QUADRATIC RECIPROCITY
THE BIG PICTURE

It takes a lot of work to prove:

> **Quadratic Reciprocity (Theorem 4.9).** *Let p, q be odd prime numbers with $p \neq q$. Then*
> $$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Quadratic Reciprocity follows pretty easily from:

> **Eisenstein's Lemma (Lemma 4.10).** *Let p, q be odd prime numbers with $p \neq q$. Then*
> $$\left(\frac{q}{p}\right) = (-1)^{N_1}, \qquad \left(\frac{p}{q}\right) = (-1)^{N_2}$$
> *where N_1 is the number of points*
> $$\{(i,j):\ 1 \leq i \leq \frac{p-1}{2}, 1 \leq j \leq \frac{q-1}{2}, i,j \in \mathbb{Z}\}$$
> *that are below the line $y = \frac{q}{p}x$, and N_2 is the number of such points above this line.*

It's enough to prove the first of these two statements, namely $\left(\frac{p}{q}\right) = (-1)^{N_1}$, because the other is just the same but with the roles of p and q switched. But, to prove this first statement, we need to use two sublemmas:

> **Gauss' Lemma (Lemma 4.7).** *Let p, q be odd prime numbers with $p \neq q$. Then*
> $$\left(\frac{q}{p}\right) = (-1)^{n_1}$$
> *where n_1 is the number of these elements:*
> $$[q], [2q], \ldots, [\tfrac{p-1}{2}q] \in \mathbb{Z}_p$$
> *that equal $[r_i]$ with $p/2 < r_i < p$, and n_2 is the number of these elements that equal $[s_i]$ with $0 < s_i < p/2$.*

> **Baby Eisenstein's Lemma (Baby Lemma 4.10).** *Let p, q be odd prime numbers with $p \neq q$. Then*
> $$N_1 \equiv n_1 \bmod 2$$
> *where N_1 and n_1 are defined as above.*

We can prove Gauss' Lemma by a calculation with the help of this sub-sublemma:

Baby Gauss' Lemma (Baby Lemma 4.7). *Let p, q be odd prime numbers with $p \neq q$. Define the numbers $r_1, \ldots, r_{n_1}$ and $s_1, \ldots, s_{n_2}$ as above. Then the set of numbers*

$$\{p - r_1, \ldots, p - r_{n_1}, s_1, \ldots, s_{n_2}\}$$

is the same as the set

$$\{1, 2, \ldots, \frac{p-1}{2}\}$$

together with Euler's Criterion:

Euler's Criterion (Theorem 4.4). *Let p be an odd prime number and let $a \in \mathbb{Z}$ have $a \not\equiv 0 \bmod p$. Then*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$$

Finally, to prove Euler's criterion, we used Fermat's Little Theorem and Wilson's Theorem! Nobody knows any easier way to prove Quadratic Reciprocity. This is why it's called a 'deep result'.

I think it is said that Gauss had ten different proofs for the law of quadratic reciprocity. Any good theorem should have several proofs, the more the better. For two reasons: usually, different proofs have different strengths and weaknesses, and they generalise in different directions – they are not just repetitions of each other. — Sir Michael Atiyah