A NOTE ON GAUSS' FIRST PROOF OF THE QUADRATIC RECIPROCITY THEOREM

L. CARLITZ

We assume that the reader is familiar with Mathews' exposition [1, pp. 45–50] of the inductive proof of the reciprocity theorem. There are three main cases:

I. \( pRq, \)

II. \( pNq, \quad q \equiv 3 \pmod{4}, \)

III. \( pNq, \quad q \equiv 1 \pmod{4}. \)

In I we have \( e^2 - p = qf, \) in II we have \( e^2 + p = qf. \) In III we have first the lemma which asserts the existence of a prime \( p' < q \) such that \( qNp'. \) This implies \( p'Nq, \) so that \( pp'Rq \) and so \( e^2 - pp' = qf. \) In each of the cases I and II it is necessary to treat two sub-cases; in case III there are four sub-cases. Thus in all there are eight cases to consider.

We should like to point out in this note that it is possible to handle all cases simultaneously by introducing a little notation. To begin with, we define

References


Thus we have the single equation

\[ e^2 - rp = qf, \]

where \( \varepsilon \) is even and \( f < q, f \) is odd and \( |f| < q \).

Next we put

\[
\begin{align*}
   d &= (f, rp), \\
   f &= df', \\
   e &= de', \\
   rp &= dd',
\end{align*}
\]

so that (1) becomes

\[ de'^2 - d' = qf', \]

moreover

\[ (f', dd') = (d, d') = (q, dd') = 1. \]

From (2) we get \( qf' \equiv -d' \pmod{4} \), so that

\[ q + d' + f' \equiv 1 \pmod{4}. \]

Now from (2) we also get

\[
\left( \frac{dd'}{f'} \right) = \left( \frac{qdf'}{d'} \right) = \left( \frac{-qdf'}{d} \right) = 1,
\]

which gives

\[
\left( \frac{q}{dd'} \right) = \left( \frac{-d'}{d} \right) \left( \frac{d}{d'} \right) \left( \frac{f'}{dd'} \right).
\]

We now apply the generalized reciprocity theorem:

\[
\left( \frac{m}{n} \right) \left( \frac{n}{m} \right) = -1^{(m-1)(n-1)/4},
\]

where \( m \) and \( n \) are odd and relatively prime; also one of the numbers may be negative. The special cases \( m \) or \( n = \pm 1 \) are included. Then we get, since \( (dd'/f') = 1 \),

\[ \left( \frac{q}{dd'} \right) = (-1)^{\lambda}, \]

where
\[ \lambda = \frac{1}{4} (d - 1)(-d' - 1) + \frac{1}{4} (f' - 1)(dd' - 1). \]

Using (3) we find that
\[
\lambda = \frac{1}{4} (d - 1)(-d' - 1) - \frac{1}{4} (q + d')(dd' - 1)
\]
\[
= \frac{1}{4} (d - 1)(-d' - 1) - \frac{1}{4} (d' + 1)(d + d' - 2)
\]
\[
- \frac{1}{4} (q - 1)(dd' - 1)
\]
\[
= - \frac{1}{4} (d' + 1)(2d + d' - 3) - \frac{1}{4} (q - 1)(dd' - 1)
\]
\[
= - \frac{1}{4} (d'^2 - 1) - \frac{1}{2} (d' + 1)(d - 1) - \frac{1}{4} (q - 1)(dd' - 1)
\]
\[
= \frac{1}{4} (q - 1)(r \rho - 1) \pmod{2};
\]

where at the last step we used \( r \rho = dd' \). Thus (4) becomes
\[
(5) \quad \left( \frac{q}{r \rho} \right) = (-1)^{(q-1)(r \rho-1)/4}.
\]

In cases I and II (5) is in obvious agreement with the reciprocity theorem; in III there is also agreement since we have \( qNp' \). Thus in III (5) reduces to
\[
\left( \frac{q}{\rho} \right) = -1,
\]

which is the desired relation.

**Reference**


Duke University