** (1976), 492-495.
15. F. Tano, *Sur quelques théorèmes de Dirichlet*, J. reine angew. Math., **105** (1889), 160-169.
16. H. C. Williams, *The quadratic character of a certain quadratic surd*, Utilitas Math., **5** (1974), 49-55.
17. K. S. Williams, *On the evaluation of $(\epsilon_{q_1 q_2})$* , Rocky Mountain J. Math., **10** (1980), 559-573.

Received January 24, 1978. Research of the third author was supported by National Research Council of Canada Grant No. A-7233.

LOUISIANA STATE UNIVERSITY
BATON ROUGE, LA 70803

ARIZONA STATE UNIVERSITY
TEMPE, AZ 85281

AND

CARLETON UNIVERSITY
OTTAWA ONTARIO, CANADA, (K1S 5B6)

PACIFIC JOURNAL OF MATHEMATICS

EDITORS

DONALD BABBITT (Managing Editor)

University of California
Los Angeles, California 90024

HUGO ROSSI

University of Utah
Salt Lake City, UT 84112

C. C. MOORE AND ANDREW OGG

University of California
Berkeley, CA 94720

J. DUGUNDJI

Department of Mathematics
University of Southern California
Los Angeles, California 90007

R. FINN AND J. MILGRAM

Stanford University
Stanford, California 94305

ASSOCIATE EDITORS

R. ARENS

E. F. BECKENBACH

B. H. NEUMANN

F. WOLF

K. YOSHIDA

SUPPORTING INSTITUTIONS

UNIVERSITY OF ARIZONA

UNIVERSITY OF BRITISH COLUMBIA

CALIFORNIA INSTITUTE OF TECHNOLOGY

UNIVERSITY OF CALIFORNIA

MONTANA STATE UNIVERSITY

UNIVERSITY OF NEVADA, RENO

NEW MEXICO STATE UNIVERSITY

OREGON STATE UNIVERSITY

UNIVERSITY OF OREGON

UNIVERSITY OF SOUTHERN CALIFORNIA

STANFORD UNIVERSITY

UNIVERSITY OF HAWAII

UNIVERSITY OF TOKYO

UNIVERSITY OF UTAH

WASHINGTON STATE UNIVERSITY

UNIVERSITY OF WASHINGTON

Printed in Japan by International Academic Printing Co., Ltd., Tokyo, Japan

Michael E. Adams and J. Sichler, Lattices with unique complementation	1
Walter Allegretto, Positive solutions and spectral properties of second order elliptic operators	15
Philip J. Boland and Sean Dineen, Holomorphy on spaces of distribution . . .	27
Duncan Alan Buell, Philip A. Leonard and Kenneth S. Williams, Note on the quadratic character of a quadratic unit	35
Herbert Busemann and Bhalchandra B. Phadke, Two theorems on general symmetric spaces	39
Emeric Deutsch, Bounds for the Perron root of a nonnegative irreducible partitioned matrix	49
Charles F. Dunkl, A difference equation and Hahn polynomials in two variables	57
Gustave Adam Efroymsen, The Riemann mapping theorem for planar Nash rings	73
John Albert Fridy and Robert Ellis Powell, Tauberian theorems for matrices generated by analytic functions	79
Denton Elwood Hewgill, John Hamilton Reeder and Marvin Shinbrot, Some exact solutions of the nonlinear problem of water waves	87
Bessie Hershberger Kirkwood and Bernard Robert McDonald, The symplectic group over a ring with one in its stable range	111
Esther Portnoy, Transitive groups of isometries on H^n	127
Jerry Ridenhour, On the sign of Green's functions for multipoint boundary value problems	141
Nina M. Roy, An M -ideal characterization of G -spaces	151
Edward Barry Saff and Richard Steven Varga, On incomplete polynomials. II	161
Takeyoshi Satō, The equations $\Delta u = Pu$ ($P \geq 0$) on Riemann surfaces and isomorphisms between relative Hardy spaces	173
James Henry Schmerl, Correction to: "Peano models with many generic classes"	195
Charles Madison Stanton, On the closed ideals in $A(W)$	199
Viakalathur Shankar Sunder, Unitary equivalence to integral operators . . .	211
Pavel G. Todorov, New explicit formulas for the n th derivative of composite functions	217
James Li-Ming Wang, Approximation by rational modules on boundary sets	237
Kenneth S. Williams, The class number of $Q(\sqrt{p})$ modulo 4, for $p \equiv 5 \pmod{8}$ a prime	241