Proving Gauss's Lemma and the Quadratic Residue of 2

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

- Prove **??**
- Classify when 2 is a quadratic residue modulo a prime. .

Read: The remainder of Strayer Section 4.2. is on Moodle.

Turn in The $p \equiv 3 \pmod 9$ case of Strayer Theorem 4.8 (scanned notes Theorem 11.4.3/Theorem 11.4.4)

Solution: Mirroring Strayer's argument for $p \equiv 1 \pmod 8$:

If $p \equiv 3 \pmod 8$, then there exists $k \in \mathbb{Z}$ such that $p = 8k + 3$. Then

$$\frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor = \frac{8k+3-1}{2} - \left\lfloor \frac{8k+3}{4} \right\rfloor = 4k + 1 - (2k) = 2k + 1 \equiv 1 \pmod 2,$$

and

$$\frac{p^2-1}{8} = \frac{(8k+3)^2 - 1}{8} = \frac{64k^2 + 48k + 9 - 1}{8} = 8k^2 + 6k + 1 \equiv 1 \pmod 2.$$

Thus, $\frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor \equiv \frac{p^2-1}{8} \pmod 8$.

Remark 1. **??** is often stated as:

Let p be an odd prime number and like $a \in \mathbb{Z}$ with $p \nmid a$. Let n be the number of least absolute residues of the integers $a, 2a, 3a, \ldots, \frac{p-1}{2}$ modulo p that are negative. Then

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

Lemma 1. Let p be an odd prime number and like $a \in \mathbb{Z}$ with $p \nmid a$. Consider

$$a, 2a, 3a, \ldots, \frac{p-1}{2}a, \frac{p+1}{2}a, \ldots, (p-1)a.$$

The least absolute residues of ak and $a(p-k)$ differ by a negative sign. In other words,

$$ak \equiv -a(p-k) \pmod p.$$

Furthermore, for each $k = 1, 2, \ldots, \frac{p-1}{2}$, the exactly one of k and $-k$ is a least absolute residue of $\{a, 2a, 3a, \ldots, \frac{p-1}{2}a\}$.

Learning outcomes:
Author(s): Claire Merriman

Proof Let p be an odd prime number and let $a \in \mathbb{Z}$ with $p \nmid a$. Then

$$ak \equiv -ap + ak \equiv -a(p-k) \pmod{p}.$$

Then

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

is a reduced residue system modulo p by **??**. From Chapter 2, **??**,

$$\left\{\frac{-(p-1)}{2}, \frac{-(p-3)}{2}, \ldots, -2, -1, 1, 2, \ldots, \frac{p-2}{2}, \frac{p-1}{2}\right\}$$

is a reduced residue system modulo p. Thus, every element of $\{a, 2a, \ldots, \frac{p-1}{2}a, \frac{p+1}{2}a, \ldots, (p-1)a\}$ is congruent to exactly one of $\left\{\frac{-(p-1)}{2}, \ldots, -1, 1, \ldots, \frac{p-2}{2}, \frac{p-1}{2}\right\}$. That is, for each $k = 1, 2, \ldots, \frac{p-1}{2}$, both k and $-k$ are least absolute residue of $\{a, 2a, 3a, \ldots, \frac{p-1}{2}a, \frac{p+1}{2}a, \ldots, (p-1)a\}$.

If k is the least absolute remainder of aj modulo p for some $j = 1, 2, \ldots, \frac{p-1}{2}$, then $-k$ is the absolute least residue of $a(p-j)$ modulo p and $p-j = \frac{p+1}{2}, \frac{p+3}{2}, \ldots, p-1$. Thus, $-k$ is not an absolute least residue of $\{a, 2a, 3a, \ldots, \frac{p-1}{2}a\}$. Since there are $\frac{p-1}{2}$ elements of $\{a, 2a, 3a, \ldots, \frac{p-1}{2}a\}$, there must be $\frac{p-1}{2}$ distinct absolute least residues modulo p. Thus, for each $k = 1, 2, \ldots, \frac{p-1}{2}$, exactly on of k and $-k$ is an absolute least residue of $\{a, 2a, 3a, \ldots, \frac{p-1}{2}a\}$. ■

In-class Problem 1 Check Lemma 1 for

(a) $a = 3, p = 7$

(b) $a = 5, p = 11$

(c) $a = 6, p = 11$

Solution: (a) $a = 3, p = 7$

$$\begin{aligned} 3 &\pmod 7,\ 3(2) \equiv -1 \pmod 7,\ 3(3) \equiv 2 \pmod 7, \\ 3(4) \equiv -2 &\pmod 7,\ 3(5) \equiv 1 \pmod 7,\ 3(6) \equiv -3 \pmod 7, \end{aligned}$$

(b) $a = 5, p = 11$

$$\begin{aligned} 5 &\pmod{11},\ 5(2) \equiv -1 \pmod{11},\ 5(3) \equiv 4 \pmod{11}, \\ 5(4) &\equiv -2 \pmod{11},\ 5(5) \equiv 3 \pmod{11}, \\ 5(6) \equiv -3 &\pmod{11},\ 5(7) \equiv -2 \pmod{11},\ 5(8) \equiv -4 \pmod{11}, \\ 5(9) &\equiv 1 \pmod{11},\ 5(10) \equiv -5 \pmod{11}, \end{aligned}$$

(c) $a = 11, p = 23$

$$\begin{aligned} 11 \pmod{23},\ 11(2) \equiv -1 \pmod{23},\ 11(3) \equiv 10 \pmod{23},\\ 11(4) \equiv -2 \pmod{23},\ 11(5) \equiv 9 \pmod{23},\ 11(6) \equiv -3 \pmod{23},\\ 11(7) \equiv 8 \pmod{23},\ 11(8) \equiv -4 \pmod{23},\ 11(9) \equiv 7 \pmod{23},\\ 11(10) \equiv -5 \pmod{23},\ 11(11) \equiv 6 \pmod{23},\\ 11(12) \equiv -6 \pmod{23},\ 11(13) \equiv 5 \pmod{23},\\ 11(14) \equiv -7 \pmod{23},\ 11(15) \equiv 4 \pmod{23},\ 11(16) \equiv -8 \pmod{23},\\ 11(17) \equiv 3 \pmod{23},\ 11(18) \equiv -9 \pmod{23},\ 11(19) \equiv 2 \pmod{23},\\ 11(20) \equiv -10 \pmod{23},\ 11(21) \equiv 1 \pmod{23},\ 11(22) \equiv -11 \pmod{23}, \end{aligned}$$

We now prove **??**.

Proof Let $r_1, r_2, \dots r_n$ be the least nonnegative residues of the integers $a, 2a, \dots, \frac{p-1}{2}a$ that are greater than $\frac{p}{2}$ and $s_1, s_2, \dots, s_m$ be the least nonnegative residues that are less that $\frac{p}{2}$. Note that no r_i or s_j is 0, since p does not divide any of $a, 2a, \dots \frac{p-1}{2}$. Consider the $\frac{p-1}{2}$ integers given by

$$p - r_1, p - r_2, \dots, p - r_n, s_1, s_2, \dots, s_m.$$

We want to show that these integers are the integers from 1 to $\frac{p-1}{2}$, inclusive, in some order. Since each integer is less than or equal to $\frac{p-1}{2}$, it suffices to show that no two of these integers are congruent modulo p.

If $p - r_i \equiv p - r_j \pmod{p}$ for some $i \neq j$, then $r_i \equiv r_j \pmod{p}$, but this implies that there exists some $k_i, k_j \in \mathbb{Z}$ such that $r_i = k_i a \equiv k_j a = r_j \pmod{p}$ with $k_i \neq k_j$ and $1 \leq k_i, k_j \leq \frac{p-1}{2}$. Since

Multiple Choice:

(a) $p \nmid a$ ✓

(b) $p \mid a$

we know that the multiplicative inverse of a modulo p

Multiple Choice:

(a) exists ✓

(b) does not exist

and thus $k_i \equiv k_j \pmod{p}$, a contradiction. Thus, no two of the first n integers are congruent modulo p.

Similarly, no two of the second m integers are congruent. Now, if $p - r_i j \pmod{p}$, for some i and j, then $-r_i j \pmod{p}$. Thus, there exists $k_i, k_j \in \mathbb{Z}$ such that $-r_i = -k_i a \equiv k_j a = s_j \pmod{p}$ with $k_i \neq k_j$ and $1 \leq k_i, k_j \leq \frac{p-1}{2}$. Since $p \nmid a$, we know that the multiplicative inverse of a modulo p exists, and thus $-k_i \equiv k_j \pmod{p}$, a contradiction. Thus, the $\frac{p-1}{2}$ integers $p - r_1, p - r_2, \dots, p - r_n, s_1, s_2, \dots, s_m$ are the integers $1, 2, \dots, \frac{p-1}{2}$ in some order.

Then,

$$(p - r_1)(p - r_2) \cdots (p - r_n) s_1 s_2 \cdots s_m \equiv \frac{p-1}{2}! \pmod{p}$$

implies that

$$(-1)^n r_1 r_2 \cdots r_n s - 1 s_2 \cdots s_m \equiv \frac{p-1}{2}! \pmod{p}.$$

By the definition of r_i and s_j, we have

$$(-1)^n a(2a)(3a)\cdots(\frac{p-1}{2}a) \equiv \frac{p-1}{2}! \pmod{p}.$$

By reordering, we have

$$(-1)^n a^{\frac{p-1}{2}} \frac{p-1}{2}! \equiv \frac{p-1}{2}! \pmod{p}.$$

Thus, $(-1)^n a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, and $a^{\frac{p-1}{2}} \equiv (-1)^n \pmod{p}$. By Euler's criterion, we get that $\left(\frac{a}{p}\right) \equiv (-1)^n \pmod{p}$. Since both sides of the congruence must be ± 1, we have $\left(\frac{a}{p}\right) = (-1)^n$. ■

We are going to prove a result about $\left(\frac{2}{p}\right)$ before our next technical lemma.

Theorem 1. Let p be an odd prime. Then

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & if\ p \equiv 1,7 \pmod 8 \\ -1 & if\ p \equiv 3,5 \pmod 8). \end{cases}$$

Proof By Gauss's Lemma, we have that $\left(\frac{2}{p}\right) = (-1)^n$, where n is the number of least positive residues of the integers $2, 2*2, 2*3, \ldots, \frac{p-1}{2}$ that are greater than $\frac{p}{2}$. Let $k \in \mathbb{Z}$ with $1 \leq k \leq \frac{p-1}{2}$. Then $2k < \frac{p}{2}$ if and only if $k < \frac{p}{4}$; so $\left\lfloor \frac{p}{4} \right\rfloor$ of the integers $2, 2*2, 2*3, \ldots, \frac{p-1}{2}$ that are less than $\frac{p}{2}$, where $\lfloor \cdot \rfloor$ is the greatest integer (or floor) function. So, $\frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor$ of these integers are greater than $\frac{p}{2}$, from which

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor}$$

by Gauss's Lemma. For the first equality, it suffices to show that

$$\frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor \equiv \frac{p^2-1}{8} \pmod 2.$$

If $p \equiv 1 \pmod 8$, the $p = 8k+1$ for some $k \in \mathbb{Z}$. That gives us

$$\frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor = \frac{(8k+1)-1}{2} - \left\lfloor \frac{8k+1}{4} \right\rfloor = 4k - 2k = 2k \equiv 0 \pmod 2$$

and

$$\frac{p^2-1}{8} = \frac{(8k+1)^2-1}{8} = 8k^2 + 2k \equiv 0 \pmod 2.$$

Thus, holds when $p \equiv 1 \pmod 8$. The rest of the cases are left as homework. ■