

Law of Quadratic Reciprocity

Let p, q be distinct odd primes, and define the following symbols:

pRq	$x^2 \equiv p \pmod{q}$ for some $x \in \mathbb{Z}$ p is a <i>quadratic residue</i> of q
pNq	$x^2 \not\equiv p \pmod{q}$ for all $x \in \mathbb{Z}$ p is a <i>quadratic nonresidue</i> of q

Case I

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

then either pRq and qRp or pNq and qNp

Case II

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

then either pRq and qNp or pNq and qRp

— *Karl Friedrich Gauss (1801)*

Law of Quadratic Reciprocity

		q													
		3	5	7	11	13	17	19	23	29	31	37	41	43	47
p	3	–	N	N	R	R	N	N	R	N	N	R	N	N	R
	5	N	–	N	R	N	N	R	N	R	R	N	R	N	N
	7	R	N	–	N	N	N	R	N	R	R	R	N	N	R
	11	N	R	R	–	N	N	R	N	N	N	R	N	R	N
	13	R	N	N	N	–	R	N	R	R	N	N	N	R	N
	17	N	N	N	N	R	–	R	N	N	N	N	N	R	R
	19	R	R	N	N	N	R	–	N	N	R	N	N	N	N
	23	N	N	R	R	R	N	R	–	R	N	N	R	R	N
	29	N	R	R	N	R	N	N	R	–	N	N	N	N	N
	31	R	R	N	R	N	N	N	R	N	–	N	R	R	N
	37	R	N	R	R	N	N	N	N	N	N	–	R	N	R
	41	N	R	N	N	N	N	N	R	N	R	R	–	R	N
	43	R	N	R	N	R	R	R	N	N	N	N	R	–	N
	47	N	N	N	R	N	R	R	R	N	R	R	N	R	–

R \rightarrow p is a quadratic residue of q

N \rightarrow p is a quadratic nonresidue of q