Quadratic Residue

Lakshmy K V

October 28, 2020

Quadratic residue

Let $a \in \mathbb{Z}_n$. We say a is a *quadratic residue* if there exists some x such that $x^2 = a$. Otherwise a is a *quadratic nonresidue*.

For example, 1 is a quadratic residue of p for any integer p. 2 is a quadratic residue of 7 ($3^2 \equiv 2 \bmod 7$), but 2 is a quadratic non-residue of 3 as $1^2 \not\equiv 2 \not\equiv 2^2$ modulo 3. $5^2 \equiv 10 \bmod 15$ implies that 10 is a quadratic residue of 15, and 40 is also a quadratic residue modulo 15 as $5^2 \equiv 40 \bmod 15$.

Proposition 5.2. *Let p be a prime. The number of quadratic residues modulo p is $\frac{p-1}{2}$.*

Proof: As $c^2 = (-c)^2$, the number of quadratic residues is at most $\frac{p-1}{2}$. On the other hand, if a is a quadratic residue of p, it follows easily that $x^2 \equiv a \bmod p$ has only two solutions modulo p as follows. Let $b \in U_p$ such that $b^2 \equiv a \bmod p$. Now

$$\begin{aligned} & x^2 \equiv a \bmod p \\ \Longrightarrow \quad & x^2 \equiv b^2 \bmod p \\ \Longrightarrow \quad & p \mid (x-b)(x+b) \\ \Longrightarrow \quad & p \mid (x-b) \text{ or } p \mid (x+b) \\ \Longrightarrow \quad & x \equiv b \text{ or } x \equiv -b \bmod p. \end{aligned}$$

As p is odd and b is coprime to p, $b \not\equiv -b \bmod p$. Hence $x^2 \equiv a \bmod p$ has precisely two solutions modulo p, namely b and $-b$. So there are exactly $\frac{p-1}{2}$ quadratic residues modulo p, and there are $\frac{p-1}{2}$ quadratic non-residues. $\square$

Euler's Criterion

PROPOSITION 5.3. *Let p be an odd prime and $(a, p) = 1$. Then a is a quadratic residue modulo p if and only if $a^{\frac{p-1}{2}} \equiv 1 \bmod p$.*

Proof: Suppose a is a quadratic residue. Then there exists an integer b coprime to p such that

$$a \equiv b^2 \bmod p$$
$$\implies \quad a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \bmod p$$

by Fermat's Little Theorem

Conversely, suppose $a^{\frac{p-1}{2}} \equiv 1 \bmod p$. We know there exists a primitive root g modulo p, so that any integer in U_p can be expressed as $g^i \bmod p$ for some $1 \leq i \leq p-1$, and $g^m \equiv 1 \bmod p$ holds only when $(p-1) \mid m$. In particular, for some $1 \leq i \leq p-1$,

we have

$$a \equiv g^i \bmod p$$
$$\implies \quad g^{i(\frac{p-1}{2})} \equiv a^{\frac{p-1}{2}} \equiv 1 \bmod p.$$

By the property of the primitive root g mentioned above, $p-1$ must divide $i(\frac{p-1}{2})$. Therefore, i must be even, say $i = 2j$. Then, $a \equiv (g^j)^2 \bmod p$, and it follows that a is a quadratic residue. $\square$

The Legendre Symbol

Definition 5.4. *Let p be an odd prime. We define*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \text{ if } a \text{ is a non-zero quadratic residue modulo } p \\ -1 \text{ if } a \text{ is a non-zero quadratic non-residue modulo } p \\ 0 \text{ if } p \mid a \end{cases} \tag{5.1}$$

For example, $\left(\frac{2}{7}\right) = 1$ as $3^2 \equiv 2 \bmod 7$. But $\left(\frac{2}{5}\right) = -1$ as the quadratic residues of 5 are precisely $(\pm 1)^2 = 1$ and $(\pm 2)^2 = 4$. Observe that as $a^{p-1} \equiv 1 \bmod p$ we must have $a^{\frac{p-1}{2}} \equiv \pm 1 \bmod p$.

Using Legendre's symbol, we can now express *Euler's Criterion* as

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \bmod p. \tag{5.2}$$

Proposition 5.5. *The Legendre symbol has the following properties:*

$$(i) \quad a \equiv b \ mod \ p \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$

$$(ii) \quad \left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \ mod \ p.$$

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

Proof: The first property is obvious, and the second is a restatement of (5.2). The third property is obvious when $p \mid ab$, as both sides of the equality are clearly zero. When p

is coprime to ab, we have

$$\begin{aligned} \left(\frac{ab}{p}\right) &\equiv (ab)^{\frac{p-1}{2}} \mod p \\ &\equiv (a)^{\frac{p-1}{2}}(b)^{\frac{p-1}{2}} \mod p \\ \implies \left(\frac{ab}{p}\right) &\equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \mod p. \end{aligned}$$

But both sides of the last congruence take values only from $\{\pm 1\}$. As the prime p is odd, one can conclude that both sides of the last congruence are same (either both 1 or both -1). Therefore the third property follows. $\square$

Proposition 5.6. *Let p be an odd prime. Then $\left(\frac{-1}{p}\right) = 1$ if and only if $p \equiv 1$ mod 4.*

Proof: By (5.2), we have $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \bmod p$. Since both sides of the congruence takes only ± 1 as values, and p is an odd prime, we have

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

Now,

$$\begin{aligned} \left(\frac{-1}{p}\right) &= 1 \\ \Leftrightarrow (-1)^{\frac{p-1}{2}} &= 1 \\ \Leftrightarrow \frac{p-1}{2} &\in 2\mathbb{Z} \\ \Leftrightarrow p &\equiv 1 \bmod 4. \qquad \square \end{aligned}$$

Proposition 5.8. *Let p be an odd prime. Then 2 is a quadratic residue modulo p if and only if $p \equiv 1$ or $p \equiv 7$ modulo 8. We can also restate this result as*

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

Theorem 5.9. *Let p and q be distinct odd primes. If p is a quadratic residue modulo q, then q is also a quadratic residue modulo p unless $p \equiv q \equiv 3 \bmod 4$.*

Remark: we can express the above theorem also as

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \text{ unless } p \equiv q \equiv 3 \bmod 4,$$

or as

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

For example, consider $p = 7$ and $p = 101$. Then,

$$\begin{aligned}\left(\frac{7}{101}\right) &= (-1)^{\left(\frac{7-1}{2}\right)\cdot\left(\frac{101-1}{2}\right)}\left(\frac{101}{7}\right) = \left(\frac{3}{7}\right)\\ &= (-1)^{\left(\frac{7-1}{2}\right)\cdot\left(\frac{3-1}{2}\right)}\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1.\end{aligned}$$

$$\begin{aligned}\left(\frac{11}{101}\right) &= (-1)^{\left(\frac{11-1}{2}\right)\cdot\left(\frac{101-1}{2}\right)}\left(\frac{101}{11}\right)\\ &= \left(\frac{2}{11}\right)\\ &= (-1)^{\frac{11^2-1}{8}}\\ &= -1.\end{aligned}$$

$$\begin{aligned}\left(\frac{35}{101}\right) &= \left(\frac{5}{101}\right)\left(\frac{7}{101}\right)\\ &= (-1)(-1) = 1. \qquad \square\end{aligned}$$

THEOREM 5.10. *Let p be an odd prime, and n be any positive integer. Then a is a quadratic residue modulo p^n if and only if it is a quadratic residue modulo p.*

THEOREM 5.11. (a) *An integer a is a quadratic residue modulo 4 if and only if $a \equiv 1 \mod 4$.*
(b) *An integer a is a quadratic residue modulo 2^n for $n \geq 3$ if and only if $a \equiv 1 \mod 8$.*

THEOREM 5.11. (a) *An integer a is a quadratic residue modulo 4 if and only if* $a \equiv 1$ *mod* 4.

(b) *An integer a is a quadratic residue modulo 2^n for $n \geq 3$ if and only if* $a \equiv 1$ *mod* 8.

Quadratic Residues of Arbitrary Moduli

Theorem 5.12. *Let n be an arbitrary integer, and let*

$$n = 2^e \cdot p_1^{e_1} \cdot \cdots \cdot p_r^{e_r}$$

be its factorization into prime powers. An integer a coprime to n is a quadratic residue if and only if

$$\begin{aligned} \left(\frac{a}{p_i}\right) &= 1 && \text{for } i = 1,\ 2,\ \cdots,\ r \\ a &\equiv 1 \bmod 4, && \text{if } 4 \mid n,\ \text{but } 8 \nmid n; \\ a &\equiv 1 \bmod 8 && \text{if } 8 \mid n. \end{aligned}$$

Example: 1. Determine whether 17 is a quadratic residue of $2^5 \cdot 13^2 \cdot 47^{100}$.

Solution: It is easy to check that $17 \equiv 2^2 \mod 13$. Hence

$$\left(\frac{17}{13}\right) = 1.$$

Applying the law of quadratic reciprocity, we find that

$$\left(\frac{17}{47}\right) = \left(\frac{47}{17}\right) = \left(\frac{-4}{17}\right) = \left(\frac{-1}{17}\right) = 1.$$

As $17 \equiv 1 \mod 8$ as well, 17 must be a quadratic residue of $2^5 \cdot 13^2 \cdot 47^{100}$ by the previous theorem. $\square$

1. Let p be an odd prime. Then show that

$$\left(\frac{-2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \bmod 8 \quad \text{or } p \equiv 3 \bmod 8 \\ -1 & \text{if } p \equiv \pm 5 \bmod 8 \quad \text{or } p \equiv 7 \bmod 8 \end{cases}$$

2. Let p be an odd prime other than 3. Then show that

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \bmod 12 \\ -1 & \text{if } p \equiv \pm 5 \bmod 12 \end{cases}$$

3. Let p be an odd prime other than 3. Then show that

$$\left(\frac{-3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \bmod 6 \\ -1 & \text{if } p \equiv 5 \bmod 6 \end{cases}$$

5. Show that

$$\sum_{i=1}^{p-1} \left(\frac{i}{p}\right) = 0.$$

13. Determine whether the following quadratic congruences have a solution or not:

(A) $x^2 \equiv 2 \bmod 71$

(B) $x^2 \equiv -2 \bmod 71$

(C) $x^2 \equiv 2 \bmod 73$

(D) $x^2 \equiv -2 \bmod 73$