16. Quadratic reciprocity

We now recall one of the most famous results in all of mathematics:

Theorem 16.1 (Quadratic reciprocity). *Let p and q be two different odd primes.*

Then

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right),$$

unless $p \equiv 3 \mod 4$ and $q \equiv 3 \mod 4$, in which case

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right),$$

Succintly

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

Proof. By Gauss's Lemma,

$$\left(\frac{q}{p}\right) = (-1)^{\mu} \qquad \text{and} \qquad \left(\frac{p}{q}\right) = (-1)^{\nu},$$

where μ is the number of elements of the sequence

$$q \qquad 2q \qquad 3q \qquad \dots \qquad (p-2)q/2 \qquad \text{and} \qquad (p-1)q/2$$

which are equivalent to an element of the interval $[-(p-1)/2, 0)$ and ν is the number of elements of the sequence

$$p \qquad 2p \qquad 3p \qquad \dots \qquad (q-2)p/2 \qquad \text{and} \qquad (q-1)p/2$$

which are equivalent to an element of the interval $[-(q-1)/2, 0)$.

Therefore we have to show that

$$\mu + \nu \equiv \frac{p-1}{2} \cdot \frac{q-1}{2} \mod 2.$$

Consider a multiple xq with $1 \leq x \leq (p-1)/2$. If we pick y such that

$$-\frac{p}{2} < qx - py < \frac{p}{2}$$

then $qx - py$ is the unique element of

$$\{\, a \in \mathbb{Z} \mid -p/2 < a < p/2 \,\}$$

equivalent to qx modulo p. If we flip the sign of the inequality above we get

$$-\frac{p}{2} < py - qx < \frac{p}{2},$$

so that

$$-\frac{1}{2} < y - \frac{q}{p}x < \frac{1}{2},$$

so that

$$\frac{q}{p}x - \frac{1}{2} < y < \frac{q}{p}x + \frac{1}{2}.$$

It follows that $y \geq -1/2$, so that $y \geq 0$. Suppose that $y = 0$. Then

$$qx - py = qx > 0,$$

and we don't get a number with negative residue. Thus we may assume that $y > 0$. On the other hand, for $x \leq (p-1)/2$, we have

$$\begin{aligned} \frac{q}{p}x + \frac{1}{2} &\leq \frac{q}{2} - \frac{q}{2p} + \frac{1}{2} \\ &< \frac{q+1}{2}. \end{aligned}$$

Thus we may assume that $y \in (0, (q-1)/2]$. It follows that μ is the number of elements in the set

$$R = \{\, (x, y) \in \mathbb{Z}^2 \mid x \in (0, (p-1)/2], y \in (0, (q-1)/2] \,\}$$

such that

$$0 > qx - py > -\frac{p}{2}.$$

Similarly ν is the number of elements in the set

$$R = \{\, (x, y) \in \mathbb{Z}^2 \mid x \in (0, (p-1)/2], y \in (0, (q-1)/2] \,\}$$

such that

$$0 > py - qx > -\frac{q}{2}.$$

Note that the points of the set R have to lie in one of four regions, the two regions describe above or

$$py - qx > \frac{p}{2} \qquad \text{or} \qquad py - qx < -\frac{q}{2}.$$

If λ is the number of points in the third region and ρ is the number of points in the fourth region, we have

$$\lambda + \mu + \nu + \rho = \frac{p-1}{2} \cdot \frac{q-1}{2},$$

since there are $(p-1)/2$ choices for x and $(q-1)/2$ choices for y.

Consider the numbers

$$x' = \frac{p+1}{2} - x \qquad \text{and} \qquad y' = \frac{q+1}{2} - y.$$

As x runs from 1 to $(p-1)/2$, x' runs down through the same numbers and similarly for y.

Suppose that we have a point of the third region, so that

$$0 > py - xy > \frac{p}{2}.$$

Then

$$
\begin{aligned}
py' - qx' &= p\left(\frac{q+1}{2} - y\right) - q\left(\frac{p+1}{2} - x\right) \\
&= \frac{p-q}{2} - (py - qx) \\
&< \frac{p-q}{2} - \frac{p}{2} \\
&< -\frac{q}{2}.
\end{aligned}
$$

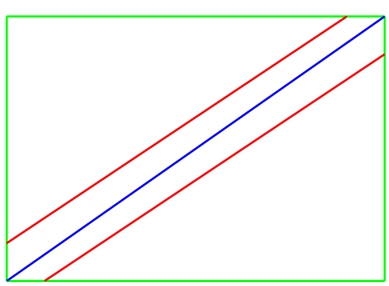
Thus (x', y') is a point of the fourth region. Vice-versa, if we start with a point (x', y') of the fourth region then we get a point (x, y) of the third region using the inverse transformation.

It follows that the third region has the same number of integer points as the fourth region, that is, $\lambda = \rho$. In this case

$$
\begin{aligned}
\frac{p-1}{2} \cdot \frac{q-1}{2} &= \lambda + \mu + \nu + \rho \\
&= 2\lambda + \mu + \nu \\
&= \mu + \nu \mod 2.
\end{aligned}
$$

□

The following picture shows the four different regions



Question 16.2. *Is* 257 *a quadratic residue modulo* 269*?*

Note that 257 and 269 are both prime numbers. 257 is congruent to one modulo 4. Therefore if we apply quadratic reciprocity we have

$$\begin{aligned}
\left(\frac{257}{269}\right) &= \left(\frac{269}{257}\right) \\
&= \left(\frac{12}{257}\right) \\
&= \left(\frac{4}{257}\right)\left(\frac{3}{257}\right) \\
&= \left(\frac{257}{3}\right) \\
&= \left(\frac{2}{3}\right) \\
&= -1.
\end{aligned}$$

Thus 257 is not a quadratic residue modulo 269.

If we fix q then we can use the law of quadratic reciprocity to decide for which primes p that q is a square modulo p.

Theorem 16.3. *Fix an odd prime q.*

If p is an odd prime then p has a unique representation of the form

$$p = 4kq \pm a \qquad 0 < a < 4q \qquad \text{and} \qquad a \equiv 1 \mod 4,$$

for some $k \in \mathbb{Z}$. With this choice of a

$$\left(\frac{q}{p}\right) = \left(\frac{a}{q}\right).$$

Proof. By the division algorithm we may write

$$p = 4ql + r,$$

where $0 \leq r < 4q$ and $l \in \mathbb{Z}$. r is odd as p is odd and $4qk$ is even. If $r \equiv 1 \mod 4$ then we take $a = r$ (and $k = l$). Otherwise $r \equiv 3 \mod 4$. In this case

$$p = 4q(l+1) + (r - 4q).$$

Let $a = 4q - r$ and $k = l + 1$. Then $0 \leq a < 4q$ and

$$p = 4qk - a.$$

It is not hard to see this representation is unique.

It remains to check that

$$\left(\frac{p}{q}\right) = \left(\frac{a}{q}\right).$$

There are two cases. If

$$p = 4qk + a,$$

then $p \equiv 1 \mod 4$ so that by quadratic reciprocity

$$\begin{aligned}\left(\frac{q}{p}\right) &= \left(\frac{p}{q}\right)\\ &= \left(\frac{a}{q}\right).\end{aligned}$$

Now suppose that

$$p = 4qk - a.$$

Then $p \equiv -1 \equiv 3 \mod 4$. There are two cases. If $q \equiv 1 \mod 4$ then

$$\left(\frac{-1}{q}\right) = 1$$

and so we can apply quadratic reciprocity to get

$$\begin{aligned}\left(\frac{q}{p}\right) &= \left(\frac{p}{q}\right)\\ &= \left(\frac{-a}{q}\right)\\ &= \left(\frac{-1}{q}\right)\left(\frac{a}{q}\right)\\ &= \left(\frac{a}{q}\right).\end{aligned}$$

Finally, suppose that $q \equiv 3 \mod 4$. Then

$$\left(\frac{-1}{q}\right) = -1$$

and so we can apply quadratic reciprocity to get

$$\begin{aligned}\left(\frac{q}{p}\right) &= -\left(\frac{p}{q}\right)\\ &= -\left(\frac{-a}{q}\right)\\ &= -\left(\frac{-1}{q}\right)\left(\frac{a}{q}\right)\\ &= \left(\frac{a}{q}\right).\end{aligned}$$

□

Lemma 16.4. *Let q be an odd prime. The integers a such that*

$$0 < a < 4q, \qquad a \equiv 1 \mod 4 \qquad \textit{and} \qquad \left(\frac{a}{q}\right) = 1$$

are the remainders modulo $4q$ of the sequence of odd squares

$$1^2 \qquad 3^2, \qquad 5^2 \qquad \dots \qquad \textit{and} \qquad (q-2)^2.$$

Proof. The remainders of the squares certainly lie between 1 and $4q-1$. If b is odd then $b^2 \equiv 1 \mod 4$, and certainly a square is a square modulo q.

Now suppose that a is an integer such that

$$0 < a < 4q, \qquad a \equiv 1 \mod 4 \qquad \text{and} \qquad \left(\frac{a}{q}\right) = 1.$$

Then the equation

$$x^2 \equiv a \mod q$$

Has a solution b and we may assume that $1 \leq b \leq q-1$. Note that $q-b$ is also a solution and one of b and $q-b$ is odd. So possibly replacing b by $q-b$ we may assume that b is odd. Therefore

$$b^2 \equiv a \mod q \qquad 1 \leq b \leq q-2 \qquad \text{and} \qquad b \equiv 1 \mod 2.$$

But then

$$a \equiv 1 \equiv b^2 \mod 4.$$

Thus

$$a \equiv b^2 \mod 4q,$$

by the Chinese remainder theorem. □

We illustrate how to use these results in a couple of interesting cases. Suppose that $q = 3$. Then we are supposed to look at the squares up to $q-2$, which is just $1^2 = 1$. So if p is an odd prime such that 3 is a square modulo p we must have

$$p = 12k \pm 1.$$

for some k, that is,

$$p \equiv \pm 1 \mod 12.$$

As p is odd, the only other possibilities are $12k \pm 3$ and $12k \pm 5$. But $12k \pm 3$ is divisible by 3 and so we must have $p = 12k \pm 5$. Putting all of this together

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \mod 12 \\ -1 & \text{if } p \equiv \pm 5 \mod 12. \end{cases}$$

Now suppose that we consider $q = 23$. We consider the squares

$$1^2 \quad 3^2 \quad 5^2 \quad 7^2 \quad 9^2 \quad 11^2 \quad 13^2 \quad 15^2 \quad 17^2 \quad 19^2 \quad 21^2.$$

Modulo $4q = 92$ we get

$$1 \quad 9 \quad 25 \quad 49 \quad 81 \quad 29 \quad 77 \quad 41 \quad 13 \quad 85 \quad 73.$$

So 23 is a square modulo an odd prime p if and only if

$$p \equiv \pm 1 \quad \pm 9 \quad \pm 13 \quad \pm 25 \quad \pm 29 \quad \pm 41 \quad \pm 49 \quad \pm 73 \quad \pm 77 \quad \pm 81 \quad \pm 85 \mod 92.$$