QUADRATIC RESIDUES

Review: Modular Arithmetic. Recall that $a \equiv b \pmod{m}$ means that a and b have the same remainder when you divide each by m. Equivalently, $a \equiv b \pmod{m}$ means exactly that m divides $a - b$. When we talk about $a \pmod{m}$ by itself, we are referring to the remainder of a divided by m (the "least residue"). This is always between 0 and $m - 1$, inclusive.

Theorem: Inverses Mod m. Let a be an integer relatively prime to m. Then there exists an integer b for which $ab \equiv 1 \pmod{m}$. The integer b is the (multiplicative) inverse of a modulo m. For instance, the inverse of 5 modulo 13 is 8 because $5 \cdot 8 = 40 \equiv 1 \pmod{13}$.

Exercise 0. Find the inverse of $7 \pmod{11}$, and the inverse of $11 \pmod{7}$. Explain why 12 could never have an inverse $\pmod{15}$; *e.g.*, why could there never be an integer b with $12b \equiv 1 \pmod{15}$?

If p is a prime number, then every integer in the range $1, 2, \ldots, p-1$ has an inverse modulo p, because all of those integers are relatively prime to p. For instance, if $p = 5$ then the numbers 1,2,3,4 have inverses 1,3,2,4 $\pmod{5}$. Notice that the sequence 1,3,2,4 is a permutation of 1,2,3,4. In related reasoning, suppose we multiplied everything in the sequence $1, 2, 3, 4$ by 2 and reduced modulo 5. We get $2, 4, 1, 3$, another permutation of 1,2,3,4. When we multiply both sequences together, we get

$$(2 \cdot 1)(2 \cdot 2)(2 \cdot 3)(2 \cdot 4) \equiv 1 \cdot 2 \cdot 3 \cdot 4 \pmod{5},$$

because after all these are the same four numbers (in a different order). On the other hand this equation reads

$$2^4 \cdot 4! \equiv 4! \pmod{5}.$$

Since 4! is relatively prime to 5, we can cancel it from both sides to get $2^4 \equiv 1 \pmod{5}$. The generalization of this was proved in 1640 by Fermat:

Fermat's Theorem. Let p be prime and let a be relatively prime to p. Then $a^{p-1} \equiv 1 \pmod{p}$.

Quadratic Residues. Let m and n be integers. We say that n is a *square* mod m if the equation $x^2 \equiv n \pmod{m}$ has a solution in x. In other words, n is a square mod m if it is congruent to a perfect square mod m. We also say that n is a *quadratic residue* for m.

Exercise 1. List the quadratic residues for the primes 3, 5, 7, and 11. Formulate a conjecture for how many quadratic residues there are for a prime p. Does your conjecture work for $p = 2$?

Exercise 2. List the quadratic residues for the composite numbers 9,15, and 21. Does your conjecture from Exercise 1 carry over?

It's straightforward enough to list the quadratic residues for any given modulus m. What's harder, and much more interesting, is to fix the integer n and see which moduli it is a residue for. Let's start with prime moduli...

Exercise 3. Of the first ten primes p, which have -1 as a quadratic residue? Which have 2 as a quadratic residue? Formulate a conjecture about this. (Compute with more primes if necessary.)

Exercise 4. In this exercise we're going to show that -1 is a square modulo an odd prime p if and only if $p \equiv 1 \pmod{4}$.

a) First, let's show that if $p \equiv 1 \pmod 4$, then there is a square root of -1 mod p. Wilson's theorem says that $(p-1)! \equiv -1 \pmod p$. In the product that defines the factorial, pair up 1 with $p-1 \equiv -1$, pair up 2 with $p-2 \equiv -2$, and so on. Conclude that $\left(\frac{p-1}{2}\right)!^2 \equiv -1 \pmod p$.

b) Now let's show that if $p \equiv 3 \pmod 4$, then there is no square root of -1 mod p. Assume there is: say $x^2 \equiv -1 \pmod p$. Raise both sides to the power of $\frac{p-1}{2}$ and use Fermat's little theorem to find a contradiction.

Generators. Consider the powers of 3 modulo 7. They are 1,3,2,6,4,5, and then we're back to 1 again. Notice that we got every number between 1 and 6 this way. This wouldn't work with the powers of 2 modulo 7, which go $1, 2, 4, 1, 2, 4 \ldots$; we are "missing" the numbers 3,5, and 6. We say that 3 is a *generator* mod 7, whereas 2 is not. Generally, g is a generator for a modulus m if every integer which is relatively prime to m is congruent mod m to a power of g.

Exercise 5. a) Show that g is a generator for a prime p if and only if the least power of g to be congruent to 1 mod p is g^{p-1}. b) Assume p is odd. If g is a generator for an odd prime p, what is $g^{\frac{p-1}{2}}$ modulo p? (Use the factorization $g^{p-1} - 1 = (g^{\frac{p-1}{2}} - 1)(g^{\frac{p-1}{2}} + 1)$.)

Exercise 6. Find generators for the moduli 4,5,7,8,9,11, and 12, or else say that there are none.

Theorem 1. Every prime number p has a generator. (In fact, every odd prime power also has a generator, but we won't be needing this.)

Let g be a generator mod p. Then for any a not divisible by p, there is a k for which $g^k \equiv a \pmod p$. Use this to solve the next exercise.

Exercise 7. (Euler's criterion.) Let a be prime to p. Show that a is a quadratic residue for p if and only if $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. What is $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ if g is a nonresidue?

The Legendre Symbol. This a very useful shorthand for dealing with quadratic residues and nonresidues. Let p be an odd prime and let a be an integer. We define *the Legendre symbol* by

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a quadratic residue and } p \nmid a, \\ -1, & \text{if } a \text{ is a quadratic nonresidue,} \\ 0, & \text{if } p \mid a. \end{cases}$$

Then by Exercise 7 we have the congruence

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

If $a = -1$, we get $(-1)^{\frac{p-1}{2}} = \left(\frac{-1}{p}\right)$ (equality, not just congruence mod p, because both sides are ± 1). Therefore -1 is a square mod p if and only if $p \equiv 1 \pmod{4}$, as in Exercise 4.

Exercise 8. Show that the Legendre symbol is multiplicative: $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Exercise 9a. Show that if $p \equiv 1 \pmod{8}$, then $\left(\frac{2}{p}\right) = 1$. Here's how the proof goes: Let g be a generator for p, and let $z = g^{\frac{p-1}{8}}$, so that $z^8 \equiv 1 \pmod{p}$. Show that $z^4 \equiv -1 \pmod{p}$. Then show that if $\tau = z + z^7$, then $\tau^2 \equiv 2 \pmod{p}$!

Exercise 9b. Show that if $p \equiv 1 \pmod{3}$, then $\left(\frac{-3}{p}\right) = 1$. Again, let g be a generator. Let $z = g^{\frac{p-1}{3}}$. Show that $z^2 + z + 1 \equiv 0 \pmod{p}$. (Remember that the polynomial $X^3 - 1$ factors as $(X-1)(X^2+X+1)$.) Now show that if $\tau = 2z + 1$, then $\tau^2 \equiv -3 \pmod{p}$. If $p \equiv 1 \pmod{3}$, what can you say about $\left(\frac{3}{p}\right)$?

It is natural to look for a rule that gives $\left(\frac{a}{p}\right)$ in general. The examples of $a = -1$, $a = 2$, and $a = 3$ suggest that $\left(\frac{a}{p}\right)$, which at first glance has to do with stuff modulo p, might actually only depend on p modulo $4a$! Here's the big shocker: not only does $\left(\frac{a}{p}\right)$ depend only on p modulo $4a$, but if a is another odd prime, then it depends on whether p is a quadratic residue mod a!!

Theorem: The Quadratic Reciprocity Law. (First proved by Gauss, 1801.) Let p be an odd prime. The Legendre symbol $\left(\frac{a}{p}\right)$ obeys the following three laws:

First, the one we know already:

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

Second, a law concerning when 2 is a quadratic residue mod p:

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

This means that 2 is a square mod p if and only if $p \equiv \pm 1 \pmod 8$. Note that Exercise 9a is a special case of this part of the law.

Finally, let q be an odd prime different from p. Then

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

This means that if either of p or q is congruent to 1 mod 4, then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$. If both p and q are 3 mod 4, then $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

Exercise 10. Using the third part of the quadratic reciprocity law, find a simple rule that determines when 5 is a square mod p.

The quadratic reciprocity law can be used as an efficient tool for calculating $\left(\frac{a}{p}\right)$. The idea is this: If a is bigger than p, you can simply reduce a modulo p in the "numerator." If p is bigger than a, factor a into primes: $a = \pm q_1 \ldots q_s$. Note that the Legendre symbol is multiplicative, so we can compute each $\left(\frac{q_i}{p}\right)$ separately. To do this use the quadratic reciprocity law to "flip" the symbol over into $\left(\frac{p}{q_i}\right)$ (or evaluate it completely, if $q_i = 2$). Then repeat the process.

For instance, to find $\left(\frac{102}{37}\right)$:

$$\begin{aligned}
\left(\frac{102}{37}\right) &= \left(\frac{28}{37}\right) \\
&= \left(\frac{4}{37}\right)\left(\frac{7}{37}\right) \\
&= \left(\frac{7}{37}\right) \text{ (4 is a square!)} \\
&= \left(\frac{37}{7}\right) \text{ } (37 \equiv 1 \pmod 4) \\
&= \left(\frac{2}{7}\right) \\
&= 1, \text{ because } 7 \equiv -1 \pmod 8.
\end{aligned}$$

Exercise 11. Calculate $\left(\frac{p}{163}\right)$ for every prime between 2 and 41, inclusive. What do you notice? Does the pattern hold up for $\left(\frac{p}{167}\right)$?

Further Reading. For more on modular arithmetic, see
`http://www.cut-the-knot.org/Curriculum/Algebra/Modulo.shtml`.

For a proof of Fermat's little Theorem, see
`http://www.cut-the-knot.org/blue/Fermat.shtml`.

The quadratic reciprocity law is one of the most often-proved theorems in mathematics. For an elementary proof of Quadratic Reciprocity, see
`http://www.mathpages.com/home/kmath075.htm`.