PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 77, Number 3, December 1979

AN OCTIC RECIPROCITY LAW OF SCHOLZ TYPE

DUNCAN A. BUELL AND KENNETH S. WILLIAMS[1]

ABSTRACT. The authors [3] have conjectured that if p and q are distinct primes satisfying

$$p \equiv q \equiv 1 \pmod 8, \qquad (p/q)_4 = (q/p)_4 = +1,$$

then

$$\left(\frac{p}{q}\right)_8\left(\frac{q}{p}\right)_8 = \begin{cases} \left(\frac{\varepsilon_p}{q}\right)_4\left(\frac{\varepsilon_q}{p}\right)_4, & \text{if } N(\varepsilon_{pq}) = -1, \\ (-1)^{h(pq)/4}\left(\frac{\varepsilon_p}{q}\right)_4\left(\frac{\varepsilon_q}{p}\right)_4, & \text{if } N(\varepsilon_{pq}) = +1, \end{cases}$$

where ε_p is the fundamental unit of $Q(\sqrt{p})$, $N(\varepsilon_{pq})$ denotes the norm of the unit ε_{pq}, and $h(pq)$ is the class number of $Q(\sqrt{pq})$. A proof of this conjecture is given, which makes use of results of Bucher [2].

In the eighteenth century the famous law of quadratic reciprocity was formulated independently by Euler and Legendre and was first proved by Gauss. This law can be expressed in the form

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4},$$

where p and q are odd distinct primes and (p/q) is the Legendre symbol, which is $+1$ or -1 according as p is or is not a quadratic residue of q.

A rational quartic analogue of this law was found by Scholz [7] in 1934. (For other proofs of Scholz's law, see [4], [5], [8], and for a discussion of rational reciprocity laws, see [6].) If $p \equiv q \equiv 1 \pmod 4$ and $(p/q) = +1$, Scholz's law of quartic reciprocity takes the form

$$\left(\frac{p}{q}\right)_4\left(\frac{q}{p}\right)_4 = \left(\frac{\varepsilon_p}{q}\right) = \left(\frac{\varepsilon_q}{p}\right), \tag{1}$$

where the symbol $(p/q)_4$ is $+1$ or -1 according as p is or is not a quartic residue of q, and ε_p (resp. ε_q) denotes the fundamental unit of the real quadratic field $Q(\sqrt{p})$ (resp. $Q(\sqrt{q})$). When evaluating (ε_p/q), ε_p is taken as an integer modulo q as p is a square modulo q.

Recently the authors [3] conjectured the octic analogue of (1), on the basis of numerical evidence, under the assumption that p and q are primes such

Received by the editors November 15, 1978.

AMS (MOS) subject classifications (1970). Primary 10A15; Secondary 12A25, 12A45, 12A50.

Key words and phrases. Legendre symbol, rational reciprocity laws, Scholz's law, fundamental unit of real quadratic field, class numbers of quadratic fields.

[1]The research of the second author was supported by the National Research Council of Canada, Grant #A-7233.

that

$$\equiv q \equiv 1 \pmod 8, \qquad (p/q)_4 = (q/p)_4 = +1, \tag{2}$$

so that the symbols $(p/q)_8$ and $(q/p)_8$ are defined. For such primes, by (1), we have $(\varepsilon_p/q) = (\varepsilon_q/p) = +1$, so that $(\varepsilon_p/q)_4$ is $+1$ or -1 according as ε_p is or is not a quartic residue of q. The norm of the fundamental unit $\varepsilon_{pq} = \frac{1}{2}(T + U\sqrt{pq})$ of $Q(\sqrt{pq})$ is denoted by $N(\varepsilon_{pq})$. The class number of $Q(\sqrt{pq})$ is denoted by $h(pq)$, and is the number of *ordinary* ideal classes of $Q(\sqrt{pq})$. It is known (see for example [**1**, p. 408] that if $p \equiv q \equiv 1 \pmod 4$, $(p/q)_4 = (q/p)_4 = +1$, then

$$h(pq) \equiv \begin{cases} 0 \pmod 8, & \text{if } N(\varepsilon_{pq}) = -1, \\ 0 \pmod 4, & \text{if } N(\varepsilon_{pq}) = +1. \end{cases} \tag{3}$$

Our conjecture asserts that if $p \equiv q \equiv 1 \pmod 8$ and $(p/q)_4 = (q/p)_4 = +1$, then

$$\left(\frac{p}{q}\right)_8\left(\frac{q}{p}\right)_8 = \begin{cases} \left(\frac{\varepsilon_p}{q}\right)_4\left(\frac{\varepsilon_q}{p}\right)_4, & \text{if } N(\varepsilon_{pq}) = -1, \\ (-1)^{h(pq)/4}\left(\frac{\varepsilon_p}{q}\right)_4\left(\frac{\varepsilon_q}{p}\right)_4, & \text{if } N(\varepsilon_{pq}) = +1. \end{cases} \tag{4}$$

It is the purpose of this note to prove this conjecture. This is done by appealing to some results of Bucher [**2**]. Bucher's work, although published as long ago as 1943, is contained in a relatively inaccessible journal, and has only recently come to our attention. We therefore give the relevant details from [**2**].

Bucher [**2**, p. 5] considered primes p and q satisfying

$$p \equiv q \equiv 1 \pmod 4, \qquad (p/q)_4 = (q/p)_4 = +1. \tag{5}$$

For such primes $h_0(pq)$, the number of *strict* ideal classes of $Q(\sqrt{pq})$, satisfies $h_0(pq) \equiv 0 \pmod 8$ (see for example, [**1**, p. 408]). $h_0(pq)$ is the class number used by Bucher, although he uses the notation $h(pq)$ for it. We have

$$h_0(pq) = \begin{cases} h(pq), & \text{if } N(\varepsilon_{pq}) = -1, \\ 2h(pq), & \text{if } N(\varepsilon_{pq}) = +1. \end{cases}$$

For primes satisfying (5), Bucher [**2**, p. 6] defines $\lambda_{p,q} = \pm 1$ by

$$\lambda_{p,q} = \operatorname{sgn}\left\{ \prod_{\substack{x=1 \\ (x/p)=1}}^{(p-1)/2} \prod_{\substack{y=1 \\ (y/q)=1}}^{(q-1)/2} \left(4\sin^2\left(\frac{x\pi}{p}\right) - 4\sin^2\left(\frac{y\pi}{q}\right)\right)\right\},$$

and observes [**2**, equation (7), p. 6] that

$$\lambda_{p,q}\lambda_{q,p} = (-1)^{(p-1)(q-1)/16}. \tag{6}$$

Further, he defines [**2**, p. 6] the totally positive numbers e_p and e_q by

$$e_p = -\sqrt{p}\,\varepsilon_p', \qquad e_q = -\sqrt{q}\,\varepsilon_q',$$

where the prime (′) indicates conjugation in $Q(\sqrt{p})$ or $Q(\sqrt{q})$ as appropriate. Factoring p as the product of two conjugate prime ideals in $Q(\sqrt{p})$, say $p = PP'$, and q as the product of two conjugate prime ideals in $Q(\sqrt{q})$, say $q = QQ'$, Bucher defines (we use a slightly different notation to avoid confusion with our residue symbols) the biquadratic symbols $[e_p/Q]_4$ and $[e_q/P]_4$ by $[e_p/Q]_4 \equiv e_p^{(q-1)/4} \pmod{Q}$ and $[e_q/P]_4 \equiv e_q^{(p-1)/4} \pmod{P}$, and notes that

$$\left[\frac{e_p}{Q}\right]_4 = \left[\frac{e_p}{Q'}\right]_4 = \pm 1, \qquad \left[\frac{e_q}{P}\right]_4 = \left[\frac{e_q}{P'}\right]_4 = \pm 1.$$

Bucher's principal result [2, Hauptsatz, p. 6] (proved by elementary means) states

$$\lambda_{q,p}\left[\frac{e_q}{P}\right]_4 \equiv \left(\frac{t}{2}\right)^{h_0(pq)/8} \pmod{p}, \quad \lambda_{p,q}\left[\frac{e_p}{Q}\right]_4 \equiv \left(\frac{t}{2}\right)^{h_0(pq)/8} \pmod{q}, \tag{7}$$

where t and u are the least positive integers such that $t^2 - pqu^2 = 4$ [2, p. 4].

Assume now that (2) holds, so that (6) becomes

$$\lambda_{p,q}\lambda_{q,p} = +1. \tag{8}$$

Relating Bucher's biquadratic residue symbols to ours, we obtain

$$\left[\frac{e_q}{P}\right]_4 = \left[\frac{-\sqrt{q}\,\varepsilon_q'}{P}\right]_4 = \left(\frac{-\sqrt{q}\,\varepsilon_q'}{p}\right)_4 = (-1)^{(p-1)/4}\left(\frac{q}{p}\right)_8\left(\frac{\varepsilon_q'}{p}\right)_4,$$

that is

$$\left[\frac{e_q}{P}\right]_4 = \left(\frac{q}{p}\right)_8\left(\frac{\varepsilon_q}{p}\right)_4, \tag{9}$$

and similarly

$$\left[\frac{e_p}{Q}\right]_4 = \left(\frac{p}{q}\right)_8\left(\frac{\varepsilon_p}{q}\right)_4. \tag{10}$$

If $N(\varepsilon_{pq}) = -1$, we have $h_0(pq) = h(pq)$, and in this case [2, p. 2]

$$\frac{1}{2}(t + u\sqrt{pq}) = \varepsilon_{pq}^2 = \left\{\frac{1}{2}(T + U\sqrt{pq})\right\}^2,$$

so

$$\frac{t}{2} = \frac{T^2 + pqU^2}{4} \equiv -1 \pmod{pq}. \tag{11}$$

Thus (7) becomes (using (9), (10), (11))

$$\lambda_{q,p}\left(\frac{q}{p}\right)_8\left(\frac{\varepsilon_q}{p}\right)_4 = (-1)^{h(pq)/8}, \quad \lambda_{p,q}\left(\frac{p}{q}\right)_8\left(\frac{\varepsilon_p}{q}\right)_4 = (-1)^{h(pq)/8}.$$

Multiplying these together, we obtain the first part of (4), in view of (8).

If $N(\varepsilon_{pq}) = +1$, we have $h_0(pq) = 2h(pq)$, and in this case [**2**, p. 2]

$$\frac{1}{2}\left(t + u\sqrt{pq}\right) = \varepsilon_{pq} = \left\{\frac{1}{2}\left(v\sqrt{p} + w\sqrt{q}\right)\right\}^2,$$

for some integers v and w with

$$\frac{pv^2 - qw^2}{4} = \alpha, \quad \alpha = \pm 1.$$

Hence we have

$$\frac{t}{2} = \frac{pv^2 + qw^2}{4} \equiv \begin{cases} -\alpha & (\operatorname{mod} p), \\ +\alpha & (\operatorname{mod} q). \end{cases} \tag{12}$$

Thus (7) becomes (using (9), (10), (12))

$$\lambda_{q,p}\left(\frac{q}{p}\right)_8\left(\frac{\varepsilon_q}{p}\right)_4 = (-\alpha)^{h(pq)/4}, \quad \lambda_{p,q}\left(\frac{p}{q}\right)_8\left(\frac{\varepsilon_p}{q}\right)_4 = \alpha^{h(pq)/4}.$$

Multiplying these together we obtain the second part of (4), in view of (8).

This completes the proof of the conjecture.

References

1. Ezra Brown, *Class numbers of quadratic fields*, Symposia Mathematica, Vol. 15, Academic Press, London, 1975, pp. 403–411. MR **52** #3111.

2. J. Bucher, *Neues über die Pell'sche Gleichung*, Mitt. Naturforsch. Ges. Luzern **14** (1943), 1–18. MR **9** #78.

3. Duncan A. Buell and Kenneth S. Williams, *Is there an octic reciprocity law of Scholz type?*, Amer. Math. Monthly **85** (1978), 483–484.

4. Dennis R. Estes and Gordon Pall, *Spinor genera of binary quadratic forms*, J. Number Theory **5** (1973), 421–432. MR **48** #10979.

5. Emma Lehmer, *On the quadratic character of some quadratic surds*, J. Reine Angew. Math. **250** (1971), 42–48. MR **44** #3986.

6. ______, *Rational reciprocity laws*, Amer. Math. Monthly **85** (1978), 467–472.

7. Arnold Scholz, *Über die Lösbarkeit der Gleichung $t^2 - Du^2 = -4$*, Math. Z. **39** (1934), 95–111.

8. Kenneth S. Williams, *On Scholz's reciprocity law*, Proc. Amer. Math. Soc. **64** (1977), 45–46.

Department of Computer Science, Bowling Green State University, Bowling Green, Ohio 43403

Department of Mathematics, Carleton University, Ottawa, Ontario, Canada K1S 5B6 (Current address of K. S. Williams)

Current address (D. A. Buell): Department of Computer Science, Louisiana State University, Baton Rouge, Louisiana 70803