Let p and q be distinct odd primes. Write $q^* = \left(\frac{-1}{q}\right) q$ where $\left(\frac{\cdot}{\cdot}\right)$ is the Legendre symbol. The version of quadratic reciprocity we prove is as follows.

Theorem 1 (Law of Quadratic Reciprocity)**.** *If p and q distinct odd primes, then $\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right)$.*

The version of QR that most are familiar with says that $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. To see that this is equivalent to the statement above, use that $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$ when $p \nmid a$ so that

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

Before beginning the proof, note that $\mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) \cong (\mathbb{Z}/q\mathbb{Z})^\times$ is cyclic, hence has a unique subgroup of index 2, corresponding to the subgroup of squares $(\mathbb{Z}/q\mathbb{Z})^{\times,2}$. Thus $\mathbb{Q}(\zeta_q)/\mathbb{Q}$ has a unique quadratic subextension $K/\mathbb{Q}$ with $\mathrm{Gal}(\mathbb{Q}(\zeta_q)/K) \cong (\mathbb{Z}/q\mathbb{Z})^{\times,2}$. As $\mathbb{Q}(\zeta_q)/\mathbb{Q}$ is ramified only at q, so too is $K/\mathbb{Q}$; hence $K = \mathbb{Q}(\sqrt{\pm q})$ where the sign is chosen so that $\pm q \equiv 1 \pmod 4$ (otherwise 2 would ramify in K). So we must take $\pm q = q^*$.

Proof (of Theorem 1). As discussed above, we have the following tower of fields, with indicated primes lying over p and indicated Frobenii.

$$\begin{array}{ccc}
\mathbb{Q}(\zeta_q) & \mathfrak{P} & \sigma_{\mathfrak{P}} \\
| & | & | \\
\mathbb{Q}(\sqrt{q^*}) & \mathfrak{p} & \sigma_{\mathfrak{p}} \\
| & | & \\
\mathbb{Q} & p &
\end{array}$$

Recall the following facts:

- The isomorphism $\mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/q\mathbb{Z})^\times$ sends $\sigma_{\mathfrak{P}} \mapsto p$.
- Frobenii are compatible with restriction: $\sigma_{\mathfrak{P}}|_{\mathbb{Q}(\sqrt{q^*})} = \sigma_{\mathfrak{p}}$.
- The prime p splits in $\mathbb{Q}(\sqrt{q^*}) = \mathbb{Q}[X]/(X^2 - q^*)$ if and only if $X^2 - q^*$ factors mod p.

Putting all this together gives the following (most easily read from the center to the left, and then from the center to the right).

$$\begin{aligned}
X^2 - q^* \text{ factors mod } p \quad &\iff \quad p \text{ splits in } \mathbb{Q}(\sqrt{q^*}) \quad \iff \quad \sigma_{\mathfrak{p}} = 1 \\
\left(\frac{q^*}{p}\right) = 1 \quad &\iff \qquad\qquad\qquad\qquad \iff \quad \sigma_{\mathfrak{P}} \in \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}(\sqrt{q^*})) \\
&\qquad\qquad\qquad\qquad\qquad\qquad \iff \quad p \in (\mathbb{Z}/q\mathbb{Z})^{\times,2} \\
&\qquad\qquad\qquad\qquad\qquad\qquad \iff \quad \left(\frac{p}{q}\right) = 1
\end{aligned}$$

$\square$