2/16: Quadratic reciprocity

Recall that we defined the Legendre symbol for \( n \in \mathbb{Z} \) and prime \( p \) as

\[
\left( \frac{n}{p} \right) = \begin{cases} 
1 & \text{if } \bar{n} = \alpha^2 \text{ for some } \alpha \in \mathbb{F}_p^* \\
0 & \text{if } \bar{n} = 0 \\
-1 & \text{else}
\end{cases}
\]

and we have

\[
\left( \frac{n}{p} \right) \equiv n^{\frac{p-1}{2}} \pmod{p}.
\]

Now we have the following almighty theorem.

**Theorem 12.1.** (Quadratic reciprocity) Let \( p \) and \( q \) be two distinct odd prime numbers. We have

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

**Proof.** For convenience, let us introduce the notation \( h_n = \frac{n-1}{2} \) for any odd integer \( n \). Let us look at the following three sets

\[
\begin{align*}
S_1 &= \{ \alpha \in (\mathbb{Z}/(pq))^* \mid \alpha \equiv a \pmod{p} \text{ for some } 1 \leq a \leq h_p \}, \\
S_2 &= \{ \alpha \in (\mathbb{Z}/(pq))^* \mid \alpha \equiv a \pmod{q} \text{ for some } 1 \leq a \leq h_q \}, \\
S_3 &= \{ \alpha \in (\mathbb{Z}/(pq))^* \mid \alpha \equiv a \pmod{pq} \text{ for some } 1 \leq a \leq h_{pq} \}.
\end{align*}
\]

We note that if \( \alpha \in S_i \), then \( -\alpha \not\in S_i \). Thus we can turn any \( S_i \) into another \( S_j \) by adding negative sign to some elements. Consider

\[
\omega_i = \prod_{\alpha \in S_i} \alpha \in (\mathbb{Z}/(pq))^* \text{, for } i = 1, 2, 3.
\]

We have \( \omega_i = \pm \omega_j \) for any \( i, j \in \{1, 2, 3\} \). On the other hand, using Chinese Remainder Theorem that \((\mathbb{Z}/(pq))^* \cong \mathbb{F}_p^* \times \mathbb{F}_q^*\) we can write

\[
\omega_1 = \left( (h_p)!^{q-1}, (q-1)!^{h_p} \right) \text{ and likewise } \omega_2 = \left( (p-1)!^{h_q}, (h_q)!^{p-1} \right).
\]

We briefly explain the above identities. Element in \( S_1 \subset (\mathbb{Z}/(pq))^* \cong \mathbb{F}_p^* \times \mathbb{F}_q^* \) can be expressed as \((\beta, \eta)\) with \( \beta \in \mathbb{F}_p^* \) and \( \eta \in \mathbb{F}_q^* \). By definition of \( S_1 \), \( \beta \) can be among \( \bar{1}, \ldots, \bar{h_p} \) and for each such \( \beta, \eta \) can be any of the \( q - 1 \) classes in \( \mathbb{F}_q^* \). Thus the product of such elements mod \( p \) are \((h_p)!\) multiplied \( q - 1 \) times. This gives the first components of \( \omega_1 \). Others are given similarly.

\[
\omega_3 = \left( \frac{(p-1)!^{h_q}(h_p)!}{q^{h_p}(h_p)!}, \frac{(q-1)!^{h_p}(h_q)!}{p^{h_q}(h_q)!} \right) = \left( \frac{(p-1)!^{h_q}}{q^{h_p}}, \frac{(q-1)!^{h_p}}{p^{h_q}} \right).
\]

This can be explained as follows. The elements in \( S_3 \) are given by \( \{1, 2, \ldots, h_{pq}\} \) excluding those divisible by \( p \) or \( q \). Excluding first those divisible by \( p \), we may sort the rest as
\{1,2,...,p-1\}, \{p+1,...,2p-1\}, \ldots, \{(h_q-1)p+1,...,(h_q-1)p+p-1\} and \{h_qp+1,...,h_qp+h_p\}. Among these, we have \(q, 2q, \ldots, h_p q\) that are divisible by \(p\). This gives the quotient in the first part of the middle term.

Recall that we had \(\omega_1 = \pm \omega_3\). To figure out the sign, looking at the \(\mathbb{F}_q^*\)-part we see that they differ by \(\pm 1\), whichever is congruent to \(p^{h_q}\) modulo \(q\). But this is just \(\left(\frac{p}{q}\right)\), namely

\[ \omega_1 = \left(\frac{p}{q}\right) \omega_3, \text{ and likewise } \omega_2 = \left(\frac{q}{p}\right) \omega_3. \tag{1} \]

However, to switch from \(\omega_1\) to \(\omega_2\) we add a minus sign to those whose residue modulo \(p\) is same as some \(1 \leq a \leq h_p\) and whose residue modulo \(q\) is congruent to some \(h_q+1 \leq b \leq q-1\). This gives

\[ \omega_1 = (-1)^{h_p h_q} \omega_2. \tag{2} \]

Combining (1) and (2) we have

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

which is the quadratic reciprocity.