Canad. Math. Bull. Vol. **20** (1), 1977

NOTE ON BURDE'S RATIONAL BIQUADRATIC RECIPROCITY LAW

KENNETH S. WILLIAMS

A short proof is given of a biquadratic reciprocity law proved by Burde in 1969.

Let p and q be primes $\equiv 1 \pmod 4$ such that $(p \mid q) = (q \mid p) = 1$. Then there are integers a, b, c, d with

$$\begin{aligned} p &= a^2 + b^2, & a &\equiv 1 \pmod 2, & b &\equiv 0 \pmod 2, \\ q &= c^2 + d^2, & c &\equiv 1 \pmod 2, & d &\equiv 0 \pmod 2. \end{aligned}$$

Set

$$(p|q)_4 = \begin{cases} +1 & \text{if } p \text{ a biquadratic residue } \pmod q, \\ -1, & \text{otherwise.} \end{cases}$$

Burde [2] proved using the law of biquadratic reciprocity that

$$(1) \qquad (p \mid q)_4 (q \mid p)_4 = (-1)^{(q-1)/4} (ad - bc \mid q).$$

Lehmer [4, 5] has given two proofs of (1) using results from cyclotomy. In this note we put together two classical results ((2) and (4) below) to give a short proof of (1).

It is easy to show that $(\pm ad \pm bc \mid q) = (ad - bc \mid q)$ for any choice of signs so that (1) is independent of the particular choices made of a, b, c, d. We choose a, b to satisfy $a - b + 1 \equiv 0 \pmod 4$ and set $\pi = a + bi$ so that $\pi\bar{\pi} = p$. For any integer $x \not\equiv 0 \pmod p$ we define a biquadratic character by

$$(x \mid \pi)_4 = i^e \quad \text{if} \quad x^{(p-1)/4} \equiv i^e \pmod \pi, \quad 0 \le e \le 3.$$

The Gauss sum corresponding to this character is

$$G = \sum_{x=0}^{p-1} (x \mid \pi)_4 \exp(2\pi\, ix/p).$$

It is well-known that (see for example [1])

$$(2) \qquad G^2 = (-1)^{(p-1)/4} p^{1/2} \pi.$$

Raising G to the qth power we obtain by a familiar argument

$$G^q \equiv (q \mid \pi)_4^{-1} G \equiv (q \mid p)_4 G \pmod q$$

that is

$$(3) \qquad G^{q-1} \equiv (q \mid p)_4 \pmod q.$$

Taking the $(q-1)/2$th power of (2) and using (3) we obtain

$$(q \mid p)_4 \equiv p^{(q-1)/4} \pi^{(q-1)/2} (\mathrm{mod}\ q).$$

or

$$(p \mid q)_4 (q \mid p)_4 \equiv (a+ib)^{(q-1)/2} (\mathrm{mod}\ q).$$

It follows from an old result of Dörrie [3] that

(4) $$(a+ib)^{(q-1)/2} \equiv (-1)^{(q-1)/4} (ad-bc \mid q)\ (\mathrm{mod}\ q)$$

which completes the proof of (1). For completeness we give a proof of (4). We have

$$d(a+bi) \equiv ad-bc \ \ (\mathrm{mod}\ c+di)$$

so that

(5) $$(a+bi)^{(q-1)/2} \equiv (-1)^{(q-1)/4} (ad-bc \mid q)\ \ (\mathrm{mod}\ c+di)$$

as it is well known that $(d \mid q) \equiv d^{(q-1)/2} \equiv (-1)^{(q-1)/4} (\mathrm{mod}\ q)$.
Also

$$d(a+bi) \equiv ad+bc\ (\mathrm{mod}\ c-di)$$

so that

(6) $$(a+bi)^{(q-1)/2} \equiv (-1)^{(q-1)/4} (ad+bc \mid q) \equiv (-1)^{(q-1/4} (ad-bc \mid q) (\mathrm{mod}\ c-di).$$

(4) now follows from (5) and (6).

References

1. P. Bachmann, *Die Lehre von der Kreisteilung*, Leipzig (1872), equation (9), p. 169.

2. K. Burde, *Ein rationales biquadratisches Reziprozitätsgesetz*, Jour. reine angew. Math., **235** (1969), 175–184.

3. H. Dörrie, *Das quadratische Reciprocitätsgesetz in quadratischen Zahlkörper mit der Classenzahl* **1**, *Gött. Diss.*, 1898.

4. E. Lehmer, *Criteria for cubic and quartic residuacity*, Mathematika **5** (1958), 20–29.

5. E. Lehmer, *On the quadratic character of some quadratic surds*, Jour. reine angew. Math., **250** (1971), 42–48.

Carleton University
Ottawa, Canada