Pacific Journal of Mathematics

THE QUADRATIC AND QUARTIC CHARACTER OF CERTAIN QUADRATIC UNITS. I

PHILIP A. LEONARD AND KENNETH S. WILLIAMS

Vol. 71, No. 1 November 1977

PACIFIC JOURNAL OF MATHEMATICS
Vol. 71, No. 1, 1977

THE QUADRATIC AND QUARTIC CHARACTER OF CERTAIN QUADRATIC UNITS I

PHILIP A. LEONARD AND KENNETH S. WILLIAMS

Let ε_m denote the fundamental unit of the real quadratic field $Q(\sqrt{m})$. It is our purpose to evaluate the rational quadratic and biquadratic residue symbols of ε_m modulo a prime p for certain values of m.

We use the notation (ε_m/p) and $(\varepsilon_m/p)_4$ throughout this paper as rational quadratic and biquadratic residue symbols, interpreting $\sqrt{m}$ as an integer modulo p. In 1969 Barrucand and Cohn [1] proved, using the arithmetic of $Q(\sqrt{-1}, \sqrt{2})$, that if $p = 8n + 1$ is prime, so that $p = c^2 + 8d^2$, then

$$\left(\frac{\varepsilon_2}{p}\right) = \left(\frac{1+\sqrt{2}}{p}\right) = (-1)^d .$$

Since then a number of similar results have been obtained for certain other quadratic and quartic symbols using such tools as cyclotomy, rational biquadratic reciprocity laws, etc. (see Brandler [2], Lehmer [4], [5], [6]).

In this paper we apply the ideas of Barrucand and Cohn [1] in other biquadratic fields with unique factorization, thereby reproving some known results, proving some conjectures of E. Lehmer [6] and obtaining some additional new results. The method succeeds in the 21 imaginary bicyclic biquadratic fields having class number 1 and which contain $Q(\sqrt{-1})$, $Q(\sqrt{-2})$ or $Q(\sqrt{2})$ as a subfield. It would be interesting to know if similar techniques can be used in the remaining 26 imaginary bicyclic biquadratic fields with class number 1 or to determine octic symbols. (For a complete list of the imaginary bicyclic biquadratic fields with class number 1 see Brown and Parry [3].)

We now sketch the method used. First the quadratic or quartic symbol under consideration is expressed in terms of the representation of p by the indefinite form associated with the real quadratic subfield of the biquadratic field. This is accomplished using Jacobi's form of the law of quadratic reciprocity, and the results are given in the table below. In the case of those results involving quartic symbols it is first necessary to observe that $2\varepsilon_m$ is a square in the quadratic subfield, and this brings in the symbol $(2/p)_4$ whose value is well known, viz., if $p = 8n + 1$ is prime so that $p = a^2 + 16b^2 = c^2 + 8d^2$ then $(2/p)_4 = (-1)^b = (-1)^{n+d}$. Next we consider a prime

FIELD	CONGRUENTIAL CHARACTER OF PRIME p	QUADRATIC PARTITIONS OF p	CHARACTER OF FUNDAMENTAL UNIT	REFERENCES
$Q(\sqrt{-1}, \sqrt{2})$	$\left(\frac{-1}{p}\right)=\left(\frac{2}{p}\right)=1$	$p=c^2+8d^2$ $=u^2-32v^2 (u>0)$	$\left(\frac{\varepsilon_2}{p}\right)=\left(\frac{-1}{u}\right)=(-1)^d$	Barrucand and Cohn [1]
$Q(\sqrt{-1}, \sqrt{m})$ $m=5, 13, 37$	$\left(\frac{-1}{p}\right)=\left(\frac{m}{p}\right)=1$	$p=c^2+md^2$ and either $p=u^2-4mv^2 (u>0)$ or $4p=u^2-mv^2 (u \text{ odd}, u>0)$	$\left(\frac{\varepsilon_m}{p}\right)=\left(\frac{-1}{u+2v}\right)=(-1)^d$	Brandler [2] Lehmer [5]
$Q(\sqrt{-2}, \sqrt{m})$ $m=5, 29$	$\left(\frac{-1}{p}\right)=\left(\frac{-2}{p}\right)=\left(\frac{m}{p}\right)=1$	$p=c^2+8d^2$ $=g^2+8mh^2$ and either (i) $p=u^2-16mv^2 (u>0)$ or (ii) $4p=u^2-mv^2 (u \text{ odd}, u>0)$	$\left(\frac{\varepsilon_m}{p}\right)=\begin{cases}\left(\frac{-1}{u}\right) & \text{(i)}\\ \left(\frac{-1}{u+2v}\right) & \text{(ii)}\end{cases}=(-1)^{d+h}$	Lehmer [5]
$Q(\sqrt{2}, \sqrt{-3})$	$\left(\frac{-1}{p}\right)=\left(\frac{2}{p}\right)=\left(\frac{-3}{p}\right)=1$ $p=8n+1$	$p=a^2+48b^2$ $=x^2+24y^2$ $=u^2-8v^2 (u>0)$	$\left(\frac{\varepsilon_2}{p}\right)=\left(\frac{-1}{u+2v}\right)=(-1)^{n+b+y}$	
$Q(\sqrt{2}, \sqrt{-11})$	$\left(\frac{-1}{p}\right)=\left(\frac{2}{p}\right)=\left(\frac{-11}{p}\right)=1$ $p=8n+1$	$p=x^2+88y^2$ $=u^2-8v^2 (u>0)$ and either (i) $p=a^2+176b^2$ or (ii) $4p=a^2+11b^2$ $(a\equiv 1 \pmod 4)$	$\left(\frac{\varepsilon_2}{p}\right)=\left(\frac{-1}{u+2v}\right)=\begin{cases}(-1)^{n+b+y} & \text{(i)}\\ \frac{a-1}{4}+y & \\ (-1) & \text{(ii)}\end{cases}$	
$Q(\sqrt{-1}, \sqrt{3})$	$\left(\frac{-1}{p}\right)=\left(\frac{3}{p}\right)=\left(\frac{2}{p}\right)=1$	$p=a^2+16b^2$ $=x^2+48y^2$ $=u^2-3v^2 (u>0)$	$\left(\frac{\varepsilon_3}{p}\right)=1$ $\left(\frac{\varepsilon_3}{p}\right)_4=\left(\frac{2}{p}\right)_4\left(\frac{-2}{u+v}\right)=(-1)^y$	Lehmer [6]

$Q(\sqrt{-1}, \sqrt{7})$	$\left(\frac{-1}{p}\right)=\left(\frac{7}{p}\right)=\left(\frac{2}{p}\right)=1$	$p=a^2+16b^2$ $=x^2+112y^2$ $=u^2-7v^2(u,\ v>0)$	$\left(\frac{\varepsilon_7}{p}\right)=1$ $\left(\frac{\varepsilon_7}{p}\right)_4=\left(\frac{2}{p}\right)_4\left(\frac{2}{u+3v}\right)=(-1)^y$	Conjectured by Lehmer **[6]**
$Q(\sqrt{-1}, \sqrt{m})$ $m=11, 19, 43$ $67, 163$	$\left(\frac{-1}{p}\right)=\left(\frac{m}{p}\right)=\left(\frac{2}{p}\right)=1$ $p=8n+1$	$p=a^2+16b^2$ $=u^2-mv^2(u>0)$ and either (i) $p=x^2+16my^2$ or (ii) $4p=x^2+my^2$ $(x\equiv 1 \pmod 4)$	$\left(\frac{\varepsilon_m}{p}\right)=1$ $\left(\frac{\varepsilon_m}{p}\right)_4=\left(\frac{2}{p}\right)_4\left(\frac{-2}{u+kv}\right)=\begin{cases}(-1)^y & \text{(i)}\\ (-1)^{(x-1/4)+n} & \text{(ii)}\end{cases}$ $k=\begin{cases}3, & m=11, 43,\\ 1, & m=19, 67, 163\end{cases}$	In part conjected by Lehmer **[6]**
$Q(\sqrt{-2}, \sqrt{-3})$	$\left(\frac{-2}{p}\right)=\left(\frac{-3}{p}\right)=\left(\frac{2}{p}\right)=1$ $p=8n+1$	$p=c^2+8d^2$ $=x^2+48y^2$ $=u^2-24v^2(u>0)$	$\left(\frac{\varepsilon_6}{p}\right)=1$ $\left(\frac{\varepsilon_6}{p}\right)_4=\left(\frac{2}{p}\right)_4\left(\frac{-2}{u+4v}\right)=(-1)^{n+d+y}$	
$Q(\sqrt{-2}, \sqrt{-7})$	$\left(\frac{-2}{p}\right)=\left(\frac{-7}{p}\right)=\left(\frac{2}{p}\right)=1$ $p=8n+1$	$p=c^2+8d^2$ $=x^2+112y^2$ $=u^2-56v^2(u>0)$	$\left(\frac{\varepsilon_{14}}{p}\right)=1$ $\left(\frac{\varepsilon_{14}}{p}\right)_4=\left(\frac{2}{p}\right)_4\left(\frac{2}{u}\right)=(-1)^{n+y}$	
$Q(\sqrt{-2}, \sqrt{-m})$ $m=11, 19, 43,$ 67	$\left(\frac{-2}{p}\right)=\left(\frac{-m}{p}\right)=\left(\frac{2}{p}\right)=1$ $p=8n+1$	$p=c^2+8d^2$ $=u^2-8mv^2(u>0)$ and either (i) $p=x^2+16my^2$ or (ii) $4p=x^2+my^2$ $(x\equiv 1 \pmod 4)$	$\left(\frac{\varepsilon_{2m}}{p}\right)=1$ $\left(\frac{\varepsilon_{2m}}{p}\right)_4=\left(\frac{2}{p}\right)\left(\frac{-2}{u+4v}\right)=\begin{matrix}(-1)^{n+d+y} & \text{(i)}\\ (-1)^{d+(x-1/4)} & \text{(ii)}\end{matrix}$	

factor of p in the biquadratic field under consideration and by computing partial norms we obtain representations of p by the three quadratic forms associated with the three quadratic subfields. This information is then used to derive appropriate congruence relations between the representations. Finally this information is combined to obtain the quadratic or quartic symbol solely in terms of representations by the positive definite quadratic forms.

If ε_m has norm-1 we require $(-1/p) = +1$ in order that (ε_m/p) be unambiguously defined.

Our results are given in the accompanying table.

As the method of proof is the same for each field we just give the details for $Q(\sqrt{-2}, \sqrt{-7})$. We have

$$2\varepsilon_{14} = 2(15 + 4\sqrt{14}) = (4 + \sqrt{14})^2 ,$$

so that $(\varepsilon_{14}/p) = 1$. Next as $u \equiv \pm 2\sqrt{14}v \pmod{p}$ with $u, v > 0$ we have

$$\begin{aligned}
\left(\frac{4 + \sqrt{14}}{p}\right) &= \left(\frac{2v}{p}\right)\left(\frac{u + 8v}{p}\right) \\
&= \left(\frac{u + 8v}{p}\right)\left(\text{as } \left(\frac{2}{p}\right) = \left(\frac{v}{p}\right) = 1\right) \\
&= \left(\frac{p}{u + 8v}\right) \quad \text{(by Jacobi's law)} \\
&= \left(\frac{8v^2}{u + 8v}\right) \quad (\text{as } p \equiv 8v^2 \pmod{u + 8v}) \\
&= \left(\frac{2}{u + 8v}\right) = \left(\frac{2}{u}\right) .
\end{aligned}$$

Now let π be a prime factor of p in $Q(\sqrt{-2}, \sqrt{-7})$ so that there are integers A, B, C, D such that

$$\pi = \frac{1}{2}(A + B\sqrt{-7} + C\sqrt{-2} + D\sqrt{14})$$

with

$$A \equiv B \pmod{2}, \quad C \equiv D \pmod{2} ,$$

see for example [7]. Forming relative norms of π in the three quadratic subfields of $Q(\sqrt{-2}, \sqrt{-7})$ (as in [1]) we can specify:

$$(c, d) = \left(\frac{1}{4}(A^2 + 7B^2 - 2C^2 - 14D^2), \quad \frac{1}{4}(AC - 7BD)\right) ,$$

$$(u, v) = \left(\frac{1}{4}(A^2 + 7B^2 + 2C^2 + 14D^2), \quad \frac{1}{4}(AD + BC)\right),$$

$$(l, m) = \left(\frac{1}{2}(A^2 - 7B^2 + 2C^2 - 14D^2), \quad AB - 2CD)\right),$$

where l and m are integers such that

$$l^2 + 7m^2 = 4p, \quad l \equiv m \pmod 2 .$$

Clearly l and m are not both odd so that $A \equiv B \equiv 0 \pmod 2$. Hence

$$x = \frac{1}{4}(A^2 - 7B^2 + 2C^2 - 14D^2), \quad y = \frac{1}{8}(AB - 2CD),$$

and so $C \equiv D \equiv 0 \pmod 2$. Setting

$$A = 2A_1, \quad B = 2B_1, \quad C = 2C_1, \quad D = 2D_1,$$

we obtain

$$u = A_1^2 + 7B_1^2 + 2C_1^2 + 14D_1^2,$$
$$d = A_1C_1 - 7B_1D_1,$$
$$y = \frac{A_1B_1}{2} - C_1D_1 .$$

Hence as u is odd exactly one of A_1, B_1 is even. We just treat the case A_1 even, B_1 odd, say $A_1 = 2A_2$, $B_1 = 2B_2 + 1$, as the other case is exactly similar. We have

$$u \equiv 4A_2^2 + 7 + 2C_1^2 + 6D_1^2 \pmod 8,$$
$$d \equiv D_1 \pmod 2,$$
$$y \equiv A_2 + C_1D_1 \pmod 2 .$$

It now easily follows from the following table that $d + y \equiv 0 \pmod 2$ if and only if $u \equiv \pm 1 \pmod 8$.

$A_2 \pmod 2$	$C_1 \pmod 2$	$D_1 \pmod 2$	$d + y \pmod 2$	$u \pmod 8$
0	0	0	0	−1
0	0	1	1	−3
0	1	0	0	+1
0	1	1	0	−1
1	0	0	1	+3
1	0	1	0	+1
1	1	0	1	−3
1	1	1	1	+3

$$\text{Since } \left(\frac{2}{p}\right)_4 = (-1)^{n+d} \quad \text{and} \quad \left(\frac{2}{u}\right) = \begin{cases} +1, & \text{if } u \equiv \pm 1 \pmod 8, \\ -1, & \text{if } u \equiv \pm 3 \pmod 8, \end{cases}$$

the proof of the result is complete.

In some of the other fields certain complexities arose. For example if either $Q(\sqrt{-1})$ or $Q(\sqrt{-3})$ is one of the subfields care had to be taken in identifying the solutions of the corresponding representation because of the presence of units $\neq \pm 1$. Whenever the question of whether p or $4p$ is represented by the appropriate form there was an increase in the number of cases to be considered. In those cases in which the parity of n is needed it was handled by relating it to an appropriate representation, for example if $p = a^2 + 16b^2 = 8n + 1$ then $n \equiv (a^2 - 1)/8 \pmod 2$ was used. Finally we mention that whenever the number of cases to consider became excessive we used Carleton University's Sigma 9 computer to treat them.

In a forthcoming paper we will discuss generalizations of these results as well as other results of a similar nature.

References

1. P. Barrucand and H. Cohn, *Note on primes of the type x^2+32y^2, class number, and residuacity*, J. reine angew. Math., **238** (1969), 67-70.
2. J. Brandler, *Residuacity properties of real quadratic units*, J. Number Theory, **5** (1973), 271-287.
3. E. Brown and C. J. Parry, *The imaginary bicyclic biquadratic fields with class number* 1, J. reine angew. Math., **266** (1974), 118-120.
4. E. Lehmer, *On the quadratic character of quadratic surds*, J. reine angew. Math., **220** (1971), 42-48.
5. ———, *On some special quartic reciprocity laws*, Acta Arith., 21 (1972), 367-377.
6. ———, *On the quartic character of quadratic units*, J. reine angew. Math., **268/269** (1974), 294-301.
7. K. S. Williams, *Integers of biquadratic fields*, Canad. Math. Bull., **13** (1970), 519-526.

Received March 11, 1976 and in revised form July 6, 1976. Research by the second author was supported by National Research Council of Canada Grant No. A-7233.

Arizona State University
and
Carleton University
Ottawa, Ontario, Canada

PACIFIC JOURNAL OF MATHEMATICS

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

Pacific Journal of Mathematics
Vol. 71, No. 1 November, 1977