ZOLOTAREV'S PROOF OF QUADRATIC RECIPROCITY

The main rule of quadratic reciprocity is

$$(p/q)\,(q/p) = (-1)^{(p-1)(q-1)/4} \quad \text{for distinct odd primes } p \text{ and } q.$$

This writeup sketches Zolotarev's proof from c.1872 in a way that may be novel. The symbols p and q denote distinct odd primes throughout. The idea of proving quadratic reciprocity this way came to me from a similar writeup by Matt Baker,

`http://people.math.gatech.edu/~mbaker/pdf/zolotarev.pdf` .

1. A Card Trick

Using a deck of pq cards, proceed as follows:

(1) Deal the cards out in a p-by-q array, in column-major order.
(2) Collect them back in, in reverse column-major order, undoing step (1).
(3) Deal them back out, in diagonal-wraparound order.
(4) Collect them back in, in reverse diagonal-wraparound order, undoing step (3).
(5) Deal them back out, in row-major order.
(6) Collect them back in, in reverse row-major order, undoing step (5).

Surely this is the world's most underwhelming card trick—not only have we done nothing, we have done nothing *three times*. And yet, we have just proved the main rule of quadratic reciprocity:

- Each of the step-pairs (1)–(2), (3)–(4), and (5)–(6) is trivial, so the entire sequence (1)–(6) is trivial.
- Consequently also the sequence (2)–(6), (1) is trivial, making the succession of step-pairs (2)–(3), (4)–(5), (6)–(1) trivial.
- But the step-pairs (2)–(3), (4)–(5), (6)–(1) are nontrivial. They are permutations whose signs will be shown to be (p/q), (q/p), and $(-1)^{(p-1)(q-1)/4}$. The fact that the product of the three signs equals 1 is the desired result.

So the issue is to establish the signs of the permutations.

2. Transitions Between Three Orders on a Product

To mathematicize the card trick, let $C_n = \{0, \cdots, n-1\}$ for any positive integer n, and let $C_{p\times q} = C_p \times C_q$.

The permutation $\tau_{rd} : C_{p\times q} \longrightarrow C_{p\times q}$ of the p-by-q array from row-major order to diagonal order (with wraparound) restricts to a permutation of each column.

For example, if $p = 3$ and $q = 7$ then we have

$$\left[\begin{array}{c|c|c|c|c|c|c} \boxed{(0,0)} & \boxed{(0,1)} & \boxed{(0,2)} & \boxed{(0,3)} & \boxed{(0,4)} & (0,5) & (0,6) \\ (1,0) & (1,1) & (1,2) & (1,3) & (1,4) & (1,5) & (1,6) \\ (2,0) & (2,1) & (2,2) & (2,3) & (2,4) & (2,5) & (2,6) \end{array}\right]$$

$$\Big\downarrow \tau_{rd}$$

$$\left[\begin{array}{c|c|c|c|c|c|c} \boxed{(0,0)} & (2,1) & (1,2) & \boxed{(0,3)} & (2,4) & (1,5) & (0,6) \\ (1,0) & \boxed{(0,1)} & (2,2) & (1,3) & \boxed{(0,4)} & (2,5) & (1,6) \\ (2,0) & (1,1) & \boxed{(0,2)} & (2,3) & (1,4) & (0,5) & (2,6) \end{array}\right]$$

Similarly, the permutation $\tau_{cd} : C_{p\times q} \longrightarrow C_{p\times q}$ from column-major order to diagonal order permutes each row,

$$\left[\begin{array}{ccccccc} \boxed{(0,0)} & \boxed{(0,1)} & (0,2) & (0,3) & (0,4) & (0,5) & (0,6) \\ \hline \boxed{(1,0)} & (1,1) & (1,2) & (1,3) & (1,4) & (1,5) & (1,6) \\ \hline \boxed{(2,0)} & (2,1) & (2,2) & (2,3) & (2,4) & (2,5) & (2,6) \end{array}\right]$$

$$\Big\downarrow \tau_{cd}$$

$$\left[\begin{array}{ccccccc} \boxed{(0,0)} & (0,5) & (0,3) & \boxed{(0,1)} & (0,6) & (0,4) & (0,2) \\ \hline (1,2) & \boxed{(1,0)} & (1,5) & (1,3) & (1,1) & (1,6) & (1,4) \\ \hline (2,4) & (2,2) & \boxed{(2,0)} & (2,5) & (2,3) & (2,1) & (2,6) \end{array}\right]$$

Also, there is the permutation $\tau_{rc} : C_{p\times q} \longrightarrow C_{p\times q}$ from row-major order to column-major order,

$$\left[\begin{array}{ccccccc} \boxed{(0,0)} & \boxed{(0,1)} & \boxed{(0,2)} & \boxed{(0,3)} & (0,4) & (0,5) & (0,6) \\ (1,0) & (1,1) & (1,2) & (1,3) & (1,4) & (1,5) & (1,6) \\ (2,0) & (2,1) & (2,2) & (2,3) & (2,4) & (2,5) & (2,6) \end{array}\right]$$

$$\Big\downarrow \tau_{rc}$$

$$\left[\begin{array}{ccccccc} \boxed{(0,0)} & \boxed{(0,3)} & (0,6) & (1,2) & (1,5) & (2,1) & (2,4) \\ \boxed{(0,1)} & (0,4) & (1,0) & (1,3) & (1,6) & (2,2) & (2,5) \\ \boxed{(0,2)} & (0,5) & (1,1) & (1,4) & (2,0) & (2,3) & (2,6) \end{array}\right]$$

By definition, $\tau_{cd}^{-1} \circ \tau_{rd} = \tau_{rc}$, and consequently, since the map from permutations to their signs is a homomorphism into $\{\pm 1\}$,

$$\operatorname{sgn}(\tau_{cd}) \operatorname{sgn}(\tau_{rd}) = \operatorname{sgn}(\tau_{rc}).$$

We will see that the equality in the previous display is quadratic reciprocity.

3. The Column–Diagonal Transition Sign: Zolotarev's Lemma

An array element (x, y) has column-major order index $py + x$ in C_{pq-1}. Meanwhile, the diagonal map from indices back into the array wraps around by reducing each index mod p for the row and mod q for the column, $i \mapsto (i \bmod p, i \bmod q)$, so that in particular the array element having diagonal index $py+x$ is $(x, py+x \bmod q)$. Thus τ_{cd} acts on $C_{p\times q}$ as $(x,y) \mapsto (x, py+x \bmod q)$, preserving the row-index and thus giving a p-fold composition of disjoint permutations, the permutation of row x being

$$C_q \longrightarrow C_q, \quad y \longmapsto py + x \bmod q.$$

(Cf. each row of the second example in section 2.) The sign of each such permutation is unaffected by the postpended x-translation, which is either trivial or a q-cycle. So we need only the sign of the permutation

$$\pi_{p,q} : C_q \longrightarrow C_q, \qquad y \longmapsto py \bmod q.$$

(For example, again with reference to the second example in section 2, shifting the middle row of the image-array one slot leftward makes the second entries match those of the top row, and similarly for the bottom row with a two-slot leftward shift.) Since p is odd, the sign of the p-fold composition τ_{dc} is simply the sign of $\pi_{p,q}$.

Zolotarev's Lemma says that in general the sign of π is the Legendre symbol,

$$\operatorname{sgn}(\pi_{a,q}) = (a/q) \quad \text{for } q \text{ an odd prime and } a \text{ coprime to } q.$$

Indeed, the map $a \mapsto \operatorname{sgn}(\pi_{a,q})$ depends only on $a+q\mathbb{Z}$, and $\pi_{a,q} \circ \pi_{a',q} = \pi_{aa',q}$, so the map lifts a homomorphism $(\mathbb{Z}/q\mathbb{Z})^\times \longrightarrow \{\pm 1\}$ to $\mathbb{Z} - q\mathbb{Z}$. When a is a generator modulo q, the permutation $\pi_{a,q}$ is a single cycle of even length $q-1$, so it is odd. Thus the homomorphism that lifts to $a \mapsto \operatorname{sgn}(\pi_{a,q})$ is nontrivial, forcing it to be the Legendre symbol as claimed.

In sum, the column–diagonal transition sign and symmetrically the row–diagonal transition sign are

$$\operatorname{sgn}(\tau_{cd}) = (p/q) \quad \text{and} \quad \operatorname{sgn}(\tau_{rd}) = (q/p).$$

4. The Row–Column Transition Sign

The sign of the row–column transition τ_{rc} is the parity of the number of array-position pairs $(x,y),(x',y') \in C_{p\times q}$ that are in row-major order but not in column-major order. The following sketch shows a generic (x,y)th position and asterisks at the relevant positions (x',y'):

$$\left[\begin{array}{cccc|c} & & & & \\ & & & & (x,y) \\ \hline * & * & * & * & \\ * & * & * & * & \\ * & * & * & * & \end{array}\right].$$

The sketch shows that the condition is $x' > x$ and $y' < y$. Thus τ_{rc} has parity $(-1)^{\binom{p}{2}\binom{q}{2}}$. Since p and q are odd, this is

$$\operatorname{sgn}(\tau_{rc}) = (-1)^{(p-1)(q-1)/4}.$$

5. Conclusion

The relation from the end of section 2,

$$\operatorname{sgn}(\tau_{cd})\operatorname{sgn}(\tau_{rd}) = \operatorname{sgn}(\tau_{rc}),$$

is the main quadratic reciprocity law by the two equalities from the end of section 3 and the equality from section 4,

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

We needed p and q to be coprime for the diagonal order to cover the entire array (cf. the Sun-Ze Theorem). We needed p and q to be odd for the row-column transition sign to be the right side of the previous display. We needed q to be prime for the column–diagonal transition sign to be (p/q), and similarly for p and the row–diagonal transition sign.