Quadratic Residues and Nonresidues

DEFINITION: If m is a positive integer, we say that an integer a is a **quadratic residue** of m if $(a, m) = 1$ and the congruence $x^2 \equiv a \pmod{m}$ has a solution. If $x^2 \equiv a \pmod{m}$ has no solution, we say that a is a **quadratic nonresidue** of m.

EXAMPLE: To determine which integers among $1, 2, 3, \ldots, 10$ are quadratic residues of 11, we compute the squares of them. We find that

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

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

EXAMPLE: A reduced residue system modulo 6 is 1 and 5. Since

$$1^2 \equiv 1 \pmod{6} \qquad \text{and} \qquad 5^2 \equiv 1 \pmod{6}$$

it follows that 1 is the only quadratic residue modulo 6.

LEMMA: Let p be an odd prime and a an integer not divisible by p. Then, the congruence $x^2 \equiv a \pmod{p}$ has either no solutions or exactly two incongruent solutions modulo p.

Proof: If $x^2 \equiv a \pmod{p}$ has a solution, say, $x = x_0$, then we can easily demonstrate that $x = -x_0$ is a second incongruent solution. Indeed, since

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

we see that $-x_0$ is a solution. We note that $x_0 \not\equiv -x_0 \pmod{p}$, for if $x_0 \equiv -x_0 \pmod{p}$, then we have $2x_0 \equiv 0 \pmod{p}$. This is impossible by Theorem 2 from Section 3.5, because p is odd and $p \nmid x_0$. (We see that $p \nmid x_0$ by noting that $x_0^2 \equiv a \pmod{p}$ and $p \nmid a$.)

To show that there are no more than two incongruent solutions, assume that $x = x_0$ and $x = x_1$ are both solutions of $x^2 \equiv a \pmod{p}$. Then we have $x_0^2 \equiv x_1^2 \equiv a \pmod{p}$, so that

$$x_0^2 - x_1^2 = (x_0 + x_1)(x_0 - x_1) \equiv 0 \pmod{p}$$

Hence, $p \mid (x_0 + x_1)$ or $p \mid (x_0 - x_1)$, so that $x_1 \equiv -x_0 \pmod{p}$ or $x_1 \equiv x_0 \pmod{p}$. Therefore, if there is a solution of $x^2 \equiv a \pmod{p}$, there are exactly two incongruent solutions. ■

This leads us to the following theorem.

THEOREM 1: 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: To find all the quadratic residues of p among the integers $1, 2, \ldots, p-1$, we compute the least positive residues modulo p of the squares of the integers $1, 2, \ldots, p-1$. Since there are $p-1$ squares to consider, and since each congruence $x^2 \equiv a \pmod{p}$ has either zero or two solutions, there must be exactly $(p-1)/2$ quadratic residues of p among the integers $1, 2, \ldots, p-1$. The remaining

$$p - 1 - (p-1)/2 = (p-1)/2$$

positive integers less than $p-1$ are quadratic nonresidues of p. ■

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

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

EXAMPLE: The previous example shows that the Legendre symbols $\left(\frac{a}{11}\right)$, $a = 1, 2, \ldots, 10$, have the following values:

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

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

We now present a criterion for deciding whether an integer is a quadratic residue of a prime. This criterion is useful in demonstrating properties of the Legendre symbol.

THEOREM 2 (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, the congruence $x^2 \equiv a \pmod{p}$ has a solution, say $x = x_0$. Using Fermat's little theorem, we see that

$$a^{(p-1)/2} \equiv (x_0^2)^{(p-1)/2} = x_0^{p-1} \equiv 1 \pmod{p}$$

Hence, if $\left(\frac{a}{p}\right) = 1$, we know that

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

Now consider the case where $\left(\frac{a}{p}\right) = -1$. Then the congruence $x^2 \equiv a \pmod{p}$ has no solutions. From Theorem 1 (Section 4.2), for each integer i with $(i, p) = 1$ there is a unique 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 $1, 2, \ldots, p-1$ into $(p-1)/2$ pairs, each with product a. Multiplying these pairs together, we find that

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

Since Wilson's theorem tells us that $(p-1)! \equiv -1 \pmod{p}$, we see that

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

In this case, we also have $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$. ■

EXAMPLE: Let $p = 23$ and $a = 5$. Since $5^{11} \equiv -1 \pmod{23}$, Euler's criterion tells us that $\left(\frac{5}{23}\right) = -1$. Hence, 5 is a quadratic nonresidue of 23.

We now prove some properties of the Legendre symbol.

THEOREM 3: 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. Hence, $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(ii) By Euler's criterion, we know that

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

and

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

Hence

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

Since the only possible values of a Legendre symbol are ± 1, we conclude that

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

(iii) Since $\left(\frac{a}{p}\right) = \pm 1$, from part (ii) it follows that

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

Part (ii) of the Theorem above has the following interesting consequence. The product of two quadratic residues, or of two quadratic nonresidues, of a prime is a quadratic residue of that prime, whereas the product of a quadratic residue and a quadratic nonresidue is a quadratic nonresidue.

Using Euler's criterion, we can classify those primes having -1 as a quadratic residue.

THEOREM 4: If p is 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, we know that

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

If $p \equiv 1 \pmod 4$, then $p = 4k + 1$ for some integer k. Thus,

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

so that $\left(\frac{-1}{p}\right) = 1$. If $p \equiv 3 \pmod 4$, then $p = 4k + 3$ for some integer k. Thus,

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

so that $\left(\frac{-1}{p}\right) = -1$. ■

THEOREM 5 (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 modulo p of the integers

$$a,\ 2a,\ 3a,\ \ldots,\ \frac{p-1}{2}a$$

that are greater than $p/2$, then

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

Proof: Consider the integers $a, 2a, 3a, \ldots, ((p-1)/2)a$. Let $u_1, u_2, \ldots, u_s$ be the least positive residues of those that are greater than $p/2$, and let $v_1, v_2, \ldots, v_t$ be the least positive residues of those integers that are less than $p/2$. Since $(ja, p) = 1$ for all j with $1 \le j \le (p-1)/2$, these least positive residues are in the set $1, 2, \ldots, p-1$.

We will show that

$$p - u_1, \quad p - u_2, \quad \ldots, \quad p - u_s, \quad v_1, \quad v_2, \quad \ldots, \quad v_t$$

comprise the set of integers $1, 2, \ldots, (p-1)/2$, in some order. To see this, we need only show that no two of these integers are congruent modulo p, since there are exactly $(p-1)/2$ numbers in the set and all are positive integers not exceeding $(p-1)/2$.

Clearly, no two of the u_i are congruent modulo p and no two of the v_j are congruent modulo p; if a congruence of either of these two sorts held, we would have

$$ma \equiv na \pmod p$$

where m and n are both positive integers not exceeding $(p-1)/2$. Since $p \nmid a$, this would imply that $m \equiv n \pmod p$, which is impossible.

In addition, one of the integers $p - u_i$ cannot be congruent to v_j, for if such a congruence held, we would have $ma \equiv p - na \pmod{p}$, so that $ma \equiv -na \pmod{p}$. Since $p \not| a$, this would imply that $m \equiv -n \pmod{p}$, which is impossible because both m and n are in the set $1, 2, \ldots, (p-1)/2$.

Now that we know that $p-u_1,\ p-u_2,\ \ldots,\ p-u_s,\ v_1,\ v_2,\ \ldots,\ v_t$ are the integers $1, 2, \ldots, (p-1)/2$, in some order, we conclude that

$$(p-u_1)(p-u_2)\ldots(p-u_s)v_1v_2\ldots v_t = \left(\frac{p-1}{2}\right)!$$

which implies that

$$(-1)^s u_1u_2\ldots u_sv_1v_2\ldots v_t \equiv \left(\frac{p-1}{2}\right)! \pmod{p} \tag{1}$$

But, because $u_1, u_2, \ldots, u_s, v_1, v_2, \ldots, v_t$ are the least positive residues of $a, 2a, \ldots, ((p-1)/2)a$, we also know that

$$\begin{aligned} u_1u_2\ldots u_sv_1v_2\ldots v_t &\equiv\ a\cdot 2a\ldots\left(\frac{p-1}{2}\right)a \\ &\equiv a^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! \pmod{p} \end{aligned} \tag{2}$$

Hence, from (1) and (2), we see that

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

Because $(p, ((p-1)/2)!) = 1$, this congruence implies that

$$(-1)^s a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

By multiplying both sides by $(-1)^s$, we obtain

$$a^{\frac{p-1}{2}} \equiv (-1)^s \pmod{p}$$

Since Euler's criterion tells us that

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

it follows that

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

establishing Gauss's lemma. ■

EXAMPLE: Let $a = 5$ and $p = 11$. To find $\left(\frac{5}{11}\right)$ by Gauss's lemma, we compute the least positive residues of

$$1\cdot 5, \quad 2\cdot 5, \quad 3\cdot 5, \quad 4\cdot 5, \quad \text{and} \quad 5\cdot 5$$

These are $5, 10, 4, 9$, and 3, respectively. Because exactly two of these are greater than $11/2$, Gauss's lemma tells us that

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