3. Quadratic Reciprocity

In this section we will study quadratic congruences to prime moduli. When p is an odd prime, then any quadratic congruence $ax^2 + bx + c \equiv 0 \pmod{p}$ (with $p \not| a$) may be reduced by completing the square to the simpler congruence $y^2 \equiv d \pmod{p}$, where $d = b^2 - 4ac$ and $y = 2ax + b$. So solving quadratic congruences reduces to the problem of taking square roots.

3.1. Quadratic Residues and Nonresidues.

Definition 3.1.1. *Let p be an odd prime and a an integer not divisible by p. We say that a is a* quadratic residue *of p when $x^2 \equiv a \pmod{p}$ has at least one solution, and a* quadratic nonresidue *otherwise.*

Note that when a is a quadratic residue with $b^2 \equiv a \pmod{p}$ then the congruence $x^2 \equiv a \pmod{p}$ has exactly two solutions, namely $x \equiv \pm b$. For these are both solutions; they are incongruent modulo p since $b \equiv -b \implies 2b \equiv 0 \implies b \equiv 0 \implies a \equiv 0$. (Here we used that $p \neq 2$.) Lastly, there are no more solutions since $p|x^2 - a \implies p|x^2 - b^2 \implies p|(x-b)(x+b) \implies p|(x-b)$ or $p|(x+b)$.

We can find the quadratic residues modulo p by reducing b^2 modulo p for $1 \leq b \leq (p-1)/2$. The other squares will repeat these (in reverse order), since $(p-b)^2 \equiv b^2 \pmod{p}$. It follows that exactly half the nonzero residues are quadratic residues and the other half quadratic nonresidues.

Examples: $p = 11$: the quadratic residues modulo 11 are:

$$1^2, 2^2, 3^2, 4^2, 5^2 \equiv 1, 4, 9, 5, 3 \equiv 1, 4, -2, 5, 3$$

while the quadratic nonresidues are $2, 6, 7, 8, 10 \equiv 2, -5, -4, -3, -1$.

$p = 13$: the quadratic residues modulo 13 are:

$$1^2, 2^2, 3^2, 4^2, 5^2, 6^2 \equiv 1, 4, 9, 3, 12, 10 \equiv 1, 4, -4, 3, -1, -3$$

while the quadratic nonresidues are ± 2, ± 5, ± 6.

The reason for the patterns we see here will become apparent later.

Another way to see that exactly half the nonzero residues are quadratic residues is to use primitive roots. Let g be a primitive root modulo p. Then the nonzero residues are g^k for $0 \leq k \leq p-2$ and every integer not divisible by p is congruent to g^k for some k in this range. The quadratic residues are the g^k for even k: that is, the powers of g^2.

For example when $p = 13$ we may take $g = 2$, so $g^2 = 4$ with successive powers $1, 4, 3, 12, 9, 10 \pmod{13}$. These are the quadratic residues; to get the quadratic nonresidues multiply them by $g = 2$ to get the odd powers $2, 8, 6, 11, 5, 7 \pmod{13}$.

3.2. **Legendre Symbols and Euler's Criterion.**

Definition 3.2.1. *The* Legendre Symbol $\left(\frac{a}{p}\right)$ *is defined as follows:*

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{if } p \not| a \text{ and } x^2 \equiv a \pmod{p} \text{ has a solution} \\ -1 & \text{if } p \not| a \text{ and } x^2 \equiv a \pmod{p} \text{ does not have a solution} \\ 0 & \text{if } p | a \end{cases}$$

In all cases, the number of (incongruent) solutions to $x^2 \equiv a \pmod{p}$ *is* $1 + \left(\frac{a}{p}\right)$.

Proposition 3.2.2. *Let* p *be an odd prime.*

(a) $a \equiv b \pmod{p} \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(b) **Euler's Criterion:** $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.

(c) $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} +1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4} \end{cases}$.

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

Corollary 3.2.3. *Let p be an odd prime.*

If $p \equiv 1 \pmod{4}$ then $\left(\frac{-a}{p}\right) = \left(\frac{a}{p}\right)$ for all a.

If $p \equiv 3 \pmod{4}$ then $\left(\frac{-a}{p}\right) = -\left(\frac{a}{p}\right)$ for all a.

If we start to ask questions such as "for which primes p is 2 a quadratic residue?" then we are led to one of the most famous results in elementary number theory. Experimental evidence for small primes easily convinces one that the answer is "primes congruent to $\pm 1 \pmod{8}$":

$$\left(\frac{2}{p}\right) = +1 \text{ for } p = 7, 17, 23, 31, 41, 47, 71, \dots$$

$$\left(\frac{2}{p}\right) = -1 \text{ for } p = 3, 5, 11, 13, 19, 29, 37, 43, \dots$$

More generally, the value of $\left(\dfrac{a}{p}\right)$ for fixed a and variable p only depends on the residue of p modulo $4a$. This is one form of Gauss's famous Law of Quadratic Reciprocity.

3.3. The Law of Quadratic Reciprocity.

Proposition 3.3.1. *[Gauss's Lemma] Let p be an odd prime and a an integer not divisible by p. Then $\left(\dfrac{a}{p}\right) = (-1)^s$, where s is the number of integers i with $0 < i < p/2$ for which the least residue of ai is negative.*

Example: Take $p = 13$ and $a = 11$; then we reduce $11, 22, 33, 44, 55, 66$ modulo 13 to $-2, -4, -6, 5, 3, 1$. As expected by the proof of the Proposition, these are, up to sign, the integers between 1 and 6. There are 3 minus signs, so $\left(\dfrac{11}{13}\right) = (-1)^3 = -1$.

If $p = 13$ and $a = 10$ then we reduce $10, 20, 30, 40, 50, 60$ to $-3, -6, 4, 1, -2, -5$ with four negative values, so $\left(\dfrac{10}{13}\right) = (-1)^4 = 1$. Indeed, $6^2 = 36 \equiv 10 \pmod{13}$.

Corollary 3.3.2. *Assume that $a > 0$, and set $a' = a$ if a is even, $a' = a - 1$ if a is odd. Then $\left(\dfrac{a}{p}\right) = (-1)^s$ where*

$$s = \sum_{k=1}^{a'} \left[(kp)/(2a)\right].$$

Example: Take $p = 13$ and $a = 11$, so $a' = 10$. Then $\left(\frac{11}{13}\right) = (-1)^s$ where $s = [13/22] + [26/22] + [39/22] + [52/22] + [65/22] + [78/22] + [91/22] + [104/22] + [117/22] + [130/22] \equiv 0 + (1+1) + (2+2) + 3 + (4+4) + (5+5) \equiv 1 \pmod 2$, so $\left(\frac{11}{13}\right) = -1$.

We can use Corollary 3.3.2 to Gauss's Lemma to evaluate $\left(\frac{2}{p}\right)$ for *all* odd primes p.

Proposition 3.3.3. *Let p be an odd prime. Then*

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} +1 & \text{if } p \equiv \pm 1 \pmod 8; \\ -1 & \text{if } p \equiv \pm 3 \pmod 8. \end{cases}$$

More generally, we can deduce that in general the value of $\left(\frac{a}{p}\right)$ only depends on $p \pmod{4a}$, our first form of *quadratic reciprocity*: although the definition of $\left(\frac{a}{p}\right)$ is in terms of $a \pmod p$, it is far from obvious that it depends on $p \pmod{4a}$!

Proposition 3.3.4. *Let p and q be odd primes and a a* positive *integer not divisible by either p or q. Then*

$$p \equiv \pm q \pmod{4a} \implies \left(\frac{a}{p}\right) = \left(\frac{a}{q}\right).$$

(For $a < 0$ a slightly modified result holds: exercise.)

The *Law of Quadratic Reciprocity* uses this result in the case that a is also prime to get a very symmetric statement.

Theorem 3.3.5. *[Quadratic Reciprocity] Let p and q be distinct odd primes. Then*

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

So $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$ *if* $p \equiv 1$ *or* $q \equiv 1 \pmod 4$, *while* $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$ *if* $p \equiv q \equiv 3 \pmod 4$.

Since the Legendre symbol $\left(\frac{a}{p}\right)$ is completely multiplicative in a for fixed p, to evaluate $\left(\frac{a}{p}\right)$ for all a we only need to know the values of $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$ and $\left(\frac{q}{p}\right)$, for odd primes q different from p. The Law of Quadratic Reciprocity tells us how to evaluate each of these! Special cases of the reciprocity law were conjectured by Euler on the basis of substantial calculations and knowledge, but Gauss first proved it, and in fact gave several proofs.

Summary of Quadratic Reciprocity: If p and q are distinct odd primes then:

- $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} +1 & \text{if } p \equiv 1 \pmod 4; \\ -1 & \text{if } p \equiv 3 \pmod 4; \end{cases}$
- $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} +1 & \text{if } p \equiv \pm 1 \pmod 8; \\ -1 & \text{if } p \equiv \pm 3 \pmod 8; \end{cases}$

- $$\left(\frac{q}{p}\right) = \begin{cases} +\left(\frac{p}{q}\right) & \text{if } \textit{either } p \equiv 1 \pmod{4} \ \textit{ or } q \equiv 1 \pmod{4}; \\ -\left(\frac{p}{q}\right) & \text{if } \textit{both } p \equiv 3 \pmod{4} \ \textit{ and } q \equiv 3 \pmod{4}. \end{cases}$$

Using QR we may easily answer questions of the form: Given a, for which p is $\left(\frac{a}{p}\right) = 1$? For example:

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = \begin{cases} +1 & \text{if } p \equiv 1, 3 \pmod{8}; \\ -1 & \text{if } p \equiv -1, -3 \pmod{8}. \end{cases}$$

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \begin{cases} +1 & \text{if } p \equiv 1 \pmod{3}; \\ -1 & \text{if } p \equiv -1 \pmod{3}. \end{cases}$$

$$\left(\frac{3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p}{3}\right) = \begin{cases} +1 & \text{if } p \equiv \pm 1 \pmod{12}; \\ -1 & \text{if } p \equiv \pm 5 \pmod{12}. \end{cases}$$

(Notice how $\left(\frac{a}{p}\right)$ sometimes depends only on p modulo a rather than modulo $4a$.)

Using Proposition 3.3.4 gives an alternative method of evaluating $\left(\frac{a}{p}\right)$ for fixed $a > 0$. Take $a = 3$, so we know that $\left(\frac{3}{p}\right)$ only depends on $\pm p \pmod{12}$; when $p = 13$ we have $\left(\frac{3}{13}\right) = +1$

and when $p = 5$ we have $\left(\dfrac{3}{5}\right) = -1$; so $\left(\dfrac{3}{p}\right) = +1$ for all $p \equiv \pm 1 \pmod{12}$ and $\left(\dfrac{3}{p}\right) = -1$ for all $p \equiv \pm 5 \pmod{12}$.

When $a < 0$ it is also true that $p \equiv q \pmod{4a} \implies \left(\dfrac{a}{p}\right) = \left(\dfrac{a}{q}\right)$, but now $p \equiv -q \pmod{4a} \implies \left(\dfrac{a}{p}\right) = -\left(\dfrac{a}{q}\right)$. (Apply Prop. 3.3.4 to $-a$ to see this.) Hence we can evaluate $\left(\dfrac{a}{p}\right)$ for $a < 0$.

For example, take $a = -5$. Then $\left(\dfrac{-5}{p}\right)$ depends on p modulo 20, giving $\varphi(20) = 8$ cases. Take the primes $p = 61, 3, 7, 29$ which are congruent respectively to $1, 3, 7, 9 \pmod{20}$; computing the four Legendre symbols $\left(\dfrac{-5}{p}\right)$, we find that they are all $+1$. Hence

$$\left(\frac{-5}{p}\right) = \begin{cases} +1 & \text{if } p \equiv 1, 3, 7, 9 \pmod{20}; \\ -1 & \text{if } p \equiv 11, 13, 17, 19 \pmod{20}. \end{cases}$$

where the second line follows from the first by the "anti-symmetry" since $-5 < 0$.