Quadratic residue of −1

Learning Objectives. By the end of class, students will be able to:

- Prove **??**

- Classify when -1 is a quadratic residue modulo an odd prime.

Reading None

Proof of Euler's Criterion

We will prove **??**.

Theorem 1 (Euler's Criterion)**.** Let p be an odd prime and $a \in \mathbb{Z}$ with $p \nmid a$. Then

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

Proof　　Let p be an odd prime and $a \in \mathbb{Z}$ with $p \nmid a$. If there exists $b \in \mathbb{Z}$ such that $b^2 \equiv a \pmod{p}$, then $\left(\frac{a}{p}\right) = 1$ by definition. Note that

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

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

If a is a quadratic nonresidue modulo p, consider the reduced residue system $\{1, 2, \ldots, p-1\}$. For each element c of the list, there exists a unique element d, also on the list, such that $cd \equiv a \pmod{p}$ by Theorem 2.6 since $(a, p) = 1$. Since a is a quadratic nonresidue by assumption, $c \not\equiv d \pmod{p}$. Thus, there are $\dfrac{p-1}{2}$ pairs c, d where $cd \equiv a \pmod{p}$. Thus,

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

by **??**. Since a is a quadratic nonresidue modulo p, $\left(\frac{a}{p}\right) = -1 \equiv a^{(p-1)/2} \pmod{p}$.　■