Quadratic Reciprocity

Theorem. (**Gauss's Lemma**) Let p be an odd prime, $(a, p) = 1$. Let k be the number of least positive residues of

$$a, 2a, \ldots, \frac{p-1}{2}a \quad \text{greater than} \quad \frac{p}{2}.$$

Then

$$\left(\frac{a}{p}\right) = (-1)^k.$$

Proof. Since p is odd, $\dfrac{p}{2}$ is not an integer. Hence, every residue of a, $2a$, $\ldots$, $\dfrac{p-1}{2}a$ is either less than $\dfrac{p}{2}$ or greater than $\dfrac{p}{2}$. Label these two sets:

$$a_1, \ldots, a_j < \frac{p}{2}, \quad b_1, \ldots, b_k > \frac{p}{2}.$$

Thus, $j + k = \dfrac{p-1}{2}$.

Step 1 $\{p - b_1, \ldots, p - b_k, a_1, \ldots, a_j\} = \left\{1, 2, \ldots, \dfrac{p-1}{2}\right\}$.

The a_i's are contained in $\left\{1, 2, \ldots, \dfrac{p-1}{2}\right\}$, because the a_i's are less than $\dfrac{p}{2}$ (so less than or equal to $\dfrac{p-1}{2}$).

What about the $p - b_i$'s?

$$b_i > \frac{p}{2}, \quad \text{so} \quad p - b_i < p - \frac{p}{2} = \frac{p}{2}.$$

Since $p - b_i$ is an integer and $\dfrac{p}{2}$ is an integer plus one-half, I have $p - b_i \le \dfrac{p-1}{2}$. This shows that the $p - b_i$'s are contained in $\left\{1, 2, \ldots, \dfrac{p-1}{2}\right\}$ as well.

There are $\dfrac{p-1}{2}$ elements in $\left\{1, 2, \ldots, \dfrac{p-1}{2}\right\}$, and $j + k = \dfrac{p-1}{2}$. So if the a_i's and $p - b_i$'s are all distinct, I'll know the two sets are equal.

Each a_i has the form ra, where $1 \le r \le \dfrac{p-1}{2}$. So if ra and sa are the same, then

$$ra = sa \pmod{p}, \quad \text{so} \quad p \mid (r - s)a.$$

$p \not| a$, so $p \mid (r - s)$. This is impossible for $1 \le r, s \le \dfrac{p-1}{2}$ unless $r = s$ — which implies $ra = sa$ to begin with.

A similar argument shows that the b_i's, and hence the $p - b_i$'s, are distinct.

Could $a_i = p - b_h$? $a_i = ra$ and $p - b_h = p - sa$ for $1 \le r, s \le \dfrac{p-1}{2}$, so

$$p - sa = ra \pmod{p}, \quad ra + sa = 0 \pmod{p}, \quad p \mid (r + s)a.$$

Again, $p \not| a$, so $p \mid (r + s)$. But $1 \le r, s \le \dfrac{p-1}{2}$ implies $2 \le r + s \le p - 1$, so $p \mid (r + s)$ is impossible.

This finishes the proof that $\{p - b_1, \ldots, p - b_k, a_1, \ldots, a_j\} = \left\{1, 2, \ldots, \dfrac{p-1}{2}\right\}$.

Step 2 Since the two sets are the same, the products of the elements in the two sets are the same:

$$(p-b_1)\cdots(p-b_k)\cdot a_1\cdots a_j = \left(\frac{p-1}{2}\right)! \pmod p.$$

Now $p - b_i = -b_i \pmod p$, so

$$(-1)^k b_1\cdots b_k\cdot a_1\cdots a_j = \left(\frac{p-1}{2}\right)! \pmod p.$$

But the a's and b's are exactly the residues of the numbers $a, 2a, \ldots, \dfrac{p-1}{2}a$, so I may replace the product of the a's and b's with the product of $a, 2a, \ldots, \dfrac{p-1}{2}a$:

$$\begin{aligned} (-1)^k a\cdot 2a\cdots\left(\frac{p-1}{2}\right)a &= \left(\frac{p-1}{2}\right)! \pmod p \\ (-1)^k a^{(p-1)/2}\left(\frac{p-1}{2}\right)! &= \left(\frac{p-1}{2}\right)! \pmod p \end{aligned}$$

Now $\left(p, \dfrac{p-1}{2}\right) = 1$, so I can cancel the $\left(\dfrac{p-1}{2}\right)!$ terms from both sides. Then applying Euler's theorem, I get

$$\begin{aligned} (-1)^k a^{(p-1)/2} &= 1 \pmod p \\ (-1)^k \left(\frac{a}{p}\right) &= 1 \pmod p \\ \left(\frac{a}{p}\right) &= (-1)^k \pmod p \end{aligned}$$

I made the last step by multiplying both sides by $(-1)^k$ and using the fact that $(-1)^{2k} = 1$. □

Example. Use Gauss's Lemma to compute $\left(\dfrac{6}{7}\right)$.

Since $p = 7$, I have $\dfrac{p}{2} = 3.5$ and $\dfrac{p-1}{2} = 3$. Look at the residues $1\cdot 6 = 6$, $2\cdot 6 = 5$, and $3\cdot 6 = 4$. All three are greater than 3.5 — they're b_i's, in the notation of the proof of Gauss's Lemma — so Gauss's Lemma says

$$\left(\frac{6}{7}\right) = (-1)^3 = -1.$$

As a check, Euler's theorem gives $\left(\dfrac{6}{7}\right) = 6^3 = -1 \pmod 7$. □

The following technical lemma will be needed for the proof of reciprocity.

Lemma. Let $a, b > 0$, where b is an odd integer. Then

$$a = b\cdot\left(\left[\frac{a}{b}\right] + e\right) + (-1)^e\cdot r \quad \text{for} \quad e = 0 \quad \text{or} \quad 1, \quad 0 \le r \le \frac{b-1}{2}.$$

Here $[\cdot]$ denotes the greatest integer function and $\left[\dfrac{a}{b}\right] + e$ is the integer closest to $\dfrac{a}{b}$.

Proof. By the Division Algorithm,

$$a = bq + r, \text{ where } 0 \le r < b.$$

Now $\dfrac{b}{2}$ is not an integer, so either $r < \dfrac{b}{2}$ or $r > \dfrac{b}{2}$.

(For example, if $a = 11$ and $b = 3$, then $r = 2 > \dfrac{3}{2} = \dfrac{b}{2}$, while if $a = 11$ and $b = 5$, $r = 1 < \dfrac{5}{2} = \dfrac{b}{2}$.)

Consider the two cases.

Case 1: $r < \dfrac{b}{2}$.

Write

$$a = b \cdot \left(\left[\frac{a}{b}\right] + 0\right) + (-1)^0 \cdot r.$$

Here $e = 0$, and $\left[\dfrac{a}{b}\right] + 0$ is the integer closest to $\dfrac{a}{b}$. $r < \dfrac{b}{2}$, but $\dfrac{b}{2}$ is not an integer, so $r \le \dfrac{b-1}{2}$, and $0 \le r \le \dfrac{b-1}{2}$.

Case 2: $r > \dfrac{b}{2}$.

Write

$$a = b \cdot \left(\left[\frac{a}{b}\right] + 1\right) + (r - b) = b \cdot \left(\left[\frac{a}{b}\right] + 1\right) + (-1)^1 \cdot (b - r).$$

Here $e = 1$, and $\left[\dfrac{a}{b}\right] + 1$ is the integer closest to $\dfrac{a}{b}$. $r < b$, so $b - r > 0$. Now $r > \dfrac{b}{2}$, so $-r < -\dfrac{b}{2}$, or $b - r < b - \dfrac{b}{2} = \dfrac{b}{2}$. Since $\dfrac{b}{2}$ is not an integer, $b - r \le \dfrac{b-1}{2}$. Therefore, $0 \le r \le \dfrac{b-1}{2}$. □

Example. Illustrate the lemma with:

(a) $a = 42$ and $b = 17$.

(b) $a = 50$ and $b = 17$.

(a) For $a = 42$ and $b = 17$, I have $\dfrac{42}{17} \approx 2.47$, so the integer closest to $\dfrac{42}{17}$ is 2. Then

$$42 = 17 \cdot 2 + 8.$$

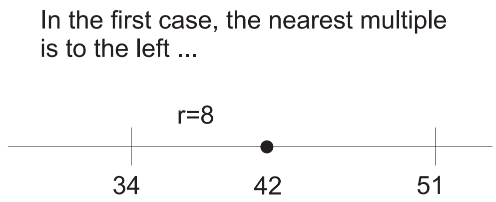
And $0 \le 8 \le \dfrac{17-1}{2}$. □

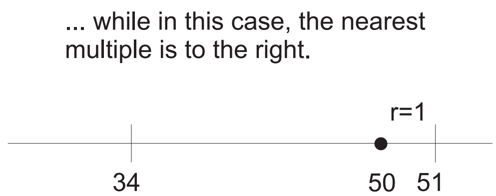
(b) For $a = 50$ and $b = 17$, I have $\dfrac{50}{17} = 2.94$, so the integer closest to $\dfrac{50}{17}$ is 3. Then

$$50 = 17 \cdot 3 + (-1) \cdot 1.$$

And $0 \le 1 \le \dfrac{17-1}{2}$. □

In other words, the r in the lemma represents the distance from a to the *nearest* multiple of b.





The $\pm$ is needed depending on whether the nearest multiple is less than or greater than a.

I'll use the lemma to give an ingenious proof of Quadratic Reciprocity due to J.S. Frame [1].

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

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

Proof. To simplify the writing, let $p' = \dfrac{p-1}{2}$ and $q' = \dfrac{q-1}{2}$.

Let $1 \le n \le q'$. Apply the Lemma with $a = np$ and $b = q$:

$$np = q \cdot \left(\left[\frac{np}{q}\right] + e_n\right) + (-1)^{e_n} r_n.$$

Here $1 \le r_n \le q'$ and $e_n = 0$ or 1.

The first thing I will show is that the remainders r_n are just a permutation of the integers 1, ..., q'.

If I take the initial equation and reduce mod q, I get

$$np = (-1)^{e_n} r_n \pmod{q}.$$

Can two of the r's be equal? Suppose $r_m = r_n$, where $1 \le m, n \le q'$. Then

$$0 = r_m - r_n = ((-1)^{e_m} m - (-1)^{e_n} n)\, p \pmod{q}.$$

In other words, $q \mid ((-1)^{e_m} m - (-1)^{e_n} n)\, p$. But $m + n \le 2q' = q - 1$, so $(-1)^{e_m} m - (-1)^{e_n} n$ is surely smaller than q in absolute value. Since $q \not| p$, this is impossible unless $(-1)^{e_m} m - (-1)^{e_n} n = 0$. This in turn is impossible unless $m = n$. Thus, the r's are distinct. Since there are q' of them, and since they're all in the range $[1, q']$, they must be some permutation of the numbers 1, ..., q'.

As a preliminary to the next computation, take the first equation and reduce mod 2. Now p and q are odd, so they equal 1 mod 2. Also, $(-1)^{e_n} = \pm 1$, and it both cases $(-1)^{e_n} = 1 \pmod{2}$. Therefore,

$$n = \left[\frac{np}{q}\right] + e_n + r_n \pmod{2}.$$

(I'm going to use this in an exponent of -1 in a second!)

Now let $1 \le m \le p'$, $1 \le n \le q'$. Then $mq - np \ne 0$, for $mq = np$ implies $p \mid m$ — which is impossible, because $1 \le m \le p' = \dfrac{p-1}{2}$.

Now here's the heart of the proof. The idea will be to define a weird product which turns out to be the Legendre symbol. Define

$$f(p,q) = \prod_{m=1}^{p'} \prod_{n=1}^{q'} \frac{mq - np}{|mq - np|}.$$

Notice that $\dfrac{mq - np}{|mq - np|}$ is a fancy way of expressing the *sign* of $mq - np$ — $+1$ when it's positive, -1 when it's negative.

When is $mq - np$ negative?

$$\begin{aligned} mq - np &< 0 \\ mq &< np \\ m &< \frac{np}{q} \\ m &\le \left[\frac{np}{q}\right] \end{aligned}$$

That is, $mq - np$ is negative for $m = 1, \ldots, \left[\dfrac{np}{q}\right]$. So the product for $f(p,q)$ for fixed n has $\left[\dfrac{np}{q}\right]$ terms equal to -1, and

$$f(p,q) = \prod_{n=1}^{q'} (-1)^{[np/q]}.$$

(The terms equal to 1 contribute nothing to the product.)

Now

$$\begin{aligned} n &= \left[\frac{np}{q}\right] + e_n + r_n \pmod 2 \\ n - r_n - e_n &= \left[\frac{np}{q}\right] \pmod 2 \\ n - r_n + e_n &= \left[\frac{np}{q}\right] \pmod 2 \end{aligned}$$

The last equality comes from the fact that $-e_n = e_n \pmod 2$.

Now if $a = b \pmod 2$ then $(-1)^a = (-1)^b$. So

$$f(p,q) = \prod_{n=1}^{q'} (-1)^{n - r_n + e_n} = \prod_{n=1}^{q'} (-1)^{n - r_n} (-1)^{e_n} = (-1)^{\sum_{n=1}^{q'} (n - r_n)} \prod_{n=1}^{q'} (-1)^{e_n}.$$

Since the r_n's are just the integers from 1 to q' and since n runs from 1 to q', the sum of the r_n's is the same as the sum of the n's from 1 to q', and

$$\sum_{n=1}^{q'} (n - r_n) = \sum_{n=1}^{q'} n - \sum_{n=1}^{q'} r_n = 0.$$

So the previous equation becomes

$$f(p,q) = \prod_{n=1}^{q'} (-1)^{e_n}.$$

Recall from above that

$$np = (-1)^{e_n} r_n \pmod q.$$

Now r_n is invertible mod q, so I may write

$$\frac{np}{r_n} = (-1)^{e_n} \pmod{q}.$$

Plugging this into the last equation for $f(p,q)$, I get

$$f(p,q) = \prod_{n=1}^{q'} \frac{np}{r_n} \pmod{q}.$$

But $\displaystyle\prod_{n=1}^{q'} \frac{n}{r_n} = 1$, because as n runs over the numbers from 1 to q', so does r_n. So by Euler's theorem,

$$f(p,q) = \prod_{n=1}^{q'} p = p^{q'} = \left(\frac{p}{q}\right).$$

Notice that

$$f(q,p) = \prod_{m=1}^{q'} \prod_{n=1}^{p'} \frac{mp - nq}{|mp - nq|} = \prod_{m=1}^{p'} \prod_{n=1}^{q'} \frac{np - mq}{|np - mq|}.$$

I got the second product by swapping m and n in the first.

Whew! The rest is easy — fortunately!

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = f(p,q)f(q,p) = \prod_{m=1}^{p'} \prod_{n=1}^{q'} \frac{mq - np}{|mq - np|}\,\frac{np - mq}{|np - mq|} = \prod_{m=1}^{p'} \prod_{n=1}^{q'} (-1) = (-1)^{p'q'}.$$

Since $p' = \dfrac{p-1}{2}$ and $q' = \dfrac{q-1}{2}$, I'm done! □

As complicated as this proof is, it's actually no worse than most proofs of this result.

Before giving an example, I want to discuss what reciprocity tells you about solutions to quadratic congruences.

An odd prime p is congruent to 1 or to 3 mod 4.

If $p = 4k+1$, then $\dfrac{p-1}{2} = 2k$, an even number. If $p = 4k+3$, then $\dfrac{p-1}{2} = 2k+1$, an odd number.

Since an even number times anything is even,

$$\frac{p-1}{2} \cdot \frac{q-1}{2} = \begin{cases} \text{even} & \text{if } p \text{ or } q = 1 \pmod{4} \\ \text{odd} & \text{if } p \text{ and } q = 3 \pmod{4} \end{cases}$$

Therefore,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = \begin{cases} +1 & \text{if } p \text{ or } q = 1 \pmod{4} \\ -1 & \text{if } p \text{ and } q = 3 \pmod{4} \end{cases}$$

However,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = +1 \quad \text{means} \quad \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = 1 \quad \text{or} \quad \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = -1$$

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1 \quad \text{means one of} \quad \left(\frac{p}{q}\right), \left(\frac{q}{p}\right) \quad \text{is} \quad +1 \quad \text{and the other is} \quad -1$$

Consider the congruences

$$x^2 = p \pmod{q} \quad \text{and} \quad x^2 = q \pmod{p}.$$

This means:

1. If at least one of p, q is congruent to 1 mod 4, then both equations are solvable or both equations are unsolvable.

2. If both p and q are congruent to 3 mod 4, then one equation is solvable and the other is unsolvable.

Corollary. Let p and q be distinct odd primes.

(a) If at least one of p, q is congruent to 1 mod 4, then

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

(b) If both p and q are congruent to 3 mod 4, then

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right). \quad \square$$

Example. Compute $\left(\frac{17}{71}\right)$.

$17 = 1 \pmod 4$, so

$$\left(\frac{17}{71}\right) = \left(\frac{71}{17}\right) = \left(\frac{3}{17}\right) = \left(\frac{17}{3}\right) = \left(\frac{2}{3}\right) = 2^{(3-1)/2} = 2 = -1 \pmod 3.$$

In other words, $x^2 = 17 \pmod{71}$ does not have any solutions. $\square$

Example. Compute $\left(\frac{299}{359}\right)$.

$$\left(\frac{299}{359}\right) = \left(\frac{13}{359}\right)\left(\frac{23}{359}\right).$$

I'll compute $\left(\frac{13}{359}\right)$ and $\left(\frac{23}{359}\right)$. First,

$$\left(\frac{13}{359}\right) = \left(\frac{359}{13}\right) = \left(\frac{8}{13}\right) = 8^{(13-1)/2} = 8^6 = 262144 = -1 \pmod{13}.$$

Next,

$$\left(\frac{23}{359}\right) = -\left(\frac{359}{23}\right) = -\left(\frac{14}{23}\right) = -\left(\frac{2}{23}\right)\left(\frac{7}{23}\right).$$

Next, I'll compute $\left(\frac{2}{23}\right)$ and $\left(\frac{7}{23}\right)$.

$$\left(\frac{2}{23}\right) = 2^{(23-1)/2} = 2^{11} = 2048 = 1 \pmod{23}.$$

$$\left(\frac{7}{23}\right) = -\left(\frac{23}{7}\right) = -\left(\frac{2}{7}\right) = -(2^{(7-1)/2}) = -8 = -1 \pmod 7.$$

Therefore, $\left(\dfrac{23}{359}\right) = -(1)(-1) = 1$, and

$$\left(\frac{299}{359}\right) = (-1)(1) = -1.$$

In other words, the congruence $x^2 = 299 \pmod{359}$ does not have a solution. $\square$

[1] J.S. Frame, A short proof of quadratic reciprocity, *Amer. Math. Monthly*, 85(10)(1978), 818–819.