Oswald Baumgart

The Quadratic Reciprocity Law.
A Comparative Presentation of its Proofs

December 4, 2010
DEDICATED TO

DR. PHIL. JOH. EDOUARD BÖTTCHER
TEACHER AT THE REALGYMNASIUM IN LEIPZIG

WITH THANKFULNESS AND ADMIRATION.
Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Translator’s Preface</td>
<td>iii</td>
</tr>
<tr>
<td>The Quadratic Reciprocity Law</td>
<td>v</td>
</tr>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>FIRST PART</td>
<td>3</td>
</tr>
<tr>
<td>1. From Fermat to Legendre</td>
<td>5</td>
</tr>
<tr>
<td>2. Gauss’s Proof by Mathematical Induction</td>
<td>9</td>
</tr>
<tr>
<td>3. Proof by Reduction</td>
<td>15</td>
</tr>
<tr>
<td>4. Eisenstein’s Proof using Complex Analysis</td>
<td>37</td>
</tr>
<tr>
<td>5. Proofs using Results from Cyclotomy</td>
<td>41</td>
</tr>
<tr>
<td>6. Proofs based on the Theory of Quadratic Forms</td>
<td>57</td>
</tr>
<tr>
<td>7. The Supplementary Laws</td>
<td>63</td>
</tr>
<tr>
<td>8. Algorithms for Determining the Quadratic Character</td>
<td>67</td>
</tr>
<tr>
<td>SECOND PART</td>
<td>73</td>
</tr>
<tr>
<td>9. Gauss’s Proof by Induction</td>
<td>75</td>
</tr>
<tr>
<td>10. Proofs by Reduction</td>
<td>79</td>
</tr>
<tr>
<td>11. Eisenstein’s Proofs using Complex Analysis</td>
<td>95</td>
</tr>
<tr>
<td>12. Proofs using Results from Cyclotomy</td>
<td>99</td>
</tr>
<tr>
<td>13. Proofs based on the Theory of Quadratic Forms</td>
<td>111</td>
</tr>
<tr>
<td>Final Comments</td>
<td>113</td>
</tr>
</tbody>
</table>
APPENDIX .................................................. 122

A. Additional Proofs ......................................... 123
   A.1 Proof by Pellet ........................................... 123
   A.2 Proof by Gegenbauer ...................................... 124

Author Index .................................................. 127

Subject Index .................................................. 129
FIRST PART

PRESENTATION OF THE PROOFS OF THE

QUADRATIC RECIPROCITY LAW
5. Proofs using Results from Cyclotomy

1. Proof by Gauss (7th Proof) [33] and Lebesgue (2nd Proof) [51]

1. Let \( \rho \) be a primitive root of the equation \( \frac{x^{p-1}-1}{x-1} = 0 \), where \( p \) is a positive odd prime, and let \( g \) be a primitive root modulo \( p \); then we can order the roots of \( \frac{x^{p-1}-1}{x-1} = 0 \) in the following way:

\[ \rho, \rho^2, \rho^4, \ldots, \rho^{p-3} \quad \text{and} \quad \rho^3, \rho^5, \ldots, \rho^{p-2}. \]

The expressions

\[ y_1 = \rho^2 + \rho^3 + \ldots + \rho^{p-2}, \quad y_2 = \rho + \rho^2 + \ldots + \rho^{p-3} \]

are called quadratic\[3\] periods of the cyclotomic equation \( \frac{x^{p-1}-1}{x-1} = 0 \). Using their property

\[ y_1 - y_2 = (\rho^{-1} - \rho)(\rho^{-3} - \rho^3) \ldots (\rho^{-p+2} - \rho^{p-2}) \]

and the relation

\[ (x - \rho^2)(x - \rho^4) \ldots (x - \rho^{2(p-1)}) = x^{p-1} + x^{p-2} + \ldots + 1 \]

we find

\[ (y_1 - y_2)^2 = (-1)^{\frac{p-1}{2}} p. \]

Now \( y_1 + y_2 = -1 \), hence we get

\[ y_1 y_2 = \frac{1 - (-1)^{\frac{p-1}{2}} \rho}{4}. \]

Thus the two periods \( y_1 \) and \( y_2 \) are roots of the quadratic equation \( f(x) = x^2 + x + \frac{1}{4}(1 - (-1)^{\frac{p-1}{2}} \rho) = 0. \)

\[3\] [FL] Baumgart uses the expression \( \frac{p-1}{2} \)-termed periods.
2. Gauss and Lebesgue now study under which conditions the congruence
\[ f(x) \equiv 0 \mod q, \tag{5.1} \]
where \( q \) as well as \( p \) is an odd positive prime, has real integral roots. This condition can be expressed in two different ways, and a comparison will then yield the quadratic reciprocity law.

The congruence \((5.1)\) turns, after substituting
\[ y = 2x + 1, \tag{5.2} \]
into the congruence
\[ y^2 \equiv (-1)^{\frac{p-1}{2}} p \mod q. \tag{5.3} \]
Thus if the congruence \((5.1)\) has real roots, then so does \((5.3)\); conversely, if \((5.3)\) is solvable, then the substitution \((5.2)\) shows that this is also true for \((5.1)\). This shows that the congruence \((5.1)\) is solvable if
\[ \left( \frac{-1}{q} \right)^{\frac{p-1}{2}} = +1, \]
or if
\[ (-1)^{\frac{p-1}{2}} p^{\frac{q-1}{2}} \equiv 1 \mod q. \tag{5.4} \]
On the other hand, \( f(x) \equiv 0 \mod q \) does not have real integral roots if
\[ (-1)^{\frac{p-1}{2}} q^{\frac{q-1}{2}} \equiv -1 \mod q. \tag{5.5} \]
Moreover, the identity
\[ x^{q-1} - 1 \equiv (x - 1)(x - 2) \cdots (x - q + 1) \mod q \]
\[ x^q - x \equiv x(x - 1)(x - 2) \cdots (x - q + 1) \mod q \]
can be transformed into
\[ (y - y_h)^q - (y - y_h) = (y - y_h)(y - 1 - y_h)(y - 2 - y_h) \cdots (y - q + 1 - y_h) \mod q \tag{5.6} \]
by the substitution \( x = y - y_h \) \((h = 1, 2)\). Now \( y_h = x^{g_h} + x^{g_{h+1}} + \cdots + x^{g_{p-1+h}}, \) so if we write
\[ q \equiv g^h \mod p \tag{5.7} \]
we find \( y_h^q \equiv y_{h+k} \mod q \) or \((y - y_h)^q \equiv y - y_{h+k} \mod q\) or finally \((y - y_h)^q - (y - y_h) \equiv y_h - y_{h+k} \mod q\). Thus congruence \((5.6)\) implies
\[ (y - y_h)(y - 1 - y_h)(y - 2 - y_h) \cdots (y - q + 1 - y_h) \equiv y_h - y_{h+k} \mod q, \]
which in turn immediately implies the following formula:
(y - y_1)(y - y_2)(y - 1 - y_1)(y - 1 - y_2) \cdots (y - q + 1 - y_1)(y - q + 1 - y_2) \\
\equiv (y_1 - y_{1+k})(y_2 - y_{2+k}) \mod q

Since \( f(y) = (y - y_1)(y - y_2) \), the last congruence can be written in the form

\[ f(y) \cdot f(y - 1) \cdots f(y - q + 1) \equiv (y_1 - y_{1+k})(y_2 - y_{2+k}) \mod q. \quad (5.8) \]

If \( f(y) \equiv 0 \mod q \) only had real integral roots, then

\[ f(y), \ldots, f(y - q + 1) \mod q \]

would represent a complete residue system modulo \( q \), and we would get

\[ f(y) \cdot f(y - 1) \cdots f(y - q + 1) \equiv 0 \mod q. \]

Conversely, if this condition is satisfied, then the congruence \( f(y) \equiv 0 \mod q \)
and hence \( f(x) \equiv 0 \mod q \) would be solvable in real integers. Taking the
congruence \((5.8)\) into account we can say: \( f(x) \) has \( q \) real roots modulo \( q \)
if \( \phi = (y_1 - y_{1+k})(y_2 - y_{2+k}) \equiv 0 \mod q \), and is not solvable modulo \( q \) if
\( \phi = (y_1 - y_{1+k})(y_2 - y_{2+k}) \not\equiv 0 \mod q \). It is clear that this depends on
the value of \( k \), which was defined by \( q \equiv g^k \mod p \). Thus if \( k \equiv 0 \mod 2 \),
i.e., \( (\frac{q}{p}) = +1 \), then \( y_k = y_{h+k} \); if \( k \equiv 1 \mod 2 \), on the other hand, then
\( y_{h+1} = y_{h+k} \). This shows: \( f(x) \equiv 0 \mod q \) has real integral roots if \( (\frac{q}{p}) = +1 \),
and does not have real integral roots if \( (\frac{q}{p}) = -1 \). Comparing this result with
the one expressed by our formulas \((5.4)\) and \((5.5)\) the quadratic reciprocity
law follows.

2. Gauss’ Fourth Proof [26]

1. Let \( p \) and \( q \) denote as usual two distinct odd primes, let \( \rho = e^{2\pi i/q} \), and
let \( a \) and \( b \) denote the quadratic residues and nonresidues modulo \( q \); then

\[
\begin{align*}
\sum_{\lambda=1}^{q-1} \rho^{\lambda^2} &= G\left(\frac{p}{q}\right) = 1 + 2 \sum_{a} \rho^{a^2}, \\
\sum_{a} \rho^{a^2} + \sum_{b} \rho^{b^2} &= \rho^p + \rho^{2p} + \ldots = -1,
\end{align*}
\]

hence\(^2\)

\[ G\left(\frac{p}{q}\right) = \sum_{\lambda} \left(\frac{\lambda}{q}\right) \rho^{\lambda^2} = \left(\frac{p}{q}\right) \sum_{\lambda} \left(\frac{\lambda}{q}\right) \rho^{\lambda^2} = \left(\frac{p}{q}\right) \sum_{\lambda} \left(\frac{\lambda}{q}\right) \rho^{\lambda}. \]

The last equation can also be written in the following form:

\[
G\left(\frac{p_i}{q}\right) = \left(\frac{p}{q}\right) G\left(\frac{i}{q}\right) = (1 + \rho + \rho^4 + \ldots + \rho^{(q-1)^2}) \left(\frac{p}{q}\right). \quad (5.10)
\]

\(^2\) [FL] The sums \( G \) are nowadays called Gauss sums.
2. **Gauss** first determined the value of $G\left(\frac{i}{q}\right)$. Using the system of equations

\[
\begin{align*}
\frac{1 - \rho^{q^{-1}}}{1 - \rho} &= \frac{1 - \rho^{-1}}{1 - \rho^2} = -\rho^{-1}, \\
\frac{1 - \rho^{q^{-2}}}{1 - \rho^2} &= \frac{1 - \rho^{-2}}{1 - \rho^4} = -\rho^{-2}, \\
&\ldots \\
\frac{1 - \rho^{q-(q-1)}}{1 - \rho^{q^{-1}}} &= \frac{1 - \rho^{-q+1}}{1 - \rho^{q^{-1}}} = -\rho^{-q+1}
\end{align*}
\]

he forms the series

\[
\begin{cases}
 f(\rho, q - 1) = 1 - \frac{1 - \rho^{q-1}}{1 - \rho} + \frac{(1 - \rho^{q-1})(1 - \rho^{q-2})}{(1 - \rho)(1 - \rho^2)} + \ldots \\
&\ldots - \frac{(1 - \rho^{q-1})(1 - \rho^{q-2})\ldots(1 - \rho)}{(1 - \rho)(1 - \rho^2)\ldots(1 - \rho^{q-1})}
\end{cases}
\]

(5.11)

If we introduce the abbreviation

\[
(q - 1, \mu) = \frac{(1 - \rho^{q-1})(1 - \rho^{q-2})\ldots(1 - \rho^{q-\mu})}{(1 - \rho)(1 - \rho^2)\ldots(1 - \rho^{\mu+1})},
\]

where $q$ is a positive integer $> \mu + 1$, and if we observe that

\[
\frac{1 - \rho^m}{1 - \rho^{\mu+1}} = \frac{1 - \rho^{m-\mu-1}}{1 - \rho^{\mu+1}} + \frac{\rho^{m-\mu-1}(1 - \rho^{\mu+1})}{1 - \rho^{\mu+1}},
\]

then we get

\[
(q - 1, \mu + 1) = \rho^{m-\mu-2}(q - 2, \mu) + (q - 2, \mu + 1).
\]

Applying this equation to (5.11) we find

\[
\begin{align*}
f(\rho, q - 1) &= (1 - \rho^{q-2}) - (1 - \rho^{q-3})(q - 2, 1) \\
&\quad + (1 - \rho^{q-4})(q - 2, 2) - (1 - \rho^{q-5})(q - 2, 3) + \ldots
\end{align*}
\]

(5.12)

Now

\[
(1 - \rho^{q-1-(\lambda+1)})(q - 2, \lambda) = (1 - \rho^{q-2})(q - 3, \lambda),
\]

hence

\[
f(\rho, q - 1) = (1 - \rho^{q-2})\{1 - (q - 3, 1) + (q - 3, 2) + \ldots\}
\]

or

\[
f(\rho, q - 1) = (1 - \rho^{q-2})f(\rho, q - 3).
\]

(5.13)

Since $q \equiv 1 \mod 2$ we find

\[
^3 \text{The following developments are valid for arbitrary odd integers.}
\]
\[ f(\rho, q - 1) = (1 - \rho^{q-2})f(\rho, q - 3), \]
\[ f(\rho, q - 3) = (1 - \rho^{q-4})f(\rho, q - 5), \]
\[ \ldots \]
\[ f(\rho, 2) = (1 - \rho), \]

and multiplying these equations yields
\[ f(\rho, q - 1) = (1 - \rho)(1 - \rho^3)(1 - \rho^5) \cdots (1 - \rho^{q-2}). \] (5.14)

Thus we have two developments for \( f(\rho, q - 1) \). Combining these two results shows that
\[ 1 + \rho^{-1} + \rho^{-3} + \ldots + \rho^{-q(q-1)/2} = (1 - \rho)(1 - \rho^3) \cdots (1 - \rho^{q-2}). \]

Taking into account that \( (\rho^{q-2})^\nu = \rho^{-2\nu} \) for integral \( \nu \) we find
\[ 1 + \rho^{-2} + \rho^{-6} + \ldots + \rho^{q(q-1)} = (1 - \rho^{-2})(1 - \rho^{-6}) \cdots (1 - \rho^{-2(q-2)}). \]

Multiplying both sides by \( \rho^{(\frac{q-1}{2})^2} = \rho \cdot \rho^3 \cdot \rho^{q-2} \) gives
\[ \rho^{(\frac{q-1}{2})^2} + \rho^2 + (\frac{q-1}{2})^2 + \ldots + \rho^{q(q-1) + (\frac{q-1}{2})^2} = (\rho - \rho^{-1})(\rho^3 - \rho^{-3}) \cdots (\rho^{q-2} - \rho^{-(q-2)}). \]

Thus we have found
\[ G\left(\frac{i}{q}\right) = (\rho - \rho^{-1})(\rho^3 - \rho^{-3}) \cdots (\rho^{q-2} - \rho^{-q+2}), \] (5.15)

or, using the fact that \( \rho^{\mu} - \rho^{-\mu} = -(\rho^{\mu} - \rho^{-q+\mu}) \):
\[ G\left(\frac{i}{q}\right) = (-1)^{\frac{q-1}{2}}(\rho^2 - \rho^{-2})(\rho^4 - \rho^{-4}) \cdots (\rho^{q-1} - \rho^{-q+1}). \] (5.16)

Multiplying (5.15) and (5.16) we get
\[ G^2\left(\frac{i}{q}\right) = (-1)^{\frac{q-1}{2}}\rho^\frac{q-1}{2}(1 - \rho^{-2})(1 - \rho^{-4}) \cdots (1 - \rho^{-2(q-1)}), \]

or, since \( \rho \) is a primitive root of \( x^q - 1 \),
\[ G^2\left(\frac{i}{q}\right) = (-1)^{\frac{q-1}{2}} \sqrt{q}. \]

This implies
\[ G\left(\frac{i}{q}\right) = \pm i^{(\frac{q-1}{2})^2} \sqrt{q} \quad \text{and} \quad G\left(\frac{p}{q}\right) = \pm i^{(\frac{q-1}{2})^2} \left(\frac{p}{q}\right) \sqrt{q}. \] (5.17)
In order to find the sign of $G$ we return to (5.15). Since $\rho^\mu - \rho^{-\mu} = 2i \sin \frac{2\pi \mu}{q}$, we find

$$G\left(\frac{i}{q}\right) = (2i)^{\frac{q-1}{2}} \sin \frac{2\pi}{q} \cdot \sin \frac{6\pi}{q} \cdot \sin \frac{10\pi}{q} \cdots \sin \frac{(q-2)2\pi}{q}.$$  

The values $\frac{2\pi}{q}, \ldots, \frac{(q-2)2\pi}{q}$ are all smaller than $2\pi$; now recall that $q$ is odd and distinguish the following two cases:

1. $q = 4n + 1$. Then $\frac{q-1}{4}$ of the angles are greater than $\pi$, hence

$$G\left(\frac{i}{q}\right) = i \left(\frac{q-1}{2}\right)^{\frac{q-1}{2}} C = C,$$

where $C$ denotes a positive constant.

2. $q = 4n + 3$. In this case the number of angles greater than $\pi$ is $\frac{q-3}{4}$, and we find

$$G\left(\frac{i}{q}\right) = i \left(\frac{q-1}{2}\right)^{\frac{q-3}{2}} C = iC.$$

Combining these two cases finally shows

$$G\left(\frac{i}{q}\right) = i \left(\frac{q-1}{2}\right)^{\frac{q-1}{2}} \sqrt{q} \quad \text{and} \quad G\left(\frac{pi}{q}\right) = i \left(\frac{q-1}{2}\right)^{\frac{q-1}{2}} \sqrt{p} \sqrt{q}. \quad (5.18)$$

3. Since we also assumed that $p$ be odd we now find

$$G\left(\frac{pi}{q}\right) G\left(\frac{qi}{p}\right) = \left(\frac{p}{q}\right) \left(\frac{q}{p}\right) i \left(\frac{q-1}{2}\right)^{\frac{q-1}{2}} \sqrt{p} \sqrt{q}. \quad (5.19)$$

Now we have, according to the definition of Gauss sums,

$$G\left(\frac{pi}{q}\right) G\left(\frac{qi}{p}\right) = \sum_{\lambda=1}^{q-1} \sum_{\mu=1}^{p-1} e^{\left(\frac{\lambda^2 p}{q} + \frac{\mu^2 q}{p}\right)2\pi i} = \sum_{\lambda} \sum_{\mu} e^{\frac{(\lambda p + \mu q)^2}{pq} 2\pi i}$$

since

$$\frac{\lambda^2 p}{q} + \frac{\mu^2 q}{p} = \frac{(\lambda p + \mu q)^2}{pq} - 2\lambda \mu.$$ 

It is clear that $\lambda p + \mu q$ attains $pq$ different values modulo $pq$ and forms, as can be seen from $p(\lambda - \lambda') = q(\mu - \mu')$, a complete set of residues modulo $pq$. Thus we get

$$G\left(\frac{pi}{q}\right) G\left(\frac{qi}{p}\right) = G\left(\frac{i}{pq}\right) = i \left(\frac{q-1}{2}\right)^{\frac{q-1}{2}} \sqrt{pq},$$

and observing (5.19) now yields

$$i \left(\frac{q-1}{2}\right)^{\frac{q-1}{2}} \sqrt{pq} = \left(\frac{p}{q}\right) \left(\frac{q}{p}\right) i \left(\frac{q-1}{2}\right)^{\frac{q-1}{2}} \sqrt{p} \sqrt{q}.$$

Since the square roots are taken to be positive, this shows that

$$i \left(\frac{q-1}{2}\right)^{\frac{q-1}{2}} = \left(\frac{p}{q}\right) \left(\frac{q}{p}\right) i \left(\frac{q-1}{2}\right)^{\frac{q-1}{2}} \left(\frac{q-1}{2}\right)^{\frac{q-1}{2}}, \quad (5.20)$$

which immediately implies the quadratic reciprocity law.
3. Gauss’ Sixth Proof [28]

1. Assume that \( p \) and \( q \) have their usual meaning and let \( G \) denote the series

\[
G = x - x^9 + x^{9^2} \mp \ldots - x^{9^{p-2}},
\]

(5.21)

where \( q \) is a primitive root modulo \( p \). Then it follows from properties of binomial coefficients that \( G^q - (x - x^9 + x^{9^2} \mp \ldots - x^{9^{p-2}})^q \equiv 0 \mod q \), or, since \( q \) is odd, that

\[
G^q - G_q \equiv 0 \mod q, \quad \text{where} \quad G_q = x^q - x^{q^9} + x^{q^{9^2}} \mp \ldots - x^{q^{9^{p-2}}}. \quad (5.22)
\]

If moreover \( q \equiv g^\mu \mod p \), then the system of equations

\[
q = g^\mu + f_1 p, \quad qg = g^{\mu+1} + f_2 p, \quad \ldots, \quad qg^{p-2} = g^{\mu+p-2} + f_3 p
\]

implies

\[
x^{g^\lambda} - x^{g^{\mu+\lambda}} = (1 - x^p)f(x),
\]

(5.23)

where \( f(x) \) is a polynomial in \( x \). Thus we find

\[
G_q - \left\{x^{g^\mu} - x^{g^{\mu+1}} \pm \ldots \pm x^{g^{\mu+p-2}}\right\} = (1 - x^p)W,
\]

(5.24)

where \( W \) is also a polynomial in \( x \). The exponents of the \( p-1 \) terms inside the brackets are just the integers \( 1, 2, \ldots, p-1 \) since \( g \) is a primitive root modulo \( p \). Since the signs alternate, we see that \( x^{\mu} - x^{\mu+1} \pm \ldots = \pm G \). The sign of \( G \) is that of \( -(-1)^{p-\mu} \), and since \( p \) is odd we conclude that \( \pm G = (-1)^\mu G \). From \( q \equiv g^\mu \mod p \) we then find \( q^{\frac{p-1}{2}} \equiv (g^{\frac{p-1}{2}})^\mu \equiv (\frac{q}{p}) \mod p \), and since \( g^{\frac{p-1}{2}} \equiv -1 \mod p \), this implies

\[
(-1)^\mu = \left(\frac{q}{p}\right)
\]

and

\[
G_q - \left(\frac{q}{p}\right)G = (1 - x^p)W.
\]

(5.25)

2. Now consider the system of identities

\[
+ xG - x^2 + x^{g+1} - x^{g^2+1} + \ldots + x^{9^{2}p-2} = 0,
\]

\[
-x^gG - x^2 + x^{g^2+g} + x^{g^3+g} + \ldots + x^{9^{p-1}+g} = x^{g+1}(x^{9^{p-2}} - 1),
\]

\[
-x^{g+1}G - x^{2}g + x^{g-1+g} + x^{g^{p-1}+g} + \ldots + x^{9^{p-2}+g^{p-2}} = x^{g^{p-1}+1}(x^{9^{p-1}} - 1) - (x^{9^{p-1}} - 1) - \ldots
\]

Adding these equations gives

\[
\Omega = G^2 - f(\lambda^{g+1}) + f(\lambda^{g+2}) \mp \ldots + f(\lambda^{g+p-2}),
\]

(5.26)
where $\Omega$ denotes the sum of the expressions on the right hand side of the above system of equations and where we have set $f(x^\lambda) = 1 + x^{\lambda} + x^{\lambda g} + \ldots + x^{\lambda g^{p-2}}$.

It is easily seen that $\Omega$ is divisible by $1 - x^p$, hence by $\frac{1-x^p}{1-x}$; on the other hand $f(x^\lambda)$ is, because $g$ is a primitive root modulo $p$, divisible by $1 - x^{\lambda p}$, hence by $\frac{1-x^p}{1-x}$. Thus $f(x^\lambda)$ will be divisible by $\frac{1-x^p}{1-x}$ if

$$\frac{1-x^{\lambda p}}{1-x} \equiv 0 \mod \frac{1-x^p}{1-x}.$$ 

For a proof we have to distinguish two cases.

I. $\lambda$ and $p$ are coprime. Then $y\lambda = hp + 1$ for integers $y$ and $h$, hence

$$\frac{1-x^{\lambda p}}{1-x} = \frac{1-x^{\lambda p}}{1-x} \cdot \frac{1-x^{y\lambda}}{1-x} = \frac{1-x^{\lambda p}}{1-x} \cdot \frac{1-x^{hp}}{1-x},$$

and this implies that $f(x^\lambda)$ is divisible by $\frac{1-x^p}{1-x}$.

II. $\lambda$ and $p$ are not coprime. Then

$$f(x^\lambda) - p = x^\lambda \{ (x^g - 1) + (x^{g^2} - 1) + \ldots + (x^{g^{p-2}} - 1) \},$$

and this immediately implies that $f(x^\lambda) - p$ is divisible by $\frac{1-x^p}{1-x}$.

Collecting everything and recalling that $g^0+1, g+1, \ldots, g^{p-2}+1$ represent the numbers 2, 3, \ldots, $p$ in some order, we can deduce from (5.26)

$$\Omega = G^{q} - (-1)^{\frac{q-1}{2}} f\left( x^{\frac{q-1}{2}} + 1 \right) \equiv 0 \mod \frac{1-x^p}{1-x} \quad (5.27)$$

or, if $Z$ denotes a polynomial in $x$,

$$G^{q} - (-1)^{\frac{q-1}{2}} p = \frac{1-x^p}{1-x} Z. \quad (5.28)$$

From (5.28) we immediately deduce

$$G^{q-1} - (-1)^{\frac{q-1}{2}} p^\frac{q-1}{2} = \frac{1-x^p}{1-x} Y. \quad (5.29)$$

3. Using equations (5.23), (5.24), (5.28) and (5.29), the reciprocity law can be proved easily. First we observe that (5.23) and (5.24) imply

$$qGX = G^{q+1} - G\left\{ (1-x^p)W + \left( \frac{q}{p} \right) G \right\},$$

where $X$ denotes a polynomial in $x$ defined by (5.22) as

$$G^{q} - G_q = qX.$$
Moreover, from (5.29) we get
\[ qGX = \left\{ (-1)^{\frac{p-1}{2}} X^{\frac{q-1}{2}} + \frac{1 - x^p}{1 - x} \right\} G^2 - G(1 - x^p)W - \frac{q}{p} G^2, \]
or, using (5.28),
\[ qGX = (-1)^{\frac{p-1}{2}} p \left\{ (-1)^{\frac{p-1}{2}} X^{\frac{q-1}{2}} - \frac{q}{p} \right\} \]
\[ + \frac{1 - x^p}{1 - x} \left\{ Z \left[ (-1)^{\frac{p-1}{2}} q \frac{q-1}{2} - \frac{q}{p} \right] + Y G^2 - W G(1 - x) \right\}. \]

According to (5.21), \( G \) has degree \( p - 1 \). If we put \( GX = \frac{1 - x^p}{1 - x} U + T \), where \( U \) and \( T \) are polynomials in \( x \), then \( T \) will be a polynomial of degree less than \( p - 1 \). Plugging the last equation into (5.30) we get
\[ qT - (-1)^{\frac{p-1}{2}} p \left\{ (-1)^{\frac{p-1}{2}} X^{\frac{q-1}{2}} - \frac{q}{p} \right\} \]
\[ = \frac{1 - x^p}{1 - x} \left\{ Z \left[ (-1)^{\frac{p-1}{2}} q \frac{q-1}{2} - \frac{q}{p} \right] \right\} \]
\[ + Y G^2 - W G(1 - x) - qU \}, \]
where the degree of the left hand side is less than \( p - 1 \). Now \( Z, Y, W \) are polynomials in \( x \), hence the degree of the right hand side is bigger than \( p - 1 \). Thus the equation above can hold only if both sides vanish. Thus we find
\[ qT = (-1)^{\frac{p-1}{2}} p \left\{ (-1)^{\frac{p-1}{2}} X^{\frac{q-1}{2}} - \frac{q}{p} \right\} \]
or
\[ (-1)^{\frac{p-1}{2}} X^{\frac{q-1}{2}} - \frac{q}{p} \equiv 0 \mod q, \]
and this is what we wanted to prove.

4. Proof by Cauchy [8], Jacobi [55, p. 391], Eisenstein [15]

Gauss has shown that
\[ G\left( \frac{q}{p} \right) = \left( \frac{q}{p} \right) G\left( \frac{i}{p} \right) \quad \text{and} \quad G^2\left( \frac{i}{p} \right) = (-1)^{\frac{p-1}{2}} p. \]

This implies without problems that
\[ G^{q+1}\left( \frac{i}{p} \right) - G\left( \frac{q}{p} \right) G\left( \frac{q}{p} \right) = (-1)^{\frac{p-1}{2} \frac{q+1}{2}} p^{\frac{q+1}{2}} - \left( \frac{q}{p} \right) G^2\left( \frac{i}{p} \right) \]
or
5. Proofs using Results from Cyclotomy

\[ G\left(\frac{j}{p}\right)[G\left(\frac{4j}{p}\right) + G\left(\frac{q}{p}\right)] = (-1)^{\frac{p-1}{2}} p \left\{-1\right\}^{\frac{q-1}{2}} p^{\frac{q-1}{2}} - \left(\frac{q}{p}\right) \}. \]  \hspace{1cm} (5.33)

Now

\[ G\left(\frac{j}{p}\right) = \sum_{\lambda=1}^{p-1} \left(\frac{j}{p}\right) \rho^\lambda, \quad G\left(\frac{q}{p}\right) = \sum_{\lambda=1}^{q-1} \left(\frac{q}{p}\right) \rho^\lambda, \]

where \( \rho \) denotes a primitive root of \( x^p = 1 \). Thus we have

\[ G\left(\frac{4j}{p}\right) = G\left(\frac{q}{p}\right) + q(A' + B' \rho + C' \rho^2 + \ldots), \]

where \( A', B', \ldots \) are integers. Now we set

\[ X = \left[(-1)^{\frac{p-1}{2}} \frac{q-1}{2} p^{\frac{q-1}{2}} \left(\frac{q}{p}\right)\right] (-1)^{\frac{q-1}{2}} p \] \hspace{1cm} (5.34)

and get

\[ X = G\left(\frac{j}{p}\right) \cdot q[A' + B' \rho + \ldots] \lor = q[A + B \rho + \ldots], \]

where \( A, B, \ldots \) are again integers. Plugging in \( \rho^2, \ldots, \rho^{p-1} \) for \( \rho \) and adding the resulting equations gives

\[ (p - 1)X = q[(p - 1)A - B - C - \ldots]. \] \hspace{1cm} (5.35)

Since \( q \) is a prime and we can assume without loss of generality that \( p - 1 < q \), \( (5.34) \) and \( (5.35) \) now imply

\[ (-1)^{\frac{p-1}{2}} \frac{q-1}{2} p^{\frac{q-1}{2}} - \left(\frac{q}{p}\right) \equiv 0 \mod q. \]

This is our well known formula.

5. Second Proof by Eisenstein [14]

1. Let \( p \) be an odd prime and let \( r \) run through a complete system of residues modulo \( p \); then \( \sum_{r} \left(\frac{r}{p}\right) = 0 \), and similarly

\[ \psi(\mu) = \left\{ \sum_{r} \left(\frac{r}{p}\right) \right\}^{\mu} = 0. \] \hspace{1cm} (5.36)

Multiplying out immediately gives

\[ \psi(\mu) = \sum_{\alpha_1, \ldots, \alpha_\mu} \left(\frac{\alpha_1}{p}\right) \cdots \left(\frac{\alpha_\mu}{p}\right), \] \hspace{1cm} (5.37)
where the summation for each $\alpha_i$ is from 1 to $p - 1$. Introducing the sum

\[ \psi(\mu, k) = \sum_{\alpha_i \equiv k \mod p} \left( \frac{\alpha_1}{p} \right) \cdots \left( \frac{\alpha_\mu}{p} \right). \]

we find

\[ \psi(\mu) = \psi(\mu, 0) + \psi(\mu, 1) + \ldots + \psi(\mu, p - 1) = 0. \] (5.38)

Setting $\alpha_1 \equiv \beta_1$, $\alpha_2 \equiv k\beta_2$, $\ldots$, $\alpha_\mu \equiv k\beta_\mu \mod p$, then $\sum \alpha_i = k \sum \beta_i$, $\sum \beta_i = 1$, and therefore

\[ \psi(\mu, k) = \left( \frac{k}{p} \right)^\mu \psi(\mu, 1). \] (5.39)

Now if $\mu$ is even, then $\psi(\mu, k) = \psi(\mu, 1)$, or

\[ \psi(\mu, 1) = \psi(\mu, 2) = \ldots = \psi(\mu, p - 1), \] (5.40)

hence using (5.38)

\[ \psi(\mu, 0) + (p - 1)\psi(\mu, 1) = 0. \] (5.41)

If $\mu$ is odd, on the other hand, then $\psi(\mu, k) = \left( \frac{k}{p} \right)\psi(\mu, 1)$, which implies that

\[ \psi(\mu, 1) + \ldots + \psi(\mu, p - 1) = \psi(\mu, 1) \sum \left( \frac{\mu}{p} \right) = 0, \]

hence

\[ \psi(\mu, 0) = 0. \] (5.42)

The defining equation $\psi(\mu, \nu) = \sum \left( \frac{\alpha_1}{p} \right) \cdots \left( \frac{\alpha_\nu}{p} \right)$, where the summation is over all $\alpha_i$ with $\sum \alpha_i \equiv \nu \mod p$, can also be written in the form

\[ \psi(\mu, \nu) = \sum \left\{ \left( \frac{\alpha_\mu}{p} \right) \sum \left( \frac{\alpha_1}{p} \right) \cdots \left( \frac{\alpha_{\mu - 1}}{p} \right) \right\}, \]

from which we see that

\[ \psi(\mu, \nu) = \sum \left\{ \left( \frac{\alpha_\mu}{p} \right) \psi(\mu - 1, \nu - \alpha_\mu) \right\}; \]

in the special case $\nu = 0$ this shows that

\[ \psi(\mu, 0) = \sum \left( \frac{\alpha_\mu}{p} \right) \psi(\mu - 1, -\alpha_\mu), \]

or, using (5.39):

\[ \psi(\mu - 1, -\alpha_\mu) = \left( \frac{-\alpha_\mu}{p} \right)^{\mu - 1} \psi(\mu - 1, 1). \]

\[4\] [FL] Such sums are nowadays called “multiple Jacobi sums”.
This implies
\[ \psi(\mu, 0) = \sum \left( \frac{-\alpha_\mu}{p} \right)^\mu \left( \frac{-1}{p} \right)^\psi(\mu - 1, 1). \]

For even \( \mu \) this shows that
\[ \psi(\mu, 0) = \left( \frac{-1}{p} \right) \psi(\mu - 1, 1) \cdot (p - 1), \]
or, using (5.41):
\[ \psi(\mu, k) = -\left( \frac{-1}{p} \right) \psi(\mu - 1, 1), \quad \mu \equiv 0 \mod 2. \tag{5.43} \]

For odd \( \mu \) the recursion formula gives us
\[
\psi(\mu, k) = \sum \left( \frac{\alpha_\mu}{p} \right) \psi(\mu - 1, k - \alpha_\mu)
= \left( \frac{k}{p} \right) \psi(\mu - 1, 0) + \sum \left( \frac{\alpha_\mu}{p} \right) \psi(\mu - 1, k - \alpha_\mu).
\]

Now formula (5.40) implies
\[
\psi(\mu, k) = \left( \frac{k}{p} \right) \psi(\mu - 1, 0) + \psi(\mu - 1, 1) \sum \left( \frac{\alpha_\mu}{p} \right)
= \left( \frac{k}{p} \right) \{ \psi(\mu - 1, 0) - \psi(\mu - 1, 1) \},
\]
or, using (5.41):
\[ \psi(\mu, k) = -\left( \frac{-1}{p} \right) p \psi(\mu - 1, 1), \quad \mu \equiv 1 \mod 2. \tag{5.44} \]

From equations (5.43) and (5.44) we easily deduce, for integers \( \lambda \), the following system of equations:
\[
\psi(2\lambda + 1, 1) = -p \cdot \psi(2\lambda, 1), \\
\psi(2\lambda, 1) = -\left( \frac{-1}{p} \right) \cdot \psi(2\lambda - 1, 1), \\
\vdots \\
\psi(2, 1) = -\left( \frac{-1}{p} \right) \cdot \psi(1, 1),
\]
and multiplying them all together gives
\[ \psi(2\lambda + 1, 1) = (-1)^{2\lambda} \left( \frac{-1}{p} \right)^\lambda p^\lambda \psi(1, 1) \]
or, since \( \psi(1, 1) = 1 \),
\[ \psi(2\lambda + 1, 1) = (-1)^{\frac{p-1}{2}} p^\lambda. \tag{5.45} \]
2. Let \( q = 2\lambda + 1 \) be, as \( p \), an odd positive prime. According to the formula just found we have

\[
\psi(q, 1) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} p^\frac{q+1}{2}.
\] (5.46)

On the other hand, the defining equation gives

\[
\psi(q, 1) = \sum_{\alpha_i \equiv 1 \mod p} \left( \frac{\alpha_1}{q} \right) \cdots \left( \frac{\alpha_q}{p} \right):
\]

for \( \alpha_1 = \ldots = \alpha_q = \alpha \) we get \( q \alpha \equiv 1 \mod p \). Thus in the sum for \( \psi(q, 1) \) there is exactly one term in which all the \( \alpha_i \) coincide. Now (5.46) implies

\[
\psi(q, 1) = \left( \frac{\alpha}{p} \right)^q + \Delta = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} p^\frac{q+1}{2}.
\]

In \( \Delta = \sum (\frac{\alpha_i}{q}) \cdots (\frac{\alpha_q}{p}) \), the summation is over all \( \alpha_i \) except \( \alpha_1 = \ldots = \alpha_q = \alpha \). From \( q \alpha \equiv 1 \mod p \) we deduce that

\[
1 = \left( \frac{q}{p} \right) \left( \frac{\alpha}{p} \right),
\]

and since \( q \) is odd, we find

\[
(-1)^{\frac{p-1}{2} \frac{q-1}{2}} p^\frac{q+1}{2} - \left( \frac{q}{p} \right) = \Delta. \tag{5.47}
\]

Writing down the sum \( \Delta \) explicitly we get

\[
\Delta = \sum \begin{cases} 
\left( \frac{\alpha_1}{p} \right) \left( \frac{\alpha_2}{p} \right) \cdots \left( \frac{\alpha_q}{p} \right) \\
\left( \frac{\alpha_2}{p} \right) \left( \frac{\alpha_3}{p} \right) \cdots \left( \frac{\alpha_1}{p} \right) \\
\vdots \\
\left( \frac{\alpha_q}{p} \right) \left( \frac{\alpha_1}{p} \right) \cdots \left( \frac{\alpha_{q-1}}{p} \right)
\end{cases}.
\] (5.48)

Thus \( \Delta \) can be decomposed into groups in such a way that each group consists of \( q \) equal summands. This shows that \( \Delta \equiv 0 \mod q \), and now (5.47) gives

\[
(-1)^{\frac{p-1}{2} \frac{q-1}{2}} p^\frac{q+1}{2} \equiv \left( \frac{q}{p} \right) \mod q,
\]

which is what we wanted to prove.

6. Proof by Liouville \[59\]

Let \( p \) be a positive odd prime and \( \rho \) a primitive root of \( x^p = 1 \). Then

\[
\frac{x^p - 1}{x - 1} = (x - \rho^2)(x - \rho^4) \cdots (x - \rho^{2(p-1)}) = 1 + x + x^2 + \ldots + x^{p-1}, \tag{5.49}
\]
and plugging in \( x = 1 \) yields

\[
p = (-1)^{\frac{p-1}{2}} (p - \rho^{-1})^2 \cdots (\rho^{\frac{p-1}{2}} - \rho^{-\frac{p-1}{2}})^2.
\]

Raising this equation to the \( \frac{q-1}{2} \)th power we get

\[
p^\frac{q-1}{2} = (-1)^{\frac{p-1}{2}} \cdot \prod_{\alpha=1}^{(p-1)/2} \frac{\rho^{\alpha q} - \rho^{-\alpha q}}{\rho^{\alpha} - \rho^{-\alpha}} \equiv \left( \frac{p}{q} \right) \mod q,
\]

where \( q \) denotes a positive odd prime distinct from \( p \). The individual factors of \( \prod_{\alpha=1}^{(p-1)/2} \frac{\rho^{\alpha q} - \rho^{-\alpha q}}{\rho^{\alpha} - \rho^{-\alpha}} \) are positive or negative according as \( \alpha q \) is congruent to a positive or negative minimal residue modulo \( p \). Applying Gauss’s Lemma to (5.50) then gives

\[
\left( \frac{p}{q} \right) \equiv (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left( \frac{q}{p} \right),
\]

a well known equation.

### 7. First Proof by Lebesgue [49]

1. Let \( p \) and \( q \) be distinct positive odd primes and consider the congruence

\[
x^2_1 + x^2_2 + \ldots + x^2_q \equiv a \mod p.
\]

Then, as \( x_1, \ldots, x_q \) run through the values 1, 2, \ldots, \( p - 1 \), which can happen in

\[
(p-1)^q
\]

different ways, \( a \) will attain certain values. Assume that \( a \) vanishes \( n^0_q \) times, that it attains a quadratic residue \( n^a_q \) and a quadratic nonresidue \( n^b_q \) times (here and below \( a \) denotes a quadratic residue, \( b \) a quadratic nonresidue). Then we have\(^5\)

\[
n^0_q + n^a_q + n^b_q = (p-1)^q.
\]

Consider a special value \( a_1 \) of \( a \), and set \( n^{a_1}_q = n_q \). Since all residues can be written in the form \( aq^2 \), we find that we have \( n^a_q = n'_q \) for an arbitrary value of \( a \). The same thing holds for the nonresidues, and thus we get, setting \( n^b_q = n'_q \):

\[
n^0_q + \frac{p-1}{2} (n_q + n'_q) = (p-1)^q.
\]

Now Lebesgue computes \( n^0_q, n_q \) and \( n'_q \). From the well known formula

\[^5\] If the \( x \) run through 0, 1, \ldots, \( p - 1 \), and if we denote the corresponding values \( a \) by \( N \), then \( N^0_q + N^a_q + N^b_q = p^q \). This formula can also be used.
$$G = \sum_{\lambda=1}^{\frac{p-1}{2}} \left( \frac{\lambda}{p} \right) \rho^\lambda = \sqrt{(-1)^{\frac{p-1}{2}} p}, \quad \rho^p = 1$$
due to GAUSS and the formula

$$1 + \rho + \rho^2 + \ldots + \rho^{p-1} = 0$$
we get

$$G = \sum \rho^\lambda = \sqrt{(-1)^{\frac{p-1}{2}} p} \quad \text{or} \quad G - 1 = \rho + \rho^2 + \ldots = \sqrt{(-1)^{\frac{p-1}{2}} p}. \quad (5.55)$$

Raising this equation to the $q$th power we get

$$(G - 1)^q = n_q^0 + n_q \sum a \rho^a + n_q' \sum b \rho^b.$$ Using $\sum a \rho^a - \sum b \rho^b = G$ and $1 + \sum a \rho^a + \sum b \rho^b = 0$ we find

$$2n_q^0 - n_q - n_q' + (n_q - n_q')G = 2(G - 1)^q. \quad (5.56)$$
Since $q$ was assumed to be odd we have $$(G - 1)^q = PG - Q$$ and thus

$$2n_q^0 - n_q - n_q' = -2Q, \quad n_q - n_q' = 2P, \quad (5.57)$$
where $P \equiv (-1)^{\frac{(p-1)(q-1)}{4}} p^{\frac{q-1}{2}} \mod q$ and $Q \equiv 1 \mod q$. Comparing (5.57) and (5.54) we find

$$n_q \equiv \frac{(p-1)^q + 1}{p} + (-1)^{\frac{p-1}{2}} \frac{q-1}{2} p^{\frac{q-1}{2}} \mod q. \quad (5.58)$$

2. The congruence $x^2 \equiv a \mod p$ has, if it is solvable at all, exactly 2 distinct solutions modulo $p$. This shows

$$n_q = 2^q S_q, \quad \text{where } S_q \text{ is an integer.} \quad (5.59)$$
If moreover

$$x_1^2 + x_2^2 + \ldots + x_q^2 \equiv a \mod p \quad (5.60)$$
holds for $x_1 = x_2 = \ldots = x_q$, then $qx_1^2 \equiv a \mod p$ or $(\frac{aq}{p}) = 1$. Conversely, if $(\frac{aq}{p}) = 1$, then we can put $qx_1^2 \equiv a \mod p$, and (5.60) holds for $x_1 = x_2 = \ldots = x_q$. Now we observe that the number of solutions of (5.60) in which the $x$ are not equal is a multiple of $q$ because $q$ is a prime; thus we find

$$S_q = \begin{cases} qR + 1 & \text{if } (\frac{q}{p}) = +1, \\ qR & \text{if } (\frac{q}{p}) = -1. \end{cases} \quad (5.61)$$

\text{We get similar formulas for } n_q^0, n_q', N_q^0, N_q, N_q'.\footnote{We get similar formulas for $n_q^0, n_q', N_q^0, N_q, N_q'$.}
On the other hand we have $n_q = 2^q S_q$, hence

\[ n_q \equiv \begin{cases} 2^q \equiv 1 + 1 \mod q & \text{if } (\frac{q}{p}) = +1, \\ 0 \equiv 1 - 1 \mod q & \text{if } (\frac{q}{p}) = -1, \end{cases} \]

and this implies

\[ n_q = 1 + \left( \frac{q}{p} \right). \tag{5.62} \]

Comparing this with (5.58) and applying Fermat’s Theorem immediately implies the reciprocity law.
SECOND PART

Comparative Presentation of the Principles on which the Proofs of the Quadratic Reciprocity Law are Based.
APPENDIX

Additional Comments by the Translator
Author Index

Aigner, 191
Bachet, 117
Bachmann, 191, 222
Berndt, 224
Bhargava, 226
Birch, 191
Bouniakowsky, 138, 139
Brown, 191
Busche, 145, 147
Carlitz, 191
Castryck, 224
Cauchy, 163, 216, 218, 220, 221, 223, 224
Digby, 117
Dirichlet, 120, 126, 175, 189, 215, 216, 218, 220, 223, 225
Eisenstein, 131, 151, 152, 163, 183, 209, 210, 220, 221
Euler, 117, 177, 215
Evans, 224
Fermat, 117
Frenicle, 117
Gauss, 118, 120, 121, 123, 126, 128, 130, 131, 138, 155, 158, 163, 169, 172, 178, 182, 184, 189–191, 213, 214, 218, 223, 225
Gegenbauer, 184
Genocchi, 132, 180, 223
Gerstenhaber, 211
Heine, 216
Ireland, 224
Jacobi, 113, 120, 163, 180, 218–221
Koenig, 191
Kaplan, 211
Kim, 207
Koschmieder, 211
Kronecker, 136, 180, 185, 190, 210, 214, 219, 220, 222–224
Kummer, 172–175, 225
Lagrange, 117, 219
Lebesgue, 155, 168, 183, 184, 216, 218, 219, 221, 223
Legendre, 118–121, 191
Lehmer, 191
Lerch, 224
Libri, 216
Liouville, 222, 223
Lipke, 191
Mathews, 191
Murty, 224
Olbers, 213
Pepin, 191
Petersen, 143, 178
Pieper, 228
Poinsot, 219
Rogers, 191
Rosen, 224
Rousseau, 207
Salvadori, 224
Schaar, 223
Schering, 142, 180, 190
Scholz, 207
Schur, 224
Serre, 211
Shapiro, 191
Smith, H.J., 113
Stern, 133, 134
Sylvester, 182
Tate, 191
Teege, 191
Voigt, 144
Waterhouse, 224
Williams, K.S., 224
Zeller, 135
Subject Index

class
    principal, 171

form
    ambiguous, 171
    first kind, 171
    positive, 171
    primitive, 171
    principal, 171
    second kind, 171
form class, 171

Gauss sum, 157
    sign, 213
Gauss’s Lemma, 130, 135
    genus
        principal, 172

Jacobi sum, 165

Pell equation, 172, 225

quadratic period, 155

theta series, 214