Pacific Journal of Mathematics

A RATIONAL OCTIC RECIPROCITY LAW

Kenneth S. Williams

Vol. 63, No. 2 April 1976

PACIFIC JOURNAL OF MATHEMATICS
Vol. 63, No. 2, 1976

A RATIONAL OCTIC RECIPROCITY LAW

KENNETH S. WILLIAMS

A rational octic reciprocity theorem analogous to the rational biquadratic reciprocity theorem of Burde is proved.

Let p and q be distinct primes $\equiv 1 (\bmod 4)$ such that $(p/q) = (q/p) = 1$. For such primes there are integers a, b, A, B with

$$(1) \qquad \begin{cases} p = a^2 + b^2,\ a \equiv 1 (\bmod 2),\ b \equiv 0 (\bmod 2)\ , \\ q = A^2 + B^2,\ A \equiv 1 (\bmod 2),\ B \equiv 0 (\bmod 2)\ . \end{cases}$$

Moreover it is well-known than $(A/q) = 1$, $(B/q) = (-1)^{(q-1)/4}$. If k is a quadratic residue $(\bmod q)$ we set

$$\left(\frac{k}{q}\right)_4 = \begin{cases} +1, \text{ if } k \text{ is a biquadratic residue } (\bmod q)\ , \\ -1, \text{ otherwise}\ . \end{cases}$$

In 1969 Burde [2] proved the following

THEOREM (Burde).

$$\left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 = (-1)^{(q-1)/4} \left(\frac{aB - bA}{q}\right)\ .$$

Recently Brown [1] has posed the problem of finding an octic reciprocity law analogous to Burde's biquadratic law for distinct primes p and q with $p \equiv q \equiv 1 (\bmod 8)$ and $(p/q)_4 = (q/p)_4 = 1$. It is the purpose of this paper to give such a law. From this point on we assume that p and q satisfy these conditions and set for any biquadratic residue $k (\bmod q)$

$$\left(\frac{k}{q}\right)_8 = \begin{cases} +1, \text{ if } k \text{ is an octic residue } (\bmod q)\ , \\ -1, \text{ otherwise}\ . \end{cases}$$

It is a familar result that there are integers c, d, C, D with

$$(2) \qquad \begin{cases} p = c^2 + 2d^2,\ c \equiv 1 (\bmod 2),\ d \equiv 0 (\bmod 2)\ , \\ q = C^2 + 2D^2,\ C \equiv 1 (\bmod 2),\ D \equiv 0 (\bmod 2)\ . \end{cases}$$

Moreover we have $(D/q) = 1$. Also from Burde's theorem we have

$$(3) \qquad \left(\frac{aB - bA}{q}\right) = 1\ ,$$

and from the law of biquadratic reciprocity after a little calculation we find that $(B/q)_4 = +1$. We prove

THEOREM. *Let p and q be distinct primes* $\equiv 1 (\bmod 8)$ *such that* $\left(\frac{p}{q}\right)_4 = \left(\frac{q}{p}\right)_4 = 1$. *Then* $\left(\frac{p}{q}\right)_8 \left(\frac{q}{p}\right)_8 = \left(\frac{aB - bA}{q}\right)_4 \left(\frac{cD - dC}{q}\right)$.

We note that it is easy to show that

$$\left(\frac{\pm aB \pm bA}{q}\right)_4 = \left(\frac{aB - bA}{q}\right)_4, \left(\frac{\pm cD \pm dC}{q}\right) = \left(\frac{cD - dC}{q}\right),$$

so that the expression on the right-hand side of the theorem is independent of the particular choices of a, b, c, d, A, B, C, D made in (1) and (2). In the course of the proof it is convenient to make a particular choice of a, b, c, d (see (9) and (10)).

We begin by proving three lemmas.

LEMMA 1. $(c + d\sqrt{-2})^{(q-1)/2} \equiv ((cD - dC)/q) \quad (\bmod q)$.

Proof. As $(p/q) = 1$ we can define an integer u by $p \equiv u^2 (\bmod q)$. Next we define integers l and m by

$$l \equiv \frac{cD - dC + Du}{2}, \; m \equiv \frac{C}{D} \cdot \frac{cD - dC - Du}{4} \quad (\bmod q),$$

so that

$$l^2 - 2m^2 \equiv cD(cD - dC) \quad (\bmod q)$$

and

$$2lm \equiv dD(cD - dC) \quad (\bmod q),$$

giving

$$D(cD - dC)(c + d\sqrt{-2}) \equiv (l + m\sqrt{-2})^2 \quad (\bmod q),$$

and so

$$D^{(q-1)/2}(cD - dC)^{(q-1)/2}(c + d\sqrt{-2})^{(q-1)/2} \equiv (l + m\sqrt{-2})^{q-1} \quad (\bmod q).$$

Now working modulo q we have

$$\begin{aligned} (l + m\sqrt{-2})^{q-1} &\equiv \frac{(l + m\sqrt{-2})^q}{l + m\sqrt{-2}} \equiv \frac{l^q + m^q(\sqrt{-2})^q}{l + m\sqrt{-2}} \\ &\equiv \frac{l + mi^q 2^{q/2}}{l + m\sqrt{-2}} \equiv \frac{l + mi\sqrt{2}}{l + m\sqrt{-2}} \\ &\equiv 1, \end{aligned}$$

also

$$D^{(q-1)/2} \equiv \left(\frac{D}{q}\right) = 1 ,$$

and

$$(cD - dC)^{(q-1)/2} \equiv \left(\frac{cD - dC}{q}\right),$$

from which the required result follows immediately.

LEMMA 2. $(a + b\sqrt{-1})^{(q-1)/4} \equiv ((aB - bA)/q)_4 \pmod q$.

Proof. As $(p/q) = 1$ we define ar integer u by $p \equiv u^2 (\bmod q)$ as in Lemma 1. Next we define integers r and s by

$$r \equiv \frac{aB - bA + Bu}{2},\ s \equiv \frac{A}{B}\cdot\frac{aB - bA - Bu}{2} \pmod q$$

so that

$$r^2 - s^2 \equiv aB(aB - bA) \pmod q$$

and

$$2rs \equiv bB(aB - bA) \pmod q$$

giving

$$B(aB - bA)(a + b\sqrt{-1}) \equiv (r + s\sqrt{-1})^2 \pmod q ,$$

and so

$$B^{(q-1)/4}(aB - bA)^{(q-1)/4}(a + b\sqrt{-1})^{(q-1)/4} \equiv (r + s\sqrt{-1})^{(q-1)/2} \pmod q .$$

Thus as $(B/q)_4 = ((aB - bA)/q) = 1$ we obtain

$$(a + b\sqrt{-1})^{(q-1)/4} \equiv \left(\frac{aB - bA}{q}\right)_4 (r + s\sqrt{-1})^{(q-1)/2} \pmod q .$$

Next we note that $r^2 + s^2 \equiv uB(aB - bA)(\bmod q)$ so that

$$\left(\frac{r^2 + s^2}{q}\right) = \left(\frac{p}{q}\right)_4 \left(\frac{B}{q}\right)\left(\frac{aB - bA}{q}\right) = 1 .$$

Hence we may define an integer w by $w^2 \equiv r^2 + s^2 (\bmod q)$. Then we define integers e and f by

$$e \equiv \frac{rB - sA + Bw}{2},\ f \equiv \frac{A}{B}\cdot\frac{rB - sA - Bw}{2} \pmod q$$

so that

$$e^2 - f^2 \equiv rB(rB - sA) \pmod q$$

and

$$2ef \equiv sB(rB - sA) \pmod q$$

giving

$$B(rB - sA)(r + s\sqrt{-1}) \equiv (e + f\sqrt{-1})^2 \pmod q ,$$

and so

$$B^{(q-1)/2}(rB - sA)^{(q-1)/2}(r + s\sqrt{-1})^{(q-1)/2} \equiv (e + f\sqrt{-1})^{q-1} \pmod q .$$

Now working modulo q we have

$$\begin{aligned}(e + f\sqrt{-1})^{q-1} &\equiv \frac{(e + f\sqrt{-1})^q}{(e + f\sqrt{-1})} \equiv \frac{e^q + f^q(\sqrt{-1})^q}{e + f\sqrt{-1}} \\ &\equiv \frac{e + f\sqrt{-1}}{e + f\sqrt{-1}} \equiv 1 ,\end{aligned}$$

and

$$B^{(q-1)/2} \equiv \left(\frac{B}{q}\right) = 1,\ (rB - sA)^{(q-1)/2} \equiv \left(\frac{rB - sA}{q}\right),$$

so

$$(r + s\sqrt{-1})^{(q-1)/2} \equiv \left(\frac{rB - sA}{q}\right),$$

giving

$$(a + b\sqrt{-1})^{(q-1)/4} \equiv \left(\frac{aB - bA}{q}\right)_4 \left(\frac{rB - sA}{q}\right) \pmod q .$$

The required result now follows as modulo q we have

$$\begin{aligned} rB - sA &\equiv \frac{B(aB - bA + Bu)}{2} - \frac{A^2}{B}\,\frac{(aB - bA - Bu)}{2} \\ &\equiv \frac{B}{2}\{(aB - bA + Bu) + (aB - bA - Bu)\} \\ &\equiv B(aB - bA) ,\end{aligned}$$

that is

$$\left(\frac{rB - sA}{q}\right) = \left(\frac{B}{q}\right)\left(\frac{aB - bA}{q}\right) = +1 .$$

Before proving the final lemma we state some results we shall need. Let $w = \exp(2\pi i/8) = (\sqrt{2} + \sqrt{-2})/2$ and let R be the ring of integers of the cyclotomic field $Q(w) = Q(\sqrt{2}, \sqrt{-1})$. R is a unique factorization domain. Let π be any prime factor of p in R, fixed once and for all. For integers $x \not\equiv 0 \pmod p$ we define an octic character $\pmod p$ by

$$\left(\frac{x}{\pi}\right)_8 = w^\lambda \text{ if } x^{(p-1)/8} \equiv w^\lambda \pmod \pi,\ 0 \leqq \lambda \leqq 7 .$$

If $x \equiv 0 \pmod p$ we set $(x/\pi)_8 = 0$. In terms of this character we define the corresponding Jacobi and Gauss sums for arbitrary integers k and l as follows:

$$J(k, l) = \sum_{x=0}^{p-1} \left(\frac{x}{\pi}\right)_8^k \left(\frac{1-x}{\pi}\right)_8^l ,$$

$$G(k) = \sum_{x=0}^{p-1} \left(\frac{x}{\pi}\right)_8^k \exp(2\pi i x/p) .$$

These sums have the following well-known properties (see for example [4], Chapter 8):

(4) $$J(k, l)\overline{J(k, l)} = p , \qquad \text{if} \quad k, l \not\equiv 0 \pmod 8 ,$$

(5) $$J(k, l) = \frac{G(k)G(l)}{G(k+l)} , \qquad \text{if} \quad k, l, k+l \not\equiv 0 \pmod 8 ,$$

(6) $$G(k)G(-k) = (-1)^{k(p-1)/8} p , \quad \text{if} \quad k \not\equiv 0 \pmod 8 .$$

We shall also need the evaluation of the familar sum

(7) $$G(4) = \sum_{x=0}^{p-1} \left(\frac{x}{\pi}\right)_8^4 \exp(2\pi i x/p) = \sum_{x=0}^{p-1} \left(\frac{x}{p}\right) \exp(2\pi i x/p) = p^{1/2}$$

and the result

(8) $$J(2, 2) = \pm J(1, 2) .$$

A more precise form of (8) follows from a theorem of Jacobi (see for Example [3], page 411, equation (99)). Finally we let $\sigma_k (k = 1, 3, 5, 7)$ be the automorphism of $Q(w)$ defined by $\sigma_k(w) = w^k$.

Now from (5) and (6) we have

$$\sigma_3(J(1, 4)) = J(3, 12) = J(3, 4) = \frac{G(3)G(4)}{G(7)} = \frac{G(1)G(4)}{G(5)} = J(1, 4) ,$$

so that $J(1, 4) \in Z[\sqrt{-2}]$. Moreover from (4) we have $J(1, 4)\overline{J(1, 4)} = p$ so we may choose the signs of c and d in (2) so that

(9) $$J(1, 4) = c + d\sqrt{-2} .$$

Also from (5) and (6) we have

$$\sigma_5(J(1, 2)) = J(5, 10) = J(5, 2) = \frac{G(5)G(2)}{G(7)} = \frac{G(1)G(2)}{G(3)} = J(1, 2) ,$$

so that $J(1, 2) \in Z[\sqrt{-1}]$. Moreover from (4) we have $J(1, 2)\overline{J(1, 2)} = p$ so we may choose the signs of a and b in (1) so that

$$J(1, 2) = a + b\sqrt{-1} , \tag{10}$$

since it is easy to prove (and well-known) that $J(1, 2) \equiv 1 (\mathrm{mod}\ 2)$.

LEMMA 3. $G(1)^8 = p(a + b\sqrt{-1})^2(c + d\sqrt{-2})^4$.

Proof. From (5), (9), (10) have

$$c + d\sqrt{-2} = J(1, 4) = \frac{G(1)G(4)}{G(5)}$$

and

$$a + b\sqrt{-1} = J(1, 2) = \frac{G(1)G(2)}{G(3)} .$$

Multiplying these together we obtain

$$(a+b\sqrt{-1})(c + d\sqrt{-2}) = \frac{G(1)^2G(2)G(4)}{G(3)G(5)} = \frac{G(1)^2G(2)}{(-1)^{(p-1)/8}p^{1/2}}$$

by (6) and (7). Hence taking the fourth power of both sides we get

$$G(1)^8G(2)^4 = p^2\ (a + b\sqrt{-1})^4(c + d\sqrt{-2})^4 . \tag{11}$$

Now from (5) and (7) we have

$$J(2, 2) = \frac{G(2)^2}{G(4)} = \frac{G(2)^2}{p^{1/2}} ,$$

so that from (8) and (10) we obtain

$$G(2)^4 = p\{J(2, 2)\}^2 = p\{J(1, 2)\}^2 = p(a + b\sqrt{-1})^2 , \tag{12}$$

and the required result now follows from (11) and (12).

Proof of theorem. Raising $G(1)$ to the qth power we obtain modulo q,

$$G(1)^q \equiv \sum_{x=0}^{p-1} \left(\frac{x}{\pi}\right)_8^q \exp(2\pi ixq/p) = \sum_{x=0}^{p-1} \left(\frac{x}{\pi}\right)_8 \exp(2\pi ixq/p) ,$$

since $q \equiv (\mathrm{mod}\ q)$, giving

$$G(1)^q \equiv \left(\frac{q}{\pi}\right)_8^{-1} \sum_{x=0}^{p-1} \left(\frac{xq}{\pi}\right)_8 \exp(2\pi i(xq)/p) = \left(\frac{q}{\pi}\right)_8^{-1} G(1) ,$$

since $(q, p) = 1$ implies that

$$\sum_{x=0}^{p-1} \left(\frac{xq}{\pi}\right)_8 \exp(2\pi ixq/p) = \sum_{y=0}^{p-1} \left(\frac{y}{\pi}\right)_8 \exp(2\pi iy/p) = G(1) .$$

Hence

$$G(1)^q \equiv \left(\frac{q}{\pi}\right)_8^{-1} G(1) = \left(\frac{q}{p}\right)_8 G(1) ,$$

that is

$$G(1)^{q-1} \equiv \left(\frac{q}{p}\right)_8 (\mathrm{mod}\ q) .$$

Hence by Lemmas 1, 2, 3 we have modulo q

$$\begin{aligned} \left(\frac{q}{p}\right)_8 &\equiv (G(1)^8)^{(q-1)/8} \\ &\equiv p^{(q-1)/8}(a + b\sqrt{-1})^{(q-1)/4}(c + d\sqrt{-2})^{(q-1)/2} \\ &\equiv \left(\frac{p}{q}\right)_8 \left(\frac{aB - bA}{q}\right)_4 \left(\frac{cD - dC}{q}\right) , \end{aligned}$$

from which the theorem follows.

EXAMPLE. We take $p = 17 \equiv 1\ (\mathrm{mod}\ 8)$ and $q = 409 \equiv 1 (\mathrm{mod}\ 8)$ so that we may choose

$$\begin{gathered} a = 1,\ b = 4,\ c = 3,\ d = 2 , \\ A = 3,\ B = 20,\ C = 11,\ D = 12 . \end{gathered}$$

Since $q \equiv 1 (\mathrm{mod}\ p)$ we clearly have

$$\left(\frac{q}{p}\right) = \left(\frac{q}{p}\right)_4 = \left(\frac{q}{p}\right)_8 = 1 .$$

As $((aB - bA)/q) = (8/409) = +1$ by Burde's theorem we have $(p/q)_4 = 1$. Finally

$$\left(\frac{aB - bA}{q}\right)_4 = \left(\frac{8}{409}\right)_4 = \left(\frac{194}{409}\right) = -1 ,$$

$$\left(\frac{cD - dC}{q}\right) = \left(\frac{14}{409}\right) = -1 ,$$

so by the theorem of this paper we have $(p/q)_8 = 1$, which is easily verified directly.

References

1. Ezra Brown, *Quadratic forms and biquadratic reciprocity*, J. für Math., **253** (1972), 214-220.

2. Klaus Burde, *Ein rationales biquadratisches Reziprozitätsgesetz*, J. für Math., **235** (1969), 175-184.

3. L. E. Dickson, *Cyclotomy, higher congruences, and Waring's problem*, Amer. J. Math., **57** (1935), 391-424.

4. Kenneth Ireland and Michael I. Rosen, *Elements of Number Theory*, Bogden and Quigley, Inc. Publishers, Tarrytown-on-Hudson, New York (1972).

Received August 4, 1975. Research supported under National Research Council of Canada grant no. A-7233.

Carleton University—Ottawa Canada

PACIFIC JOURNAL OF MATHEMATICS

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be in typed form or offset-reproduced, (not dittoed), double spaced with large margins. Please do not use built up fractions in the text of your manuscript. You may however, use them in the displayed equations. Underline Greek letters in red, German in green, and script in blue. The first paragraph or two must be capable of being used separately as a synopsis of the entire paper. Items of the bibliography should not be cited there unless absolutely necessary, in which case they must be identified by author and Journal, rather than by item number. Manuscripts, in triplicate, may be sent to any one of the editors. Please classify according to the scheme of Math. Reviews, Index to Vol. **39**. All other communications should be addressed to the managing editor, or Elaine Barth, University of California, Los Angeles, California, 90024.

The Pacific Journal of Mathematics expects the author's institution to pay page charges, and reserves the right to delay publication for nonpayment of charges in case of financial emergency.

100 reprints are provided free for each article, only if page charges have been substantially paid. Additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* is issued monthly as of January 1966. Regular subscription rate: $72.00 a year (6 Vols., 12 issues). Special rate: $36.00 a year to individual members of supporting institutions.

Subscriptions, orders for back numbers, and changes of address should be sent to Pacific Journal of Mathematics, 103 Highland Boulevard, Berkeley, California, 94708.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.), 8-8, 3-chome, Takadanobaba, Shinjuku-ku, Tokyo 160, Japan.

Pacific Journal of Mathematics

Vol. 63, No. 2 April, 1976