Monday, March 25: Quadratic residue of -1

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

- Prove Euler's Criterion
- Classify when -1 is a quadratic residue modulo an odd prime .

Reading None

Proof of Euler's Criterion

We will prove Euler's Criterion.

Theorem (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 Fermat's Little Theorem. 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 Wilson's Theorem. Since a is a quadratic nonresidue modulo p, $\left(\frac{a}{p}\right) = -1 \equiv a^{(p-1)/2} \pmod{p}$. ■

Remark 1. *Some sources define $\left(\frac{a}{p}\right) = 0$ when $p \mid a$. In this case, Let p be an odd prime and $a \in \mathbb{Z}$. If $p \mid a$, then $a^{(p-1)/2} \equiv 0^{(p-1)/2} \equiv 0 \equiv \left(\frac{a}{p}\right) \pmod{p}$.*

When is -1 a quadratic residue?

Theorem (Theorem 4.6)**.** *Let p be an odd prime number. Then*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & p \equiv 1 \pmod{4} \\ -1, & p \equiv 3 \pmod{4} \end{cases}.$$

Proof Let p be an odd prime number. Then from Euler's Criterion, $\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \pmod{p}$. Since both values are ± 1, we can say $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.

If $p \equiv 1 \pmod{4}$, then there exists $k \in \mathbb{Z}$ such that $p = 4k+1$. Thus, $\frac{p-1}{2} = 2k$ and

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

If $p \equiv 3 \pmod{4}$, then there exists $k \in \mathbb{Z}$ such that $p = 4k+3$. Thus, $\frac{p-1}{2} = 2k+1$ and

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

■

Wednesday, March 27: Introduction to quadratic reciprocity

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

- Use quadratic reciprocity to find the Legendre symbol of an integer modulo p.
- Characterize the primes where $3, -3, 5, -5, 7, -7$ are quadratic residues. .

Reading: Scanned notes, Pommersheim-Marks-Flapan Section 11.2 and part of 11.3.

Turn in: *Use the results from the reading* to find $\left(\frac{-3}{71}\right)$.

Solution: From Theorem 4.5(c), $\left(\frac{-3}{71}\right) = \left(\frac{-1}{71}\right)\left(\frac{3}{71}\right)$. Since $71 \equiv 3 \pmod{4}$, from Theorem 4.6, $\left(\frac{-1}{71}\right) = -1$, and from Quadratic Reciprocity (first statement) $\left(\frac{3}{71}\right) = -\left(\frac{71}{3}\right)$. Putting this together, we get

$$\begin{aligned}\left(\frac{-3}{71}\right) &= \left(\frac{-1}{71}\right)\left(\frac{3}{71}\right) = (-1)\left(-\left(\frac{71}{3}\right)\right) \\ &= \left(\frac{71}{3}\right) = \left(\frac{2}{3}\right) = -1\end{aligned}$$

from Theorem 4.5(b) and the fact that 2 is a quadratic nonresidue modulo 3.

Quadratic reciprocity (20 minutes)

Theorem (Quadratic Reciprocity (first statement))**.** *Let p and q be distinct primes.*

(a) If $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$, then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$.

(b) If $p \equiv q \equiv 3 \pmod 4$, then $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

It will take time to prove the lemmas for quadratic reciprocity, but we can immediately prove some results. The first is that this initial statement is equivalent to the more standard statement. This is our first example where one statement of a result (Quadratic Reciprocity (first statement)) is more useful in calculations and proofs, but the proof involves proving an equivalent statement (Law of Quadratic Reciprocity).

Theorem (Law of Quadratic Reciprocity)**.** *(Theorem 4.9) Let p and q be distinct primes. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)/2\ (q-1)/2} = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \\ -1, & \text{if } p \equiv q \equiv 3 \pmod 4. \end{cases}$$

Remark 2. *We can quickly prove the second equality,*

$$(-1)^{(p-1)/2\ (q-1)/2} = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \\ -1, & \text{if } p \equiv q \equiv 3 \pmod 4. \end{cases}$$

If $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$, then one of $\frac{p-1}{2}$ and $\frac{q-1}{2}$ is even. Thus $(-1)^{(p-1)/2\ (q-1)/2} = 1$. If $p \equiv q \equiv 3 \pmod 4$, then $\frac{p-1}{2}$ and $\frac{q-1}{2}$ are both odd. Thus $(-1)^{(p-1)/2\ (q-1)/2} = -1$.

Proposition 1. *Quadratic Reciprocity (first statement) is equivalent to Law of Quadratic Reciprocity. That is, Quadratic Reciprocity (first statement) implies Law of Quadratic Reciprocity and Law of Quadratic Reciprocity implies Quadratic Reciprocity (first statement) .*

Proof We will first show that Law of Quadratic Reciprocity implies Quadratic Reciprocity (first statement).

Let p and q be distinct primes. Then Law of Quadratic Reciprocity says that

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \\ -1, & \text{if } p \equiv q \equiv 3 \pmod 4. \end{cases}$$

Since $\left(\frac{p}{q}\right) = \pm 1$ and $\left(\frac{q}{p}\right) = \pm 1$, we know that $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1$ if and only if $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$. Thus, when $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$, $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$. Similarly, $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1$ if and only if $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$. Thus, when $p \equiv q \equiv 3 \pmod 4$, $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

The other direction is on next homework assignment. ■

Notice that we also proved the converse of Quadratic Reciprocity (first statement):

Corollary 1. *Let p and q be distinct primes.*

(a) If $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$, *then* $p \equiv 1 \pmod 4$ *or* $q \equiv 1 \pmod 4$.

(b) If $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$, *then* $p \equiv q \equiv 3 \pmod 4$.

Quadratic reciprocity practice (30 minutes)

In-class Problem 1 *Let p be an odd prime number. Prove the following statements the following provided outlines, which will help solve the next problem, as well.*

(b) $\left(\frac{3}{p}\right) = 1$ *if and only if* $p \equiv \pm 1 \pmod{12}$.

(c) $\left(\frac{-3}{p}\right) = 1$ *if and only if* $p \equiv 1 \pmod 6$.

Proof (b) Since $3 \equiv \boxed{3} \pmod 4$,[1] we need two cases for Quadratic Reciprocity (first statement).

(i) If $p \equiv 1 \pmod 4$, then $\left(\frac{3}{p}\right) = \boxed{\left(\frac{p}{3}\right)}$ by Quadratic Reciprocity (first statement), and $\left(\frac{p}{3}\right) = 1$ if and only if $p \equiv \boxed{1 \pmod 3}$. Then $p \equiv \boxed{1} \pmod{12}$, and this is the unique equivalence class modulo 12 by the Chinese Remainder Theorem.

(ii) If $p \equiv 3 \equiv -1 \pmod 4$, then $\left(\frac{3}{p}\right) = \boxed{-\left(\frac{p}{3}\right)}$ by Quadratic Reciprocity (first statement), and $\left(\frac{p}{3}\right) = -1$ if and only if $p \equiv \boxed{2 \equiv -1 \pmod 3}$. Then $p \equiv \boxed{-1} \pmod{12}$, and this is the unique equivalence class modulo 12 by the Chinese Remainder Theorem.

Therefore, $\left(\frac{3}{p}\right) = 1$ if and only if $p \equiv \pm 1 \pmod{12}$.

(c) From Theorem 4.25(c), $\left(\frac{-3}{p}\right) = \boxed{\left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)}$. Again, we have two cases.

(i) If $p \equiv 1 \pmod 4$, then $\left(\frac{-1}{p}\right) = \boxed{1}$ by Theorem 4.6 and $\left(\frac{3}{p}\right) = \boxed{\left(\frac{p}{3}\right)}$ by Quadratic Reciprocity (first statement). Thus, $\left(\frac{-3}{p}\right) = \boxed{\left(\frac{p}{3}\right)} = 1$ if and only if $p \equiv \boxed{1 \pmod 3}$. Then $p \equiv \boxed{1} \pmod{12}$, and this is the unique equivalence class modulo 12 by the Chinese Remainder Theorem.

(ii) If $p \equiv 3 \equiv -1 \pmod 4$, then $\left(\frac{-1}{p}\right) = \boxed{-1}$ by Theorem 4.6 and $\left(\frac{3}{p}\right) = \boxed{-\left(\frac{p}{3}\right)}$ by Quadratic

[1] In this problem, this step is repetitive, but it is needed when $p \neq 3$.

Reciprocity (first statement). Thus, $\left(\frac{-3}{p}\right) = \boxed{\left(\frac{p}{3}\right)} = 1$ if and only if $p \equiv \boxed{1 \pmod 3}$. Then $p \equiv \boxed{7} \pmod{12}$, and this is the unique equivalence class modulo 12 by the Chinese Remainder Theorem.

Therefore, $\left(\frac{-3}{p}\right) = 1$ if and only if $p \equiv \boxed{1, 7} \pmod{12}$, which is equivalent to $p \equiv 1 \pmod 6$.

■

In-class Problem 2 *Find congruences characterizing all prime numbers p for which the following integers are quadratic residues modulo p, as done in the previous exercise.*

Outline is provided for the first part. Outline for second part added after class.

(a) 5

(b) -5

(c) 7

(d) -7

Solution: (a) Since $5 \equiv \boxed{1} \pmod 4$, $\boxed{\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)}$ by Quadratic Reciprocity (first statement). Then $\left(\frac{5}{p}\right) = \boxed{\left(\frac{p}{5}\right)} = 1$ if and only if $p \equiv \boxed{\pm 1 \pmod 5}$.

(b) From Theorem 4.25(c), $\left(\frac{-5}{p}\right) = \boxed{\left(\frac{-1}{p}\right)\left(\frac{5}{p}\right)} = \boxed{\left(\frac{-1}{p}\right)\left(\frac{p}{5}\right)}$ by Quadratic Reciprocity (first statement). Again, we have two cases.

(i) If $p \equiv 1 \pmod 4$, then $\left(\frac{-1}{p}\right) = \boxed{1}$ by Theorem 4.6 and $\left(\frac{5}{p}\right) = \boxed{\left(\frac{p}{5}\right)}$ by Quadratic Reciprocity (first statement). Thus, $\left(\frac{-5}{p}\right) = \boxed{\left(\frac{p}{5}\right)} = 1$ if and only if $p \equiv \boxed{\pm 1 \pmod 5}$. When $p \equiv \boxed{1} \pmod 5$, we have $p \equiv \boxed{1} \pmod{\boxed{20}}$ and when $p \equiv \boxed{-1} \pmod 5$, we have $p \equiv \boxed{9} \pmod{\boxed{20}}$. In each case, there is a unique equivalence class modulo $\boxed{20}$ by the Chinese Remainder Theorem.

(ii) If $p \equiv 3 \pmod 4$, then $\left(\frac{-1}{p}\right) = \boxed{-1}$ by Theorem 4.6 and $\left(\frac{5}{p}\right) = \boxed{\left(\frac{p}{5}\right)}$ by Quadratic Reciprocity (first statement). Thus, $\left(\frac{-5}{p}\right) = \boxed{-\left(\frac{p}{5}\right)} = 1$ if and only if $p \equiv \boxed{\pm 2} \pmod 5$. When $p \equiv \boxed{2} \pmod 5$, we have $p \equiv \boxed{7} \pmod{\boxed{20}}$ and when $p \equiv \boxed{3} \pmod 5$, we have $p \equiv \boxed{3} \pmod{\boxed{20}}$. In each case, there is a unique equivalence class modulo $\boxed{20}$ by the Chinese Remainder Theorem.

Therefore, $\left(\frac{-5}{p}\right) = 1$ if and only if $p \equiv \boxed{1, 3, 7, 9} \pmod{\boxed{20}}$.

Friday March 29: No class for Good Friday