Section 2: Quadratic Reciprocity

The next logical step after conquering linear congruences is studying quadratic congruences. In this section, we will focus our attention on questions involving quadratic congruences of the type $x^2 \equiv a \pmod{m}$. In particular, we will learn the answers to questions such as:

Is 3 congruent to the square of some number modulo 7?
Does the quadratic congruence $x^2 \equiv -1 \pmod{13}$ have a solution?
For which primes p does the congruence $x^2 \equiv 2 \pmod{p}$ have a solution?

These questions, and more just like them, are answered completely by the Law of Quadratic Reciprocity. This theorem was first stated by Euler and Lagrange, but it remained for Carl Gauss to give the first proof in 1801. Gauss discovered the law by himself (at the age of 19 no less), and throughout his lifetime he found seven different proofs of it! Gauss is widely considered to be one of the greatest mathematicians of all time. In addition to his vast contributions to many different branches of mathematics, he is also renowned for three monumental achievements, any one of which would earn him great acclaim. In geometry, it is the construction of the 17-gon using only a straightedge and compass; in algebra, it is the first completely satisfactory proof of the Fundamental Theorem of Algebra; and in number theory, it is his proof of quadratic reciprocity.

So our general question is this: Given a natural number m, determine all integers a for which $x^2 \equiv a \pmod{m}$ has a solution. Stated another way, find all the squares modulo m. The three questions given above are all examples of questions of this type. We begin with some terminology.

Definition 2.2.1 An integer a is called a ***quadratic residue modulo m*** if $x^2 \equiv a \pmod{m}$ has a solution. Otherwise, a is called a ***quadratic nonresidue modulo m***.

Definition 2.2.2 Let m be a natural number and let a be an integer. We define the ***Legendre symbol*** $\left(\frac{a}{m}\right)$ as follows:

$$\left(\frac{a}{m}\right) = \begin{cases} +1 & \text{if } a \text{ is a quadratic residue modulo } m \\ -1 & \text{if } a \text{ is a quadratic nonresidue modulo } m \end{cases}.$$

This symbol will make the determination of whether a given number is a quadratic residue or not much easier. In general we have two main questions to answer.

1. Find all quadratic residues modulo a given natural number m. This is easily solved by squaring every integer from 0 to $m-1$.

2. Find all natural numbers m such that the given integer a is a quadratic residue modulo m. This is what The Law of Quadratic Reciprocity will answer.

Example 2.2.3 Compute $\left(\frac{3}{5}\right)$.

Simply by squaring every number from 0 to 4, we see that the squares modulo 5 are 0, 1 and 4. Therefore, $\left(\frac{3}{5}\right) = -1$

Exercise 2.2.4 Compute $\left(\frac{3}{6}\right)$ and $\left(\frac{3}{7}\right)$.

I will now present a series of results, all of which can be proven but whose proofs require more advanced notes.

Proposition 2.2.5 Let p be an odd prime, and let a and b be integers, then $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Proposition 2.2.6 (Euler's Criterion) Let p be an odd prime, and let a be an integer, then $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

If we apply Euler's Criterion to $a = -1$, we see that $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$. Clearly, this means that -1 will be a square modulo p if and only if $\frac{p-1}{2}$ is even. Stated another way, -1 is a square modulo p if and only if $\frac{p-1}{2} = 2n$ (for some n). This implies that $p-1$ is a multiple of 4. This gives us the first part of quadratic reciprocity (which I call "Part Negative One" since it applies to the number -1).

Theorem 2.2.7 (Law of Quadratic Reciprocity – Part -1) Let p be an odd prime. Then $\left(\frac{-1}{p}\right) = +1$ if and only if $p \equiv 1 \pmod{4}$.

Example 2.2.8 Compute $\left(\frac{-1}{379}\right)$.

Of course, we could simply square every integer from 0 to 378 (and reduce modulo 379) and see if we ever get 378 (which is -1 modulo 379). But it's much easier to use the division algorithm and note that $379 = 4 \cdot 94 + 3$. This means that $379 \equiv 3 \pmod{4}$, so $\left(\frac{-1}{379}\right) = -1$.

Exercise 2.2.9 Compute $\left(\frac{-1}{2459}\right)$.

The next theorem is the second part of our Law of Quadratic Reciprocity. Since it happens to deal with the number 2, we get to conveniently call it part 2.

Theorem 2.2.10 (Law of Quadratic Reciprocity – Part 2) Let p be an odd prime. Then $\left(\frac{2}{p}\right) = +1$ if and only if $p \equiv 1 (\text{mod } 8)$ or $p \equiv 7 (\text{mod } 8)$.

Exercise 2.2.11 Compute $\left(\frac{2}{487}\right)$.

So now we can handle 2 and –1. What about any other integer? We know from Proposition 2.2.5 that we only need to have a rule for primes. For instance, if I want to compute $\left(\frac{70}{1789}\right)$, I can factor the top number and write it as $\left(\frac{2}{1789}\right)\cdot\left(\frac{5}{1789}\right)\cdot\left(\frac{7}{1789}\right)$. We know how to compute the first Legendre symbol, but we are still clueless about the next two.

Theorem 2.2.12 (Law of Quadratic Reciprocity – Part Big) Let p, q be odd primes. Then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ if and only if $p \equiv 1 (\text{mod } 4)$ or $q \equiv 1 (\text{mod } 4)$.

So if one of the primes involved is congruent to 1 modulo 4, we can interchange the two numbers and keep the same Legendre symbol value. If not, we can interchange them and get the opposite value.

Example 2.2.13

(a) $\left(\frac{11}{97}\right) = \left(\frac{97}{11}\right)$ since $97 \equiv 1 (\text{mod } 4)$

(b) $\left(\frac{31}{379}\right) = -\left(\frac{379}{31}\right)$ since neither prime is congruent to 1 modulo 4.

How does this (the ability to flip the Legendre symbol – either with an additional negative sign or without) help us? Let's examine the last examples more completely.

Example 2.2.13 (Cont.)

(a) We can flip the Legendre symbol and then reduce the larger top number modulo the bottom number. Since 97 is congruent to 9 modulo 11, we get $\left(\frac{11}{97}\right) = \left(\frac{97}{11}\right) = \left(\frac{9}{11}\right)$. 9 is clearly a square modulo 11 (in fact modulo any number larger than 9), we get a Legendre symbol of +1.

(b) Here we can flip the Legendre symbol by adding a negative sign and then reduce the larger top number modulo the bottom number. So we get $\left(\frac{31}{379}\right) = -\left(\frac{379}{31}\right) = -\left(\frac{7}{31}\right)$. Since now have two primes again, we can flip again (picking up another negative sign since both primes are 3 modulo 4). So we have:

$$\left(\frac{31}{379}\right) = -\left(\frac{379}{31}\right) = -\left(\frac{7}{31}\right) = -\left(-\left(\frac{31}{7}\right)\right) = \left(\frac{3}{7}\right).$$

Down to two primes again, we flip again…

$$\left(\tfrac{31}{379}\right) = -\left(\tfrac{379}{31}\right) = -\left(\tfrac{7}{31}\right) = -\left(-\left(\tfrac{31}{7}\right)\right) = \left(\tfrac{3}{7}\right) = -\left(\tfrac{7}{3}\right) = -\left(\tfrac{1}{3}\right) = -(+1) = -1.$$

So the three parts of the Law of Quadratic Reciprocity combine to give a powerful tool for determining whether a given number is a square modulo another. Gauss. At age 19. Wow.

Example 2.2.14 Compute $\left(\tfrac{650}{1109}\right)$.

$\left(\tfrac{650}{1109}\right) = \left(\tfrac{2\cdot 5^2\cdot 13}{1109}\right) = \left(\tfrac{2}{1109}\right)\left(\tfrac{5^2}{1109}\right)\left(\tfrac{13}{1109}\right)$. Since 5^2 is clearly a square and 1109 is congruent to 5 modulo 8, we have,

$$\left(\tfrac{650}{1109}\right) = \left(\tfrac{2\cdot 5^2\cdot 13}{1109}\right) = \left(\tfrac{2}{1109}\right)\left(\tfrac{5^2}{1109}\right)\left(\tfrac{13}{1109}\right) = (-1)(+1)\left(\tfrac{13}{1109}\right) = -\left(\tfrac{13}{1109}\right).$$

Since 1109 is congruent to 1 modulo 4, we can flip and reduce that last Legendre symbol without needing to introduce a negative sign. So we have,

$$\left(\tfrac{650}{1109}\right) = \left(\tfrac{2\cdot 5^2\cdot 13}{1109}\right) = \left(\tfrac{2}{1109}\right)\left(\tfrac{5^2}{1109}\right)\left(\tfrac{13}{1109}\right) = (-1)(+1)\left(\tfrac{13}{1109}\right) = -\left(\tfrac{13}{1109}\right) = -\left(\tfrac{1109}{13}\right) = -\left(\tfrac{4}{13}\right) = -(+1) = -1.$$

So 650 is NOT a square modulo 1109.

Exercise 2.2.15 Compute $\left(\tfrac{100}{4603}\right)$.

Exercise 2.2.16 Compute $\left(\tfrac{617}{971}\right)$.

Exercise 2.2.17 Compute $\left(\tfrac{80}{331}\right)$.