BIQUADRATIC RECIPROCITY LAWS

EZRA BROWN

ABSTRACT. Let \( p \equiv q \equiv 1 \pmod{4} \) be distinct primes such that \((p|q)=1\), and let \( g=[k, 2m, n] \) be a binary quadratic form of determinant \( q \) which represents \( p \). Subject to certain restrictions on \( k \) and \( q \), we obtain some reciprocity laws for the fourth-power residue symbols \((p|q)_4\) and \((q|p)_4\).

In [3], K. Bürde proved the following reciprocity law for fourth powers; in this paper, \( p \) and \( q \) are distinct odd primes, \((p|q)\) is the Legendre symbol and \((p|q)_4=1\) or \(-1\) according as \( p \) is or is not a fourth-power residue of \( q \).

**Lemma 1.** Write \( p=x_1^2+x_2^2 \) and \( q=a^2+b^2 \) with \( x_1 \) and \( a \) odd, \( x_1x_2>0 \), \( ab>0 \) and \((p|q)=1\). Then

\[
(p|q)_4(q|p)_4 = (-1)^{(q-1)/4}(ax_2 - bx_1 | q).
\]

This result can be formulated in terms of a representation of \( p \) by a form \( g \) of determinant \( q \). In the case \( g=[1, 0, q] \), Lemma 1 has the form

\[
(p|q)_4(q|p)_4 = 1 \text{ or } (-1)^s,
\]

according as \( q \equiv 1 \) or \( 5 \pmod{8} \), where \( p=r^2+qs^2 \) (see [1]). In the case \( g=[2, 2, (a+1)/2] \) and \( q \equiv 1 \pmod{8} \), Lemma 1 becomes

\[
(p|q)_4(q|p)_4 = (e | q),
\]

where \( q=2e^2-f^2 \) (see [2]). The aim of this paper is to generalize the results of [1] and [2] in the following manner.

**Theorem 1.** Let \( p \equiv 1 \pmod{4} \) and \( q \equiv 1 \pmod{8} \) be distinct primes for which \( p=kr^2+2mrs+ns^2 \), where \( s \) is odd and the integral form \([k, 2m, n]\) has determinant \( q \). Suppose each prime divisor of \( k \) is a quadratic residue of \( q \). Suppose \( q=ke^2-f^2 \) for some integers \( e \) and \( f \). Then

\[
(p|q)_4(q|p)_4 = (e | q).
\]

Proof of this theorem employs the techniques of [2]. First we obtain
parametric representations of the solutions to the diophantine equations

(1) \[ x_1^2 + x_2^2 = kr^2 + 2mrs + ns^2 \]

and

(2) \[ -q = A^2 - kB^2 - kC^2 \]

with appropriate restrictions on the above numbers. Then we use these solutions to prove, first

(3) \[ (bB - aC \mid q) = (ax_2 - bx_1 \mid q). \]

then

(4) \[ (bB - aC \mid q) = (e \mid q). \]

The solutions of (1) and (2) are obtained exactly as in [2], with 2 replaced by k, with the following slight modifications. In order to find the solutions of (1), we find it necessary to apply the following theorem of Kneser to the form \( F = x^2 + y^2 - kx^2 - kw^2 \), whose reduced determinant is \(-k\):

Lemma 2 [4]. An indefinite quadratic form in at least three variables is in a genus of one class provided its reduced determinant is divisible neither by the cube of an odd prime nor by 16.

We may assume, without loss of generality, that \( F \) satisfies the hypothesis of Lemma 2. For, if \( 4 \mid k \), then \( q = kn - m^2 \equiv m^2 \pmod{4} \) implies \(-1\) is a square \( \pmod{4} \), which is impossible. Furthermore, the class of \( g \) contains a form with leading coefficient \( p \), since \( g \) represents \( p \); hence we may assume that the leading coefficient \( k \) of \( g \) is not divisible by the cube of an odd prime. Thus \( F \) is in a genus of one class, and we may do the rest of the procedure as in [2], with 2 replaced by \( k \).

The relation (3) is simply a restatement of Lemma 4 of [2] with 2 replaced by \( k \), and (4) is a restatement of Lemma 5 of [2] with \( d \) replaced by \( f \) and \( A^2 - 2(B^2 + C^2) \) replaced by \( A^2 - k(B^2 + C^2) \). This is where the assumptions that (a) every prime divisor of \( k \) is a \( q \) quadratic residue of \( q \), and (b) \( q \equiv 1 \pmod{8} \) are needed. For, in following the proof of Lemma 5 of [2], we obtain

(5) \[ (bB - aC \mid q) = (e \mid q)(N(t) \mid q); \]

here, \( N(t) \) is an integer which divides \( 4 \det f_1 \), where \( f_1 = kX^2 - Y^2 - Z^2 \). Since (a) and (b) are in effect, every divisor of \( 4 \det f_1 = 4k \) is a quadratic residue of \( q \), and (4) is proved.

Theorem 1 follows from Lemma 1, the fact that \( q \equiv 1 \pmod{8} \), and relations (3) and (4).
 COMMENTS. 1. Under the hypotheses of the theorem, it follows that $(p|q)_4(q|p)_4=1$ or $-1$ according as the form $[e, 2f, ke]$ is or is not in the principal genus of forms of determinant $q$.

2. Under the hypotheses of the theorem, if $h(-q)$ is the class number of $O((-q))$ and $O_k$ is the order of $[k, 2f, e^2]$ in the class group, then

$$h(-q) \equiv 0 \text{ or } 2O_k \pmod{4O_k}$$

according as $(p|q)_4(q|p)_4=1$ or $-1$. This is a consequence of the first comment.

3. Under the hypotheses of the theorem, let $h(-q) \equiv 2O_k \pmod{4O_k}$; then $(p|q)_4(q|p)_4=-1$. As a consequence of this, the fundamental unit of $Q((\sqrt{-q}))$ has norm $+1$, for it is known (see [7]) that if $x^2-pqy^2=-1$ has an integral solution, then $(p|q)_4(q|p)_4=1$.

4. Using different methods, Emma Lehmer (see [5]) has obtained results similar to the ones in this paper; my thanks to her for some helpful correspondence on this subject.

REFERENCES


DEPARTMENT OF MATHEMATICS, VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY, BLACKSBURG, VIRGINIA 24061