Quadratic Reciprocity (Gauss)

This theorem from about 1800 might be considered the first modern theorem in number theory.

The statement of the theorem is of substantial interest in itself, and is useful in computations, but, in fact, the *proof* given here is even more interesting than the result itself.

(The first pseudoprimality test with *provable* properties, Solovay-Strassen, used quadratic symbols.)

Recall that x is said to be a **square mod** p if there is an integer y such that

$$y^2 = x \bmod p$$

For a prime p and integer x define the **quadratic symbol**

$$\left(\frac{x}{p}\right)_2 = \begin{cases} 0 & (p \text{ divides } x) \\ 1 & (x \text{ non-zero square mod } p) \\ -1 & (x \text{ non-square mod } p) \end{cases}$$

That is, the quadratic symbol is a function of two variables, written in a funny way, that essentially tells whether or not the thing on the top is a square modulo the thing on the bottom, which should be a prime. (If the prime on the bottom divides the thing on the top, we get 0.)

Theorem: (Quadratic Reciprocity) For distinct odd primes p and q

$$\left(\frac{p}{q}\right)_2 \cdot \left(\frac{q}{p}\right)_2 = (-1)^{(p-1)(q-1)/4}$$

$$= \begin{cases} 1 & p = 1 \bmod 4 \textbf{ or } q = 1 \bmod 4) \\ -1 & p = 3 \bmod 4 \textbf{ and } q = 3 \bmod 4) \end{cases}$$

This assertion ought to be *amazing*! Why should there be any connection between what goes on modulo p and what happens mod q? (If you think that there is some obvious relation, just try...)

Based on extensive numerical examples, these theorems were *believed* since about 1750, but many excellent mathematicians tried and failed to prove it. Gauss succeeded around 1800.

An important auxiliary part, also very difficult (historically) to prove, concerns whether 2 is a square or not modulo p.

Theorem: For an odd prime p

$$\left(\frac{2}{p}\right)_2 = (-1)^{(p^2-1)/8}$$

$$= \begin{cases} 1 & p = 1 \bmod 8) \\ -1 & p = 3 \bmod 8) \\ -1 & p = 5 \bmod 8) \\ 1 & p = 7 \bmod 8) \end{cases}$$

We will prove this supplementary part first, to illustrate the technique.

Lemma: For any b not divisible by odd prime p,

$$\left(\frac{b}{p}\right)_2 = b^{(p-1)/2} \bmod p$$

Proof: The formula of the lemma is essentially Euler's criterion. Half the proof is a consequence of Fermat's Little Theorem, and half depends more seriously on the existence of primitive roots modulo primes.

On one hand, if $b = c^2 \bmod p$, then by Fermat

$$b^{(p-1)/2} = c^{p-1} = 1 \bmod p$$

which matches the quadratic symbol's value. And whatever $b^{(p-1)/2}$ is modulo p, its *square* is $b^{p-1} = 1 \bmod p$, by Fermat. By earlier discussions, there are exactly two

square roots of 1 modulo p, namely ± 1. Thus, for $b \neq 0 \bmod p$, if $b^{(p-1)/2} \neq 1 \bmod p$ then it is -1.

To prove the lemma for non-square b (and in fact to reprove the first part) let $b = g^\ell$ where g is a *primitive root* mod p and $0 \leq \ell \leq p-2$. Recall that $g^t = 1 \bmod p$ if and only if $(p-1)|t$,

$$b^{(p-1)/2} = g^{(p-1)\ell/2} = 1 \text{ if and only if } 2|\ell$$

That is, if b is *not* a square then we get value -1, which is the *other* square root of 1 mod p. That is, if b is a square then

$$b^{(p-1)/2} = 1 = \left(\frac{b}{p}\right)_2 \bmod p$$

and if b is *not* a square

$$b^{(p-1)/2} = -1 = \left(\frac{b}{p}\right)_2 \bmod p$$

In either case, the values match.

///

Proof of theorem about $\left(\frac{2}{p}\right)_2$

This discussion will take place inside the *ring*

$$\mathbf{Z}[i] = \{a + bi : a, b \in \mathbf{Z}\}$$

where $i = \sqrt{-1}$. *It should be striking that we use complex numbers to prove something about ordinary integers.*

Note that while only the integers ± 1 have multiplicative inverses in $\mathbf{Z}$, in $\mathbf{Z}[i]$ there are *four* things with this property, ± 1 and $\pm i$. These are called **units** in the ring $\mathbf{Z}[i]$.

The integer 2, which is *prime* in $\mathbf{Z}$, actually *factors* in $\mathbf{Z}[i]$

$$2 = -i \cdot (1 + i)^2$$

That is, except for the *unit* i, 2 is a *square* in $\mathbf{Z}[i]$. This will be used in a critical way!

Now we will look at equalities modulo p of elements of $\mathbf{Z}[i]$, not just elements of $\mathbf{Z}$.

Modulo p

$$\left(\frac{2}{p}\right)_2 = 2^{(p-1)/2} = (-i(1+i)^2)^{(p-1)/2}$$

$$= (-i)^{(p-1)/2} \cdot (1+i)^{p-1} \bmod p$$

Multiply both sides by $1+i$ to obtain

$$(1+i)\left(\frac{2}{p}\right)_2 = (-i)^{(p-1)/2} \cdot (1+i)^p \bmod p$$

Note that we have used the expression of 2 as very nearly a square in $\mathbf{Z}[i]$ to get to the relatively simple expression $(1+i)^p$, which we now exploit.

Use the Binomial Theorem to expand

$$(1+i)^p = 1 + \binom{p}{1} i + \ldots + \binom{p}{p-1} i^{p-1} + i^p$$

Since the inner binomial coefficients are all $0 \bmod p$ (this uses the primality of p)

$$(1+i)^p = 1 + i^p \bmod p$$

Thus, so far,

$$(1+i)\left(\frac{2}{p}\right)_2 = (-i)^{(p-1)/2} \cdot (1+i^p) \bmod p$$

Apparently, from the left-hand side, the right hand side is $\pm(1+i)$. By direct computation

$$(-i)^{\frac{p-1}{2}}(1+i^p) = \begin{cases} 1+i & p = 1 \bmod 8) \\ -i(1-i) & p = 3 \bmod 8) \\ -(1+i) & p = 5 \bmod 8) \\ i(1-i) & p = 7 \bmod 8) \end{cases}$$

That is, simplifying a little,

$$(-i)^{\frac{p-1}{2}}(1+i^p) = \begin{cases} 1+i & p=1 \bmod 8) \\ -(1+i) & p=3 \bmod 8) \\ -(1+i) & p=5 \bmod 8) \\ 1+i & p=7 \bmod 8) \end{cases}$$

Thus,

$$(1+i)\left(\frac{2}{p}\right)_2 = \begin{cases} 1+i & p=1 \bmod 8) \\ -(1+i) & p=3 \bmod 8) \\ -(1+i) & p=5 \bmod 8) \\ 1+i & p=7 \bmod 8) \end{cases}$$

Since $p > 2$, this implies that

$$\left(\frac{2}{p}\right)_2 = \begin{cases} 1 & p=1 \bmod 8) \\ -1 & p=3 \bmod 8) \\ -1 & p=5 \bmod 8) \\ 1 & p=7 \bmod 8) \end{cases}$$

proving the *supplement* to Quadratic Reciprocity. ///

Remark: No, there was no obvious reason to get $\mathbf{Z}[i]$ involved! It was probably only because Gauss had been investigating $\mathbf{Z}[i]$ for other reasons, and surely observed that 2 essentially became a square in $\mathbf{Z}[i]$, that he may have been inspired to pursue this line. Gauss had studied many other rings $\mathbf{Z}[\sqrt{d}]$ where d is a non-square integer.

For example, already by about 1650 Fermat had studied the number of ways to represent an integer as a sum of two squares

$$n = a^2 + b^2$$

Using $\mathbf{Z}[i]$, we can factor the right hand side

$$n = a^2 + b^2 = (a+bi)(a-bi) = (a+bi)\overline{(a+bi)}$$

From this observation it is easy to derive the fact that *if m and n are both expressible as a sum of two squares, then so is mn.*

From $m = a^2 + b^2$ and $n = c^2 + d^2$, using the property of complex conjugation that

$$\overline{\alpha \cdot \beta} = \overline{\alpha} \cdot \overline{\beta}$$

compute

$$mn = (a^2 + b^2)(c^2 + d^2)$$

$$= (a + bi)\overline{(a + bi)}(c + di)\overline{(c + di)}$$

$$= (a + bi)(c + di) \cdot \overline{(a + bi)(c + di)}$$

$$= [(ac - bd) + i(bc + ad)] \cdot \overline{[(ac - bd) + i(bc + ad)]}$$

$$= (ac - bd)^2 + (bc + ad)^2$$

This formula would be wretchedly obscure otherwise.

Now return to proof of the main part of quadratic reciprocity.

As we used $\mathbf{Z}[i]$ to express 2 as something nearly a square, we will do a similar thing for an odd prime p. Again, we use complex numbers, and in particular a p^{th} *root of unity*

$$\zeta_p = \cos\frac{2\pi}{p} + i\,\sin\frac{2\pi}{p} = e^{\frac{2\pi i}{p}}$$

Note that for any integer

$$\zeta_p^k = \cos\frac{2\pi k}{p} + i\,\sin\frac{2\pi k}{p} = e^{\frac{2\pi ik}{p}}$$

Define a (quadratic) **Gauss sum**

$$\gamma_p = \sum_{x \bmod p} \zeta_p^x \left(\frac{x}{p}\right)_2 = \sum_{x\neq 0 \bmod p} \zeta_p^x \left(\frac{x}{p}\right)_2$$

It is totally unclear from the definition itself what kind of number this is.

We need

Lemma:

$$\left(\frac{ab}{p}\right)_2 = \left(\frac{a}{p}\right)_2 \left(\frac{b}{p}\right)_2$$

Proof: From Euler's criterion

$$\left(\frac{c}{p}\right)_2 = c^{(p-1)/2} \bmod p$$

and the latter expression has the indicated multiplicative property. ///

Remark: The latter *multiplicativity* is a key property of the quadratic symbol.

Lemma: For odd prime p

$$\left(\frac{-1}{p}\right)_2 = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & p = 1 \bmod 4 \\ -1 & p = 3 \bmod 4 \end{cases}$$

The following lemma is a prototype for many cancellation mechanisms throughout number theory, algebra, harmonic analysis, and other parts of mathematics.

Lemma:

$$\sum_{x \bmod p} \left(\frac{x}{p}\right)_2 = 0$$

Proof: Let $y \neq 0 \bmod p$. Then y has a multiplicative inverse mod p, and therefore the map $x \to xy$ is a *bijection* of $\mathbf{Z}/p$ to itself. Take y to be a non-square mod p. Then, by the observation about $x \to xy$ just made

$$\sum_{x \bmod p} \left(\frac{x}{p}\right)_2 = \sum_{x \bmod p} \left(\frac{xy}{p}\right)_2$$

By the multiplicativity of the quadratic symbol

$$\sum_{x \bmod p} \left(\frac{xy}{p}\right)_2 = \left(\frac{y}{p}\right)_2 \sum_{x \bmod p} \left(\frac{x}{p}\right)_2$$

Thus,

$$\sum_{x \bmod p} \left(\frac{x}{p}\right)_2 = \left(\frac{y}{p}\right)_2 \cdot \sum_{x \bmod p} \left(\frac{x}{p}\right)_2$$

In general, in the complex numbers, if $S = -S$ then $S = 0$. Thus,

$$\sum_{x \bmod p} \left(\frac{x}{p}\right)_2 = 0$$

as claimed. ///

Remark: We could also reach the same conclusion by talking about the number of squares and non-squares mod p, but that vanishing occurs for a more general abstract reason, as the next lemma illustrates further.

Another cancellation lemma.

Lemma: Let y be an integer.

$$\sum_{x \bmod p} \zeta_p^{xy} = \begin{cases} 0 & (\text{for } y \neq 0 \bmod p) \\ p & (\text{for } y = 0 \bmod p) \end{cases}$$

Proof: Certainly if $y = 0 \bmod p$, then $\zeta_p^y = 1$, and the second equality follows. Now suppose $y \neq 0 \bmod p$. Then $\zeta_p^y \neq 1$.

The map $x \to x + 1$ permutes the set $\mathbf{Z}/p$. Thus

$$\sum_{x \bmod p} \zeta_p^{xy} = \sum_{x \bmod p} \zeta_p^{(x+1)y} = \zeta_p^y \cdot \sum_{x \bmod p} \zeta_p^{xy}$$

Thus,

$$(1 - \zeta_p^y) \cdot \sum_{x \bmod p} \zeta_p^{xy} = 0$$

from which

$$\sum_{x \bmod p} \zeta_p^{xy} = 0$$

as asserted. ///

Surprisingly, we have

Lemma: $|\gamma|^2 = p$. In particular, γ is not 0. Further,

$$\gamma^2 = \left(\frac{-1}{p}\right)_2 \cdot p$$

Proof: Note that

$$\overline{\zeta_p} = \zeta_p^{-1}$$

Then compute

$$|\gamma|^2 = \sum_{x,y \neq 0 \bmod p} \zeta_p^x \left(\frac{x}{p}\right)_2 \zeta_p^{-y} \left(\frac{y}{p}\right)_2$$

$$= \sum_{x,y} \zeta_p^{x-y} \left(\frac{xy}{p}\right)_2$$

Replace x by xy to get

$$|\gamma|^2 = \sum_{x,y \bmod p} \zeta_p^{y(x-1)} \left(\frac{xy^2}{p}\right)_2$$
$$= \sum_x \left(\frac{x}{p}\right)_2 \sum_{y \neq 0} \zeta_p^{y(x-1)}$$

For $x = 1$, the inner sum over y is $p-1$. For $x \neq 1$, the cancellation lemma shows that the sum over *all* y mod p is 0, but we're missing the $y = 0$ term, so the sum is -1 instead. Thus

$$\sum_{x,y \neq 0 \bmod p} \zeta_p^{y(x-1)} \left(\frac{x}{p}\right)_2$$
$$= (p-1) \sum_{x=1} \left(\frac{x}{p}\right)_2 - \sum_{x \neq 1} \left(\frac{x}{p}\right)_2$$
$$= p - \sum_{\text{all} x} \left(\frac{x}{p}\right)_2 = p$$

by the other cancellation lemma. Thus, $|\gamma|^2 = p$.

Similarly, with just a little sign change in front of the y,

$$\gamma^2 = \sum_{x,y \neq 0 \bmod p} \zeta_p^x \left(\frac{x}{p}\right)_2 \zeta_p^y \left(\frac{y}{p}\right)_2$$

$$= \sum_{x,y} \zeta_p^{x+y} \left(\frac{xy}{p}\right)_2$$

Replace x by xy to get

$$\gamma^2 = \sum_{x,y \bmod p} \zeta_p^{y(x+1)} \left(\frac{xy^2}{p}\right)_2$$

$$= \sum_x \left(\frac{x}{p}\right)_2 \sum_{y \neq 0} \zeta_p^{y(x+1)}$$

For $x = -1$, the inner sum over y is $p - 1$. For $x \neq -1$, the cancellation lemma shows that the sum over *all* y mod p is 0, but

we're missing the $y = 0$ term, so the sum is -1 instead. Thus

$$\sum_{x,y \neq 0 \bmod p} \zeta_p^{y(x-1)} \left(\frac{x}{p}\right)_2$$

$$= (p-1) \sum_{x=-1} \left(\frac{x}{p}\right)_2 - \sum_{x \neq 1} \left(\frac{x}{p}\right)_2$$

$$= p \left(\frac{-1}{p}\right)_2 - \sum_{\text{all} x} \left(\frac{x}{p}\right)_2 = p \left(\frac{-1}{p}\right)_2$$

by the other cancellation lemma. Thus, $\gamma^2 = p \left(\frac{-1}{p}\right)_2$. ///

The main proof: From Euler's criterion,

$$\left(\frac{p}{q}\right)_2 = p^{(q-1)/2} \bmod q$$

$$= \left(\left(\frac{-1}{p}\right)_2 \gamma^2\right)^{(q-1)/2}$$

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

$$= (-1)^{(p-1)(q-1)/4} \cdot \gamma^{q-1}$$

Multiply both sides by γ

$$\gamma \cdot \left(\frac{p}{q}\right)_2 = (-1)^{(p-1)(q-1)/4} \cdot \gamma^q$$

Now modulo q, since the inner multinomial coefficients are divisible by the prime q

$$\gamma^q = \sum_{x \bmod p} \zeta^{xq} \left(\frac{x}{p}\right)_2^q$$

$$= \sum_{x \bmod p} \zeta^{xq} \left(\frac{x}{p}\right)_2$$

since q is odd.

Replace x by $xq^{-1} \bmod p$ to obtain

$$\sum_{x \bmod p} \zeta^{xq} \left(\frac{x}{p}\right)_2 = \sum_{x \bmod p} \zeta^{x} \left(\frac{xq^{-1}}{p}\right)_2$$

$$= \left(\frac{q^{-1}}{p}\right)_2 \sum_{x \bmod p} \zeta^{x} \left(\frac{x}{p}\right)_2 = \left(\frac{q}{p}\right)_2 \cdot \gamma$$

since q^{-1} is a square if and only if q is. In summary, modulo q

$$\gamma \cdot \left(\frac{p}{q}\right)_2 = (-1)^{(p-1)(q-1)/4} \left(\frac{q}{p}\right)_2 \cdot \gamma$$

We should not be too hasty to 'cancel' the γ. Instead, multiply through by $\overline{\gamma}$ to get

$$p \cdot \left(\frac{p}{q}\right)_2 = (-1)^{(p-1)(q-1)/4} \left(\frac{q}{p}\right)_2 \cdot p \bmod q$$

Since p is invertible mod q, we can cancel

$$\left(\frac{p}{q}\right)_2 = (-1)^{(p-1)(q-1)/4} \left(\frac{q}{p}\right)_2 \bmod q$$

which is Quadratic Reciprocity. ///