QUADRATIC RECIPROCITY

SIMON RUBINSTEIN-SALZEDO

We'll begin by discussing modular arithmetic. If m is a positive integer, and a and b are any integers, we say that $a \equiv b \pmod{m}$ if a and b leave the same remainder upon division by m, or equivalently, if $a - b$ is a multiple of m. For any m, we can do arithmetic modulo m: we can unambiguously add or multiply two numbers modulo m:

Exercise 1. Prove that if $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$, then $a + b \equiv a' + b' \pmod{m}$, $a - b \equiv a' - b' \pmod{m}$, and $ab \equiv a'b' \pmod{m}$.

Furthermore, if p is prime, we can divide modulo p.

Exercise 2. If a and b are integers, with $b \not\equiv 0 \pmod{p}$, then there is some integer c so that $a \equiv bc \pmod{p}$.

We think of c here as being a/b modulo p. The situation is slightly more complicated modulo a composite number, and we won't need it in what follows.

Let's write $\mathbb{Z}/m\mathbb{Z}$ for the integers modulo m; we might think of this as the numbers from 0 to $m-1$. If p is prime, then $\mathbb{Z}/p\mathbb{Z}$ is a lot like the real (or complex) numbers in key ways. First of all, we can add, subtract, multiply, and divide (as long as we're not dividing by zero). More subtly, we can also solve polynomial equations over $\mathbb{Z}/p\mathbb{Z}$. For example, suppose we wish to solve $x^3 - x \equiv 6 \pmod{7}$. Then we can easily check that the only solution in $\mathbb{Z}/7\mathbb{Z}$ is $x = 2$. Equivalently, all solutions in $\mathbb{Z}$ satisfy $x \equiv 2 \pmod{7}$.

A very important fact about polynomials over $\mathbb{Z}/p\mathbb{Z}$ is that they have unique factorization, just like integers or polynomials over the real numbers. The factors work the same way, so if $x = a$ is a solution of $f(x) \equiv 0 \pmod{p}$, then $f(x) \equiv (x - a)g(x) \pmod{p}$ for some polynomial $g(x)$. A consequence of this is that a polynomial of degree n over $\mathbb{Z}/p\mathbb{Z}$ has at most n roots in $\mathbb{Z}/p\mathbb{Z}$.

Now, we can start talking about quadratic residues. For a prime p, we'd like to understand for which integers a the equation $x^2 \equiv a \pmod{p}$ has solutions. With this in mind, we'll define a symbol $\left(\frac{a}{p}\right)$, called the Legendre symbol, to be $+1$ if this equation has solutions, -1 if it doesn't, and, for technical reasons, we'll also set $\left(\frac{a}{p}\right) = 0$ if a is a multiple of p. Hence, $\left(\frac{a}{p}\right) + 1$ is the number of solutions to $x^2 \equiv a \pmod{p}$ in $\mathbb{Z}/p\mathbb{Z}$. We call a a (quadratic) residue modulo p if $\left(\frac{a}{p}\right) = 1$ and a (quadratic) nonresidue if $\left(\frac{a}{p}\right) = -1$.

Date: 8 December, 2010.

Let's try working out what $\left(\frac{a}{p}\right)$ is when $p = 5$. Clearly, $\left(\frac{a}{p}\right)$ only depends on $a \pmod p$, so we only have to check $a = 0, 1, 2, 3, 4$. We also only have to check x values from 0 to 4. So, let's write down what x^2 is modulo p for $x = 0, 1, 2, 3, 4$. When we do this, we see that if $a = 1$ or 4, then $\left(\frac{a}{p}\right) = 1$; if $a = 2$ or 3, then $\left(\frac{a}{p}\right) = -1$; and if $a = 0$, then $\left(\frac{a}{p}\right) = 0$.

We'd like to investigate the properties of $\left(\frac{a}{p}\right)$, so let's make a big table.

Exercise 3. For p up to 40, make a table of $\left(\frac{a}{p}\right)$.

What do we notice? Probably, we notice that if p is not 2, then half of the numbers between 1 and $p - 1$ are residues, and half are nonresidues.

Exercise 4. Prove this!

What happens when $a = p - 1$? When is a a residue? When is it a nonresidue? What if $a = 2$?

What can we say about $\left(\frac{ab}{p}\right)$ in terms of $\left(\frac{a}{p}\right)$ and $\left(\frac{b}{p}\right)$?

Exercise 5. Prove that $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. (Hint: Use the previous exercise!)

Now, suppose p and q are both odd primes. How does $\left(\frac{p}{q}\right)$ compare to $\left(\frac{q}{p}\right)$? This relationship is called quadratic reciprocity.

It might be hard to find a pattern here, so let's suppose that $p = 3$. What is the relationship between $\left(\frac{3}{q}\right)$ and $\left(\frac{q}{3}\right)$?

Exercise 6. For several primes p, find a relationship between $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$.

We won't prove the relationship here, but we will look at several steps involved in the proof. The first step is to find a formula for $\left(\frac{a}{p}\right)$ in terms of other quantities we might understand a bit better. The first ingredient we need is Fermat's Little Theorem.

Theorem 1 (Fermat's Little Theorem)**.** *If a is not divisible by p, then $a^{p-1} \equiv 1 \pmod p$.*

Hence, if p is an odd prime, and a is not divisible by p and $b = a^{(p-1)/2}$, then $b^2 \equiv 1 \pmod p$. Since the polynomial $x^2 - 1$ has only two roots, 1 and -1, modulo p, then b must be either 1 or -1 modulo p.

Exercise 7. Show that $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p$.

Okay, so we've turned the Legendre symbol into something involving the exponential function; this is an improvement! Almost all proofs of quadratic reciprocity start with this observation. Many involve the following observation as well.

For p an odd prime and a an integer, there is a unique integer $t(a)$ between $-\frac{p-1}{2}$ and $\frac{p-1}{2}$ so that $a \equiv t(a) \pmod p$. We call $t(a)$ the minimal residue of a modulo p. Now, let $\mu(a)$ be the number of k from 1 to $\frac{p-1}{2}$ so that $t(ak)$ is negative.

Exercise 8. Show that if a is not divisible by p, $\left(\frac{a}{p}\right) = (-1)^{\mu(a)}$.

Exercise 9. Use the previous exercise to prove your conjectures about $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$.

Exercise 10. Let p be an odd prime, and let a be an integer not divisible by p. What is the relationship between $\left(\frac{a}{p}\right)$ and $\left(\frac{-a}{p}\right)$?

Exercise 11. Show that any $a \in \mathbb{Z}/p\mathbb{Z}$ is the sum of two squares in $\mathbb{Z}/p\mathbb{Z}$.

Exercise 12. Show that if a is an integer, and p and q are two primes so that $p \equiv q \pmod{4a}$, then $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$. This explains why a 4 shows up in $\left(\frac{-1}{p}\right)$ and an 8 shows up in $\left(\frac{2}{p}\right)$.

Theorem 2 (Quadratic reciprocity theorem)**.** *Suppose p and q are distinct odd primes. Then*

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

Exercise 13. Assuming the quadratic reciprocity theorem, evaluate $\left(\frac{37}{103}\right)$.

Exercise 14. Evaluate $\left(\frac{-3}{p}\right)$ for odd primes p. Use this to prove that there are infinitely many primes of the form $6n + 1$.

Department of Mathematics, Stanford University, Stanford, CA 94305
E-mail address: simonr@math.stanford.edu