

## Law of Quadratic Reciprocity

Let  $p, q$  be odd primes and  $p \neq q$

Let  $pRq$  mean  $x^2 \equiv p \pmod{q}$  for some  $x \in \mathbb{Z}$

Let  $pNq$  mean  $x^2 \not\equiv p \pmod{q}$  for all  $x \in \mathbb{Z}$

### Case I

If  $p = 1 + 4n$ , for some  $n \in \mathbb{Z}$

then either  $pRq$  and  $qRp$  or  $pNq$  and  $qNp$

### Case II

If  $p = 3 + 4m$ ,  $q = 3 + 4n$  for some  $m, n \in \mathbb{Z}$

then either  $pRq$  and  $qNp$  or  $pNq$  and  $qRp$

- *Karl Friedrich Gauss (1801)*