CLASS 25, GIVEN ON 11/17/2010, FOR MATH 25

1. Evaluating $\left(\frac{-1}{p}\right)$

We begin by evaluating $\left(\frac{-1}{p}\right)$. Fortunately, we have done most of the work already.

Proposition 1 (Corollary 7.7)**.**

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \textit{if } p \equiv 1 \mod 4, \\ -1 & \textit{if } p \equiv 3 \mod 4. \end{cases}$$

An equivalent way of writing this is

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

Proof. Apply Euler's criterion. Indeed,

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

and $(p-1)/2$ is odd exactly when $p \equiv 3 \mod 4$. □

So, for instance, this result proves that $\left(\frac{-a}{p}\right) = \left(\frac{a}{p}\right)$ if and only if $p \equiv 1 \mod 4$. Even though this result was trivial given the theorems we knew, there are surprising facts we can prove using this result. For instance, recall that we could prove that there were infinitely many primes of the form $4k+3$ using a straightforward generalization of Euclid's proof of the infinitude of prime numbers, but that such a generalization would not work for primes of the form $4k+1$ (the obstruction being that a number of form $4k+1$ does not need to have a prime of form $4k+1$ as a factor). We can now adopt Euclid's proof to prove that there are infinitely many primes of form $4k+1$.

Proposition 2 (Corollary 7.8)**.** *There are infinitely many primes of form* $4k+1$.

Proof. Suppose there are only finitely many primes of the form $4k+1$. Let $p_1, \dots, p_r$ be all such primes. Let $N = (2p_1 \dots p_r)^2 + 1$. Then N has form $4k+1$, and is not divisible by any p_i. Let p be any prime dividing N. Then $(2p_1 \dots p_r)^2 \equiv -1 \mod p$, but this means that -1 is a square mod p, which is only possible if $p \equiv 1 \mod 4$. This contradicts the fact that no p_i divides N. Therefore there must be infinitely many primes of the form $4k+1$. □

2. Gauss' Lemma, evaluating $\left(\frac{2}{p}\right)$

To compute $\left(\frac{a}{p}\right)$ for $a \neq \pm 1$, we will repeatedly use the following fundamental fact. Let $P = \{1, 2, \dots, (p-1)/2\} \subset U_p$ be the set of elements of U_p which can be represented by $1, 2, \dots (p-1)/2$, and let $N = \{-1, -2, \dots, -(p-1)/2\} \subset U_p$ be the set of elements of U_p which can be represented by $-1, -2, \dots, -(p-1)/2$. Notice that P, N are disjoint and that $P \cup N = U_p$. For instance, if $p = 7$, then $P = \{1, 2, 3\}$, and $N = \{-1, -2, -3\}$. For $a \in U_p$, let aP be the subset of U_p obtained by multiplying each element of P by a. For instance, if $p = 7, a = 3$, then $aP = \{3, 6, 9\} = \{2, 3, 6\}$.

Theorem 1 (Theorem 7.9, Gauss' Lemma)**.** *Let $a \in U_p$. Then $\left(\frac{a}{p}\right) = (-1)^\mu$, where $\mu = \#(aP \cap N)$.*

Proof. The proof is a variation on the method used to prove Fermat's Little Theorem. The first observation is to notice that not only are the various elements of aP distinct; that is, not only is $ai \equiv aj \mod p$ possible only if $i = j$, but also that $ai \equiv -aj \mod p$ is impossible. Indeed, if $ai \equiv -aj \mod p$, then $a(i+j) \equiv 0 \mod p$, and since a is invertible mod p, this implies that $i + j \equiv 0 \mod p$. But since $1 \le i, j \le (p-1)/2$, $i + j \equiv 0 \mod p$ is impossible.

As a consequence, this implies that each of the $(p-1)/2$ subsets $\{\pm 1\}, \{\pm 2\}, \ldots, \{\pm(p-1)/2\}$ contains exactly none or one element of aP. Since aP has size $(p-1)/2$, and these $(p-1)/2$ subsets contain every element of U_p, so that each element of aP is in one of these subsets, we see that each of these $(p-1)/2$ subsets contains exactly one element of aP.

Therefore, for each $j = 1, 2, \ldots, (p-1)/2$ (ie, each $j \in P$), we may uniquely write $aj = \varepsilon_j j_a$ (this equation is taking place in U_p), where $\varepsilon_j = \pm 1$ and $j_a = 1, 2, \ldots, (p-1)/2$. Furthermore, the j_a are just a permutation of the elements of P. (Another way of saying this is that the map $j \mapsto j_a$ is a bijection of P into itself.)

How many of the ε_j are equal to -1? Notice that $\varepsilon_j = -1$ if and only if $aj \in N$. Therefore, the number of ε_j equal to -1 is equal to the number of elements in $aP \cap N$.

Take the $(p-1)/2$ equations $aj \equiv \varepsilon_j j_a \mod p$, and multiply them together. We get

$$a^{(p-1)/2}((p-1)/2)! \equiv (-1)^\mu((p-1)/2)! \mod p,$$

where we are using the fact that the j_a are just a rearrangement of the elements of P. Since $((p-1)/2)!$ is relatively prime to p, we can cancel this term from both sides, to obtain

$$a^{(p-1)/2} \equiv (-1)^\mu \mod p.$$

However, Euler's criterion says that $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \mod p$, so $\left(\frac{a}{p}\right) \equiv (-1)^\mu \mod p$, and since these two numbers are either ± 1, we really have an equality of integers.

□

Example. Let's illustrate the idea of the proof with an example. Let $p = 7$, and let $a = 3$. We want to calculate $\left(\frac{3}{7}\right)$ using the ideas in the proof of Gauss' Lemma. First, $P = \{1, 2, 3\}$, while $N = \{4, 5, 6\}$. We then have $aP = 3P = \{3, 6, 9\} = \{2, 3, 6\}$. Therefore, $aP \cap N = \{6\}$, so $\mu = 1$, and Gauss' Lemma says that $\left(\frac{3}{7}\right) = -1$, which agrees with all the other calculations we have done.

Let's work through the actual steps of the proof with this example. First, we determine $\varepsilon_j, j_a = j_3$ as follows:

$$a \cdot 1 = 3 \cdot 1 = (1) \cdot 3, a \cdot 2 = 6 \equiv (-1) \cdot 1 \mod 7, a \cdot 3 = 9 \equiv (1) \cdot 2 \mod 7,$$

so $\varepsilon_1 = \varepsilon_3 = 1, \varepsilon_2 = -1$, and $1_3 = 3, 2_3 = 1, 3_3 = 2$. Notice that the number of ε_j equal to -1 is precisely the size of $aP \cap N$, and that the j_3 are a permutation of $1, 2, 3$. Multiplying the congruences listed above together gives

$$a^3(1)(2)(3) \equiv (1)^2(-1)^1(3)(1)(2) \mod 7,$$

which reduces to $a^3 \equiv -1 \mod 7$, and $a^3 \equiv \left(\frac{a}{7}\right) \mod 7$ by Euler's criterion.

Using Gauss' Lemma, we can immediately compute $\left(\frac{2}{p}\right)$.

Proposition 3 (Corollary 7.10)**.**

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \textit{if } p \equiv 1,7 \mod 8, \\ -1 & \textit{if } p \equiv 3,5 \mod 8. \end{cases}$$

An equivalent way of writing this is

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

Proof. First, it is easy to check that the two formulas above are identical, because $(p^2-1)/8$ is even exactly when $p \equiv 1,7 \mod 8$, and odd when $p \equiv 3,5, \mod 8$.

To check that these formulas are true, we apply Gauss' Lemma with $a = 2$. We have $2P = \{2, 4, \ldots, p-1\}$. How many of these are elements of N? Every element which is greater than $(p-1)/2$ is in N. In other words, we want to count the number of i, with $1 \leq i \leq (p-1)/2$, such that $2i > (p-1)/2$, or $4i > (p-1)$. At this point things are perhaps simplest if we separately consider the cases where $p \equiv 1 \mod 4, p \equiv 3 \mod 4$.

When $p \equiv 1 \mod 4$, the i with $4i > (p-1)$ are $(p-1)/4+1, (p-1)/4+2, \ldots, (p-1)/2$; there are evidently $(p-1)/4$ such numbers. Then Gauss' Lemma says that

$$\left(\frac{2}{p}\right) = (-1)^{(p-1)/4}.$$

The exponent $(p-1)/4$ is even exactly when $p \equiv 1 \mod 8$, and is odd when $p \equiv 5 \mod 8$.

Now suppose that $p \equiv 3 \mod 4$. Then the i with $i > (p-1)/4$ are $(p-3)/4+1, (p-3)/4+2, \ldots, (p-1)/2 = (p-3)/4+(p+1)/4$. There are evidently $(p+1)/4$ such numbers. Then Gauss' Lemma says that

$$\left(\frac{2}{p}\right) = (-1)^{(p+1)/4}.$$

The exponent $(p+1)/4$ is even exactly when $p \equiv -1 \equiv 7 \mod 8$, and is odd when $p \equiv 3 \mod 8$. Taken together, these two cases prove the original proposition. □

So far, we have seen that determining whether $-1, 2$ are quadratic residues mod p boils down to checking which congruence class p lives in mod $4, 8$ respectively – a calculation which is easy and fast to do. What about more general numbers?

3. The quadratic reciprocity law: statement

Recall that

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

This means that, at least in principle, if we know how to calculate $\left(\frac{q}{p}\right)$ for various primes q (and maybe also $q = -1$, for convenience), then we can calculate $\left(\frac{a}{p}\right)$ for arbitrary a, once we factor a. We've already computed $\left(\frac{q}{p}\right)$ for $q = -1, 2$. From now on we will let q be an odd prime.

The result which lets us calculate $\left(\frac{q}{p}\right)$ efficiently is the celebrated *law of quadratic reciprocity.* We will state the result and give a few examples of its use in computing Legendre symbols, and give the proof next class.

Theorem 2 (Quadratic Reciprocity, Theorem 7.11)**.** *Let p, q be distinct odd primes. Then*

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

An alternate formulation is as follows: if either p, q is $\equiv 1 \mod 4$ (possibly both), then $\left(\frac{p}{q}\right), \left(\frac{q}{p}\right)$ are equal; if both $p, q \equiv 3 \mod 4$, then $\left(\frac{p}{q}\right), \left(\frac{q}{p}\right)$ have opposite sign.

First, notice that it is obvious that the alternate formulation is equivalent to the first formulation of the quadratic reciprocity law. Indeed, the exponent of -1, which is $\frac{p-1}{2}\frac{q-1}{2}$, is even exactly when at least one of $\frac{p-1}{2}, \frac{q-1}{2}$ is even, and these are even when $p, q \equiv 1 \mod 4$. When the exponent of -1 is even, then $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1$, and so are equal; when the exponent of -1 is odd, then $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1$, and then are unequal.

This may very well be the best theorem we learn in this class. It is of fundamental importance to the subject of quadratic residues, because (as we will see) it drastically speeds up the computation of Legendre symbols and makes it clear that the phenomenon we observed already, where determining whether $-1, 2$ are quadratic residues mod p or not is reduced to finding $p \mod 4, 8$, holds in general.

The theorem is also very surprising. After all, there is nothing on the surface which suggests that whether p is a square mod q should have anything to do with q being a square mod p. Indeed, the name 'quadratic reciprocity' arises exactly from this fact, because there is some sort of 'reciprocal relationship' between the primes p, q and their quadratic residues.

Not only is the theorem surprising and its applications important and varied, the theorem also has many elegant, clever, and deep proofs. Like the Pythagorean Theorem, there are hundreds of proofs of quadratic reciprocity (something like 230 or so by one person's count) that exist. The various proofs of quadratic reciprocity all share the feature that none are obvious, but many of them are elegant and clever. As a matter of fact, Euler and Legendre had already conjectured quadratic reciprocity, but neither of them could prove it. It was Gauss who gave the first proof, in his late teenage years. Throughout his life he kept returning to this problem and ended up giving something like six different proofs of this theorem. Gauss himself held this theorem in the highest esteem, calling it his *Theorem aureum*, or 'golden theorem'. The various standard proofs of quadratic reciprocity all draw on different techniques, and illuminate different aspects of the theory.

Furthermore, the quadratic reciprocity law was the starting point of many related investigations in number theory. The most obvious potential generalizations of quadratic reciprocity are to 'cubic reciprocity' and 'biquadratic reciprocity', which involve asking whether $x^3 \equiv a \mod p, x^4 \equiv a \mod p$ have solutions or not. Obviously, the theory is more complicated than quadratics, but a lot of progress was made towards these problems in the 19th century. The search for a general reciprocity law which contained all these results (in some form or another) eventually led to the Artin reciprocity law, which is a central part of algebraic number theory and class field theory. The problem of searching for what is known as 'non-abelian class field theory', which in its essence is supposed to be a further generalization of the Artin reciprocity law, is one of the central problems of modern number theory.

Let's return to concrete calculations. The following examples should make some of the power of quadratic reciprocity clear.

Examples.

- Characterize all primes p for which 5 is a quadratic residue. First, notice that $\left(\frac{5}{2}\right) = 1$. Let $p > 2$ be an odd prime not equal to 5. Then $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$ by quadratic reciprocity, because $5 \equiv 1 \mod 4$. But $\left(\frac{p}{5}\right) = 1$ if and only if $p \equiv 1, 4 \mod 5$, because those are the only quadratic residues mod 5. Therefore 5 is a quadratic residue mod p if and only if $p \equiv 1, 4 \mod 5$.

- Consider the prime $p = 401$. Evaluate $\left(\frac{132}{401}\right)$. We first factor $132 = 2^2 \cdot 3 \cdot 11$. Then
$$\left(\frac{132}{401}\right) = \left(\frac{2}{401}\right)^2 \left(\frac{3}{401}\right) \left(\frac{11}{401}\right) = \left(\frac{3}{401}\right) \left(\frac{11}{401}\right).$$
To evaluate these two Legendre symbols we use quadratic reciprocity. First, notice $401 \equiv 1 \mod 4$, so
$$\left(\frac{3}{401}\right) = \left(\frac{401}{3}\right) = \left(\frac{2}{3}\right) = -1,$$
and
$$\left(\frac{11}{401}\right) = \left(\frac{401}{11}\right) = \left(\frac{5}{11}\right) = \left(\frac{11}{5}\right) = \left(\frac{1}{5}\right) = 1.$$
(We used quadratic reciprocity with $5, 11$ in this calculation!) Therefore $\left(\frac{132}{401}\right) = -1$, so 132 is not a quadratic residue mod 401.