A remark on rational octic reciprocity

By Soonhak KWON

Department of Mathematics and Institute of Basic Science, Sungkyunkwan University, Suwon 440-746, S. Korea

(Communicated by Shokichi IYANAGA, M. J. A., Feb. 12, 2002)

Abstract: We present a new type of rational octic reciprocity law, which is different from the one discovered by Williams.

Key words: Reciprocity; octic; power residue.

Let p and q be distinct primes congruent to 1 (mod 8). Write

$$p = a_1^2 + b_1^2 = a_2^2 + 2b_2^2, \quad q = c_1^2 + d_1^2 = c_2^2 + 2d_2^2,$$

where a_i, b_i, c_i, d_i, $i = 1, 2$ are integers and a_1, c_1 are odd. For a prime r and an integer a, define $(a/r)_4 = +1$ if a is a quartic residue $\pmod r$ and $(a/r)_4 = -1$ otherwise. In a similar way, define $(a/r)_8$ and $(a/r)_2$. Assume $(p/q)_4 = (q/p)_4 = 1$. A rational octic reciprocity law proved independently by Williams[5] and Wu[6] says

$$\left(\frac{p}{q}\right)_8 \left(\frac{q}{p}\right)_8 = \left(\frac{a_1d_1 - b_1c_1}{q}\right)_4 \left(\frac{a_2d_2 - b_2c_2}{q}\right)_2.$$

Since p, $q \equiv 1 \pmod 8$, we may also express p and q as

$$p = a_3^2 - 2b_3^2, \quad q = c_3^2 - 2d_3^2,$$

for some integers a_3, b_3, c_3, d_3. Then a computational evidence says that the following statement is also true.

Theorem.

$$\left(\frac{p}{q}\right)_8 \left(\frac{q}{p}\right)_8 = \left(\frac{a_1d_1 - b_1c_1}{q}\right)_4 \left(\frac{a_3d_3 - b_3c_3}{q}\right)_2.$$

It is our purpose to prove above statement. Note that, because of the existence of the fundamental unit $\epsilon = 1 + \sqrt{2}$, there are infinitely many choices of a_3, b_3, c_3, d_3. Also notice that $((a_1d_1 - b_1c_1)/q)_2 = 1$ by Burde's rational biquadratic reciprocity law. We will give two proofs of above theorem. The first proof uses Jacobi sum technique which is applied in the paper of Williams [5]. The second proof follows the idea of Helou[2], where he avoids Jacobi sum argument and uses Eisenstein's general octic reciprocity. Let $\zeta = \zeta_8$ be a primitive 8th root of unity. We have the cyclotomic field $\mathbf{Q}(\zeta) = \mathbf{Q}(\sqrt{2}, \sqrt{-1})$ and the group of units $\mathbf{Q}(\zeta)^\times = \langle \zeta, \epsilon \rangle$ where $\epsilon = 1 + \sqrt{2}$. The Galois group $\mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$ consists of the elements σ_s with $\sigma_s(\zeta) = \zeta^s$ where $s = 1, 3, 5, 7$. We say $\alpha \in \mathbf{Z}[\zeta]$ is primary if $\alpha \equiv 1 \pmod{2 + 2\zeta}$. It is easy to see that for any $\alpha \in \mathbf{Z}[\zeta]$ with odd norm, there is a unit $u \in \mathbf{Q}(\zeta)^\times$ such that $u\alpha$ is primary. There are infinitely many choices of such u because $\epsilon^4 \equiv 1 \pmod{2 + 2\zeta}$. To prove the theorem, we will use the property of primary primes above p and q, which at first restricts the choices of a_i, b_i, c_i, d_i, $i = 1, 2, 3$. However, it will be easily seen that the theorem is independent of such choices.

First proof. Let $\pi = \pi_1 \in \mathbf{Z}[\zeta]$ be a primary prime above p. Letting $\pi_s = \sigma_s(\pi)$, we see that all π_s are primary and $p = \pi_1\pi_3\pi_5\pi_7$. Let $\chi = \chi_\pi$ be the residue character $(\cdot/\pi)_8$ of order 8 on $\mathbf{F}_p$. Then we have the following well known relation between Gauss and Jacobi sums,

$$G(\chi)^8 = \chi(-1)pJ(\chi,\chi)J(\chi,\chi^2)\cdots J(\chi,\chi^6).$$

Also using the well known expression of Jacobi sums $J(\chi, \chi^j)$, $j = 1, 2, \ldots, 6$, we have (see [4] or [5])

$$G(\chi)^8 = \pi_1^7\pi_3^5\pi_5^3\pi_7 = p\pi_1^6\pi_3^4\pi_5^2.$$

From the observations $\zeta^3 + \zeta = \sqrt{-2}$, $\zeta^2 = \sqrt{-1}$ and $\zeta + \zeta^{-1} = \sqrt{2}$, we may write $\pi_1\pi_3 = a_2 + b_2\sqrt{-2}$, $\pi_1\pi_5 = a_1 + b_1\sqrt{-1}$ and $\pi_1\pi_7 = a_3 + b_3\sqrt{2}$. Then we get

$$p = a_1^2 + b_1^2 = a_2^2 + 2b_2^2 = a_3^2 - 2b_3^2.$$

Note that above integers a_1, b_1, a_2, b_2 may have different signs from the corresponding ones in the theorem. Also note that $a_1 \equiv 1 \pmod 4$ since π is primary. Now from

$$G(\chi) = \sum_{x=0}^{p-1} \chi(x) \exp(2\pi x\sqrt{-1}/p),$$

2000 Mathematics Subject Classification. Primary 11A15, 11R04.

we find

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

Letting λ be a primary prime above q in $\mathbf{Q}(\zeta)$,

$$\begin{aligned}
\left(\frac{q}{p}\right)_8 &\equiv G(\chi)^{q-1} \equiv G(\chi)^{8\{(q-1)/8\}} \pmod\lambda \\
&\equiv (G(\chi)^8\pi_7^8)^{(q-1)/8} \pmod\lambda \\
&\equiv (p\pi_1^6\pi_3^4\pi_5^2\pi_7^8)^{(q-1)/8} \pmod\lambda \\
&\equiv (p^3\pi_1^4\pi_3^2\pi_7^6)^{(q-1)/8} \pmod\lambda \\
&\equiv (p\pi_1^4\pi_3^2\pi_7^6)^{(q-1)/8} \pmod\lambda \\
&\qquad\qquad \text{because } \left(\frac{p}{q}\right)_4 = 1. \\
&\equiv \left(\frac{p}{q}\right)_8 (\pi_3\pi_7)^{(q-1)/4}(\pi_1\pi_7)^{(q-1)/2} \pmod\lambda.
\end{aligned}$$

Note that $\pi_3\pi_7 = \sigma_3(\pi_1\pi_5) = a_1 - b_1\sqrt{-1}$. Thus writing $\lambda\sigma_5(\lambda) = c_1 - d_1\sqrt{-1}$ and using $\sqrt{-1} \equiv c_1 d_1'$ $(\text{mod } c_1 - d_1\sqrt{-1})$ with $d_1 d_1' \equiv 1 \pmod q$, we have

$$(\pi_3\pi_7)^{(q-1)/4} \equiv \left(\frac{a_1 - b_1\sqrt{-1}}{c_1 - d_1\sqrt{-1}}\right)_4 \pmod\lambda,$$

where

$$\begin{aligned}
&\left(\frac{a_1 - b_1\sqrt{-1}}{c_1 - d_1\sqrt{-1}}\right)_4 \\
&= \left(\frac{a_1 - b_1c_1d_1'}{c_1 - d_1\sqrt{-1}}\right)_4 \\
&= \left(\frac{d_1}{c_1 - d_1\sqrt{-1}}\right)_4 \left(\frac{a_1d_1 - b_1c_1}{c_1 - d_1\sqrt{-1}}\right)_4 \\
&= \left(\frac{d_1}{q}\right)_4 \left(\frac{a_1d_1 - b_1c_1}{q}\right)_4.
\end{aligned}$$

Since $c_1 - d_1\sqrt{-1}$ is primary, i.e. $c_1 \equiv 1 \pmod 4$, $d_1 \equiv 0 \pmod 4$, using a biquadratic reciprocity law, it is routine to check that $(d_1/q)_4 = 1$ (see [3], pp. 122–123). Also using the fact that $p, q \equiv 1 \pmod 8$ and $(q/p)_4 = 1 = (p/q)_4$, one easily deduce that the expression $((a_1 - b_1\sqrt{-1})/(c_1 - d_1\sqrt{-1}))_4$ is independent of the signs of a_1, b_1, c_1, d_1. For example, $((a_1 - b_1\sqrt{-1})/(c_1 - d_1\sqrt{-1}))_4((a_1 + b_1\sqrt{-1})/(c_1 - d_1\sqrt{-1}))_4 = (p/(c_1 - d_1\sqrt{-1}))_4 = (p/q)_4 = 1$. In a similar way, writing $\lambda\sigma_7(\lambda) = c_3 + d_3\sqrt{2}$ and expressing $\sqrt{2}$ as $\sqrt{2} \equiv -c_3d_3'$ $(\text{mod } c_3 + d_3\sqrt{2})$ with $d_3d_3' \equiv 1 \pmod q$, we have

$$(\pi_1\pi_7)^{(q-1)/2} \equiv \left(\frac{a_3 + b_3\sqrt{2}}{c_3 + d_3\sqrt{2}}\right)_2 \pmod\lambda,$$

where

$$\begin{aligned}
\left(\frac{a_3 + b_3\sqrt{2}}{c_3 + d_3\sqrt{2}}\right)_2 &= \left(\frac{a_3 - b_3c_3d_3'}{c_3 + d_3\sqrt{2}}\right)_2 \\
&= \left(\frac{d_3}{c_3 + d_3\sqrt{2}}\right)_2 \left(\frac{a_3d_3 - b_3c_3}{c_3 + d_3\sqrt{2}}\right)_2 \\
&= \left(\frac{d_3}{q}\right)_2 \left(\frac{a_3d_3 - b_3c_3}{q}\right)_2 \\
&= \left(\frac{a_3d_3 - b_3c_3}{q}\right)_2.
\end{aligned}$$

It is also clear that above expression is independent of the signs of a_3, b_3, c_3, d_3 because $(p/q)_2 = 1$ and p, $q \equiv 1 \pmod 8$. Moreover, if A_3, B_3, C_3, D_3 are any integers satisfying

$$p = A_3^2 - 2B_3^2, \quad q = C_3^2 - 2D_3^2,$$

then we have

$$\begin{aligned}
A_3 + B_3\sqrt{2} &= \pm\epsilon^{2m}(a_3 \pm b_3\sqrt{2}), \\
C_3 + D_3\sqrt{2} &= \pm\epsilon^{2n}(c_3 \pm d_3\sqrt{2}),
\end{aligned}$$

for some integers m and n. Therefore

$$\begin{aligned}
&\left(\frac{A_3D_3 - B_3C_3}{q}\right)_2 \\
&= \left(\frac{A_3 + B_3\sqrt{2}}{C_3 + D_3\sqrt{2}}\right)_2 = \left(\frac{\pm\epsilon^{2m}(a_3 \pm b_3\sqrt{2})}{\pm\epsilon^{2n}(c_3 \pm d_3\sqrt{2})}\right)_2 \\
&= \left(\frac{\pm\epsilon^{2m}(a_3 \pm b_3\sqrt{2})}{c_3 \pm d_3\sqrt{2}}\right)_2 = \left(\frac{a_3 + b_3\sqrt{2}}{c_3 + d_3\sqrt{2}}\right)_2 \\
&= \left(\frac{a_3d_3 - b_3c_3}{q}\right)_2.
\end{aligned}$$

Now, the proof is complete after we replace $(\pi_3\pi_7)^{(q-1)/4}$ and $(\pi_1\pi_7)^{(q-1)/2}$ by the corresponding residue symbols $((a_1d_1 - b_1c_1)/q)_4$ and $((a_3d_3 - b_3c_3)/q)_2$ in the expression

$$\left(\frac{q}{p}\right)_8 \equiv \left(\frac{p}{q}\right)_8 (\pi_3\pi_7)^{(q-1)/4}(\pi_1\pi_7)^{(q-1)/2} \pmod\lambda.$$

□

Second proof. Let n be a positive integer and let p, q be distinct primes of $\mathbf{Q}$ which are congruent to $1 \pmod n$. Note that such primes p, q split completely in $\mathbf{Q}(\zeta_n)$. Let π, λ be primes of $\mathbf{Q}(\zeta_n)$ lying above p, q. Suppose that $\pi = f(\zeta_n)$ for some polynomial $f \in \mathbf{Z}[x]$. Let z be a rational integer such that $z \equiv \zeta_n \pmod\lambda$. Helou [2] found the following result and used it to give unified proofs of rational cubic, quartic and octic reciprocity laws.

Proposition.

$$\left(\frac{q}{\pi}\right)_n \left(\frac{p}{\lambda}\right)_n^{-1} = e(q,\pi)\left(\frac{m}{\lambda}\right)_n,$$

where $e(q,\pi) = (q/\pi)_n(\pi/q)_n^{-1}$ *and* m *is a rational integer determined by*

$$m \equiv \prod_k f(z^k)^{k'-1} \pmod q,$$

where the product runs through all $1 \leqq k < n$ *with* $\gcd(k,n) = 1$ *and* $kk' \equiv 1 \pmod n$.

Helou applied above result for the case $n = 8$ and derived

$$\left(\frac{q}{\pi}\right)_8 \left(\frac{p}{\lambda}\right)_8^{-1} = e(q,\pi)\left(\frac{f(z^3)f(z^5)^2f(z^7)^3}{\lambda}\right)_4.$$

Assuming π is primary, he showed that $e(q,\pi) = 1$ using Eisenstein's general octic reciprocity law. Therefore, since we have assumed $(q/p)_4 = 1 = (p/q)_4$,

$$\begin{aligned}\left(\frac{q}{p}\right)_8\left(\frac{p}{q}\right)_8 &= \left(\frac{q}{\pi}\right)_8\left(\frac{p}{\lambda}\right)_8\\ &= \left(\frac{f(z^3)f(z^5)^2f(z^7)^3}{\lambda}\right)_4.\end{aligned}$$

The right part of above expression can be rewritten as

$$\begin{aligned}&\left(\frac{f(z^3)f(z^5)^2f(z^7)^3}{\lambda}\right)_4\\ &= \left(\frac{f(z)^4f(z^3)f(z^5)^2f(z^7)^3}{\lambda}\right)_4\\ &= \left(\frac{pf(z)^3f(z^5)f(z^7)^2}{\lambda}\right)_4\\ &= \left(\frac{f(z)f(z^5)}{\lambda}\right)_4\left(\frac{f(z)f(z^7)}{\lambda}\right)_2.\end{aligned}$$

Now letting $\sigma_s \in \mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$, $\zeta = \zeta_8$ be as in the first proof, we have $\sigma_s f(\zeta) = f(\zeta^s)$ for $s = 1,3,5,7$. Note that

$$f(\zeta)f(\zeta^5) = f(\zeta)\sigma_5(f(\zeta)) = \pi\sigma_5(\pi) = a_1 + b_1\sqrt{-1},$$

and

$$f(\zeta)f(\zeta^7) = f(\zeta)\sigma_7(f(\zeta)) = \pi\sigma_7(\pi) = a_3 + b_3\sqrt{2}.$$

Write also

$$\lambda\sigma_5(\lambda) = c_1 + d_1\sqrt{-1}, \quad \lambda\sigma_7(\lambda) = c_3 + d_3\sqrt{2}.$$

Then the proof is complete as soon as we show

$$\left(\frac{f(z)f(z^5)}{\lambda}\right)_4 = \left(\frac{a_1d_1 - b_1c_1}{q}\right)_4,$$

$$\left(\frac{f(z)f(z^7)}{\lambda}\right)_2 = \left(\frac{a_3d_3 - b_3c_3}{q}\right)_2.$$

Since $\sqrt{-1} \equiv -c_1d_1' \pmod{c_1 + d_1\sqrt{-1}}$ where $d_1d_1' \equiv 1 \pmod q$,

$$\begin{aligned}\left(\frac{f(z)f(z^5)}{\lambda}\right)_4 &= \left(\frac{f(\zeta)f(\zeta^5)}{\lambda}\right)_4\\ &= \left(\frac{a_1 + b_1\sqrt{-1}}{c_1 + d_1\sqrt{-1}}\right)_4\\ &= \left(\frac{a_1 - b_1c_1d_1'}{c_1 + d_1\sqrt{-1}}\right)_4\\ &= \left(\frac{d_1}{c_1 + d_1\sqrt{-1}}\right)_4\left(\frac{a_1d_1 - b_1c_1}{c_1 + d_1\sqrt{-1}}\right)_4\\ &= \left(\frac{d_1}{q}\right)_4\left(\frac{a_1d_1 - b_1c_1}{q}\right)_4\\ &= \left(\frac{a_1d_1 - b_1c_1}{q}\right)_4.\end{aligned}$$

Since $\sqrt{2} \equiv -c_3d_3' \pmod{c_3 + d_3\sqrt{2}}$ where $d_3d_3' \equiv 1 \pmod q$,

$$\begin{aligned}\left(\frac{f(z)f(z^7)}{\lambda}\right)_2 &= \left(\frac{f(\zeta)f(\zeta^7)}{\lambda}\right)_2\\ &= \left(\frac{a_3 + b_3\sqrt{2}}{c_3 + d_3\sqrt{2}}\right)_2\\ &= \left(\frac{a_3 - b_3c_3d_3'}{c_3 + d_3\sqrt{2}}\right)_2\\ &= \left(\frac{d_3}{c_3 + d_3\sqrt{2}}\right)_2\left(\frac{a_3d_3 - b_3c_3}{c_3 + d_3\sqrt{2}}\right)_2\\ &= \left(\frac{d_3}{q}\right)_2\left(\frac{a_3d_3 - b_3c_3}{q}\right)_2\\ &= \left(\frac{a_3d_3 - b_3c_3}{q}\right)_2.\end{aligned}$$

□

An obvious corollary is the following.

Corollary. *Let* p, q *be distinct primes congruent to* $1 \pmod 8$. *Write*

$$p = a_2^2 + 2b_2^2 = a_3^2 - 2b_3^2, \quad q = c_2^2 + 2d_2^2 = c_3^2 - 2d_3^2,$$

where a_i, b_i, c_i, d_i, $i = 2, 3$ *are integers. Suppose that* $(p/q)_4 = (q/p)_4 = 1$. *Then*

$$\left(\frac{a_2d_2 - b_2c_2}{q}\right)_2 = \left(\frac{a_3d_3 - b_3c_3}{q}\right)_2.$$

Acknowledgements. This work was supported in part by KRF 1999-015-DP0008.

References

[1] Burde, K.: Ein rationales biquadratisches reziprozitätsgesetz. J. Reine Angew. Math., **235**, 175–184 (1969).

[2] Helou, C.: On rational reciprocity. Proc. Amer. Math. Soc., **108**, 861–866 (1990).

[3] Ireland, K., and Rosen, M.: A Classical Introduction to Modern Number Theory. Springer, New York (1990).

[4] Lemmermeyer, F.: Reciprocity Laws: from Euler to Eisenstein. Springer, New York (2000).

[5] Williams, K.: A rational octic reciprocity law. Pacific J. Math., **63**, 563–570 (1976).

[6] Wu, P.: A rational reciprocity law. Ph. D. thesis, Univ. Southern California (1975).