# Day 3: Quadratic Residues

We concluded our session last week with a brief introduction to Quadratic Residues. That brief introduction is repeated below, and is built on from there.

## Quadratic Residues: An Introduction

First, recall from the Problem Set 2 that $\mathbb{Z}_p^* = \{1, 2, 3..., p-1\}$. That is, every non-zero element of $\mathbb{Z}_p$ is invertible! We'll focus our treatment to *odd* primes (i.e. $p \neq 2$ and is prime) since $\mathbb{Z}_2^* = \{1\}$ and there's nothing interesting happening there.

**Definition:** Let $p$ be an odd prime and let $a \in \mathbb{Z}_p^*$. We say $a$ is a **quadratic residue modulo** $p$ if there exists an element $x \in \mathbb{Z}_p^*$ such that $x^2 \equiv a \pmod{p}$. That is, $a$ is a square modulo $p$.

In Problem Set 1 you were asked to analyze squares modulo different values of $n$. Let's take a look at the squares (and non-squares) modulo primes starting at $p = 5$. For brevity, we'll truncate $x^2 \pmod 5$ as $x^2$ (5).

$\mathbb{Z}_5$

| $x$ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| $x^2$ (5) | 1 | 4 | 4 | 1 |

**squares:** $1, 4$

**non-squares:** $2, 3$

$\mathbb{Z}_7$

| $x$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| $x^2$ (7) | 1 | 4 | 2 | 2 | 4 | 1 |

**squares:** $1, 2, 4$

**non-squares:** $3, 5, 6$

There are a few patterns at play here. For the moment, we'll focus on the fact that values of $x^2$ repeat in reverse order after passing $\dfrac{p-1}{2}$. Indeed, modulo 5, we have $-1 \equiv 4 \pmod 5$ and $-2 \equiv 3 \pmod 5$. Modulo 7, we have $-1 \equiv 6 \pmod 7$, $-2 \equiv 5 \pmod 7$, and $-3 \equiv 4 \pmod 7$. In general, it makes sense that $(-x)^2 \equiv x^2 \pmod n$ as $(-x)^2 = x^2$ in the integers themselves! Thus, we can consider fewer values to build these tables. Let's do this again for $\mathbb{Z}_{11}$ and $\mathbb{Z}_{13}$.

$\mathbb{Z}_{11}$

| $x$ | $\pm1$ | $\pm2$ | $\pm3$ | $\pm4$ | $\pm5$ |
|---|---|---|---|---|---|
| $x^2$ (11) | 1 | 4 | 9 | 5 | 3 |

**squares:** $1, 3, 4, 5, 9$

**non-squares:** $2, 6, 7, 8, 10$

$\mathbb{Z}_{13}$

| $x$ | $\pm1$ | $\pm2$ | $\pm3$ | $\pm4$ | $\pm5$ | $\pm6$ |
|---|---|---|---|---|---|---|
| $x^2$ (13) | 1 | 4 | 9 | 3 | 12 | 10 |

**squares:** $1, 3, 4, 9, 10, 12$

**non-squares:** $2, 5, 6, 7, 8, 11$

A couple of patterns are emerging from these tables. These patterns hold true for general odd primes $p$.

1. In $\mathbb{Z}_p^*$, **exactly** *half* of the elements are squares/residues. The other half are not.

2. Every square in $\mathbb{Z}_p^*$ has exactly 2 distinct square roots.

The first result is left for the exercises in Problem Set 3. The second result requires the following theorem to prove:

**Theorem:** Let $a, b \in \mathbb{Z}$. If $ab \equiv 0 \pmod{p}$, then $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$.

**Proof:** If $a \equiv 0 \pmod{p}$, then the result is clear as $0b \equiv 0 \pmod{p}$. Suppose instead that $a \not\equiv 0 \pmod{p}$. Then $a^{-1} \pmod{p}$ exists in $\mathbb{Z}_p^*$. Our hypothesis is that $ab \equiv 0 \pmod{p}$, so we can start with this congruence and then multiply it by $a^{-1}$. We have

$$\begin{aligned} & ab \equiv 0 \pmod{p} \\ \Rightarrow\ & a^{-1}(ab) \equiv a^{-1} \cdot 0 \pmod{p} \\ \Rightarrow\ & (a^{-1}a)b \equiv 0 \pmod{p} \\ \Rightarrow\ & 1b \equiv 0 \pmod{p} \\ \Rightarrow\ & b \equiv 0 \pmod{p}. \end{aligned}$$

□

**Remarks:**

*(i)* This is also a key property of prime numbers. If $a, b \in \mathbb{Z}$ and $p \in \mathbb{Z}$ is a prime number, then $p \mid (ab)$ if and only if $p \mid a$ or $p \mid b$.

*(ii)* The above theorem is false for all composite numbers. For example, $3 \cdot 4 \equiv 0 \pmod{12}$.

**Theorem 2:** Let $p$ be an odd prime and suppose that $a \in \mathbb{Z}_p^*$ is a residue modulo $p$. Then there are *exactly* two distinct solutions to $x^2 \equiv a \pmod{p}$. Moreover, if $x^2 \equiv y^2 \equiv a \pmod{p}$, then $x \equiv \pm y \pmod{p}$.

**Proof:** Suppose that $x^2 \equiv a \pmod{p}$. Let $y$ also be a square root of $a$ in $\mathbb{Z}_p^*$, so $y^2 \equiv a \pmod{p}$. Therefore, we have

$$\begin{aligned} & x^2 - y^2 \equiv a - a \equiv 0 \pmod{p} \\ \Rightarrow\ & (x-y)(x+y) \equiv 0 \pmod{p} \\ \Rightarrow\ & x - y \equiv 0 \pmod{p} \quad \text{or} \quad x + y \equiv 0 \pmod{p} \\ \Rightarrow\ & x \equiv y \pmod{p} \quad \text{or} \quad x \equiv -y \pmod{p}. \end{aligned}$$

Therefore, if $x$ and $y$ are two square roots of $a$ modulo $p$, then it **must** be the case that $x \equiv \pm y \pmod{p}$. As $p$ is odd, we know that $x \not\equiv -x \pmod{p}$ when $x \in \mathbb{Z}_p^*$, thus our result holds. □

Now we can break for Problem Set 3.

## Legendre Symbols and Quadratic Reciprocity

**Definition:** Let $a$ be an integer and let $p$ be an odd prime. We define the **Legendre symbol** as

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \gcd(a,p) > 1, \\ 1, & \text{if } a \text{ is a quadratic residue modulo } p, \\ -1, & \text{if } a \text{ is } \textit{not} \text{ a quadratic residue modulo } p. \end{cases}$$

**Note:** This notation is not to be confused with the ratio $\frac{a}{p} \in \mathbb{Q}$.

Before listing some properties of the Legendre Symbol, a pre-requisite result in establishing some of the rules:

**Theorem 3: Fermat's Little Theorem!** Let $a \in \mathbb{Z}_p^*$. Then $a^{p-1} \equiv 1 \pmod{p}$.

Properties of the Legendre Symbol:

**1) It's multiplicative!** $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

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

**Remark:** Can prove $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$ using Fermat's Little Theorem and difference of squares.

**3) Law of Quadratic Reciprocity:** Let $p$ and $q$ be *distinct* odd primes. Then

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

The Law of Quadratic Reciprocity is an astounding one! It directly relates the question of whether or not $\sqrt{p}$ exists in $\mathbb{Z}_q^*$ to the existence of $\sqrt{q}$ in $\mathbb{Z}_p^*$. Gauss was the first mathematician to successfully prove this result, and produced six unique proofs of it. To date, there are over 240 unique proofs!

Let's demonstrate the utility of the reciprocity law.

**Example:** Is 5 a square modulo 31? We now have three methods to answer this question.

*Method 1:* Check the square of every integer modulo 31.

We've done this in the past $\left(\text{check } n^2 \text{ for } 1 \le n \le \frac{p-1}{2}\right)$. As the modulus grows in size, this method becomes very inefficient. We won't use this again.

*Method 2:* Use Euler's Criterion. We know $\left(\dfrac{5}{31}\right) \equiv 5^{\frac{31-1}{2}} \equiv 5^{15} \pmod{31}$. Ouch! There are ways of simplifying this without as much effort as computing the product of 5 with itself fifteen times, but they rely on understanding notions of *primitive elements* and *Euler's totient function*. Both are worth looking up, but we aren't equipped with these tools yet.

*Method 3:* Use Quadratic Reciprocity! We'll do this in one line!

$$\left(\frac{5}{31}\right) = \left(\frac{31}{5}\right)\Big(-1\Big)^{\frac{5-1}{2}\cdot\frac{31-1}{2}} = \left(\frac{1}{5}\right)(-1)^{30} = 1 \cdot 1 = 1.$$

Therefore, 5 is a square modulo 31. ■

**Note:** $\left(\dfrac{31}{5}\right) = \left(\dfrac{1}{5}\right)$ as $31 \equiv 1 \pmod{5}$. This is where Quadratic Reciprocity obtains its utility! We can use this property to continue to reduce the Legendre symbol until it is manageable.

To compute Legendre symbols involving even numbers, the next theorem will be of great use.

**Theorem 4:** Let $p$ be an odd prime. Then

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

**Example:** Is 6 a square modulo 31? Let's use reciprocity again.

$$\begin{aligned} \left(\frac{6}{31}\right) &= \left(\frac{2}{31}\right) \cdot \left(\frac{3}{31}\right) \qquad \textit{Legendre symbol is multiplicative} \\ &= 1 \cdot \left(\frac{31}{3}\right)\Big(-1\Big)^{\frac{3-1}{2}\cdot\frac{31-1}{2}} \\ &= \left(\frac{1}{3}\right) \cdot (-1)^{15} = 1 \cdot -1 = -1. \end{aligned}$$

No, 6 is not a square modulo 31. ■

And with that, we're ready for Problem Set 4!