ACTA ARITHMETICA
XXXIX (1981)

Rational reciprocity laws

by

RONALD J. EVANS (La Jolla, Calif.)

1. Introduction. Let $k = 2^r$ for a natural number r. If n is a (nonzero) 2^{r-1}-th power residue modulo an odd prime q, one defines the rational residue symbol $\left(\frac{n}{q}\right)_k$ of order k by

$$\left(\frac{n}{q}\right)_k = \begin{cases} 1, & \text{if } n \text{ is a } k\text{-th power residue } (\mathrm{mod}\ q), \\ -1, & \text{otherwise}. \end{cases}$$

This is the Legendre symbol $\left(\frac{n}{q}\right)$ in the case $r = 1$. In 1969, Burde [2] proved that if $p = a^2+b^2$ and $q = A^2+B^2$ are odd primes with $\left(\frac{p}{q}\right) = 1$, $2 \nmid aA$, then

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

Burde's law is independent of the choice of signs for a, b, A, B. Other proofs may be found in [3], [7], [13]. An analogous rational octic law was obtained independently by Williams [12] and Wu [14]. In 1977, Leonard and Williams [9] proved a rational bioctic law. For a discussion of these and related reciprocity laws, see an article of E. Lehmer [8].

In this paper, we obtain systematically 2^r-th power rational reciprocity laws for each $r \geqslant 2$, in terms of parameters (defined in § 3) which are solutions of certain Diophantine equations and congruences. The parameters occurring in the laws for $r \leqslant 5$ are explicitly exhibited in § 4. In § 5, a general reciprocity law (akin to a quartic law of Burde [3], (2.16)) is proved and the rational 2^r-th power reciprocity laws follow (Corollary 7). These laws are explicitly presented for $r = 2$, 3, and 4, in § 6. Our law for $r = 4$ is different from that given in [9], Theorem 3, because we do not incorporate the parameters in [9], (1.4). A general 2^r-th power reciprocity law less explicit than ours was proved in 1958 by Furuta [4], who used class-field theory.

For supplementary theorems to the 2^r-th power rational reciprocity laws, see the papers [3A], [4A].

2. Notation and preliminary lemmas. The following notation will be used throughout this paper. Let $h = 2^s$, where $2 \leqslant s \leqslant r$. Write $\beta_s = \exp(2\pi i/h)$, $\Omega_s = \boldsymbol{Z}[\beta_s]$. If j is odd, define $\sigma_j \in \mathrm{Gal}(\boldsymbol{Q}(\beta_s)/\boldsymbol{Q})$ by $\sigma_j(\beta_s) = \beta_s^j$. Let p be a prime $\equiv 1 \pmod{2^r}$. For a nontrivial character $\lambda \pmod p$, define the Jacobi sum

$$K(\lambda) = \sum_{n \,(\mathrm{mod}\, p)} \lambda(1-n)\left(\frac{n}{p}\right)$$

and the Gauss sum

$$G(\lambda) = \sum_{n\,(\mathrm{mod}\, p)} \lambda(n) e^{2\pi i n/p}.$$

Since $p \equiv 1 \pmod 4$, we have the well-known result of Gauss that

$$(2) \qquad G(\lambda) = \sqrt{p}, \quad \text{when } \lambda \text{ has order } 2.$$

Moreover, for a character $\lambda_s \pmod p$ of order h, we have ([1], Theorems 2.2 and 2.5),

$$(3) \qquad |K(\lambda_s)|^2 = p,$$

$$(4) \qquad \sigma_{h/2-1} \text{ fixes } K(\lambda_s),$$

and

$$(5) \qquad \bar{\lambda}_s(4) K(\lambda_s) = G^2(\lambda_s)/G(\lambda_s^2) = \sum_{n\,(\mathrm{mod}\, p)} \lambda_s\big(n(1-n)\big).$$

LEMMA 1. *For a character $\lambda_s \pmod p$ of order h,*

$$(6) \qquad K(\lambda_s) \equiv -1 \big(\mathrm{mod}\ 2(1-\beta_s)\big)$$

and

$$(7) \qquad \mathrm{Re}\, K(\lambda_s) - 1 \equiv \mathrm{Im}\, K(\lambda_s) \equiv 0 \pmod 2.$$

Proof. We have

$$K(\lambda_s) = -p + \sum_{n\,(\mathrm{mod}\, p)} \big(\lambda_s(1-n)-1\big)\left(\left(\frac{n}{p}\right)-1\right) \equiv -p \equiv -1 \big(\mathrm{mod}\ 2(1-\beta_s)\big),$$

since $2 \Big| \left(\left(\frac{n}{p}\right)-1\right)$ and $(1-\beta_s) \big| \big(\lambda_s(1-n)-1\big)$ unless $n \equiv 0$ or $1 \pmod p$. This proves (6). By (5),

$$\begin{aligned} K(\lambda_s) + K(\lambda_s^{1+h/2}) &= \sum_{n\,(\mathrm{mod}\, p)} \lambda_s\big(4n(1-n)\big)\left\{1 + \left(\frac{n(1-n)}{p}\right)\right\} \\ &= 2 \sum_{\substack{n\,(\mathrm{mod}\, p) \\ \left(\frac{n(1-n)}{p}\right)=1}} \lambda_s\big(4n(1-n)\big) = 2 + 2 \sum_{\substack{n \not\equiv 2^{-1}\,(\mathrm{mod}\, p) \\ \left(\frac{n(1-n)}{p}\right)=1}} \lambda_s\big(4n(1-n)\big). \end{aligned}$$

Since the transformation $n \to 1-n$ leaves $\lambda_s\big(4n(1-n)\big)$ unchanged and since $n \not\equiv (1-n) \pmod p$ when $n \not\equiv 2^{-1} \pmod p$, it follows that

$$K(\lambda_s) + K(\lambda_s^{1+h/2}) \equiv 2 \pmod 4.$$

By (4), $K(\lambda_s^{1+h/2}) = K(\bar{\lambda}_s)$, so consequently $\mathrm{Re}\, K(\lambda_s) \equiv 1 \pmod 2$. Thus (7) follows, with the aid of (6).

LEMMA 2. *Let λ_s be a character* $\pmod p$ *of order h, with $s \geqslant 3$. Then*

$$(8) \qquad K(\lambda_s) = d_0 + \sum_{\substack{1 \leqslant j < h/4 \\ j \text{ even}}} d_j(\beta_s^j + \bar{\beta}_s^j) + i \sum_{\substack{1 \leqslant j < h/4 \\ j \text{ odd}}} d_j(\beta_s^j + \bar{\beta}_s^j),$$

where $d_0, d_1, \ldots, d_{h/4-1}$ are integers satisfying $d_0 \equiv -1 \pmod 4$ and $2 | d_j$ for $j > 0$.

Proof. Let $J = \{j \in \boldsymbol{Z}\colon 1 - h/4 \leqslant j \leqslant h/4\}$. As $\{\beta_s^j\colon j \in J\}$ is an integral basis for $\boldsymbol{Q}(\beta_s)$ over $\boldsymbol{Q}$, there are integers c_j such that

$$K(\lambda_s) = \sum_{j \in J} c_j \beta_s^j.$$

By (4),

$$\sum_{j\in J} c_j \beta_s^j = \sum_{j \in J} c_{1-j} \beta_s^{1-j} = \sum_{j\in J} c_{1-j} \beta_s^{(1-j)(h/2-1)} = \sum_{j \in J} c_{1-j} (-1)^{j-1} \beta_s^{j-1}.$$

Thus $c_{h/4} = 0$ and $c_j = (-1)^j c_{-j}$ for $|j| < h/4$.

Consequently,

$$K(\lambda_s) = c_0 + \sum_{\substack{1 \leqslant j < h/4 \\ j \text{ even}}} c_j(\beta_s^j + \bar{\beta}_s^j) + \sum_{\substack{1 \leqslant j < h/4 \\ j \text{ odd}}} c_j(\beta_s^j - \bar{\beta}_s^j),$$

and (8) follows with

$$d_j = \begin{cases} c_j, & \text{if } 2 | j, \\ c_{h/4-j}, & \text{if } 2 \nmid j. \end{cases}$$

Now $\{\beta_{s-1}^j\colon 1 - h/8 \leqslant j \leqslant h/8\}$ is an integral basis for $\boldsymbol{Q}(\beta_{s-1})$ over $\boldsymbol{Q}$. Since $\mathrm{Re}\, K(\lambda_s) - 1 \equiv 0 \pmod 2$ by (7), it follows from (8) that d_0 is odd and d_j is even for $1 \leqslant j < h/4$, $2|j$. Similarly, since $\beta^s \mathrm{Im}\, K(\lambda^s) \equiv 0 \pmod 2$ by (7), it follows that d_j is even for $1 \leqslant j < h/4$, $2 \nmid j$. It remains to prove that $d_0 \equiv -1 \pmod 4$. If $1 \leqslant j < h/4$, then $\beta_s^j + \bar{\beta}_s^j \equiv 0 \pmod{1-\beta_s}$, so $d_j(\beta_s^j + \bar{\beta}_s^j) \equiv 0 \big(\mathrm{mod}\ 2(1-\beta_s)\big)$. Thus, by (8), $K(\lambda_s) \equiv d_0 \big(\mathrm{mod}\ 2(1-\beta_s)\big)$. Therefore, by (6), $d_0 \equiv -1 \big(\mathrm{mod}\ 2(1-\beta_s)\big)$, so $d_0 \equiv -1 \pmod 4$. ∎

Given any prime (ideal) factor P_s of $p\Omega_s$, the factorization of $p\Omega_s$ into distinct primes is given by

$$(9) \qquad p\Omega_s = \prod_{\substack{1 \leqslant j < h \\ j \text{ odd}}} \sigma_j(P_s).$$

Let χ_{P_s} denote the standard residue class character of order h defined on Ω_s/P_s, so χ_{P_s} can be viewed as the character (mod p) of order h for which $\chi_{P_s}(n) \equiv n^{(p-1)/h} (\bmod P_s)$ for all $n (\bmod p)$. The following lemma gives the prime factorization of the ideal $\Omega_s K(\chi_{P_s})$.

Lemma 3. *Let P_s be a prime factor of $p\Omega_s$. Then*

$$\Omega_s K(\chi_{P_s}) = \prod_{\substack{1 \leqslant j < h/2 \\ j \text{ odd}}} \sigma_j^{-1}(P_s). \tag{10}$$

Proof. This result is due to Stickelberger [11]; see also Lang's book [6], p. 98.

Lemma 4. *Let P_{s-1}, P_s be prime factors of $p\Omega_{s-1}, p\Omega_s$, respectively, such that $P_{s-1} \subset P_s$. Then $P_{s-1}\Omega_s = P_s \sigma_{h/2+1}(P_s)$.*

Proof. Since $P_{s-1} \subset P_s$, we have

$$P_{s-1} = \sigma_{h/2+1}(P_{s-1}) \subset \sigma_{h/2+1}(P_s).$$

Hence P_s and $\sigma_{h/2+1}(P_s)$ are prime factors of $P_{s-1}\Omega_s$. Moreover, these are the only prime factors, since $|\boldsymbol{Q}(\beta_s) : \boldsymbol{Q}(\beta_{s-1})| = 2$.

Lemma 5. *If all the algebraic conjugates of $\alpha \in \Omega_s$ have absolute value 1, then α is a power of β_s.*

Proof. By [10], Lemma 10.10, α is a root of unity. It follows easily from [5], Corollary, p. 204, that the only roots of unity in Ω_s are powers of β_s.

3. Specification of parameters. For each fixed r, the 2^r-th power reciprocity law is expressed in terms of integers a, b (called "parameters of level 2") and integers $d_j(s)$ (called "parameters of level s") with $3 \leqslant s \leqslant r$, $0 \leqslant j < h/4$. We specify these parameters in this section, beginning with a and b. The formulation is rather complex, so the reader is advised to refer to the concrete examples provided in § 4.

Set

$$\gamma_2 = a + bi, \tag{11a}$$

where (a, b) is a fixed one of the four solutions to $p = a^2 + b^2$, $2|b$. Since $\gamma_2 \bar{\gamma}_2 = p$, it follows from (9) that $\Omega_2\gamma_2$ is some prime factor P_2 of $p\Omega_2$, so by Lemma 3,

$$\Omega_2\gamma_2 = P_2 = \Omega_2 K(\chi_{P_2}). \tag{11b}$$

Thus $\gamma_2 = \mu K(\chi_{P_2})$ where $\mu^4 = 1$. Since a is odd and since $\operatorname{Re} K(\chi_{P_2})$ is odd by Lemma 1, $\mu = \pm 1$. Thus

$$\gamma_2 = \pm K(\chi_{P_2}). \tag{11c}$$

For the rest of this section, unless otherwise stated, assume that $3 \leqslant s \leqslant r$ with r fixed. Write

$$\gamma_s = d_0(s) + \sum_{\substack{1 \leqslant j < h/4 \\ j \text{ even}}} d_j(s)(\beta_s^j + \bar{\beta}_s^j) + i \sum_{\substack{1 \leqslant j < h/4 \\ j \text{ odd}}} d_j(s)(\beta_s^j + \bar{\beta}_s^j). \tag{12}$$

In order to specify the parameters of level $s+1$, we need to define certain integers $(\beta_s^j + \bar{\beta}_s^j)_p (\bmod p)$ for $1 \leqslant j < h/4$, which in turn are defined in terms of the parameters of level $\leqslant s$. We proceed to do this.

Suppose that for each ν with $2 \leqslant \nu \leqslant s$, the parameters of level ν have been specified in such a way that $|\gamma_\nu|^2 = p$ and

$$\{\gamma_2, \gamma_3, \ldots, \gamma_\nu\} \subset P_\nu \tag{13}$$

for prime factors P_ν of $p\Omega_\nu$ satisfying

$$P_2 \subset P_3 \subset \ldots \subset P_s. \tag{14}$$

(This supposition will be justified later by induction.) Suppose moreover that for each number $\beta_{s-1}^j + \bar{\beta}_{s-1}^j$ $(1 \leqslant j < h/8)$, a corresponding integer $(\beta_{s-1}^j + \bar{\beta}_{s-1}^j)_p$ has been defined in terms of the parameters of level $< s$ in such a way that

$$(\beta_{s-1}^j + \bar{\beta}_{s-1}^j) \equiv (\beta_{s-1}^j + \bar{\beta}_{s-1}^j)_p (\bmod P_{s-1}). \tag{15}$$

Then for odd t with $1 \leqslant t < h/4$, inductively define $(\beta_s^t + \bar{\beta}_s^t)_p$ to be the integer (mod p) for which

$$(\beta_s^t + \bar{\beta}_s^t)_p \equiv \big((\beta_s^t + \bar{\beta}_s^t)(\operatorname{Im}\gamma_s)a/b\big)^* / (\operatorname{Re}\gamma_s)^* (\bmod p), \tag{16}$$

where an asterisk attached to an expression indicates that it is to be written in the form

$$Z_0 + \sum_{1 \leqslant j < h/8} Z_j(\beta_{s-1}^j + \bar{\beta}_{s-1}^j)$$

for some integers $Z_j (\bmod p)$ and then each $(\beta_{s-1}^j + \bar{\beta}_{s-1}^j)$ is to be replaced by $(\beta_{s-1}^j + \bar{\beta}_{s-1}^j)_p$. We now show that $(\beta_s^t + \bar{\beta}_s^t)_p$ is a well-defined number satisfying

$$(\beta_s^t + \bar{\beta}_s^t)_p \equiv \beta_s^t + \bar{\beta}_s^t \ (\bmod P_s). \tag{17}$$

By (15),

$$(\operatorname{Re}\gamma_s)^* \equiv (\operatorname{Re}\gamma_s) \ (\bmod P_{s-1}). \tag{18}$$

Since $\gamma_s\bar{\gamma}_s = p$, it follows from (9) and (13) that $\bar{\gamma}_s \notin P_s$. Thus

$$\operatorname{Re}\gamma_s \notin P_s, \tag{19}$$

so by (14), (18), and (19), $(\operatorname{Re}\gamma_s)^* \not\equiv 0 (\bmod p)$. This shows that the left side of (16) is well-defined. Moreover, by (15) and (16),

$$(\operatorname{Re}\gamma_s)(\beta_s^t + \bar{\beta}_s^t)_p \equiv (\beta_s^t + \bar{\beta}_s^t)(\operatorname{Im}\gamma_s)a/b \ (\bmod P_{s-1}). \tag{20}$$

Since by (13) and (14),

$$\gamma_s \equiv \mathrm{Re}\,\gamma_s - (\mathrm{Im}\,\gamma_s)\,a/b \equiv 0 \pmod{P_s},$$

(17) follows from (19) and (20).

We are now ready to specify γ_s (i.e., to specify the parameters of level s) for $3 \leqslant s \leqslant r$. Assume that for each ν with $2 \leqslant \nu < s$, γ_ν has already been specified such that $|\gamma_\nu|^2 = p$ and such that there are prime factors P_ν of $p\Omega_\nu$ satisfying

(21) $$P_2 \subset P_3 \subset \ldots \subset P_{s-1} \quad \text{and} \quad \{\gamma_2, \ldots, \gamma_\nu\} \in P_\nu.$$

This assumption is valid for $s = 3$. We specify a fixed choice of γ_s such that

(22) $$\gamma_s \bar{\gamma}_s = p,$$

and for each odd t with $1 < t < h/4$,

(23) $$\left(\mathrm{Re}\,\gamma_s \mathrm{Re}\,\sigma_t(\gamma_s) + \mathrm{Im}\,\gamma_s \mathrm{Im}\,\sigma_t(\gamma_s)\right)^* \equiv 0 \pmod{p},$$

where the asterisk means the same as in (16). We proceed to show that such choices of γ_s exist and that moreover for any such choice of γ_s, there is a prime factor P_s of $p\Omega_s$ satisfying

(24) $$P_2 \subset P_3 \subset \ldots \subset P_s \quad \text{and} \quad \{\gamma_2, \gamma_3, \ldots, \gamma_s\} \subset P_s.$$

By Lemma 4, there is a prime factor P_s' of $p\Omega_s$ such that

(25) $$P_{s-1}\Omega_s = P_s' \sigma_{h/2+1}(P_s').$$

To show that choices of γ_s exist, we show that if one were to put $\gamma_s = K(\chi_{P_s'})$, then the conditions (22) and (23) would be satisfied. For the moment, put $\gamma_s = K(\chi_{P_s'})$. By (8), $\gamma_s = K(\chi_{P_s'})$ has the form required by (12). By (3), (22) holds. By (10), $\sigma_t(\gamma_s) \equiv 0 \pmod{P_s'}$ for $1 \leqslant t < h/4$, $2 \nmid t$. Thus

$$\mathrm{Re}\,\sigma_t(\gamma_s) \equiv -i\,\mathrm{Im}\,\sigma_t(\gamma_s) \pmod{P_s'}$$

and

$$\mathrm{Re}\,\gamma_s \equiv -i\,\mathrm{Im}\,\gamma_s \pmod{P_s'}.$$

Multiplying, we have

$$\mathrm{Re}\,\gamma_s \mathrm{Re}\,\sigma_t(\gamma_s) + \mathrm{Im}\,\gamma_s \mathrm{Im}\,\sigma_t(\gamma_s) \equiv 0 \pmod{P_s'}.$$

Applying (15), we conclude that (23) holds. This completes the proof that choices of γ_s exist. We now drop the stipulation $\gamma_s = K(\chi_{P_s'})$ and consider any γ_s satisfying (22). Since $\gamma_s \bar{\gamma}_s = p \in P_s'$, exactly one of P_s' and $\bar{P}_s'$ contains γ_s, by (9). As $\sigma_{h/2-1}$ fixes γ_s by (12), exactly one of P_s' and $\sigma_{h/2+1}(P_s')$ contains γ_s. Define P_s to be the one of these which contains γ_s. By (25), $P_{s-1} \subset P_s$, so (24) follows from the assumption (21). We have thus shown by induction that (24) holds for $2 \leqslant s \leqslant r$, in view of (11b).

We next prove that

(26) $$\gamma_s = \pm K(\chi_{P_s}).$$

By (15) and (23),

(27) $$\mathrm{Re}\,\gamma_s \mathrm{Re}\,\sigma_t(\gamma_s) + \mathrm{Im}\,\gamma_s \mathrm{Im}\,\sigma_t(\gamma_s) \equiv 0 \pmod{P_s}$$

for $1 < t < h/4$, $2 \nmid t$. Congruence (27) also holds for $t = 1$, by (22). By (19) and (24),

$$0 \not\equiv \mathrm{Re}\,\gamma_s \equiv -i\,\mathrm{Im}\,\gamma_s \pmod{P_s}.$$

It thus follows from (27) that

$$\sigma_t(\gamma_s) \equiv 0 \pmod{P_s} \quad \text{for} \quad 1 \leqslant t < h/4,\ 2 \nmid t.$$

As $\sigma_{h/2-1}$ fixes γ_s by (12), we have $\sigma_t(\gamma_s) = \sigma_{h/2-t}(\gamma_s)$. Thus

$$\sigma_t(\gamma_s) \equiv 0 \pmod{P_s} \quad \text{for} \quad 1 \leqslant t < h/2,\ 2 \nmid t.$$

By (10), this proves that

$$\Omega_s \gamma_s = \Omega_s K(\chi_{P_s}),$$

so for some $\eta \in \Omega_s$,

(28) $$\gamma_s = \eta K(\chi_{P_s}).$$

By Lemma 5, there is an integer j such that

(29) $$\eta = \beta_s^j.$$

Since $\sigma_{h/2-1}$ fixes γ_s and $K(\chi_{P_s})$, it follows from (28) and (29) that

(30) $$\eta = \sigma_{h/2-1}(\eta) = (-1)^j \bar{\eta}.$$

Thus $\beta_s^{4j} = \eta^4 = 1$, so $2 \mid j$ because $s \geqslant 3$. Therefore (30) implies that $\eta = \pm 1$, and (26) follows from (28).

Since $P_s \cap \Omega_{s-1} = P_{s-1}$, we have $\chi_{P_s}^2 = \chi_{P_{s-1}}$. Hence, by (26) and (11c),

(31) $$K(\chi_{P_r}^{2^{r-s}}) = \pm \gamma_s \quad (2 \leqslant s \leqslant r).$$

We remark that once $\gamma_2, \gamma_3, \ldots, \gamma_{s-1}$ have been fixed, there are exactly four distinct ways of specifying γ_s. For, (22) and (23) hold with $\pm\gamma_s$ or $\pm\bar{\gamma}_s$ in place of γ_s, so there are at least four distinct choices of γ_s. On the other hand, by (26), there are no more than four possible choices of γ_s, because there are only two possible choices of P_s (by definition of P_s).

Observe that if γ_2 is specified as in (11a) with the additional condition that $a \equiv -\left(\frac{2}{p}\right) \pmod 4$, and that if for $3 \leqslant s \leqslant r$, γ_s is specified by (22) and (23) and in addition by the congruence $d_0(s) \equiv -1 \pmod 4$, then by [1], Theorem 3.9, and Lemma 2, we have $\gamma_s = K(\chi_{P_s})$ for $2 \leqslant s \leqslant r$, that is, the plus sign may be taken in (26) and (31).

To summarize, we have given an algorithm (call it A) for successively specifying $\gamma_2, \ldots, \gamma_r$ (of the form given in (11a) and (12)) in such a way that there exists a character $\chi \pmod p$ of order k (namely $\chi = \chi_{P_r}$) for which $\gamma_s = K(\chi^{2^{r-s}})$ for each s $(2 \leqslant s \leqslant r)$. The specification is accomplished by a system of Diophantine equations (those in (22)) and Diophantine congruences (those in (23) together with the congruences $a \equiv -\left(\frac{2}{p}\right) \pmod 4$ and $d_0(s) \equiv -1 \pmod 4$ $(3 \leqslant s \leqslant r)$). Of course two persons can separately apply Algorithm A and end up with different values of γ_r (or equivalently, different characters χ). This situation could occur, for example, if one person starts with a parameter b which is the negative of the other's. The rational reciprocity law (46) will turn out the same for each person's set of parameters because the proofs of (42) and (46) are based on no more specific information about the parameters than that they are specified by Algorithm A. (The restrictions $a \equiv -\left(\frac{2}{p}\right) \pmod 4$ and $d_0(s) \equiv -1 \pmod 4$ are in fact irrelevant for the purposes of this paper. However, they are quite necessary in [3A], where Algorithm A is used to obtain an unambiguous supplementary theorem to the general rational reciprocity law.)

4. Explicit characterization of the parameters of level $\leqslant 5$. We begin by expressing the condition $\gamma_r\bar{\gamma}_r = p$ in a more explicit fashion, for general r. Write $k = 2^r$. Take $s = r$ in (12), formally multiply the right side of (12) by its complex conjugate, and then simplify using the fact that

$$\beta_r^{2j} + \bar{\beta}_r^{2j} = -(\beta_r^{2(k/4-j)} + \bar{\beta}_r^{2(k/4-j)})$$

to obtain

$$p = \gamma_r\bar{\gamma}_r = m_0(r) + \sum_{1 \leqslant t < k/8} m_t(r)(\beta_r^{2t} + \bar{\beta}_r^{2t}), \tag{32}$$

where

$$m_0(r) = d_0^2(r) + 2\sum_{1 \leqslant j < k/4} d_j^2(r) \tag{33}$$

and where the $m_t(r)$ are integral quadratic forms in the $d_j(r)$. Now, $\{\beta_r^{2j}: |j| < k/8\}$ is a linearly independent set over Q, so by (32) and (33),

$$p = d_0^2(r) + 2\sum_{1 \leqslant j < k/4} d_j^2(r) \tag{34a}$$

and

$$m_t(r) = 0 \quad \text{for} \quad 1 \leqslant t < k/8. \tag{34b}$$

We can view (34) as a system of $k/8$ Diophantine equations in integer variables $d_0(r), \ldots, d_{k/4-1}(r)$, namely, the quadratic partition of p given by (34a) together with the "side conditions" in (34b). To say the system (34) has the solution $(d_0(r), \ldots, d_{k/4-1}(r))$ is equivalent to saying $p = \gamma_r\bar{\gamma}_r$.

We proceed to explicitly characterize γ_3, γ_4, and γ_5 (γ_2 was characterized in (11a)). To simplify notation, write c, d for $d_0(3)$, $d_1(3)$; write x, w, v, u for $d_0(4), \ldots, d_3(4)$; and write $e_0, \ldots, e_7$ for $d_0(5), \ldots, d_7(5)$.

The case $r = 3$. For $s = r = 3$, the condition (22) is equivalent to (34a), which states that $p = c^2 + 2d^2$. Thus $\gamma_3 = c + di\sqrt{2}$ where (c, d) is a fixed one of the four solutions to $p = c^2 + 2d^2$.

The case $r = 4$. In order to specify γ_4, we must first define $(\beta_3 + \bar{\beta}_3)_p$. By (16) with $s = 3$,

$$(\beta_3 + \bar{\beta}_3)_p \equiv 2ad/bc \equiv -ac/bd \pmod p. \tag{35}$$

Thus,

$$\begin{aligned}\gamma_4 &= x + v(\beta_4^2 + \bar{\beta}_4^2) + iw(\beta_4 + \bar{\beta}_4) + iu(\beta_4^3 + \bar{\beta}_4^3) \\ &= x + v\sqrt{2} + iw\sqrt{2+\sqrt{2}} + iu\sqrt{2-\sqrt{2}},\end{aligned}$$

where (x, v, u, w) is any fixed one of the four solutions of the system

$$p = x^2 + 2u^2 + 2v^2 + 2w^2, \tag{36a}$$

$$u^2 - 2uw - w^2 - 2xv = 0, \tag{36b}$$

$$bd(x^2 - 2v^2) \equiv ac(u^2 + 2uw - w^2) \pmod p. \tag{36c}$$

Here (36a) and (36b) come from (34a) and (34b), respectively, and (36c) comes from (23) and (35), since

$$\sigma_3(\gamma_4) = x - v\sqrt{2} + iu\sqrt{2+\sqrt{2}} - iw\sqrt{2-\sqrt{2}}.$$

The case $r = 5$. In order to specify γ_5, we must first define $(\beta_4 + \bar{\beta}_4)_p$ and $(\beta_4^3 + \bar{\beta}_4^3)_p$. By (16),

$$(\beta_4 + \bar{\beta}_4)_p \equiv \frac{a(2bdw - ac(w+u))}{b(bdx - acv)} \pmod p$$

and

$$(\beta_4^3 + \bar{\beta}_4^3)_p \equiv \frac{a(2ubd - ac(w-u))}{b(bdx - acv)} \pmod p.$$

Simpler versions of these congruences have been given by E. Lehmer (written communication) as follows. By (10) and (26), $\sigma_3(\gamma_4) \equiv \gamma_4 \equiv 0 \pmod{P_4}$. Using the formulas for γ_4 and $\sigma_3(\gamma_4)$ given in the previous case $r = 4$, we deduce that

$$x - v(\beta_4^2+\bar\beta_4^2) + iu(\beta_4+\bar\beta_4) - iw(\beta_4^3+\bar\beta_4^3) \equiv 0 \pmod{P_4}$$

and

$$x + v(\beta_4^2+\bar\beta_4^2) + iw(\beta_4+\bar\beta_4) + iu(\beta_4^3+\bar\beta_4^3) \equiv 0 \pmod{P_4}.$$

Adding, we have

$$2x \equiv i(w-u)(\beta_4^3+\bar\beta_4^3) - i(w+u)(\beta_4+\bar\beta_4) \pmod{P_4}.$$

Multiplying by $\beta_4+\bar\beta_4$ and by $\beta_4^3+\bar\beta_4^3$, we have respectively

$$\beta_4+\bar\beta_4 \equiv -ix^{-1}\big(u(\beta_4^2+\bar\beta_4^2)+(w+u)\big) \pmod{P_4}$$

and

$$\beta_4^3+\bar\beta_4^3 \equiv -ix^{-1}\big(w(\beta_4^2+\bar\beta_4^2)+(u-w)\big) \pmod{P_4}.$$

Thus, by (17), (24), and (35),

$$(\beta_4+\bar\beta_4)_p \equiv \frac{acu - bd(w+u)}{adx} \pmod p \tag{37}$$

and

$$(\beta_4^3+\bar\beta_4^3)_p \equiv \frac{acw + bd(w-u)}{adx} \pmod p. \tag{38}$$

Thus

$$\gamma_5 = e_0 + \sum_{j=2,4,6} e_j(\beta_5^j+\bar\beta_5^j) + i\sum_{j=1,3,5,7} e_j(\beta_5^j+\bar\beta_5^j), \tag{39}$$

where $(e_0, e_1, \ldots, e_7)$ is any fixed one of the four solutions of the system

$$p = e_0^2 + 2\sum_{i=1}^{7} e_i^2, \tag{40a}$$

$$e_7^2 - e_1^2 = 2\sum_{i=0}^{5} e_i e_{i+2}, \tag{40b}$$

$$e_6^2 - e_2^2 = 2(e_0e_4 + e_1e_5 + e_2e_6 + e_3e_7 + e_1e_3 - e_5e_7), \tag{40c}$$

$$e_5^2 - e_3^2 = 2(e_0e_6 + e_1e_7 + e_2e_4 + e_1e_5 - e_4e_6 - e_3e_7), \tag{40d}$$

$$\delta_{0t} + \sum_{j=1}^{3} \delta_{jt}(\beta_4^j+\bar\beta_4^j)_p \equiv 0 \pmod p \quad \text{for} \quad t = 3, 5, 7, \tag{40e}$$

where (40e) results from expanding in (23); (40a) comes from (34a); and (40b), (40c), (40d) come from (34b). In (40e), the $(\beta_4^j+\bar\beta_4^j)$ are given explicitly by (35), (37), and (38), and the δ_{jt} are computed with the aid of the facts that $\sigma_3(\gamma_5)$, $\sigma_5(\gamma_5)$, and $\sigma_7(\gamma_5)$ are obtained from the right side of (39) by replacing $(e_0, \ldots, e_7)$ by $(e_0, e_5, -e_6, -e_1, -e_4, e_7, e_2, e_3)$, $(e_0, -e_3, e_6, e_7, -e_4, e_1, -e_2, e_5)$, and $(e_0, e_7, -e_2, -e_5, e_4, e_3, -e_6, -e_1)$, respectively. For example,

$$\delta_{03} = e_0^2 + 2(e_1e_5 + e_3e_7 + e_5e_7 - e_1e_3 - e_4^2),$$
$$\delta_{13} = e_7^2 - e_1^2 + 2e_3e_5 + e_0e_2 - e_0e_6 + 2e_4e_6,$$
$$\delta_{23} = e_3^2 + e_5^2 - e_1^2 - e_7^2 + e_2^2 - e_6^2 - 2e_2e_6,$$
$$\delta_{33} = e_5^2 - e_3^2 + 2e_1e_7 + e_0e_2 + e_0e_6 - 2e_2e_4.$$

As a numerical example, note that for $p = 97$, the parameters may by specified by:

$$(a, b) = (-9, -4); \quad (c, d) = (-5, 6); \quad (x, v, w, u) = (7, -2, -4, -2);$$

and

$$(e_0, \ldots, e_7) = (-5, -4, 2, -2, 2, 2, 0, -2).$$

5. The 2^r-th power reciprocity laws. Let $2 \leqslant s \leqslant r$, $k = 2^r$. Let p and q be distinct primes $\equiv 1 \pmod k$. The symbols $a, b, c, d, x, v, u, w, e_j, d_j(s), P_s$, and χ_{P_s} have been defined in terms of p. We denote the corresponding symbols defined in terms of q by $A, B, C, D, X, V, U, W, E_j, D_j(s), Q_s$, and χ_{Q_s}. Let $(\gamma_2)_q \equiv a - bA/B \pmod q$, and for $s \geqslant 3$, let $(\gamma_s)_q$ be the integer $(\operatorname{mod} q)$ obtained from the right side of (12) by replacing i by $-A/B$ and by replacing each $\beta_s^j+\bar\beta_s^j$ by $(\beta_s^j+\bar\beta_s^j)_q$. For example, $(\gamma_3)_q \equiv c - dC/D \pmod q$. By the q-analogue of (17), we have for $2 \leqslant s \leqslant r$,

$$(\gamma_s)_q \equiv \gamma_s \pmod{Q_s}. \tag{41}$$

THEOREM 6. *Let p and q be distinct primes $\equiv 1 \pmod k$, where $k = 2^r \geqslant 4$. Then*

$$\chi_{P_r}(q)\chi_{Q_r}(p) = \bar\chi_{Q_r}\Big(\prod_{s=2}^{r} (\gamma_s)_q^{2^{s-1}}\Big). \tag{42}$$

Proof. By the binomial theorem,

$$G^q(\chi_{P_r}) \equiv \sum_{n \,(\operatorname{mod} p)} \chi_{P_r}^q(n) e^{2\pi i n q/p} = \bar\chi_{P_r}(q) G(\chi_{P_r}) \pmod q,$$

so

$$G^{q-1}(\chi_{P_r}) \equiv \bar\chi_{P_r}(q) \pmod q. \tag{43}$$

Using (5) for $2 \leqslant s \leqslant r$ and also (2), we have

$$G^k(\chi_{P_r}) = p\prod_{s=2}^{r} K(\chi_{P_r}^{2^{r-s}})^{2^{s-1}}. \tag{44}$$

By (43) and (44),

$$\bar{\chi}_{P_r}(q) \equiv p^{(q-1)/k}\left\{\prod_{s=2}^{r} K(\chi_{P_r}^{2^{r-s}})^{2^{s-1}}\right\}^{(q-1)/k} \pmod{q}.$$

Therefore, by (31) and (41),

$$\bar{\chi}_{P_r}(q) \equiv \chi_{Q_r}(p)\,\chi_{Q_r}\left(\prod_{s=2}^{r} (\gamma_s)_q^{2^{s-1}}\right) \pmod{Q_r}. \tag{45}$$

Since both members of (45) are kth roots of unity, the members must in fact be equal, so (42) follows. ■

The rational reciprocity law is given in the following corollary, which is a direct consequence of the preceding theorem.

Corollary 7. *Let p and q be distinct primes $\equiv 1 \pmod{k}$, where $k = 2^r \geqslant 4$. Suppose that* $\left(\frac{p}{q}\right)_{k/2} = \left(\frac{q}{p}\right)_{k/2} = 1$. *Then*

$$\left(\frac{p}{q}\right)_k\left(\frac{q}{p}\right)_k = \left(\frac{\prod_{s=2}^{r} (\gamma_s)_q^{2^{s-2}}}{q}\right)_{k/2}. \tag{46}$$

6. Examples of the rational reciprocity laws for $r \leqslant 4$.

The case $r = 2$. Here (46) clearly becomes

$$\left(\frac{p}{q}\right)_4\left(\frac{q}{p}\right)_4 = \left(\frac{(\gamma_2)_q}{q}\right) = \left(\frac{a-bA/B}{q}\right) = \left(\frac{B}{q}\right)\left(\frac{aB-bA}{q}\right).$$

This can be simplified to yield (1), as follows. Since A is odd by (7),

$$\left(\frac{A}{q}\right) = \left(\frac{q}{|A|}\right) = \left(\frac{A^2+B^2}{|A|}\right) = \left(\frac{B^2}{|A|}\right) = 1,$$

so

$$\left(\frac{B}{q}\right) = \left(\frac{B^2}{q}\right)_4 = \left(\frac{-A^2}{q}\right)_4 = (-1)^{(q-1)/4}\left(\frac{A}{q}\right) = (-1)^{(q-1)/4}.$$

The case $r = 3$. Here (46) becomes

$$\left(\frac{p}{q}\right)_8\left(\frac{q}{p}\right)_8 = \left(\frac{(\gamma_2)_q}{q}\right)_4\left(\frac{(\gamma_3)_q}{q}\right) = \left(\frac{a-bA/B}{q}\right)_4\left(\frac{c-dC/D}{q}\right).$$

This can also be simplified to yield

$$\left(\frac{p}{q}\right)_8\left(\frac{q}{p}\right)_8 = \left(\frac{aB-bA}{q}\right)_4\left(\frac{cD-dC}{q}\right).$$

since $\left(\frac{B}{q}\right)_4 = 1$ (see [12]) and

$$\left(\frac{D}{q}\right) = \left(\frac{q}{|D'|}\right) = \left(\frac{C^2+2D^2}{|D'|}\right) = \left(\frac{C^2}{|D'|}\right) = 1,$$

where D' is the largest odd factor of D.

The case $r = 4$. Here (46) becomes

$$\left(\frac{p}{q}\right)_{16}\left(\frac{q}{p}\right)_{16} = \left(\frac{(\gamma_2)_q(\gamma_3)_q^2}{q}\right)_8\left(\frac{(\gamma_4)_q}{q}\right).$$

Using the q-analogues of (35), (37), and (38), we can rewrite this as

$$\left(\frac{p}{q}\right)_{16}\left(\frac{q}{p}\right)_{16} = \left(\frac{(a-bA/B)(c-dC/D)^2}{q}\right)_8\left(\frac{X(BDL_1-ACL_2)}{q}\right),$$

where

$$L_1 = Xx + Ww + Uu + Uw - uW$$

and

$$L_2 = Uw + uW + vX.$$

References

[1] B. Berndt and R. Evans, *Sums of Gauss, Jacobi, and Jacobsthal*, J. Number Theory 11 (1979), pp. 349–398.

[2] K. Burde, *Ein rationales biquadratisches Reziprozitätsgesetz*, J. Reine Angew. Math. 235 (1969), pp. 175–184.

[3] — *Zur Herleitung von Reziprozitätsgesetzen unter Benutzung von endlichen Körpern*, ibid. 293/294 (1977), pp. 418–427.

[3A] R. J. Evans, *The 2^r-th power character of 2*, ibid. 315 (1980), pp. 174–189.

[4] Y. Furuta, *A reciprocity law of the power residue symbol*, J. Math. Soc. Japan 10 (1958), pp. 46–54.

[4A] H. Hasse, *Der 2^n-te Potenzcharakter von 2 im Körper der 2^n-ten Einheitswurzeln*, Rend. Circ. Mat. di Palermo 7 (1958), pp. 185–244.

[5] S. Lang, *Algebra*, Addison-Wesley, Reading, Mass., 1965.

[6] — *Algebraic number theory*, Addison-Wesley, Reading, Mass., 1970.

[7] E. Lehmer, *On the quadratic character of some quadratic surds*, J. Reine Angew. Math. 250 (1971), pp. 42–48.

[8] — *Rational reciprocity laws*, Amer. Math. Monthly 85 (1978), pp. 467–472.

[9] P. Leonard and K. Williams, *A rational sixteenth power reciprocity law*, Acta Arith. 33 (1977), pp. 365–377.

[10] H. Pollard, *The theory of algebraic numbers*, Carus Monograph, Amer. Math. Soc., 1950.

[11] L. Stickelberger, *Über eine Verallgemeinerung der Kreistheilung*, Math. Annalen 37 (1890), pp. 321–367.
[12] K. Williams, *A rational octic reciprocity law*, Pacific J. Math. 63 (1976), pp. 564–570.
[13] — *Note on Burde's rational biquadratic reciprocity law*, Canad. Math. Bull. 20 (1977), pp. 145–146.
[14] P. Wu, *A rational reciprocity law*, Ph. D. thesis, Univ. S. California, 1975.

Received on 4. 12. 1978 (1121)

ACTA ARITHMETICA
XXXIX (1981)

Corps cubiques de discriminant donné

par

PH. SATGÉ (Caen)

Introduction. Soit $d \neq -3$ un discriminant de corps quadratique imaginaire et $q \neq 2, 3$ un nombre premier. On sait ([2], [3], [4] par exemple) que la congruence $q \equiv \left(\frac{d}{q}\right) \bmod 3$ est une condition nécessaire pour que dq^2 soit un discriminant de corps cubique, et que cette condition est suffisante si 3 ne divise pas le nombre de classes de $Q(\sqrt{d})$. L'exemple $d = -23$ et $q = 5$ montre que cette congruence n'est plus suffisante lorsque 3 divise le nombre de classes de $Q(\sqrt{d})$: en effet, on a $5 \equiv \left(\frac{-23}{5}\right) \bmod 3$ mais $-23 \cdot 5^2 = -575$ n'est pas un discriminant de corps cubique. Depuis le mémoire de Hasse [2], la question suivante est donc posée: soit d un discriminant de corps quadratique imaginaire dont le nombre de classes est divisible par 3; quels sont les nombres premiers q tels que dq^2 est discriminant d'un corps cubique? Nous répondons ici à cette question (théorème du § 4): si δ est le discriminant du corps $Q(\sqrt{-3d})$, il existe un ensemble fini de formes quadratiques binaires de discriminant $3^r\delta$, avec $r = 0, 2$ ou 4, telles que dq^2 est un discriminant de corps cubique si et seulement si l'on a $q \equiv \left(\frac{d}{q}\right) \bmod 3$ et si q est représenté par l'une de ces formes. Dans le cas $d = -23$ par exemple, nous montrons que cet ensemble de formes peut être réduit à la forme $X^2+3XY-153Y^2$; ainsi $-23q^2$ est un discriminant de corps cubique si et seulement si q est congru à $\left(\frac{-23}{q}\right) \bmod 3$ et est de la forme $x^2+3xy-153y^2$ avec x et y entiers rationnels.

Notations. Soit k un corps quadratique imaginaire de discriminant $d \neq -3$ et q un nombre premier différent de 2 et 3. On désigne par J, J_Q les groupes des idèles des corps k et Q (où Q est le corps des rationnels), par W_1 le sous groupe de J formé des idèles dont les composantes en toutes les places finies sont des unités, et par W_q le sous groupe de W_1 formé