Quadratic Residues and Nonresidues

Let p be a prime and $n \in \mathbb{Z}$ be such that $\gcd(n,p)=1$. We wish to analyze the answer to the following question.

Is n a perfect square modulo p?

Using the congruence, the above question can be re-written as follows.

Does $x^2 \equiv n \pmod{p}$ have a solution?

We start our quest with a definition.

Definition: Let $m, a \in \mathbb{Z}$ with $m>0$ and $\gcd(m,a)=1$. We say that a is a quadratic residue of m if

$$x^2 \equiv a \pmod{m}$$

has a solution.

ex: Let's find the quadratic residues of 11. We see that

$$1^2 \equiv 10^2 \equiv 1 \pmod{11}$$
$$2^2 \equiv 9^2 \equiv 4 \pmod{11}$$
$$3^2 \equiv 8^2 \equiv 9 \pmod{11}$$
$$4^2 \equiv 7^2 \equiv 5 \pmod{11}$$
$$5^2 \equiv 6^2 \equiv 3 \pmod{11}$$

Hence, the quadratic residues of 11 are 1, 3, 4, 5 and 9. The integers 2, 6, 7, 8 and 10 are quadratic nonresidues of 11.

<u>Lemma 11.1:</u> Let p be an odd prime and $a \in \mathbb{Z}$ be such that $p \nmid a$. Then,

$$x^2 \equiv a \pmod{p}$$

has either no solutions or exactly two incongruent solutions modulo p.

Proof: If $x = x_0$ is a solution of $x^2 \equiv a \pmod{p}$, then it follows that $x = -x_0$ is also a solution because

$$(-x_0)^2 = x_0^2 \equiv a \pmod{p}.$$

We show that x_0 and $-x_0$ are incongruent solution.

If $x_0 \equiv -x_0 \pmod{p}$, then

$$2x_0 \equiv 0 \pmod{p}$$

$$\Rightarrow \quad x_0 \equiv 0 \pmod{p} \quad (\because \gcd(2,p) = 1)$$

a contradiction because $p \nmid x_0$ (if $p \mid x_0$, then $p \mid x_0^2$ and then $p \mid a$ since $x_0^2 \equiv a \pmod{p}$, a contradiction to a given condition).

$\therefore$ if there is a solution, then there is another

incongruent solution. We show that there are no more solutions.

Suppose $x = x_0$ and $x = x_1$ are both solutions of $x^2 \equiv a \pmod{p}$. Then, we've

$$x_0^2 \equiv x_1^2 \pmod{p}$$

$$\Rightarrow (x_0 - x_1)(x_0 + x_1) \equiv 0 \pmod{p}$$

$$\Rightarrow p \mid (x_0 - x_1) \text{ or } p \mid (x_0 + x_1).$$

$$\Rightarrow x_1 \equiv x_0 \pmod{p} \text{ or } x_1 \equiv -x_0 \pmod{p}$$

$\therefore$ any third solution is congruent to x_0 or $-x_0$.

<u>Theorem 11.1</u>: If p is an odd prime, then there are exactly $(p-1)/2$ quadratic residues of p and $(p-1)/2$ quadratic nonresidues of p among the integers $1, 2, \ldots, p-1$.

Proof: We consider the least positive residue of the squares of the integers $1, 2, \ldots, p-1$.

Then, the congruence

$$x^2 \equiv a \pmod{p}$$

has either zero or two solutions.

Therefore, there should be exactly $(p-1)/2$ quadratic residues of p among $1, 2, \cdots, p-1$.

The remaining $(p-1)/2$ positive integers are the quadratic nonresidues of p.

ex: As we have seen in the previous example, when $p=11$, the five quadratic residues were $1, 3, 4, 5$ and 9, and the quadratics nonresidues were $2, 6, 7, 8$ and 10.

Definition: Let p be an odd prime and a be an integer not divisible by p. The Legendre symbol $\left(\frac{a}{p}\right)$ is defined by

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

ex: From a previous example, when $p=11$,

$$\left(\frac{1}{11}\right) = \left(\frac{3}{11}\right) = \left(\frac{4}{11}\right) = \left(\frac{5}{11}\right) = \left(\frac{9}{11}\right) = 1 \text{ and}$$

$$\left(\frac{2}{11}\right) = \left(\frac{6}{11}\right) = \left(\frac{7}{11}\right) = \left(\frac{8}{11}\right) = \left(\frac{10}{11}\right) = -1.$$

Theorem 11.3: Euler's Criterion

Let p be an odd prime and let a be an integer not divisible by p. Then,

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

Proof: First assume that $\left(\frac{a}{p}\right) = 1$.

Then, $x^2 \equiv a \pmod{p}$ has a solution.
Let it be $x = x_0$. Then, $x_0^2 \equiv a \pmod{p}$
Then,

$$\begin{aligned} a^{(p-1)/2} &\equiv (x_0^2)^{(p-1)/2} \\ &\equiv x_0^{(p-1)} \\ &\equiv 1 \pmod{p} \quad \text{(by Fermat's little theorem)} \end{aligned}$$

$\therefore$ if $\left(\frac{a}{p}\right) = 1$, then $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.

Next, assume that $\left(\frac{a}{p}\right) = -1$.

Then, $x^2 \equiv a \pmod{p}$ has no solution.

By Corollary 4.11.1, for each integer i with $\gcd(i, p) = 1$, there is an integer j such that $ij \equiv a \pmod{p}$.
Furthermore, since $x^2 \equiv a \pmod{p}$ has no

solutions, we know that $i \neq j$.

Thus, we can group the integers $1, 2, \cdots, p-1$ into $(p-1)/2$ pairs, each with product congruent to a modulo p.

Multiply these pairs together to get

$$(p-1)! \equiv a^{(p-1)/2} \pmod{p}$$

By Wilson's theorem

$$(p-1)! \equiv -1 \pmod{p}.$$

$$\therefore \quad -1 \equiv a^{(p-1)/2} \pmod{p}$$

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

Hence, for any a not divisible by p,

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

<u>ex</u>: Let $p = 23$ and $a = 5$.

It can be shown that

$$5^{(23-1)/2} = 5^{11} \equiv -1 \pmod{23}.$$

$$\therefore \left(\frac{5}{23}\right) = -1.$$

$\therefore$ 5 is a quadratic nonresidue of 23.

Theorem 11.4: Let p be an odd prime and a and b be integers not divisible by p. Then,

(i) if $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

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

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

Proof: (i) If $a \equiv b \pmod{p}$, then $x^2 \equiv a \pmod{p}$ has a solution if and only if $x^2 \equiv b \pmod{p}$ has a solution.

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

(ii) By Euler's criterion,

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

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

$$\therefore \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{(p-1)/2} \cdot b^{(p-1)/2} \pmod{p}$$

$$\equiv (ab)^{(p-1)/2} \pmod{p}$$

Also, $\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} \pmod{p}$

$$\therefore \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv \left(\frac{ab}{p}\right) \pmod{p}$$

Because the only possible values for Legendre symbols are ± 1, we conclude that

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

(iii) In part (ii), letting $b = a$, we get

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

Note that, according to part (ii) of the above theorem, the product of two quadratic residues or quadratic nonresidues is again a quadratic residue, whereas the product of a quadratic residue and a quadratic nonresidue is a quadratic nonresidue.

<u>ex</u>: Let p be an odd prime not exceeding 20. For which p is -1 a quadratic residue of p? In other words, for what p does the congruence

$$x^2 \equiv -1 \pmod{p}$$

has a solution?

It easily follows that

$$2^2 \equiv -1 \pmod{5}$$

$$5^2 \equiv -1 \pmod{13} \text{ and}$$

$$4^2 \equiv -1 \pmod{17}.$$

$\therefore$ -1 is a quadratic residue of 5, 13 and 17.

It can also be verified that -1 is a quadratic nonresidue of 3, 7, 11 and 19. You just need to show that the congruent $x^2 \equiv -1 \pmod{p}$ has no solutions for $p = 3, 7, 11$ and 19.

From the above example, we conjecture that -1 is a quadratic residue of p if and only if $p \equiv 1 \pmod{4}$.

<u>Theorem 11.5:</u> Let p be an odd prime. Then,

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv -1 \pmod{4} \end{cases}$$

Proof: By Euler's criterion,

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

If $p \equiv 1 \pmod{4}$, then $p = 4k+1$ for some $k \in \mathbb{Z}^+$.

$\therefore$ $(-1)^{(p-1)/2} = (-1)^{4k/2} = (-1)^{2k} = 1$

$\therefore$ $\left(\frac{-1}{p}\right) \equiv 1 \pmod{p}$

$\therefore$ $\left(\frac{-1}{p}\right) = 1$

If $p \equiv -1 \pmod{4}$, then $p \equiv 3 \pmod{4}$.

Then, $p = 4k+3$ for some $k \in \mathbb{Z}^+$.

$$\therefore (-1)^{(p-1)/2} = (-1)^{(4k+2)/2} = (-1)^{2k+1} = -1$$

$$\therefore \left(\frac{-1}{p}\right) \equiv -1 \pmod{p}.$$

$$\therefore \left(\frac{-1}{p}\right) = -1$$

Lemma 11.2: Gauss's Lemma

Let p be an odd prime and a an integer with $(a,p)=1$. If s is the number of least positive residues of the integers $a, 2a, 3a, \ldots, ((p-1)/2)a$ modulo p that are greater than $p/2$, then

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

Proof: Exercise.

ex: Let $p=11$ and $a=5$. Let's find $\left(\frac{5}{11}\right)$.
Note that $(p-1)/2 = 5$.
First, we find the least positive residues of $1\cdot 5, 2\cdot 5, 3\cdot 5, 4\cdot 5, 5\cdot 5$ modulo 11.

They are 5, 10, 4, 9 and 3 respectively.

Only 2 of these, namely 10 and 9, are greater than $11/2$.

$$\therefore \left(\frac{5}{11}\right) = (-1)^2 = 1.$$