Quadratic reciprocity

The story starts with the French "amateur" mathematician Fermat in the 17th century. Fermat was once interested in representing integers as the sum of two squares. He was amazed when he found an elegant criterion as to whether a prime number can be written in the form $x^2 + y^2$ and could not wait to communicate his result to another French mathematician, Mersenne, on Christmas day of 1640.

Example 1. $5 = 1^2 + 2^2$, $13 = 2^2 + 3^2$, $17 = 1^2 + 4^2$, $29 = 2^2 + 5^2$. But other primes like $7, 11, 19, 23$ cannot be represented in this way. The difference seems to depend on $p \bmod 4$.

Theorem 1 (Fermat)**.** *An odd prime p can be written as $p = x^2 + y^2$ if and only if $p \equiv 1 \pmod 4$.*

But why? The "only if" is obvious, but the other direction is far from trivial. In his letter, Fermat claimed that he had a "solid proof". But nobody was able to find the proof among his work — apparently the margin was never big enough for Fermat. The only clue is that he used a "descent argument": if such a prime p is not of the required form, then one can construct another smaller prime and so on, until a contradiction occurs when one encounters 5, the smallest such prime.

Euler later gave the first rigorous proof, which consists of two steps:

1. If $p \mid x^2 + y^2$ with $(x, y) = 1$, then $p = x^2 + y^2$. This assertion uses a descent argument.
2. If $p \equiv 1 \pmod 4$, then $p \mid x^2 + y^2$ with $(x, y) = 1$.

We will not go into details of the first step but concentrate on the second. Historically, it took more time for Euler to figure out the proof of the second step. From the modern point of view, the key observation is that it has to do with whether or not -1 is a quadratic residue mod p.

Definition 1. Let p be a prime and a be an integer. We say a is a **quadratic residue mod p** if $x^2 \equiv a \pmod p$ has a solution, i.e., $a \bmod p$ is a square in $\mathbb{F}_p$.

The following lemma then follows easily.

Lemma 1. *Let p be an odd prime, then $p \mid x^2 + y^2$ with $(x, y) = 1$ if and only if -1 is a quadratic residue.*

Proof. Because $x^2 + y^2 \equiv 0 \pmod p$ if and only if $(xy^{-1})^2 \equiv -1 \pmod p$. □

So the remaining question is to find a way to determine all the quadratic residues.

Example 2. One naive way is to enumerate all the squares. For example when $p = 11$,

x	1	2	3	4	5	6	7	8	9	10
x^2	1	4	9	5	3	3	5	9	4	1

we find that $1, 3, 4, 5, 9$ are quadratic residues mod 11 and $2, 6, 7, 8, 10$ are not quadratic residues mod 11.

We now introduce a more powerful tool in dealing with quadratic residues — the Legendre symbol.

Definition 2 (Legendre Symbol)**.** Let p be an odd prime and a be an integer coprime to p. We define the **Legendre symbol**

$$\left(\frac{a}{p}\right)=\begin{cases}+1, & a \text{ is a quadratic residue mod } p,\\ -1, & a \text{ is not a quadratic residue mod } p.\end{cases}$$

Remark. This definition seems a bit arbitrary. It is a good time for us to translate things in a more conceptual manner. Consider the inclusion $(\mathbb{F}_p^\times)^2 \hookrightarrow \mathbb{F}_p^\times$. Since $\mathbb{F}_p^\times$ is a cyclic group of order $p-1$, we know that the subgroup $(\mathbb{F}_p^\times)^2$ consisting of squares has index 2. So we have an exact sequence

$$1 \to (\mathbb{F}_p^\times)^2 \to \mathbb{F}_p^\times \to \{\pm 1\} \to 1.$$

Therefore the Legendre symbol $\left(\frac{\cdot}{p}\right)$ is nothing but the quotient map $\mathbb{F}_p^\times \to \{\pm 1\}$. In particular, this map is a group homomorphism, so we have

Proposition 1. The Legendre symbol is **multiplicative**, namely,

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

The multiplicativity pins down the above seemingly arbitrary definition.

To actually compute the Legendre symbol, one way is to find out an explicit expression of the map $\mathbb{F}_p^\times \to \{\pm 1\}$.

Proposition 2. Suppose $a \in \mathbb{F}_p^\times$, then

$$\boxed{\left(\frac{a}{p}\right)=a^{\frac{p-1}{2}} \in \pm 1.}$$

Proof. Since $\mathbb{F}_p^\times$ is a cyclic group of order $p-1$, we know that $a^{p-1}=1$ (Fermat's little theorem), thus $a^{\frac{p-1}{2}} \in \{\pm 1\}$. It is clear that the kernel consists of $(\mathbb{F}_p^\times)^2$. □

This proposition allows us to compute the Legendre symbol without enumerating all squares in $\mathbb{F}_p^\times$.

Example 3. Let us compute $\left(\frac{3}{11}\right)$. By the previous proposition,

$$\left(\frac{3}{11}\right) \equiv 3^5 \equiv (-2)^2 \cdot 3 \equiv 1 \pmod{11}.$$

This coincides with the fact that 3 is a quadratic residue mod 11: $5^2 \equiv 3 \pmod{11}$.

Obviously this could become tedious when p is bigger. We can do better using Proposition 3 together with the famous quadratic reciprocity law we will introduce in a moment.

Proposition 3. The following formulas hold:

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}=\begin{cases}+1, & p\equiv 1 \pmod 4,\\ -1, & p \equiv -1 \pmod 4,\end{cases}$$

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}=\begin{cases}+1, & p\equiv \pm 1 \pmod 8,\\ -1, & p \equiv \pm 3 \pmod 8.\end{cases}$$

Proof. The first formula follows from Proposition 2. For the second formula, we need to compute $2^{\frac{p-1}{2}}$ in $\mathbb{F}_p$. Let α be a 8th root of unity in $\overline{\mathbb{F}_p}$ such that $\alpha^8 = 1$ and $\alpha^4 = -1$. Then $x = \alpha + \alpha^{-1}$ satisfies $x^2 = 2$ and $2^{\frac{p-1}{2}} = x^{p-1}$. Notice that $x^p = \alpha^p + \alpha^{-p}$, we know that

$$x^p = \begin{cases} \alpha + \alpha^{-1} = x, & p \equiv \pm 1 \pmod 8, \\ \alpha^3 + \alpha^{-3} = -x, & p \equiv \pm 3 \pmod 8). \end{cases}.$$

Therefore $x^{p-1} = \pm 1$ according to the residue of p mod 8. □

Theorem 2 (Quadratic Reciprocity)**.** Let p and q be distinct odd primes. Then

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

Before giving its proof, some examples are in order to demonstrate how the quadratic reciprocity can help us to simplify the computation of Legendre symbols.

Example 4. Let us compute $\left(\frac{3}{11}\right)$ in the previous example again. By quadratic reciprocity,

$$\left(\frac{3}{11}\right) = -\left(\frac{11}{3}\right) = -\left(\frac{2}{3}\right) = -(-1) = 1.$$

Observe that the quadratic reciprocity helps us to decrease the size of the modulus quite effectively!

Example 5. Let us compute $\left(\frac{137}{227}\right)$. Notice that

$$\left(\frac{137}{227}\right) = \left(\frac{-90}{227}\right) = \left(\frac{-1}{227}\right)\left(\frac{2}{227}\right)\left(\frac{3^2}{227}\right)\left(\frac{5}{227}\right).$$

By definition, $\left(\frac{3^2}{227}\right) = 1$. By Proposition 3, we know that

$$\left(\frac{-1}{227}\right) = -1, \left(\frac{2}{227}\right) = -1.$$

The quadratic reciprocity gives

$$\left(\frac{5}{227}\right) = \left(\frac{227}{5}\right) = \left(\frac{2}{5}\right) = -1.$$

So

$$\left(\frac{137}{227}\right) = -1.$$

Now let us come back to the proof of the quadratic reciprocity law. Gauss discovered the quadratic reciprocity law in his youth. Like many fundamental results in mathematics (e.g. the fundamental theorem of algebra), tons of different proofs of the quadratic reciprocity law have been found (6 of them are due to Gauss), varying from counting lattice points to infinite product expansion of sine functions. In the book **Reciprocity Laws: From Euler to Eisenstein** by Franz Lemmermeyer, 233 different proofs are collected[1] with bibliography! Here we give a simple lowbrow group-theoretic proof due to Rousseau. The only thing we really need is the Chinese remainder theorem.

[1] An on-line list: `http://www.rzuser.uni-heidelberg.de/~hb3/fchrono.html`

Proof of Quadratic Reciprocity. By the Chinese remainder theorem, we have $\mathbb{Z}/pq \cong \mathbb{Z}/p \times \mathbb{Z}/q$, thus

$$(\mathbb{Z}/pq)^\times \cong \mathbb{F}_p^\times \times \mathbb{F}_q^\times.$$

Now we choose a set of coset representatives of $\{\pm 1\}$ of $(\mathbb{Z}/pq)^\times$ in two ways.

1. We choose the coset representatives
$$S = \left\{(a,b) \in \mathbb{F}_p^\times \times \mathbb{F}_q^\times : a = 1, \dots, p-1; b = 1, \dots, \frac{q-1}{2}\right\}.$$
2. We choose the coset representatives
$$T = \left\{(c \bmod p, c \bmod q) \in \mathbb{F}_p^\times \times \mathbb{F}_q^\times : c = 1, \dots, \frac{pq-1}{2}.\right\}.$$

Now let us compute the product of elements of S and the product of elements of T and compare the results. The products should differ at most by a sign since S can be obtained by replacing elements of T by their opposites. For the first case,

$$\prod_{(a,b)\in S} (a,b) = \left((p-1)!^{\frac{q-1}{2}}, ((q-1)/2)!^{p-1}\right).$$

For the second case, the first factor $(\mathrm{mod} p)$ equals to

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

by Proposition 2. By symmetry, we know that

$$\prod_{(c,c)\in T} (c,c) = \left((p-1)!^{\frac{q-1}{2}}\left(\frac{q}{p}\right), (q-1)!^{\frac{p-1}{2}}\left(\frac{p}{q}\right)\right).$$

Notice that

$$((q-1)/2)!^2 = (-1)^{\frac{q-1}{2}}(q-1)! \mod q,$$

so comparing the two products we conclude that

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

as desired. □

Remark. The quadratic reciprocity has been vastly generalized to the **Artin reciprocity**, in the framework of class field theory. Hopefully we will be able to give another highbrow proof after introducing some elements of class field theory, one of the greatest mathematical achievement in the 20th century.

Remark. Next time we will introduce the notion of number fields and number rings and reformulate Fermat's result on $p = x^2 + y^2$ as prime decomposition in the number ring $\mathbb{Z}[i]$.

Exercise. Does the equation

$$2x^2 \equiv -21 \pmod{79}$$

have a solution?

Exercise (Optional)**.** Show that there are infinitely many primes $p \equiv 1 \pmod 4$.