13. Quadratic Residues

We now turn to the question of when a quadratic equation has a solution modulo $m$. The general quadratic equation looks like

$$ax^2 + bx + c \equiv 0 \mod m.$$ 

Assuming that $m$ is odd or that $b$ is even we can always complete the square (the usual way) and so we are reduced to solving an equation of the form

$$x^2 \equiv a \mod m.$$ 

In fact, we are usually only interested in solving the equation modulo a prime, in which we are only missing the prime 2.

**Definition 13.1.** We say $a \in \mathbb{Z}_m$ is a **quadratic residue** of $p$ if $a$ is a square modulo $m$, that is, the equation

$$x^2 \equiv a \mod m$$

has a solution.

**Theorem 13.2** (Euler’s Criterion). Let $p$ be an odd prime.

The congruence

$$x^2 \equiv a \mod p$$

has a solution, that is, $a$ is a quadratic residue of $p$ if and only if either $p$ divides $a$ or $a^{(p-1)/2} \equiv 1$. If $a$ is not a quadratic residue then $a^{(p-1)/2} \equiv -1$.

**Proof.** If $p|a$ then $a \equiv 0$ and $0^2 = 0 \equiv a \mod p$, so that 0 is a quadratic residue of $p$.

Now suppose that $a$ is coprime to $p$. By assumption there is an integer $k$ such that $p = 2k + 1$. In this case

$$\frac{(p - 1)}{2} = k.$$ 

If we put

$$b = a^k$$

then

$$b^2 = (a^k)^2 = a^{2k} = a^{p-1} \equiv 1 \mod p,$$

by Fermat. Thus $b$ is a solution of the equation

$$x^2 \equiv 1 \mod p,$$
so that $b$ is a root of the polynomial $x^2 - 1$. As $\mathbb{Z}_p$ is a field, this polynomial has at most two roots. Now $\pm 1$ are two roots of this equation. It follows that

$$b \equiv \pm 1 \mod p.$$ Suppose that $a$ is a quadratic residue. Then $c^2 \equiv a \mod p$ for some integer $c$ so that

$$b = a^k \equiv (c^2)^k \mod p = c^{p-1} \equiv 1 \mod p,$$ by Fermat. Thus $a$ is a quadratic residue if and only if $a$ is a root of the polynomial

$$x^k - 1.$$ This polynomial has at most $k$ roots.

But if $a$ is coprime to $p$ then the polynomial

$$x^2 - a \equiv 0 \mod p,$$ either has two solutions or no solutions. Thus precisely $k$ residues classes are quadratic residues and so all of the roots of the polynomial $x^k - 1$ are quadratic residues.

In fact it is possible to write down, in some sense, the quadratic residues. Note that

$$S = \{ a \in \mathbb{Z} \mid -k \leq a \leq k \}$$ is a compete residue system modulo $p$. It follows that $\pm 1$ are the roots of $x^2 - 1^2$, $\pm 2$ are the roots of $x^2 - 2^2$, $\pm 3$ are the roots of $x^2 - 3^2$ and so on.

It turns out to be very convenient to define a symbol which keeps track of when $a$ is a quadratic residue modulo a prime $p$.

**Definition 13.3.** Let $p$ be a prime and let $a$ be an integer.

We define the *Legendre symbol* by the rule:

$$\left( \frac{a}{p} \right) = \begin{cases} 0 & \text{if } p \text{ divides } a. \\ 1 & \text{if } (a, p) = 1 \text{ and } a \text{ is a quadratic residue of } p. \\ -1 & \text{if } (a, p) = 1 \text{ and } a \text{ is not a quadratic residue of } p. \end{cases}$$

**Corollary 13.4.** If $p$ is an odd prime and $a \in \mathbb{Z}$ then

$$\left( \frac{a}{p} \right) \equiv a^{(p-1)/2} \mod p.$$
Proof. Immediate from (13.2) and the definition of the Legendre symbol.

Here are some of the key properties of the Legendre symbol:

**Theorem 13.5.** Let $p$ be an odd prime and let $a$ and $b$ be two integers.

1. If $a \equiv b \mod p$ then
   
   \[
   \left( \frac{a}{p} \right) = \left( \frac{b}{p} \right).
   \]

2. If $p$ does not divide $a$ then
   
   \[
   \left( \frac{a^2}{p} \right) = 1.
   \]

3. \[
   \left( \frac{-1}{p} \right) = (-1)^{(p-1)/2}.
   \]
   Thus $-1$ is a quadratic residue if and only if $p \equiv 1 \mod 4$.

4. \[
   \left( \frac{ab}{p} \right) = \left( \frac{a}{p} \right) \left( \frac{b}{p} \right).
   \]

**Proof.** If $a \equiv b \mod p$ then $x^2 - a$ and $x^2 - b$ have the same roots modulo $p$. Thus (1) is clear. $a^2$ is obviously a quadratic residue. Thus (2) is also clear.

(13.2) implies that

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

If $p = 4k + 1$ then

\[
\frac{p - 1}{2} = 2k,
\]

is even so that

\[
(-1)^{(p-1)/2} = (-1)^{2k} = 1.
\]

Thus $-1$ is a quadratic residue of $p$ if $p = 4k + 1$. On the other hand, if $p = 4k + 3$ then

\[
\frac{p - 1}{2} = 2k + 1,
\]

is odd so that

\[
(-1)^{(p-1)/2} = (-1)^{2k+1} = -1.
\]
Thus \(-1\) is not a quadratic residue of \(p\) if \(p = 4k + 3\). This gives (3).

If either \(a\) or \(b\) is a multiple of \(p\) then \(ab\) is also a multiple of \(p\). Vice-versa, if \(ab\) is a multiple of \(p\) then one of \(a\) and \(b\) is a multiple of \(p\). In this case

\[ \left( \frac{ab}{p} \right) = \left( \frac{a}{p} \right) \left( \frac{b}{p} \right) \]

holds, as zero equals zero.

Thus we may assume that \(a\), \(b\) and \(ab\) are all coprime to \(p\). In this case

\[ \left( \frac{a}{p} \right) \equiv a^{(p-1)/2} \mod p \quad \text{and} \quad \left( \frac{b}{p} \right) \equiv b^{(p-1)/2} \mod p. \]

Then

\[ \left( \frac{ab}{p} \right) \equiv (ab)^{(p-1)/2} \mod p \]

\[ = a^{(p-1)/2}b^{(p-1)/2} \]

\[ \equiv \left( \frac{a}{p} \right) \left( \frac{b}{p} \right) \mod p. \]

This is (4).

\[ \square \]

It seems worth pointing out that one case of (4) of (13.5) is straightforward. If \(a\) and \(b\) are quadratic residues then we may find \(\alpha\) and \(\beta\) such that

\[ \alpha^2 \equiv a \mod p \quad \text{and} \quad \beta^2 \equiv b \mod p. \]

In this case

\[ (\alpha\beta)^2 = \alpha^2\beta^2 \]

\[ \equiv ab \mod p. \]

Thus if \(a\) and \(b\) are quadratic residues then so is \(ab\). In this case

\[ \left( \frac{ab}{p} \right) = \left( \frac{a}{p} \right) \left( \frac{b}{p} \right), \]

holds as both sides are 1.

It is interesting to see how to relate the problem of being a quadratic residue modulo \(m\) to being a quadratic residue modulo a prime.

**Theorem 13.6.** Let \(m\) be a natural number bigger than one and let \(a\) be coprime to \(m\).

Then \(a\) is a quadratic residue of \(m\) if and only if \(a\) is a quadratic residue of every odd prime dividing \(m\) and if \(m = 2^2m'\) where \(m'\) is
odd then \( a \) is congruent to one modulo 4 and if 8 divides \( m \) then \( a \) is congruent to one modulo 8.

*Proof.* Let \( m = 2^e p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r} \) be the prime factorisation of \( m \). We want to solve the equation

\[
x^2 \equiv a \pmod{m}.
\]

By the Chinese remainder theorem it is enough to solve the equation for every prime dividing \( m \). \( \square \)