* .I Zolotareff's Proof of Quadratic Reciprocity

This proof requires a fair amount of preparations on permutations and their signs. Most of the material will be familiar to those who have taken a course in Abstract Algebra. However, for the convenience of the reader I include a full discussion of the algebraic prerequisites.

A *permutation* of a finite set is the same as a bijective function. The elements of the set will be often be denoted $1, 2, 3, \ldots n$ or $0, 1, 2, \ldots n-1$. The latter notation will be the most natural in dealing with residue classes mod n, for instance.

Permutations are often notated like this:

$$s : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}$$

Each element in the second row is the image of the one above it, that is, $s(1) = 2, s(2) = 1, s(3) = 4, s(4) = 5, s(5) = 3$.

The product of two permutations is defined as their composition: $st(m) = s(t(m))$. The product of s taken d times is of course denoted s^d. The inverse permutation is denoted s^{-1}. It can be visualized by swapping the two rows in the representation above, and permuting the columns so as to get the first row in straight order:

$$s^{-1} : \begin{pmatrix} 2 & 1 & 4 & 5 & 3 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \end{pmatrix}$$

As there are finitely many permutations on a finite set, for a given s two powers must be equal: $s^d = s^e$, $d < e$. Multiplying by $s^{-d} = (s^{-1})^d$ gives $s^{e-d} = \mathrm{id}$, the identical permutation, $\mathrm{id}(m) = m$.

The least positive k with $s^k = \mathrm{id}$ is called the *order* of s. The reader is invited to check that the order of the s given above is 6.

We have already encountered the inverse of s If the order of s is d, so that $s^d = \mathrm{id}$, then $s^{-1} = s^{d-1}$.

A permutation on a set partitions the set into disjoint *orbits*.

The elements m, n belong to the same orbit if $n = s^k(m)$ for some non-negative k. The reader familiar with the concept will easily check that this is

an equivalence relation. For instance, symmetry follows as $n = s^k(m) \iff m = s^{d-k}(n)$, where d is the order of s.

The elements of one orbit are permutated *cyclically*. Imagine them arranged in a circular fashion with the permutation acting counter-clock-wise, mapping one element to the next along the circle.

In our example, one orbit is 1, 2: $s(1) = 2$, $s(2) = 1$. We use the notation $s = (1\,2)$ to describe this permutation. It could also be written $(2\,1)$.

There is one other orbit, 3, 4, 5: $s(3) = 4$, $s(4) = 5, s(5) = 3$, denoted by $s = (3\,4\,5) = (4\,5\,3) = (5\,3\,4)$. Then s is the product of these two in arbitrary order: $s = (1\,2)(3\,4\,5) = (3\,4\,5)(1\,2)$ (the right factor acts first). The two cycles commute, because they are disjoint.

We now define the *sign* of a permutation. It is commonly defined as $(-1)^N$ where N is the number of *inversions*, the number of times a larger number precedes a smaller number in the second row of the matrix described above.

In our example the inversions are $2 = s(1) > s(2) = 1)$, $4 = s(3) > s(4) = 3$, and $5 = s(4) > s(5) = 3$. Their number is odd, hence the sign is -1. The cyclic permutation $(3\,4\,5)$ has two inversions: $4 = s(3) > s(5) = 3$, $5 = s(4) > s(5) = 3$. Their number is even, hence the sign $+1$.

We use the terms *odd* and *even* for permutations having sign -1 or $+1$, respectively.

We now determine the sign of a product.

Let us introduce the expression

$$\Delta = \prod_{n \geq k > j \geq 1} (X_k - X_j)$$

where the X_j are indeterminates, and the elements of the set are notated $1, 2, \ldots, n$.

Set

$$\Delta^s = \prod (X_{s(k)} - X_{s(j)}).$$

Each factor of the first product enters this second product exactly once, possibly with the opposite sign. The number of factors in either case is $n(n-1)/2$.

Therefore

$$\Delta^s = \pm\Delta.$$

Each factor $(X_{s(k)} - X_{s(j)})$ having $s(k) < s(j)$ contributes a minus sign to the product, the remaining factors a plus sign. The number of minus signs therefore equals the number of inversions, that is:

$$\Delta^s = \text{sign}(s)\Delta$$

where $\text{sign}(s)$ denotes the sign of s.

For instance, for $s = (1\,2\,3)$ $(n = 3)$ we have

$$\Delta = (X_3 - X_1)(X_3 - X_2)(X_2 - X_1)$$

and

$$\Delta^s = (X_1 - X_2)(X_1 - X_3)(X_3 - X_2) = (-1)^2\Delta = \Delta.$$

For $s = (1\,2)$ the reader easily checks that $\Delta^s = -\Delta$.

.I.1 Lemma. *sign*$(st) =$ *sign*(s)*sign*(t).

Proof. By definition, $\Delta^t = \text{sign}(t)\Delta$. Then also

$$\Delta^{st} = \prod(X_{st(k)} - X_{st(j)}) = \big(\prod(X_{t(k)} - X_{t(j)})\big)^s = (\Delta^t)^s$$

(note that t acts first) so that

$$\begin{aligned}\text{sign}(st) = \frac{\Delta^{st}}{\Delta} = \frac{\Delta^{st}}{\Delta^t}\cdot\frac{\Delta^t}{\Delta} = \frac{(\Delta^t)^s}{\Delta^t}\cdot\frac{\Delta^t}{\Delta} = \frac{(\pm\Delta)^s}{\pm\Delta}\cdot\frac{\Delta^t}{\Delta}\\ = \frac{\Delta^s}{\Delta}\cdot\frac{\Delta^t}{\Delta} = \text{sign}(s)\cdot\text{sign}(t).\end{aligned}$$

□

.I.2 Corollary. *A permutation and its inverse have the same sign.*

Proof. Apply the product rule just derived to

$$s^{-1}s = \text{id}$$

and use the fact that id is even as it has no inversions at all. □

We now determine the signs of cyclic permutations. Once they are known, we can determine the sign of *any* permutation by decomposing it into disjoint cycles.

.I.3 Lemma. *The sign of a simple transposition (2-cycle)* $(i \quad i+1)$ *is* -1.

Proof. There is exactly one inversion. □

.I.4 Lemma. *The sign of an arbitrary transposition* $(i \quad i+m)$ *is also* -1.

Proof. We need to prove that the given transposition is the product of an odd number of simple ones.

This follows easily by induction once we prove:

$$(i \quad i+k+1) = (i+k \quad i+k+1)(i \quad i+k)(i+k \quad i+k+1)$$

We only have to check the product action, in three steps, on the three elements entering the parentheses.

$$\begin{array}{ccccccccc} i+k+1 & \to & i+k & \to & i & \to & i \\ i+k & \to & i+k+1 & \to & i+k+1 & \to & i+k \\ i & \to & i & \to & i+k & \to & i+k+1 \end{array}$$

□

We finally deal with cycles of arbitrary length:

.I.5 Lemma. *The sign of a* k*-cycle* $(p_1\, p_2\, \ldots\, p_k)$ *is* $(-1)^{k+1}$. *That is, a cycle of even length is an odd permutation, a cycle of odd length is even.*

Proof. This follows easily by induction from the case $k = 2$ just proved, and the following relation:

$$(p_1\, p_2\, \ldots\, p_{k+1}) = (p_1\, p_2\, \ldots\, p_k)(p_k\, p_{k+1}).$$

The reader is invited to check the action of either member on the elements in parentheses. □

The Multiplication Permutation

We now begin the proof of Quadratic Reciprocity. p, q are two different odd prime numbers. Let g denote a primitive root modulo p. It acts on the classes of $1, 2, \ldots, p-1$ by multiplication. By invertibility the elements $g \cdot 1, g\cdot 2, \ldots, g\cdot(p-1)$ are pairwise incongruent modulo p, that is, multiplication by g permutes the invertible classes modulo p.

.I.6 Lemma. *The permutation s just described is* odd.

Proof. It is cyclic: $(1\, g\, g^2\, \ldots\, g^{p-2})$, of even length, as

$$s(1) \equiv g,\ s(g) \equiv g^2, \ldots, s(g^{p-3}) \equiv g^{p-2},\ s(g^{p-2}) \equiv q^{p-1} \equiv 1 \pmod{p}.$$

□

Now consider the permutation performed by *any* invertible class, on multiplication.

.I.7 Lemma. *Let $1 \le r \le p-1$. The permutation $s(m) \equiv rm \pmod{p}$, $m = 1, 2, \ldots, p-1$, has the sign (r/p), i.e., it is even if and only if r is quadratic residue modulo p.*

Proof. Writing $r \equiv g^k \pmod{p}$ we know that $(r/p) = (-1)^k$. As g performs a permutation of sign -1, g^k performs a permutation of sign $(-1)^k$. □

.I.8 Example. We exemplify this for $p = 7$. Multiplying 1, 2, 3, 4, 5, 6 by 2 yields, on reduction modulo p, 2, 4, 6, 1, 3, 5, i.e., the permutation is

$(1\,2\,4)(3\,6\,5)$ which is even. This is due to 2 being a quadratic residue, $2 \equiv 3^2 \pmod 7$.

3 is a quadratic non-residue, in fact a primitive root modulo 7. It affords the cyclic permutation $(1\,3\,2\,6\,4\,5)$, which is of even length, hence odd. □

The Matrix Transpose Permutation

We now consider an (m, n)–matrix elements of which we denote by $X(i, j)$, $1 \leq i \leq m$, $1 \leq j \leq n$. We start from the standard order, reading the elements row-wise.

That is, $(i, j) < (k, l)$ if $k > i$ (second element lower), or if $i = k, l > j$ (elements in the same row, second element further to the right). Equivalently, the element $X(i, j)$ has the number $(i - 1)n + j$ in that enumeration.

In the matrix

$$\begin{pmatrix} X(1,1) & X(1,2) & X(1,3) \\ X(2,1) & X(2,2) & X(2,3) \end{pmatrix}$$

the element $X(1, 3)$ succeeds $X(1, 1)$ and precedes $X(2, 1)$.

We will need to know the sign of the permutation effected by transposing the matrix. In our example we want to compare the standard enumeration of the above matrix with that of

$$\begin{pmatrix} X(1,1) & X(2,1) \\ X(1,2) & X(2,2) \\ X(1,3) & X(2,3). \end{pmatrix}$$

.I.9 Lemma. *The sign of the permutation just described is*

$$(-1)^{mn(m-1)(n-1)/4}.$$

Proof. We count the number of inversions.

Consider an arbitrary pair of positions $(k, l), (i, j)$, where $k > i$ or $k = i$, $l > j$. Transposing amounts to interchanging the column and row indices, yielding the pair (l, k), (j, i). In the second case, $k = i$, no inversion results.

In the first case there are $m(m-1)/2$ possible pairs k, i. One such pair results in an inversion if and only $l < j$, which means $n(n-1)/2$ possible cases. The total number of inversions is therefore $mn(m-1)(n-1)/4$. So the permutation afforded by transposing the matrix is of sign

$$(-1)^{(m-1)(n-1)mn/4}.$$

□

.I.10 Lemma. *Suppose the elements of the matrix are not in standard order. The sign of the transposition permutation will then still be*

$$(-1)^{mn(m-1)(n-1)/4}.$$

Proof. Suppose the given ordering arises from the standard arrangement by the permutation s. Denote the permutation discussed above by u. Then our permutation can be described as first performing s^{-1} to get everything back in straight order, followed by the transposition t, and then by s. The resulting permutation, $u = sts^{-1}$, has the same sign as t by the product rule, as s and s^{-1} have the same sign. □

Remark: An alternative proof is to note that those moves (and only these) that would produce an inversion from the standard order will, from the given order, either create an inversion or destroy the one we already had. So the numbers of inversions in the two situations are congruent modulo 2.

.I.11 Example. The matrix

$$\begin{pmatrix} 2 & 3 & 4 \\ 5 & 6 & 1 \end{pmatrix}$$

arises from the standard order by the cyclic permutation

$$s = (1\,2\,3\,4\,5\,6), \quad s^{-1} = (6\,5\,4\,3\,2\,1).$$

The composition sts^{-1} then reads:

$$\begin{pmatrix} 2 & 3 & 4 \\ 5 & 6 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \to \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix} \to \begin{pmatrix} 2 & 5 \\ 3 & 6 \\ 4 & 1 \end{pmatrix}.$$

Straightening out the matrices it reads

$$sts^{-1} = (1\,2\,3\,4\,5\,6)(2\,4\,5\,3)(6\,5\,4\,3\,2\,1) = (5\,1\,2\,6).$$

□

We will apply this to the case $m = p$ and $n = q$, both odd. The factors m, n in the exponent do not affect the sign. So in this case the sign is simply

$$(-1)^{(p-1)(q-1)/4} \qquad (*)$$

The proof of Quadratic Reciprocity

Write down the numbers $0, 1, 2, \ldots pq-1$,corresponding to all the classes modulo pq, in straight order in a p/q–matrix :

$$\begin{pmatrix} 0 & 1 & 2 & \ldots & q-1 \\ q & q+1 & q+2 & \ldots & 2q-1 \\ \ldots & & & & \ldots \\ (p-1)q & (p-1)q+1 & (p-1)q+2 & \ldots & pq-1 \end{pmatrix}$$

The elements of each row are mutually incongruent modulo q.

The elements of a column are mutually congruent modulo q, but incongruent modulo p. This because we move down the columns by repeated addition of q, and different multiples of q are incongruent modulo p

From the bottom of the column we reach the top by adding yet another q and reducing modulo pq, i.e., dividing by pq and keeping the least positive remainder.

We now permute the elements within each row by replacing the j term in $(m-1)q + j$ with the least positive remainder of pj modulo q. We thus perform the same permutation within each row so that the whole columns are permuted.

We have proved that each such permutation is of sign (p/q). As the number of rows is odd, the resulting product too is of sign (p/q).

The first column is not affected by this operation. In the second column the first element is now p', the least positive remainder of p modulo q. The following elements are $p' + q$, $p' + 2q$, etc.

One of these, say the j :th one is p. Several cyclic permutations within the column will bring p to the top.

As the length of each column is odd, all these permutations are even. On performing further cyclic permutations within the second column we can bring $2p$ to the top. In the same manner we bring $3p$ to the top of the third column, etc. All these permutations are even.

We finally arrive at the following matrix:

$$\begin{pmatrix} 0 & p & 2p & \dots & (q-1)p \\ q & q+p & q+2p & \dots & q+(q-1)p \\ \dots & & & & \dots \\ (p-1)q & (p-1)q+p & (p-1)q+2p & \dots & (p-1)q+(q-1)p \end{pmatrix} \quad (**)$$

everything taken modulo pq. The total sign of this permutation is still (p/q).

But we could have achieved the same result by a different route. Start by writing down the same elements in the same order, but in a q/p–matrix:

$$\begin{pmatrix} 0 & 1 & 2 & \dots & p-1 \\ p & p+1 & p+2 & \dots & 2p-1 \\ \dots & & & & \dots \\ (q-1)p & (q-1)p+1 & (q-1)p+2 & \dots & pq-1 \end{pmatrix}$$

We then permute the rows in the same way as before, but with p and q interchanged. A permutation of sign (q/p) will result in the transpose of (**).

We retrieve (**) by transposing the last matrix, a permutation whose sign we determined above, (*).

We finally arrive at Quadratic Reciprocity:

$$\boxed{(\frac{p}{q}) = (-1)^{(p-1)(q-1)/4}(\frac{q}{p})}.$$

.I.12 Example. The following Example illustrates all the steps in the case $p = 5, q = 7$. We started from

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 14 & 15 & 16 & 17 & 18 & 19 & 20 \\ 21 & 22 & 23 & 24 & 25 & 26 & 27 \\ 28 & 29 & 30 & 31 & 32 & 33 & 34 \end{pmatrix}$$

We then multiplied the first row by 5, and reduced it modulo 7: $\begin{pmatrix}0 & 5 & 3 & 1 & 6 & 4 & 2\end{pmatrix}$, and permuted the remaining rows in the same manner. As a result the whole columns were permuted:

$$\begin{pmatrix}0 & 5 & 3 & 1 & 6 & 4 & 2\\ 7 & 12 & 10 & 8 & 13 & 11 & 9\\ 14 & 19 & 17 & 15 & 20 & 18 & 16\\ 21 & 26 & 24 & 22 & 27 & 25 & 23\\ 28 & 33 & 31 & 29 & 34 & 32 & 30\end{pmatrix}$$

We then permuted the columns cyclically several times so as to bring the elements $0, p, 2p, \ldots (q-1)p$ to the top:

$$\begin{pmatrix}0 & 5 & 10 & 15 & 20 & 25 & 30\\ 7 & 12 & 17 & 22 & 27 & 32 & 2\\ 14 & 19 & 24 & 29 & 34 & 4 & 9\\ 21 & 26 & 31 & 1 & 6 & 11 & 16\\ 28 & 33 & 3 & 8 & 13 & 18 & 23\end{pmatrix} \qquad (***)$$

The sign of the resulting permutation is $(5/7) = -1$.

We then started afresh from

$$\begin{pmatrix}0 & 1 & 2 & 3 & 4\\ 5 & 6 & 7 & 8 & 9\\ 10 & 11 & 12 & 13 & 14\\ 15 & 16 & 17 & 18 & 19\\ 20 & 21 & 22 & 23 & 24\\ 25 & 26 & 27 & 28 & 29\\ 30 & 31 & 32 & 33 & 34\end{pmatrix}$$

This time we multiplied by the remainder of 7 modulo 5, that is, by 2:

$$\begin{pmatrix}0 & 2 & 4 & 1 & 3\\ 5 & 7 & 9 & 6 & 8\\ 10 & 12 & 14 & 11 & 13\\ 15 & 17 & 19 & 16 & 18\\ 20 & 22 & 24 & 21 & 23\\ 25 & 27 & 29 & 26 & 28\\ 30 & 32 & 34 & 31 & 33\end{pmatrix}$$

We then permuted each column cyclically several times so as to get the row

$\begin{pmatrix} 0 & 7 & 14 & 21 & 28 \end{pmatrix}$ on top:

$$\begin{pmatrix} 0 & 7 & 14 & 21 & 28 \\ 5 & 12 & 19 & 26 & 33 \\ 10 & 17 & 24 & 31 & 3 \\ 15 & 22 & 29 & 1 & 8 \\ 20 & 27 & 34 & 6 & 13 \\ 25 & 32 & 4 & 11 & 18 \\ 30 & 2 & 9 & 16 & 23 \end{pmatrix}$$

The resulting permutation is of sign $(7/5) = (2/5) = -1$ Transposing finally led to

$$\begin{pmatrix} 0 & 5 & 10 & 15 & 20 & 25 & 30 \\ 7 & 12 & 17 & 22 & 27 & 32 & 2 \\ 14 & 19 & 24 & 29 & 34 & 4 & 9 \\ 21 & 26 & 31 & 1 & 6 & 11 & 16 \\ 28 & 33 & 3 & 8 & 13 & 18 & 23 \end{pmatrix} \qquad (**)$$

The sign of the transposition is

$$(-1)^{(7-1)(5-1)/4}$$

$= 1.$ □