# Quadratic residues

*We will review a some points about quadratic residues and the Legendre symbol from before break, and finish those sections.*

**Question 1** *Let $p > 2$ be a prime, and let $a$ be an integer between 0 and $p - 1$.*

- *If $a$ is a quadratic residue modulo $p$, then $a^{\frac{p-1}{2}} = 1$.*
- *If $a$ is a quadratic nonresidue modulo $p$, then $a^{\frac{p-1}{2}} = -1$.*
- *Otherwise, $a^{\frac{p-1}{2}} = 0$.*

---

**Question 2** *Euler's identity: Let $p > 2$ be a prime, and let $a$ be an integer. Then $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.*

---

**Theorem 1.** *Let $p > 2$ be prime.*

- *If $p \equiv 1 \pmod 4$, then $-1$ is a quadratic residue modulo $p$.*
- *If $p \equiv 3 \pmod 4$, then $-1$ is a quadratic nonresidue modulo $p$.*

***Proof*** For an arbitrary prime $p > 2$, Euler's identity tells us that $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$. Note that, we have that $\left(\frac{-1}{p}\right)$ is either $+1$ or $-1$ by definition, and $(-1)^{\frac{p-1}{2}}$ is also either $+1$ or $-1$. Since $1 \not\equiv -1 \pmod{p}$, the two sides of the congruence are actually equal. That is, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

The completion of the proof involves applying the answer to the preclass assignment, and the proof is on homework 9. ■

**Question 3** *Let $p > 2$ be prime, and let $a$ and $b$ be integers between 1 and $p - 1$.*

---

Learning outcomes:
Author(s):

- *If $ab$ is a quadratic residue, then*

  ***Select All Correct Answers:***

  (a) *$a$ and $b$ are both quadratic residues* ✓
  (b) *$a$ and $b$ are both quadratic nonresidues* ✓
  (c) *One of $a$ and $b$ is a quadratic residue and the other is a quadratic nonresidue*

- *If $ab$ is a quadratic nonresidue, then*

  ***Select All Correct Answers:***

  (a) *$a$ and $b$ are both quadratic residues* ✓
  (b) *$a$ and $b$ are both quadratic nonresidues* ✓
  (c) *One of $a$ and $b$ is a quadratic residue and the other is a quadratic nonresidue*