4-8-2019

# Quadratic Residues

In this section, we'll begin our discussion of quadratic congruences. The central result to come is called **Quadratic Reciprocity**.

Gauss considered the proofs he gave of quadratic reciprocity one of his crowning achievements; in fact, he gave 6 distinct proofs during his lifetime. Reciprocity is a deep result: Proofs eluded both Euler and Legendre.

The reciprocity law is simple to state. For $p$ and $q$ odd primes, it relates solutions to the two congruences

$$x^2 = p \pmod{q} \quad \text{and} \quad x^2 = q \pmod{p}.$$

(Note how $p$ and $q$ switch places: This explains why it's called a *reciprocity* law.) The law of quadratic reciprocity says:

The congruences are either both solvable or both unsolvable, unless both primes are congruent to 3 mod 4. In that case, one is solvable while the other is not.

Gauss first gave a proof of this when he was 19!

Gauss's masterwork, the *Disquisitiones Arithmeticae*, was published in 1801 when Gauss was 24. It changed the course of number theory, collecting scattered results into a unified theory.

We'll look at some important computational devices before we consider reciprocity.

**Definition.** Let $(a, m) = 1$, $m > 0$. $a$ is a **quadratic residue** mod $m$ if the following equation has a solution:

$$x^2 = a \pmod{m}.$$

Otherwise, $a$ is a **quadratic nonresidue** mod $m$.

**Example.** (a) Is 8 a quadratic residue mod 17?

(b) Find all the quadratic residues mod 18.

(a) 8 is a quadratic residue mod 17, since $5^2 = 8 \pmod{17}$. □

(b) I list the elements in $\{1, 2, \ldots 17\}$ which are relatively prime to 18 and compute their squares mod 18:

| $x$ | 1 | 5 | 7 | 11 | 13 | 17 |
|---|---|---|---|---|---|---|
| $x^2 \pmod{18}$ | 1 | 7 | 13 | 13 | 7 | 1 |

The quadratic residues are the *squares*: that is, 1, 7, and 13.

Since $x^2 = (-x)^2$, the second row of the table is symmetric left-to-right. □

---

**Lemma.** Let $p$ be an odd prime, and consider the congruence

$$x^2 = a \pmod{p}.$$

(a) The only solution is $x = 0$ if $a = 0$.

(b) There are exactly 0 or 2 solutions if $p \nmid a$.

**Proof.** $x = 0$ solves $x^2 = 0 \pmod{p}$. Conversely, if $x^2 = 0 \pmod{p}$, then $p \mid x^2$, so $p \mid x$, and hence $x = 0 \pmod{p}$.

Suppose $p \nmid a$. To show there are 0 or 2 solutions, suppose there is at least one solution $b$. Then $b^2 = a \pmod{p}$, so $(-b)^2 = a \pmod{p}$. I claim that $b$ and $-b$ are distinct.

If not, then $b = -b \pmod{p}$, so $p \mid 2b$. $p$ is an odd prime, so $p \not| 2$. Therefore, $p \mid b$, $b = 0 \pmod{p}$, $b^2 = 0 \pmod{p}$, and finally $a = 0 \pmod{p}$ — contradicting $p \not| a$. Hence, $b \neq -b \pmod{p}$.

Now I have two distinct solutions; since a quadratic equation mod $p$ has at most two solutions (Prove it!), there are exactly two. □

For example, $x^2 = 8 \pmod{17}$ has 5 and 12 as solutions, and $5 = -12 \pmod{17}$.

On the other hand, you can check that the quadratic residues mod 17 are $\{1, 2, 4, 8, 9, 13, 15, 16\}$. Thus, $x^2 = 5 \pmod{17}$ has no solutions.

Note that the result is false if $p = 2$, since $x^2 = 1 \pmod{2}$ has exactly one solution: $x = 1 \pmod{2}$.

**Corollary.** Let $p$ be an odd prime. There are $\dfrac{p-1}{2}$ quadratic residues and $\dfrac{p-1}{2}$ quadratic nonresidues mod $p$ in $\{1, \ldots, p-1\}$.

**Proof.** $k$ and $-k = p - k$ have the same square mod $p$. That is, 1 and $p-1$ have the same square, 2 and $p-2$ have the same square, ..., and $\dfrac{p-1}{2}$ and $\dfrac{p-1}{2} + 1$ have the same square.

Thus, the number of different squares is $\dfrac{p-1}{2}$ — these squares are the quadratic residues, and the other $\dfrac{p-1}{2}$ numbers in $\{1, 2, \ldots, p-1\}$ are quadratic nonresidues. □

**Definition.** Let $p$ be an odd prime, and let $(a, p) = 1$. The **Legendre symbol** $\left(\dfrac{a}{p}\right)$ is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } p \\ -1 & \text{if } a \text{ is a quadratic nonresidue mod } p \end{cases}$$

Note that $a = 0$ is disallowed (since $(0, p) = p \neq 1$) even though $x^2 = 0 \pmod{p}$ has a solution.

As an easy example, $\left(\dfrac{4}{11}\right) = 1$, since $4 = 2^2 \pmod{11}$. On the other hand, $\left(\dfrac{5}{17}\right) = -1$, because as I noted above $x^2 = 5 \pmod{17}$ has no solutions.

You might wonder about the case where $p = 2$, or the case where the modulus is composite. For $p = 2$, there are only two quadratic congruences:

$$x^2 = 0 \pmod{2} \quad \text{and} \quad x^2 = 1 \pmod{2}.$$

These have the solutions $x = 0 \pmod{2}$ and $x = 1 \pmod{2}$ — nothing much is going on.

If the modulus has prime factorization $n = p_1^{r_1} \cdots p_k^{r_k}$, then relative primality implies that it's enough to solve the congruences $x^2 = a \pmod{p_i^{r_i}}$ for each $i$. It turns out that solving such a congruence reduces to determining whether $a$ is a quadratic residue mod $p_i$. Therefore, there is little harm in concentrating on the case of a single prime.

---

**Example.** Solve the congruence

$$x^2 = 79 \pmod{91}.$$

I'll solve the congruences

$$x^2 = 79 \pmod{7} \quad \text{and} \quad x^2 = 79 \pmod{13}.$$

$x^2 = 79 \pmod{7}$ reduces to $x^2 = 2 \pmod{7}$. Making a table of squares mod 7, I find that the solutions are $x = 3$ and $x = 4$ mod 7.

$x^2 = 79 \pmod{13}$ reduces to $x^2 = 1 \pmod{13}$. The solutions are $x = 1$ and $x = -1 = 12$ mod 13.

I'll consider the $2 \cdot 2 = 4$ possibilities, solving using the Chinese Remainder Theorem. But note that since $m^2 = (-m)^2$, the solutions will come in pairs. So once I find a solution $m$, I know that $-m$ is also a solution.

Consider

$$x = 3 \pmod 7$$
$$x = 1 \pmod{13}$$

| $m$ | 7 | 13 |
|---|---|---|
| $p$ | 13 | 7 |
| $s = p^{-1} \pmod m$ | 6 | 2 |
| $a$ | 3 | 1 |

$$x = 13 \cdot 6 \cdot 3 + 7 \cdot 2 \cdot 1 = 248 = 66 \pmod{91}.$$

Then $x = -66 = 25 \pmod{91}$ is another solution.
Consider

$$x = 3 \pmod 7$$
$$x = 12 \pmod{13}$$

| $m$ | 7 | 13 |
|---|---|---|
| $p$ | 13 | 7 |
| $s = p^{-1} \pmod m$ | 6 | 2 |
| $a$ | 3 | 12 |

$$x = 13 \cdot 6 \cdot 3 + 7 \cdot 2 \cdot 12 = 402 = 38 \pmod{91}.$$

Then $x = -38 = 53 \pmod{91}$ is another solution.
It's possible that the second computation might have given me 25, the solution I got earlier. In that case, I'd have to move on to one of the other two cases. I got lucky and had to only do two cases, instead of three. □

---

Here are some tools for computing Legendre symbols.

**Theorem.** (Euler) Let $p$ be an odd prime, $a > 0$, $(a, p) = 1$. Then

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

**Proof.** There are two cases. Suppose that $\left(\frac{a}{p}\right) = 1$. Then there is a number $b$ such that $b^2 = a \pmod p$. So

$$(b^2)^{(p-1)/2} = a^{(p-1)/2} \pmod p$$
$$b^{p-1} = a^{(p-1)/2} \pmod p$$

If $p \mid b$, then $p \mid b^2 = a$, a contradiction. So $p \not| b$, and Fermat's theorem implies that $b^{p-1} = 1 \pmod p$. So

$$a^{(p-1)/2} = 1 \pmod p, \quad \text{and} \quad \left(\frac{a}{p}\right) = a^{(p-1)/2} \pmod p.$$

The other possibility is $\left(\frac{a}{p}\right) = -1$. In this case, consider the set $\{1, 2, \ldots, p-1\}$. I claim that these integers occur in pairs $s$, $t$, such that $st = a$.

First, if $s \in \{1, 2, \ldots, p-1\}$, then $s$ is invertible mod $p$. So I can write $s(s^{-1}a) = a$, and the pair $s$, $s^{-1}a$, multiplies to $a$.

Moreover, $s$ and $s^{-1}a$ are distinct. If not, $s = s^{-1}a$, or $s^2 = a$, which contradicts $\left(\frac{a}{p}\right) = -1$.

Since the integers $\{1, 2, \ldots, p-1\}$ divide up into pairs, each multiplying to $a$, and since there are $\dfrac{p-1}{2}$ pairs, I have

$$1 \cdot 2 \cdots (p-1) = a^{(p-1)/2} \pmod{p}.$$

By Wilson's theorem,

$$-1 = a^{(p-1)/2} \pmod{p}$$
$$\left(\frac{a}{p}\right) = a^{(p-1)/2} \pmod{p} \quad \square$$

---

**Example.** Use Euler's formula to compute $\left(\dfrac{10}{13}\right)$.

$$a^{(p-1)/2} = 10^6 = 1 \pmod{13}.$$

Hence, $\left(\dfrac{10}{13}\right) = 1$, and $x^2 = 10 \pmod{13}$ should have a solution. Indeed,

$$7^2 = 49 = 10 \pmod{13}. \quad \square$$

---

Euler's formula gives an expression for the Legendre symbol, but it becomes tedious to compute with it if the numbers are large. We'll see that you can use the properties of the Legendre symbol given below together with Quadratic Reciprocity to simplify computations.

**Proposition.** If $a = b \pmod{p}$, then $\left(\dfrac{a}{p}\right) = \left(\dfrac{b}{p}\right)$.

**Proof.** If $a = b \pmod{p}$, then $x^2 = a \pmod{p}$ if and only if $x^2 = b \pmod{p}$. Thus, one of these equations is solvable or not solvable if and only if the same is true for the other — which means $\left(\dfrac{a}{p}\right) = \left(\dfrac{b}{p}\right)$. $\square$

Note that I can use this result to apply Euler's formula to $\left(\dfrac{a}{p}\right)$ for $a < 0$ by simply replacing $a$ with $b > 0$ such that $a = b \pmod{p}$.

**Proposition.** Let $p$ be an odd prime, $a, b > 0$, $(a, p) = (b, p) = 1$. Then

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

**Proof.** By Euler's formula,

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = a^{(p-1)/2} b^{(p-1)/2} \pmod{p}, \quad \text{and} \quad \left(\frac{ab}{p}\right) = (ab)^{(p-1)/2} \pmod{p}.$$

Therefore,

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

The two sides of this equation are $\pm 1$. Since $p$ is an odd prime, the two sides can't differ by 2. Hence, they must be equal as integers:

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

**Corollary.** Let $p$ be an odd prime, $a > 0$, $(a, p) = 1$. Then

$$\left(\frac{a^2}{p}\right) = 1. \quad \square$$

**Proof.**

$$\left(\frac{a^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{p}\right) = \left(\left(\frac{a}{p}\right)\right)^2 = (\pm 1)^2 = 1. \quad \square$$

You can use the results above to compute $\left(\frac{a}{p}\right)$ for specific values of $a$ and arbitrary $p$.

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

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p = 4k+1 \\ -1 & \text{if p = 4 k + 3} \end{cases}.$$

**Proof.** By Euler's formula,

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

$$\begin{cases} (-1)^{2k} & \text{if } p = 4k+1 \\ (-1)^{2k+1} & \text{if p = 4 k + 3} \end{cases} = \begin{cases} 1 & \text{if } p = 4k+1 \\ -1 & \text{if p = 4 k + 3} \end{cases}. \quad \square$$

As examples, $\left(\frac{-1}{13}\right) = 1$, because $13 = 4 \cdot 3 + 1$. Thus, $x^2 = -1 \pmod{13}$ has solutions. And in fact,

$$5^2 = 25 = 12 = -1 \pmod{13}.$$

Likewise, $\left(\frac{-1}{23}\right) = -1$, because $23 = 4 \cdot 5 + 3$. Hence, $x^2 = -1 \pmod{23}$ has no solutions.

Using Gauss's lemma, which I'll prove shortly, you can also show that

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

Note that $\frac{p^2-1}{8}$ is actually an integer: Since $p = 2k+1$, I have $p^2 - 1 = 4k(k+1)$. And $4k(k+1)$ is divisible by 8, because one of $k$, $k+1$, must be even.

So, for example,

$$\left(\frac{2}{7}\right) = (-1)^{(7^2-1)/8} = 1.$$

Therefore, $x^2 = 2 \pmod{7}$ has solutions. $x = 3$ works, for instance.