PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 30, Number 2, October 1971

A THEOREM ON BIQUADRATIC RECIPROCITY

EZRA BROWN

ABSTRACT. The following theorem on biquadratic reciprocity is proved: if $p\equiv q\equiv 1 \pmod 4$ are primes for which $(p|q)=1$, and if $p=r^2+qs^2$ for some integers r and s, then

$$(p\mid q)_4(q\mid p)_4 = 1, \qquad \text{if } q\equiv 1 \pmod 8;$$
$$= (-1)^s, \qquad \text{if } q\equiv 5 \pmod 8.$$

Simple expressions for the biquadratic character of some small primes are also obtained.

K. Burde [2] has proven the following interesting theorem about biquadratic reciprocity:

THEOREM 1. *If* $p=a^2+b^2$, $q=c^2+d^2$, $a\equiv c\equiv 1$, $b\equiv d\equiv 0 \pmod 2$, $ab>0$, $cd>0$, p *and* q *are primes, and* $(p|q)=1$, *then* $(p|q)_4(q|p)_4 = (-1)^{(p-1)/4}(ad-bc|p)$.

If it happens that p can be written as r^2+qs^2, with r and s integers, then Burde's results acquire a particularly simple form. We shall prove the following theorem:

THEOREM 2. *If* $p\equiv q\equiv 1 \pmod 4$ *are primes such that* $(p|q)=1$, *and* p *is representable as* r^2+qs^2, *where* r *and* s *are integers, then*

$$(p\mid q)_4(q\mid p)_4 = 1, \qquad q\equiv 1 \pmod 8;$$
$$= (-1)^s, \qquad q\equiv 5 \pmod 8.$$

Throughout this paper, we assume that p and q satisfy the hypotheses in Theorem 1; $(p|q)$ is the Legendre symbol, and we write $(p|q)_4=1$ or -1 according as p is or is not a biquadratic residue $(\operatorname{mod} q)$.

LEMMA 1. *All prime solutions of the diophantine equation*

$$a^2+b^2 = r^2+qs^2 \tag{1}$$

are contained in the following sets of expressions:

Received by the editors January 19, 1971.

AMS 1970 *subject classifications*. Primary 10A15; Secondary 10B05, 10C05.

Key words and phrases. Power residues, biquadratic residues, reciprocity, quadratic diophantine equations.

Copyright © 1971, American Mathematical Society

$$(2)\qquad \begin{aligned} a &= c(t_0^2 + t_1^2 - t_2^2 - t_3^2) + 2d(-t_0t_2 + t_1t_3) \\ b &= 2c(-t_0t_3 + t_1t_2) + 2d(t_0t_1 + t_2t_3) \\ r &= c(t_0^2 + t_3^2 - t_1^2 - t_2^2) + 2d(-t_0t_2 - t_1t_3) \\ s &= 2(-t_0t_1 + t_2t_3), \end{aligned} \qquad (\textit{if } s \textit{ is even})$$

$$(3)\qquad \begin{aligned} a &= c(t_0^2 + t_1^2 - t_2^2 - t_3^2) + 2d(t_0t_3 + t_1t_2) \\ b &= 2c(-t_0t_3 + t_1t_2) + d(t_0^2 + t_2^2 - t_1^2 - t_3^2) \\ r &= 2c(t_0t_1 - t_2t_3) + 2d(t_0t_2 + t_1t_3) \\ s &= t_0^2 + t_3^2 - t_1^2 - t_2^2 \end{aligned} \qquad (\textit{if } s \textit{ is odd}).$$

Here, the t_i are independent integer-valued parameters, one or three of which are odd.

PROOF. See [1, §5]. The roles of x_1, x_2, x_5 and x_6 in [1] are taken here by a, b, r and s, respectively.

LEMMA 2. *For any prime solution of* (1), *we have* $(cb-da|q)=(2|q)$ *if s is even, and* $(cb-da|q)=1$ *if s is odd.*

PROOF. If s is even, then from (2) we have

$$\begin{aligned} cb - da &= 2c^2(-t_0t_3 + t_1t_2) + 2cd(t_0t_1 + t_2t_3) \\ &\quad - cd(t_0^2 + t_1^2 - t_2^2 - t_3^2) - 2d^2(-t_0t_2 + t_1t_3) \\ &\equiv - cd((t_1 - t_0)^2 - (t_2 + t_3)^2) - 2d^2(t_1 - t_0)(t_2 + t_3) \pmod{q}, \end{aligned}$$

since $c^2 \equiv -d^2 \pmod{q}$. Multiplying both sides by d, we obtain the congruence

$$d(cb - da) \equiv - c(c(t_1 - t_0) + d(t_2 + t_3))^2 \pmod{q}.$$

Now

$$\begin{aligned} (cb - da)(cb + da) &= c^2(a^2 + b^2) - a^2(c^2 + d^2) \\ &= c^2p - a^2q \equiv c^2p \not\equiv 0 \pmod{q}, \end{aligned}$$

since $(c, q)=1$. Hence $cb-da \not\equiv 0 \pmod{q}$ and we may write $(cb-da|q) =(-1|q)(c|q)(d|q)$. But by Theorem 5 of [1], $(c|q)=1$ and $(d|q) =(2|q)$; hence $(cb-da|q)=(2|q)$, since $q\equiv 1 \pmod{4}$. Proof of the second statement is similar, relying on the expressions in (3), and is omitted.

PROOF OF THEOREM 2. By Lemma 2 and Theorem 1, if s is even, then (reversing the roles of p and q in Theorem 1) $(p|q)_4(q|p)_4$

$=(-1)^{(q-1)/4}(2|p)=1$, since $q\equiv 1 \pmod 4$. If s is odd, then $(q|p)_4$ $(q|p)_4=(-1)^{(q-1)/4}=1$ or -1 according as $q\equiv 1$ or $5 \pmod 8$. Hence $(p|q)_4(q|p)_4=1$ or $(-1)^s$, according as $q\equiv 1$ or $5 \pmod 8$.

As an application we determine the biquadratic characters of some small primes. Let $q=5$ or 13 and let $p\equiv 1 \pmod 4$ be a prime such that $(p|q)=1$. It can be shown, using Thue's lemma on linear congruences, that every such prime is representable as r^2+qs^2, with integral r and s. It is also the case that $(p|q)_4=1$ or -1 according as $[(p-1)/q]$ is even or odd (here $[X]$ = greatest integer in X). For, $(p|5)_4=1$ or -1 according as $p\equiv 1$ or $9 \pmod{10}$, $(p|13)_4=1$ if $p\equiv 1$, 3 or $9 \pmod{26}$, and $(p|13)_4=-1$ if $p\equiv 17$, 23 or $25 \pmod{26}$. This information, together with Theorem 2, yields the following result.

THEOREM 3. *Let p be a prime* $\equiv 1 \pmod 4$. *Then*:
(a) *If* $(p|5)=1$, *then* $(5|p)_4=(-1)^{s+[(p-1)/5]}$, *where* $p=r^2+5s^2$.
(b) *If* $(p|13)=1$, *then* $(13|p)_4=(-1)^{s+[(p-1)/13]}$, *where* $p=r^2+13s^2$.

It also happens that every prime $p\equiv 1 \pmod 4$ such that $(p|37)=1$ can be represented as r^2+37s^2. The conditions that $(p|37)_4$ be 1 or -1 are not particularly simple: $(p|37)_4=1$ or -1 according as $[(p^9-1)/37]$ is odd or even. Nevertheless, we do have the following.

THEOREM 4. *If* $p\equiv 1 \pmod 4$ *is a prime such that* $(p|37)=1$, *then* $(37|p)_4=(-1)^s(p|37)_4$, *where* $p=r^2+37s^2$.

REFERENCES

1. Ezra Brown, *Representations of discriminantal divisors by binary quadratic forms*, J. Number Theory **3** (1971).

2. Klaus Burde, *Ein rationales biquadratisches Reziprozitätsgesetz*, J. Reine Angew. Math. **235** (1969), 175–184. MR **39** #2694.

VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY, BLACKSBURG, VIRGINIA 24061