Klaus Hoechsmann, Oct. 13, 2008

An Easy Proof of Quadratic Reciprocity.

In the Journal of the Australian Math. Society (1991), G. Rousseau of the University of Leicester (UK) published a particularly simple version of Gauss’s fifth proof of the Law of Quadratic Reciprocity. The present write-up is an attempt to digest it.

The proof consists in computing the product over \( \mathbb{Z}_{pq}^\times/\{\pm1\} \), where \( p \) and \( q \) denote odd primes, in two different ways, by choosing a “natural” system of representatives on either side of the isomorphism

\[
\mathbb{Z}_{pq}^\times \rightarrow \mathbb{Z}_p^\times \times \mathbb{Z}_q^\times, \tag{\*}
\]

which takes the group \( \{\pm1\} \) into the one generated by \((-1, -1)\). Here \( \mathbb{Z}_m \) stands for \( \mathbb{Z}/m\mathbb{Z} \); moreover we shall set \( h(m) = (m-1)/2 \) for any odd \( m \).

On the right of (\*), the elements are pairs, and we choose the \( h(p) \times (q-1) \) rectangular array

\[
\{(i, j) \mid 1 \leq i \leq h(p), 1 \leq j < q\} \tag{1}
\]
as our system of representatives. Multiplying across the \( i \)th row yields \((i^{q-1}, (q-1)!)_1\), and we get

\[
\left( (h(p)!)^{q-1}, ((q-1)!)_1 \right)^{h(p)} = \left( (h(p)!)^{p-1}, (q-1)!_1 \right)^{h(q)}, \left( (q-1)!_1 \right)^{h(p)} \tag{2}
\]

by going across the whole array — using \( \mathbb{Z}_p^\times = \{\pm1, \pm2, \ldots, \pm h(p)\} \) for the expansion in the first component.

On the left of (\*), we choose the first half of the natural numbers \( < pq \), without the multiples of \( p \) and \( q \), explicitly:

\[
\{1, 2, \ldots, h(p)q\} - \{p, 2p, \ldots, h(q)p\} - \{q, 2q, \ldots, h(p)q\}. \tag{3}
\]
The plan is to take the product over this system modulo both \( p \) and \( q \), obtaining an element \((\pi(p), \pi(q)) \in \mathbb{Z}_p^\times \times \mathbb{Z}_q^\times\), which can then be compared with (2). For \( \pi(q) \), we begin with the \( h(p) \times (q-1) \) rectangular array

\[
\{(iq + j) \mid 0 \leq i < h(p), 1 \leq j < q\} \tag{4}
\]
which falls short of \( h(pq) \) by the numbers \( h(p)q + 1, h(p)q + 2, \ldots, h(p)q + h(q) = h(pq) \), but retains the \( p \)-multiples \( p, 2p, \ldots, h(q)p \). We cunningly substitute the former for the latter; i.e., change \( kp \) into \( k + h(p)q \), for \( 1 \leq k \leq h(q) \), and now have an array which is both clean and complete.

Modulo \( q \), each \( kp \) has changed by a factor \( p^{-1} \). Multiplying all this, we thus obtain

\[
\pi(q) = ((q-1)!)_1^{h(p)} p^{-h(q)} \in \mathbb{Z}_q, \tag{5}
\]
the first factor from the \( h(p) \) rows in (4), the second one from these \( h(q) \) changes. Mutatis mutandis we get \( \pi(p) \). Now Euler’s Criterion ties \( p^{-h(q)} \) to the Legendre Symbol \( \left(\frac{p}{q}\right) \), and, comparing \((\pi(p), \pi(q))\) with (2), we finally have

\[
\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{h(p)h(q)} \quad \text{Q.E.D.} \tag{6}
\]