CLASS 26, GIVEN ON 11/19/2010, FOR MATH 25

1. Proof #1 of Quadratic Reciprocity

We will now give the proof of quadratic reciprocity given in the book. It has the advantage of being elementary (although very clever) and its methods draw upon ideas we have already been using. Recall that p, q are distinct odd primes, and we want to prove that

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

Gauss' Lemma says that $\left(\frac{q}{p}\right) = (-1)^{\mu}$, where μ is the number of elements in $qP \cap N$, with $P = \{1, 2, \ldots, (p-1)/2\}, N = \{-1, -2, \ldots, -(p-1)/2\}$. Let us try to think of the number μ in a slightly different way. Let $1 \leq x \leq (p-1)/2$. Then $xq \in N$ if and only if $qx \equiv n \mod p$ for some n satisfying $-(p-1)/2 \leq n \leq -1$. Another way of saying this is that $py = qx - n$ for some integer y, or $qx - py = n$. Since $-(p-1)/2 \leq n \leq -1$, and $qx - py = n$ is an integer, this is equivalent to the inequalities

$$-p/2 < qx - py < 0.$$

So, in summary, $qx \in N$ if and only if there is some integer y which makes the above pair of inequalities true. Notice that if there is a value of y which makes the above pair of inequalities true, it is the only integer y which can do so, because changing y by 1 changes $qx - py$ by $\pm p$, and the inequalities above define an interval of length $p/2$.

Now let us think about the actual values y might be able to take if the above inequalities are satisfied. First, notice that $y > 0$, because if $y \leq 0$, then $qx - py \geq qx > 0$, so that $qx - py < 0$ would be impossible. Next, notice that $-p/2 < qx - py$ implies $py < qx + p/2$, or $y < qx/p + 1/2$. The maximum value of the right hand side occurs when $x = (p-1)/2$, so

$$y < \frac{q(p-1)}{2p} + \frac{1}{2} = \frac{q+1}{2} - \frac{q}{2p} < \frac{q+1}{2}.$$

Since $y, (q+1)/2$ are integers, this is equivalent to

$$y \leq \frac{q-1}{2}.$$

So altogether, we see that if $-p/2 < qx - py < 0$, then given the restrictions $1 \leq x \leq (p-1)/2$ on x, we must have $1 \leq y \leq (q-1)/2$.

Therefore, the following is an alternate characterization of the number μ: μ is equal to the number of lattice points (x, y) (a lattice point being a point in the plane with integer coordinates) which satisfy

$$1 \leq x \leq \frac{p-1}{2}, 1 \leq y \leq \frac{q-1}{2}, -\frac{p}{2} < qx - py < 0. \tag{1}$$

The first two inequalities describe a box of lattice points, of dimension $(p-1)/2 \times (q-1)/2$, and the last pair of inequalities describes a region bounded by a pair of lines, which we will graph shortly.

Quadratic reciprocity is a symmetric statement in p, q, so it might be natural to try to use a symmetric argument with the roles of p, q above interchanged. As a matter of fact, we can repeat the entire argument we just did with the roles of q, p interchanged, and doing that will yield

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

where ν is the number of lattice points (x, y) satisfying

$$1 \leq x \leq \frac{p-1}{2}, 1 \leq y \leq \frac{q-1}{2}, 0 < qx - py < \frac{q}{2}. \tag{2}$$

We are interested in computing $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)$; what we see is that

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\mu+\nu}.$$

The inequalities 1, 2 show that μ, ν have interpretations as the number of lattice points in our box satisfying $-p/2 < qx - py < 0, 0 < qx - py < q/2$, respectively. Notice that inequalities cannot be simultaneously satisfied by a pair of integers (x, y), since the first pair requires $qx - py$ be negative while the second pair requires $qx - py$ be positive. Furthermore, notice that $qx - py = 0$ is impossible, if x, y are integers, because $qx = py$ implies that $p \mid (qx)$, which implies $p \mid q$ or $p \mid x$, both of which are impossible since q, p are distinct primes, and $1 \leq x \leq (p-1)/2$. So we may interpret $\mu + \nu$ as the number of lattice points (x, y) in our box satisfying

$$-\frac{p}{2} < qx - py < \frac{q}{2}.$$

This pair of inequalities defines a region bounded by two parallel lines of slope q/p, with one intersecting the x-axis at $(1/2, 0)$ and the other intersecting the y-axis at $(0, 1/2)$. These two lines split the box we are interested in into three parts: one part is given by the pair of inequalities defined above and has $\mu + \nu$ lattice points in it. Another is the region A described by the inequality $qx - py \leq -p/2$, and the third is the region B described by the inequality $qx - py \geq q/2$.

Let α, β be the number of lattice points in the box in regions A, B respectively. Then $\alpha + \beta + \mu + \nu = \frac{p-1}{2}\frac{q-1}{2}$. Therefore, we will be able to show that

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

if we can show that $\alpha + \beta$ is even.

We will do so by showing that $\alpha = \beta$, and we will do this by showing that these regions are symmetric! Consider the map ρ, which sends (x, y) to $\left(\frac{p+1}{2} - x, \frac{q+1}{2} - y\right)$. This map is exactly the same as reflection of the point (x, y) across the point $((p+1)/4, (q+1)/4)$. The claim is that this map sends A to B and B to A.

The region A is defined by the inequalities

$$1 \leq x \leq \frac{p-1}{2}, 1 \leq y \leq \frac{q-1}{2}, qx - py \leq -p/2.$$

First, notice that ρ preserves the first two inequalities; that is, if a lattice point (x, y) is in our box, then $\rho(x, y)$ is still in the box. Indeed, $\rho(1, 1) = ((p-1)/2, (q-1)/2), \rho((p-1)/2, (q-1)/2) = (1, 1)$. Let us see what happens when a point which satisfies the last inequality above is acted on by ρ.

Suppose $qx - py \leq -p/2$. Let $\rho(x, y) = (x', y')$, so that $x' = (p+1)/2 - x$, say. We want to show that (x', y') is in B, so we should try to show that $qx' - py' \geq q/2$. We have

$$qx' - py' = q\left(\frac{p+1}{2} - x\right) - p\left(\frac{q+1}{2} - y\right) = \frac{q-p}{2} - (qx - py).$$

We know that $qx - py \leq -p/2$, so using the expression above,

$$qx' - py' \geq \frac{q-p}{2} + \frac{p}{2} = \frac{q}{2}.$$

(The inequality sign flips because we are subtracting an inequality involving $qx - py$, and subtracting flips inequality signs.) But this inequality describes B. In a similar way, one shows that $\rho(B) \subset A$. As ρ is a bijection, this means that ρ places the lattice points of A, B in one-to-one correspondence with each other, so that $\alpha = \beta$, as desired. $\square$

Wow! Even though this proof might seem really convoluted, there really are two key ideas: the first is that using Gauss' Lemma can be reduced to a lattice point counting problem in some region bounded by lines, and the second is that a symmetry argument can be used to relate the result we want to the lattice point counting problem we set up in the first part. In general, lattice point counting is a useful and common problem in number theory, which we did not have a lot of time to explore in this class.

2. Proof #2 of Quadratic Reciprocity

Just for the sake of variety, we now give a second proof of quadratic reciprocity. This proof is also elementary (in the sense that it doesn't require advanced math), but even more clever than the first proof we gave. This is the proof alluded to in the book, given by Eisenstein in the mid 19th century. We start with a strange-looking lemma:

Lemma 1. *Let m be an odd positive integer. Then*

$$\frac{\sin mx}{\sin x} = (-4)^{\frac{m-1}{2}} \prod_{j=1}^{(m-1)/2} \left(\sin^2 x - \sin^2 \frac{2\pi j}{m}\right).$$

Proof. This lemma might look nearly impossible to prove, but actually is quite elementary. First, we express $\sin mx$ as a polynomial in $\sin x$ and $\cos x$. This is done by using the relation $(\cos x + i \sin x)^m = (\cos mx + i \sin mx)$; for instance, this can be seen from Euler's relation $e^{ix} = \cos x + i \sin x$, which in turn can be seen from the power series expressions for $e^x, \sin x, \cos x$. In particular, if we want to write $\sin mx$ as a polynomial in $\cos x, \sin x$, what we should be looking for is the imaginary part of $(\cos x + i \sin x)^m$, after expanding it using the binomial theorem. More specifically, the binomial theorem applied to $(\cos x + i \sin x)^m$ yields

$$(\cos x + i \sin x)^m = \cos^m x + \binom{m}{1} i(\cos^{m-1} x) \sin x) - \binom{m}{2} (\cos^{m-2} x)(\sin^2 x) - i\binom{m}{3} (\cos^{m-3} x)(\sin^3 x) + \ldots + i^m s$$

The imaginary part of this expression is

$$\binom{m}{1} (\cos^{m-1} x)(\sin x) - \binom{m}{3} (\cos^{m-3} x)(\sin^3 x) + \ldots + (-1)^{\frac{m-1}{2}} \sin^m x.$$

As a matter of fact, each expression involving cos is a power of cos to an even power, so we can use $\cos^2 x = 1 - \sin^2 x$ to replace all the powers of cosine with powers of $(1 - \sin^2 x)$. The upshot of this is that $\sin mx$ is a polynomial in $\sin x$ alone. Furthermore, the powers of $\sin x$ in this expression are all odd powers. Therefore, $\sin mx / \sin x$ is actually a polynomial

in $\sin x$ where all powers of $\sin x$ are even, or alternately $\sin mx/\sin x$ is a polynomial in $\sin^2 x$, with integer coefficients.

So let $\sin mx/\sin x = f(\sin^2 x)$, where $f(x)$ is a polynomial with integer coefficients. What are the roots of $f(\sin^2 x)$? On the one hand, $\sin mx/\sin x$ is equal to 0 exactly when $x = n\pi/m$, where n is any integer, and also perhaps when $m \nmid n$ (to ensure that $\sin x \neq 0$). On the other hand, when these values of x are plugged into $\sin^2 x$, we get numbers

$$\sin^2 \frac{n\pi}{m},$$

and these numbers repeat with period m; for instance, we can get all such nonzero numbers by letting $n = 1, 2, \ldots, m-1$. As a matter of fact, we can get all such numbers with just $n = 1, 2, \ldots, (m-1)/2$, because

$$\sin^2\left(\pi - \frac{n\pi}{m}\right) = \sin^2\left(\frac{(m-n)\pi}{m}\right) = \sin^2 \frac{n\pi}{m},$$

so that the values of $\sin^2 x$ at $(m-n)\pi/m$ is the same as the value of $\sin^2 x$ at $n\pi/m$. The upshot of this is that the numbers

$$\sin^2 \frac{\pi}{m}, \ldots, \sin^2 \frac{(m-1)\pi}{2m},$$

give $(m-1)/2$ different roots of $f(x)$. And $f(x)$ itself has degree $(m-1)/2$, because $f(\sin^2 x)$ is a polynomial of degree $m-1$ in $\sin x$, so these $(m-1)/2$ roots above are all the roots of $f(x)$. Therefore, we may write

$$f(\sin^2 x) = c\left(\prod_{j=1}^{(m-1)/2}\left(\sin^2 x - \sin^2 \frac{j\pi}{m}\right)\right),$$

where c is some constant which gives the leading coefficient of $f(x)$. Before calculating c, first let us observe that we can actually replace j with $2j$. This is because the numbers $\sin^2 j\pi/m$ and $\sin^2 2j\pi/m$ really give the same set of numbers, if we restrict $1 \leq j \leq (m-1)/2$. This ultimately boils down to the fact that the subsets $\{\pm 1\}, \ldots, \{\pm(m-1)/2\}$ contain exactly one of the numbers $2, 4, \ldots, m-1$, considered mod m, which is basically what we proved when proving Gauss' Lemma! (The difference here is that m is not prime, but rather an odd integer; however, the proof of Gauss' Lemma we used still works because $2, m$ are coprime.)

To determine c we just calculate the leading coefficient of $f(x)$. This is the same as the coefficient of $\sin^{m-1} x$ in the expression for $\sin mx/\sin x$. The binomial theorem expression shows that this coefficient is equal to

$$\binom{m}{1} + \binom{m}{3} + \ldots + \binom{m}{m},$$

and it is not hard to show that this expression is equal to $(-1)^{(m-1)/2}2^{m-1}$. (Short proof: one can check that summing the binomial coefficients $\binom{m}{n}, n = 0, \ldots, m$ gives 2^m by applying the binomial theorem to $(1+1)^m$, and then there is a symmetry $\binom{m}{n} = \binom{m}{m-n}$, and when m is odd this shows that $\binom{m}{1} + \ldots + \binom{m}{m} = \binom{m}{m-1} + \ldots + \binom{m}{0}$, and if their sum is 2^m then each of these terms is 2^{m-1}.) And we can rewrite $2^{m-1} = 4^{(m-1)/2}$, so $c = (-4)^{(m-1)/2}$, as desired. □

Now we prove quadratic reciprocity proper. First, recall that $\left(\frac{q}{p}\right)$ is equal to $(-1)^\mu$, where μ is the number of elements of $qP \cap N$ ($P = \{1, 2, \ldots, (p-1)/2\}, N = \{-1, -2, \ldots, -(p-1)/2\}$. We saw that an alternate interpretation of this was as the number of $\varepsilon_j = -1$, where

$\varepsilon_j = \pm 1$, with sign being chosen to ensure that $qj \equiv \varepsilon_j j_q \mod p$, where $1 \leq j_q \leq (p-1)/2$. In particular,

$$\left(\frac{q}{p}\right) = \prod_{j=1}^{(p-1)/2} \varepsilon_j.$$

On the other hand, because $qj \equiv \varepsilon_j j_q \mod p$, we have

$$\sin\left(\frac{2\pi}{p}(qj)\right) = \sin\left(\frac{2\pi qj}{p}\right) = \sin\left(\frac{2\pi}{p}(\varepsilon_j j_q)\right) = \varepsilon_j \sin\frac{2\pi j_q}{p}.$$

Multiply these equalities together, for $j = 1, 2, \ldots, (p-1)/2$:

$$\prod_{j=1}^{(p-1)/2} \sin\left(\frac{2\pi qj}{p}\right) = \left(\prod_{j=1}^{(p-1)/2} \varepsilon_j\right)\left(\prod_{j=1}^{(p-1)/2} \sin\frac{2\pi j_q}{p}\right).$$

We now divide by the term on the right of the right hand side, and then use the fact that the j_q are a permutation of $1, 2, \ldots, (p-1)/2$:

$$\prod_{j=1}^{(p-1)/2} \frac{\sin\frac{2\pi qj}{p}}{\sin\frac{2\pi j}{p}} = \prod_{j=1}^{(p-1)/2} \varepsilon_j.$$

We now apply the lemma to each of the expressions on the left hand side, with $m = q, x = 2\pi j/p$. The individual term $\dfrac{\sin\frac{2\pi qj}{p}}{\sin\frac{2\pi j}{p}}$ becomes

$$\frac{\sin\frac{2\pi qj}{p}}{\sin\frac{2\pi j}{p}} = (-4)^{\frac{q-1}{2}} \prod_{i=1}^{(q-1)/2} \left(\sin^2\frac{2\pi j}{p} - \sin^2\frac{2\pi i}{q}\right).$$

When we multiply each of these equalities together, for $j = 1, 2, \ldots, (p-1)/2$, we get the following expression, where the indices on the products satisfy $1 \leq j \leq (p-1)/2, 1 \leq i \leq (q-1)/2$:

$$\prod_{j=1}^{(p-1)/2} \frac{\sin\frac{2\pi qj}{p}}{\sin\frac{2\pi j}{p}} = (-4)^{\frac{p-1}{2}\frac{q-1}{2}} \prod_{i,j} \left(\sin^2\frac{2\pi j}{p} - \sin^2\frac{2\pi i}{q}\right).$$

On the other hand we also know that the left hand side equals $\left(\frac{q}{p}\right)$. So the end result of our calculations is that

$$\left(\frac{q}{p}\right) = (-4)^{\frac{p-1}{2}\frac{q-1}{2}} \prod_{i,j} \left(\sin^2\frac{2\pi j}{p} - \sin^2\frac{2\pi i}{q}\right).$$

We can repeat the same calculation with the roles of p, q interchanged, and this yields

$$\left(\frac{p}{q}\right) = (-4)^{\frac{p-1}{2}\frac{q-1}{2}} \prod_{i,j} \left(\sin^2\frac{2\pi j}{q} - \sin^2\frac{2\pi i}{p}\right),$$

where this time $1 \leq i \leq (p-1)/2, 1 \leq j \leq (q-1)/2$. Interchanging the indices i, j in the last expression gives

$$\left(\frac{p}{q}\right) = (-4)^{\frac{p-1}{2}\frac{q-1}{2}} \prod_{i,j} \left(\sin^2\frac{2\pi i}{q} - \sin^2\frac{2\pi j}{p}\right),$$

which is identical to the corresponding expression except that each term in the product has sign flipped! In particular, there are $\frac{p-1}{2}\frac{q-1}{2}$ such terms, so this says that

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

But since $\left(\frac{q}{p}\right) = \pm 1$, this is the same as saying

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

as desired.