5.2. **A proof of quadratic reciprocity.** The law of quadratic reciprocity is so fundamentally important that many people tried to prove it in different ways. Gauss gave the first proof in 1796 and found eight separate proofs in his life. There are over a hundred now in existence. In these proofs, a lot of new techniques were developed which have become standard in modern number theory. Here we present an elementary but ingenious proof due to Gauss. It relies on a clever geometric observation which we explain now.

Lemma 5.3. *Let p and q be distinct odd primes. Then*

$$\sum_{l=1}^{\frac{p-1}{2}} \left[\frac{lq}{p}\right] + \sum_{k=1}^{\frac{q-1}{2}} \left[\frac{kp}{q}\right] = \frac{p-1}{2} \cdot \frac{q-1}{2}. \tag{5.3}$$

Proof. For simplicity we write $r = \frac{p-1}{2}$ and $s = \frac{q-1}{2}$. In the (x, y)-plane, we consider the number of integral points in the interior of the rectangle with four vertices at $(0, 0)$, $(\frac{p}{2}, 0)$, $(\frac{p}{2}, \frac{q}{2})$ and $(0, \frac{q}{2})$. Any such integral point is given by a pair of integers (x, y) with $1 \leqslant x \leqslant r$ and $1 \leqslant y \leqslant s$. Therefore the number of such integral points is rs, which is the right-hand side of (5.3).

We want to count the number of integral points in a different way to obtain the left hand side of (5.3). We connect the points $(0, 0)$ and $(\frac{p}{2}, \frac{q}{2})$ by a line segment to cut the rectangle into two triangles. We notice that there is no interior integral point lying on this line segment. Indeed, if there is an interior integral point (x, y) on this line segment, then we will have $qx = py$, which implies $p \mid x$, contradicting the requirement $1 \leqslant x \leqslant r$. Hence any integral point in the interior of the rectangle lies in the interior of one of the triangles.

We count the number of interior integral points in the triangle with vertices at $(0, 0)$, $(\frac{p}{2}, 0)$ and $(\frac{p}{2}, \frac{q}{2})$. For each $l = 1, 2, \cdots, r$, we fix $x = l$ and think how many integral points of the form (l, y) lie in the interior this triangle. The intersection of the vertical line $x = l$ and the diagonal of the rectangle is the point $(l, \frac{lq}{p})$. We find that y can only take positive integral values not larger than $\frac{lq}{p}$, hence has $\left[\frac{lq}{p}\right]$ choices. Therefore the number of integral points in the whole triangle is given by $\sum_{l=1}^{r} \left[\frac{lq}{p}\right]$. Similarly, the number of integral points in the other triangle is given by $\sum_{k=1}^{s} \left[\frac{kp}{q}\right]$. They add up to the left-hand side of (5.3). □

Finally we explain why the above lemmas prove the quadratic reciprocity.

Proof of the Law of Quadratic Reciprocity. For distinct odd primes p and q, by Lemma 5.2 we can write

$$\begin{aligned}\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) &= (-1)^{\sum_{l=1}^{\frac{p-1}{2}}\left[\frac{lq}{p}\right]} \cdot (-1)^{\sum_{k=1}^{\frac{q-1}{2}}\left[\frac{kp}{q}\right]} \\ &= (-1)^{\sum_{l=1}^{\frac{p-1}{2}}\left[\frac{lq}{p}\right]+\sum_{k=1}^{\frac{q-1}{2}}\left[\frac{kp}{q}\right]} \\ &= (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}},\end{aligned}$$

where the last equality follows from Lemma 5.3. □

To close this topic, we show how quadratic residues can help to give a refinement of Theorem 1.15 on infinitely many primes. The following results are special cases of the so-called Dirichlet's theorem.

Proposition 5.4. *The following statements hold*

(1) *There are infinitely many primes which are congruent to* -1 *modulo* 4.

(2) *There are infinitely many primes which are congruent to* 1 *modulo* 4.

Proof. We follow the idea in the proof of Theorem 1.15.

For (1), we assume by contradiction that the set of all primes congruent to -1 modulo 4 is finite, say, $S = \{p_1, p_2, \cdots, p_n\}$. Then we consider $N = 4p_1p_2\cdots p_n - 1$. Obviously $p_i \nmid N$ for each i. Let p be any prime factor of N. Then $p \notin S$ hence $p \equiv 1 \pmod 4$. This implies N is the product of primes which are all congruent to 1 modulo 4, hence $N \equiv 1 \pmod 4$. Contradiction.

For (2), we similarly assume by contradiction that the set of all primes congruent to 1 modulo 4 is finite, say, $T = \{q_1, q_2, \cdots, q_m\}$. Then we consider $M = (2q_1q_2\cdots q_m)^2 + 1$. Obviously $q_j \nmid M$ for each j. Let q be any prime factor of M. Then $q \notin T$ hence $q \equiv -1 \pmod 4$. However $q \mid M$ implies $(2q_1q_2\cdots q_m)^2 \equiv -1 \pmod q$, i.e. -1 is a quadratic residue modulo q. By Proposition 4.5 (1) we get $q \equiv 1 \pmod 4$. Contradiction. □

Corollary 5.5. *There are infinitely many odd primes* p *for which* -1 *is a quadratic residue. There are also infinitely many odd primes* p *for which* -1 *is a quadratic non-residue.*

Proof. This is a immediate consequence of Propositions 4.5 (1) and 5.4. □