PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 111, Number 3, March 1991

ON YAMAMOTO'S RECIPROCITY LAW

KENNETH S. WILLIAMS

(Communicated by William Adams)

ABSTRACT. A simple proof of Yamamoto's reciprocity law is given.

Let p and q be distinct odd primes with $p \equiv q \equiv 1 \pmod 4$. Define the symbol $[p, q] = \pm 1$ by

$$[p, q] \equiv p^{(q-1)/4} (\tfrac{t}{2})^{h(pq)/2} \pmod q,$$

where $h(pq)$ is the classnumber of the real quadratic field $Q(\sqrt{pq})$ and $\varepsilon(pq) = \frac{1}{2}(t + u\sqrt{pq}) > 1$ is its fundamental unit (t, u positive integers). Yamamoto's reciprocity law [5, Theorem 3] states that

$$[p, q] = [q, p].$$

We give a simple proof of a slightly stronger result:

Theorem. *Let p and q be distinct primes with $p \equiv q \equiv 1 \pmod 4$; let $A(p, q)$ be the number of pairs (x, y) of integers satisfying*

$$0 < x < \tfrac{p}{2}, \qquad 0 < y < \tfrac{q}{2}, \qquad qx < py, \qquad (\tfrac{x}{p}) = -(\tfrac{y}{q}),$$

where (x/p) is the familiar Legendre symbol. Then

$$[p, q] = [q, p] = (-1)^{A(p,q)} (\tfrac{p}{q}).$$

The following lemma is well known; notation is as above.

Lemma. *$h(pq)$ is even; furthermore*

(a) $h(pq) \equiv 0 \pmod 4$, *if* $(\frac{p}{q}) = 1$, $(\frac{p}{q})_4 = (\frac{q}{p})_4$ [1, Theorem 4; 4, p. 603],

(b) $(\frac{t}{2})^2 - pq(\frac{u}{2})^2 = +1$, *if* $(\frac{p}{q}) = 1$, $(\frac{p}{q})_4 = -(\frac{q}{p})_4$ [4, p. 603],

(c) $h(pq) \equiv 2 \pmod 4$, $(\frac{t}{2})^2 - pq(\frac{u}{2})^2 = -1$, *if* $(\frac{p}{q}) = -1$ [1, Theorem 4; 3, §3].

Received by the editors June 7, 1989 and, in revised form, March 26, 1990.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11A15; Secondary 11R11.
Key words and phrases. Reciprocity, quadratic fields, classnumber.
Research supported by Natural Sciences and Engineering Research Council of Canada Grant A-7233.

Proof of the theorem. By the lemma, a straightforward calculation shows that

$$[p, q]^2 \equiv \left(p^{(q-1)/4}\left(\tfrac{t}{2}\right)^{h(pq)/2}\right)^2 \equiv 1 \pmod{q};$$

hence, the symbol $[p, q]$ is indeed $+1$ or -1.

Let $\delta = \pm 1$, $\varepsilon = \pm 1$. An application of Dirichlet's classnumber formula applied to each of the real quadratic fields $Q(\sqrt{p})$, $Q(\sqrt{q})$, $Q(\sqrt{pq})$ gives

$$\prod_{\substack{0<k<pq/2 \\ (k/p)=\delta,\ (k/q)=\varepsilon}} 2\sin(k\pi/pq) = \varepsilon(p)^{-\delta(1-(q/p))h(p)/4}\varepsilon(q)^{-\varepsilon(1-(p/q))h(p)/4}\varepsilon(pq)^{-\delta\varepsilon\, h(pq)/4}. \tag{1}$$

The trigonometric product on the left side of (1) is an integer of the cyclotomic field $Q(e^{2\pi i/pq})$. Next, if $\mathscr{P}$ (resp. $\mathscr{Q}$) is a prime ideal of $Q(e^{2\pi i/pq})$ dividing $1-e^{2\pi i/p}$ (resp. $1-e^{2\pi i/q}$), we can show using the method of Bucher [2]

(2)

$$\prod_{\substack{0<k<pq/2 \\ (k/p)=\delta,\ (k/q)=\varepsilon}} 2\sin(k\pi/pq) \equiv \begin{cases} (-1)^{N(p,q,\delta,\varepsilon)+(p-1)(q-1)/16} q^{(p-1)/8}\varepsilon(q)^{-(p/q)\varepsilon h(q)(p-1)/4} \pmod{\mathscr{P}}, \\ (-1)^{N(p,q,\delta,\varepsilon)} p^{(q-1)/8}\varepsilon(q)^{-(q/p)\delta h(p)(q-1)/4} \pmod{\mathscr{Q}}, \end{cases}$$

where $N(p, q, \delta, \varepsilon) =$ number of pairs (x, y) of integers satisfying

$$0 < x < p/2, \qquad 0 < y < q/2, \qquad qx < py, \qquad \left(\tfrac{x}{p}\right) = \left(\tfrac{q}{p}\right)\delta, \qquad \left(\tfrac{y}{q}\right) = \left(\tfrac{p}{q}\right)\varepsilon. \tag{3}$$

From (1) and (2), we have

$$q^{(p-1)/8} \equiv (-1)^{N(p,q,\delta,\varepsilon)+(p-1)(q-1)/16}\varepsilon(p)^{-\delta(1-(p/q))(h(p)/4)} \times \varepsilon(q)^{\varepsilon((p/q)-1)(h(q)/4)}\varepsilon(pq)^{-\delta\varepsilon h(pq)/4} \pmod{\mathscr{P}} \tag{4}$$

and

$$p^{(q-1)/8} \equiv (-1)^{N(p,q,\delta,\varepsilon)}\varepsilon(p)^{\delta((q/p)q-1)(h(p)/4)} \times \varepsilon(q)^{-\varepsilon(1-(p/q))(h(q)/4)}\varepsilon(pq)^{-\delta\varepsilon h(pq)/4} \pmod{\mathscr{Q}}. \tag{5}$$

Mapping $p \to q$, $q \to p$, $\delta \to \varepsilon$, $\varepsilon \to \delta$ in (4), so that $\mathscr{P} \to \mathscr{Q}$, we obtain

$$N(p, q, \delta, \varepsilon) \equiv N(q, p, \varepsilon, \delta) + (p-1)(q-1)/16 \pmod{2}. \tag{6}$$

Taking $(\delta, \varepsilon) = (1, -1)$ and $(-1, 1)$ in (5) and multiplying the resulting two congruences together, we deduce

$$p^{(q-1)/4} \equiv (-1)^{N(p,q,1,-1)+N(p,q,-1,1)}\varepsilon(pq)^{h(pq)/2} \pmod{\mathscr{Q}}. \tag{7}$$

As $\mathscr{Q}$ divides $(1-e^{2\pi i/q})$ and $(1-e^{2\pi i/q})$ divides $\sqrt{q}$, we deduce from (7)

$$p^{(q-1)/4} \equiv (-1)^{N(p,q,1,-1)+N(p,q,-1,1)}(t(pq)/2)^{h(pq)/2} \pmod{\mathscr{Q}}. \tag{8}$$

Further, as both sides of (8) are integers $(\mathrm{mod}\ q)$, we have

$$p^{(q-1)/4} \equiv (-1)^{N(p,q,1,-1)+N(p,q,-1,1)}(t(pq)/2)^{h(pq)/2} \pmod{q}. \tag{9}$$

Multiplying both sides of (9) by $p^{(q-1)/4}(-1)^{N(p,q,1,-1)+N(p,q,-1,1)}$, we obtain

$$[p, q] = (-1)^{N(p,q,1,-1)+N(p,q,-1,1)}\left(\tfrac{p}{q}\right). \tag{10}$$

Similarly, from (4), we obtain

$$[q, p] = (-1)^{N(p,q,1,-1)+N(p,q,-1,1)}\left(\tfrac{q}{p}\right). \tag{11}$$

Hence, by the law of quadratic reciprocity, we have Yamamoto's reciprocity law in the form

$$[p, q] = [q, p] = (-1)^{A(p,q)}\left(\tfrac{p}{q}\right), \tag{12}$$

where $A(p, q) =$ number of pairs (x, y) of integers satisfying

$$0 < x < \tfrac{p}{2}, \qquad 0 < y < \tfrac{q}{2}, \qquad qx < py, \qquad \left(\tfrac{x}{p}\right) = -\left(\tfrac{y}{q}\right). \tag{13}$$

Acknowledgment

The author would like to acknowledge the help of Mr. Nicholas Buck (College of New Caledonia) who did some computing for the author in connection with this paper.

References

1. E. Brown, *Class numbers of quadratic fields*, Sympos. Math. **15** (1975), 403–411.
2. J. Bucher, *Neues über die Pell'sche Gleichung*, Mitt. Naturforsch. Ges. Luzern **14** (1943), 1–18.
3. P.G.L. Dirichlet, *Einige neue Sätze über unbestimmte Gleichungen*, Abh. Königlich Preussischen Akad. Wiss. 1834, pp. 649–664.
4. P. Kaplan, *Divisibilité par* 8 *du nombre des classes des corps quadratiques dont le* 2*-groupe des classes est cyclique, et réciprocité biquadratique*, J. Math. Soc. Japan **25** (1973), 596–608.
5. Y. Yamamoto, *Congruences modulo* 2^i $(i = 3, 4)$ *for the class numbers of quadratic fields*, Proc. Internat. Conf. on Class Numbers and Fundamental Units of Algebraic Number Fields, Katata, Japan, June 24–28, 1986, pp. 205–215.

Department of Mathematics and Statistics, Carleton University, Ottawa, Ontario, K1S 5B6 Canada