1 The Pledge

Let $m, n$ be odd positive integers. Suppose you have a deck consisting of $mn$ different cards $0, 1, \ldots, mn - 1$. You first deal the cards into $m$ rows of $n$ cards each, dealing one row at a time from left to right, so that once the deck is exhausted the cards form an $m \times n$ rectangle. Now you pick up the cards one column at a time, from left to right, putting each successive card under the previous one. The reassembled deck is now a permutation $\sigma_{m,n}$ of the original deck. (For example, if $m = 3$ and $n = 5$ and the cards are originally in ascending order $0, 1, \ldots, 14$, then the reassembled deck is $0, 5, 10, 1, 6, 11, \ldots, 4, 9, 14$.)

Now for a combinatorial puzzle: what is the sign of the permutation $\sigma_{m,n}$? (If you’d like to think about this before seeing the answer, stop reading now!)

The answer is that $\text{sign}(\sigma_{m,n}) = 1$ if either $m \equiv 1 \pmod{4}$ or $n \equiv 1 \pmod{4}$, and $\text{sign}(\sigma_{m,n}) = -1$ if $m \equiv n \equiv 3 \pmod{4}$. In other words,

$$\text{sign}(\sigma_{m,n}) = (-1)^{\frac{(m-1)(n-1)}{4}}.$$  \hspace{1cm} (1)

To prove (1), recall that the sign of a permutation $\sigma$ of a totally ordered finite set is equal to $(-1)^{I(\sigma)}$, where $I(\sigma)$ is the number of inversions of $\sigma$. (An inversion is a pair $(i, i')$ with $i < i'$ and $\sigma(i) > \sigma(i')$.) If we index the rows by $0, 1, \ldots, m - 1$ and the columns by $0, 1, \ldots, n - 1$, then it is straightforward to verify that the cards whose initial positions in the rectangle are $(i, j)$ and $(i', j')$ yield an inversion of $\sigma_{m,n}$ if and only if $i < i'$ and $j > j'$. The number of such inversion pairs $((i, j), (i', j'))$ is $\binom{m}{2} \cdot \binom{n}{2}$, since each 2-element subset $\{i, i'\}$ of $\{0, 1, \ldots, m\}$ and $\{j, j'\}$ of $\{0, 1, \ldots, n\}$ gives rise to a unique inversion (by ordering the elements so that $i < i'$ and $j > j'$). This establishes (1) since $m$ and $n$ are assumed to be odd.

Formula (1) may bring to mind Gauss’s Law of Quadratic Reciprocity. Is this just a coincidence? Continue on, dear reader...
2 The Turn

In the previous section, the cards were originally dealt into an \( m \times n \) rectangular array. Let us assume in this section that \( m \) and \( n \) are relatively prime in addition to being odd and positive. If we index the rows by \( 0, 1, \ldots, m-1 \) and the columns by \( 0, 1, \ldots, n-1 \), as above, then the card dealt into position \((x, y)\) is \( nx + y \). By the Chinese Remainder Theorem, this formula naturally determines a permutation \( \alpha \) of the set \( C = \{0, 1, \ldots, mn-1\} \): send the unique element of \( C \) congruent to \( x \) (mod \( m \)) and \( y \) (mod \( n \)) to the unique element of \( C \) congruent to \( nx + y \) (mod \( m \)) and \( y \) (mod \( n \)). If we originally dealt the cards into columns rather than rows, we would (by symmetry) obtain a permutation \( \beta \) of \( C \) sending the unique element of \( C \) congruent to \( x \) (mod \( m \)) and \( y \) (mod \( n \)) to the unique element of \( C \) congruent to \( x \) (mod \( m \)) and \( x + my \) (mod \( n \)).

The point of this discussion is that the permutation \( \sigma_{m,n} \) from the previous section is just \( \beta \circ \alpha^{-1} \). Since sign is a homomorphism, we deduce that

\[
\text{sign}(\alpha) \cdot \text{sign}(\beta) = \text{sign}(\sigma_{m,n}).
\] (2)

We already obtained a formula for the right-hand side of (2) in the previous section. We claim that \( \text{sign}(\alpha) \) is equal to the sign of the permutation of \( \mathbb{Z}/m\mathbb{Z} \) induced by multiplication by \( n \), which we write as \( \left[ \frac{n}{m} \right] \). (By symmetry, we will have \( \text{sign}(\beta) = \left[ \frac{m}{n} \right] \).)

To see this, note that \( \alpha \) is the product over \( y \in \{0, 1, \ldots, n-1\} \) of permutations \( \tau_y \) of \( \{0, 1, \ldots, m-1\} \), where \( \tau_y(x) \equiv nx + y \) (mod \( m \)). But \( \tau_y \) is a composition of \( \left[ \frac{n}{m} \right] \) with the permutation \( x \mapsto x + y \) (mod \( m \)), which has sign +1 since it’s either trivial (if \( y = 0 \)) or an \( m \)-cycle (if \( y \neq 0 \)), and we’re assuming that \( m \) is odd. This proves the claim. We have therefore established the following result:

**Theorem 1.** Let \( m, n \) be relatively prime odd positive integers. Then

\[
\left[ \frac{n}{m} \right] \cdot \left[ \frac{m}{n} \right] = (-1)^{(m-1)(n-1)/4}.
\]

Formula (1) is very strongly reminiscent of Gauss’s Law of Quadratic Reciprocity — surely this is not just a coincidence! But what is the connection with the Legendre symbol? Now that you are hooked, dear friend, there is no choice but to continue reading...
3 The Prestige

The connection between (1) and Gauss’s Law of Quadratic Reciprocity is given by:

**Lemma 1 (Zolotarev’s Lemma).** If \( p \) is an odd prime and \( a \) is a positive integer not divisible by \( p \), then

\[
\left[ \frac{a}{p} \right] = \left( \frac{a}{p} \right)
\]

where \( \left( \frac{a}{p} \right) \) denotes the Legendre symbol.

To prove Zolotarev’s Lemma, it suffices to note that \( \left[ \frac{\cdot}{p} \right] \) is a surjective homomorphism from \((\mathbb{Z}/p\mathbb{Z})^\times\) to \(\{\pm 1\}\); surjectivity follows from the fact that if \( g \) is a primitive root mod \( p \) (i.e., a cyclic generator of \((\mathbb{Z}/p\mathbb{Z})^\times\)) then \( \left[ \frac{g}{p} \right] \) is a \((p - 1)\)-cycle and thus has signature \(-1\). The kernel of \( \left[ \frac{\cdot}{p} \right] \) is therefore a subgroup of \((\mathbb{Z}/p\mathbb{Z})^\times\) of index 2, but the only such subgroup is the group of quadratic residues. Thus \( \left[ \frac{\cdot}{p} \right] \) coincides with the Legendre symbol \( \left( \frac{\cdot}{p} \right) \).

Combining Zolotarev’s Lemma with Theorem 1 yields:

**Corollary 1 (Law of Quadratic Reciprocity).** If \( p \) and \( q \) are distinct odd primes, then

\[
\left( \frac{p}{q} \right) \cdot \left( \frac{q}{p} \right) = (-1)^{\frac{(p-1)(q-1)}{4}}.
\]