Monday, April 1: Gauss's Lemma and Practice

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

- Find the Legendre symbol using Gauss's Lemma
- Find the Legendre symbol using several different methods.

Reading None

Statement of Guass's Lemma (20 minutes)

Lemma 1 (Gauss's Lemma)**.** *Let p be an odd prime number and like $a \in \mathbb{Z}$ with $p \nmid a$. Let n be the number of least positive residues of the integers $a, 2a, 3a, \ldots, \frac{p-1}{a}$ modulo p that are greater than $\frac{p}{2}$. Then*

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

Example 1. *Find* $\left(\frac{6}{11}\right)$

(a) *Using Gauss's Lemma*

Solution: *Note that* $\frac{11-1}{2} = 5$.

First, we list $6, 2(6), 3(6), 4(6), 5(6)$ *and find the least nonnegative residues modulo* 11 :

$$6,\ 2(6) \equiv 1 \pmod{11},\ 3(6) \equiv 7 \pmod{11},\ 4(6) \equiv 2 \pmod{11},\ 5(6) \equiv 8 \pmod{11}.$$

Now we count $n = 3$ *of the least nonnegative residues modulo* 11 *are greater than* $\frac{11}{2} = 5.5$

Thus, $\left(\frac{6}{11}\right) = (-1)^3 = -1.$

(b) *Factoring and using quadratic reciprocity*

Solution: *Using Proposition 4.5 and the fact that* $2 \equiv -9 \pmod{11}$,

$$\left(\frac{6}{11}\right) = \left(\frac{2}{11}\right)\left(\frac{3}{11}\right) = \left(\frac{-9}{11}\right)\left(\frac{3}{11}\right) = \left(\frac{-1}{11}\right)\left(\frac{9}{11}\right)\left(\frac{3}{11}\right) = \left(\frac{-1}{11}\right)(1)\left(\frac{3}{11}\right)$$

Since $11 \equiv 3 \pmod 4$, $\left(\frac{-1}{11}\right) = -1$ *by Theorem 4.6 and* $\left(\frac{3}{11}\right) = -\left(\frac{11}{3}\right)$. *Thus,*

$$\left(\frac{6}{11}\right) = \left(\frac{-1}{11}\right)\left(\frac{3}{11}\right) = (-1)(-1)\left(\frac{11}{3}\right) = \left(\frac{-1}{3}\right) = -1.$$

Example 2. *Find* $\left(\frac{-11}{7}\right)$

(a) *Using Gauss's Lemma*

Solution: *Since* $\frac{7-1}{2} = 3$, *we need to find the least nonnegative residues of* $-11, 2(-11), 3(-11)$ *modulo* 7. *These are*

$$-11 \equiv 3 \pmod 7,\ 2(-11) \equiv 6 \pmod 7,\ 3(-11) \equiv 2 \pmod 7.$$

Then $n = 1$ *is greater than* $\frac{7}{2} = 3.5$ *and* $\left(\frac{-11}{7}\right) = (-1)^1 = -1$.

(b) *By reducing modulo* 7 *then using Gauss's Lemma*

Solution: *By Theorem 4.5(b)* $\left(\frac{-11}{7}\right) = \left(\frac{3}{11}\right)$. *Since* $\frac{7-1}{2} = 3$, *we need to find the least nonnegative residues of* $3, 2(3), 3(3)$ *modulo* 7. *These are*

$$3 \pmod 7,\ 6 \pmod 7,\ 3(3) \equiv 2 \pmod 7.$$

Then $n = 1$ *is greater than* $\frac{7}{2} = 3.5$ *and* $\left(\frac{-11}{7}\right) = (-1)^1 = -1$.

(c) *By reducing modulo* 7 *and using quadratic reciprocity*

Solution: *By Theorem 4.5(b)* $\left(\frac{-11}{7}\right) = \left(\frac{3}{11}\right)$. *Since* $11 \equiv 3 \equiv 3 \pmod 4$, $\left(\frac{3}{11}\right) = -\left(\frac{11}{3}\right)$ *By Theorem 4.5(b)* $-\left(\frac{11}{3}\right) = -\left(\frac{-1}{3}\right) = 1$ *using Theorem 4.6.*

Practice Problems (30 minutes)

We can combine these results to find the Legendre symbol many different ways.

In-class Problem 1 *Use the following methods to find* $\left(\frac{-6}{11}\right)$:

(a) *Euler's Criterion, from March 22:*

Solution: $\left(\frac{-6}{11}\right) \equiv (-6)^{(11-1)/2} \equiv (-6)^5 \pmod{11}$ *By Euler's Criterion. Then*

$$(-6)^5 \equiv ((6)^2)^2(-6) \equiv 3^2(-6) \equiv -54 \equiv 1 \pmod{11}$$

(b) *Factor into* $\left(\frac{-6}{11}\right) = \left(\frac{-1}{11}\right)\left(\frac{2}{11}\right)\left(\frac{3}{11}\right) = (\boxed{-1})\left(\frac{2}{11}\right)\left(\frac{3}{11}\right)$. *From here, we will explore the various was to find* $\left(\frac{2}{11}\right)$ *and* $\left(\frac{3}{11}\right)$.

(i) *Find* $\left(\frac{2}{11}\right)$

- *Using Euler's Criterion.*

Solution: *From Euler's Criterion,*

$$\left(\frac{2}{11}\right) \equiv 2^{(11-1)/2} \equiv 32 \equiv -1 \pmod{11}.$$

- *Using Gauss's Lemma.*

Solution: *First, find the least nonnegative residues of* $2, 2(2), 3(2), 4(2), 5(2)$ *modulo* 11. *These are*

$$2, 4, 6, 8, 10,$$

and $n = \boxed{3}$ *are greater than* $\frac{11}{2}$. *Thus, by Gauss's Lemma,*

$$\left(\frac{2}{11}\right) = (-1)^{\boxed{3}} = \boxed{3}.$$

(ii) *Find* $\left(\frac{3}{11}\right)$

- *Using Euler's Criterion.*

Solution: *From Euler's Criterion,*

$$\left(\frac{3}{11}\right) \equiv 3^{(11-1)/2} \equiv (-2)^2(3) \equiv 1 \pmod{11}.$$

- *Using quadratic reciprocity*

Solution: *Since* $11 \equiv 3 \pmod 4$, $\left(\frac{3}{11}\right) = -\left(\frac{11}{3}\right) = -\left(\frac{2}{3}\right) = 1.$

- *Using Gauss's Lemma.*

Solution: *First, find the least nonnegative residues of* $3, 2(3), 3(3), 4(3), 5(3)$ *modulo* 11. *These are*

$$\boxed{3, 6, 9, 1, 4}$$

and $n = \boxed{2}$ *are greater than* $\frac{11}{2}$. *Thus, by Gauss's Lemma,*

$$\left(\frac{3}{11}\right) = (-1)^{\boxed{2}} = \boxed{2}.$$

Thus, $\left(\frac{-6}{11}\right) =$

(c) *Use that* $-6 \equiv 5 \pmod{11}$, *so* $\left(\frac{-6}{11}\right) = \left(\frac{5}{11}\right)$. *Then find* $\left(\frac{5}{11}\right)$ *using Euler's Criterion.*

(i) *Using Euler's Criterion.*

Solution: *From Euler's Criterion,*

$$\left(\frac{5}{11}\right) \equiv 5^{(11-1)/2} \equiv (3)^2(5) \equiv 1 \pmod{11}.$$

(ii) *Using quadratic reciprocity*

Solution: *Since* $5 \equiv 1 \pmod 4$, $\left(\frac{5}{11}\right) = \left(\frac{11}{5}\right) = \left(\frac{1}{5}\right) = 1$.

(iii) *Using Gauss's Lemma.*

Solution: *First, find the least nonnegative residues of* $5, 2(5), 3(5), 4(5), 5(5)$ *modulo* 11. *These are*

$$\boxed{5, 10, 4, 9, 2},$$

and $n = \boxed{2}$ *are greater than* $\frac{11}{2}$. *Thus, by Gauss's Lemma,*

$$\left(\frac{5}{11}\right) = (-1)^{\boxed{2}} = \boxed{2}.$$

In-class Problem 2 *Now we will examine the Legendre symbol of 2 using Gauss's Lemma. First, note that* $2, 2(2), 3(2), \ldots, 2(\frac{p-1}{2})$ *are already least nonnegative residues modulo* p. *It will be slightly easier to count how many are* less than $\frac{p}{2}$, *then subtract from the total number,* $\frac{p-1}{2}$.

Let $k \in \mathbb{Z}$ *with* $1 \leq k \leq \frac{p-1}{2}$. *Then* $2k < \frac{p}{2}$ *if and only if* $k < \boxed{\frac{p}{4}}$. *Thus,* $\frac{p-1}{2} - \lfloor \boxed{\frac{p}{4}} \rfloor$ *of* $2, 2(2), 3(2), \ldots, 2(\frac{p-1}{2})$ *are greater than* $\frac{p}{2}$. (Hint: *The two blanks should be the same, and also go in the blanks in the table headers)*

Now complete this table

p	$\lfloor \boxed{\frac{p}{4}} \rfloor$	$\frac{p-1}{2} - \lfloor \boxed{\frac{p}{4}} \rfloor$	$2, 2(2), 3(2), \ldots, 2(\frac{p-1}{2})$	$\left(\frac{2}{p}\right)$
3	$\boxed{0}$	$\boxed{1}$	*Less than* $\frac{3}{2}$: $\boxed{N/A}$ *Greater than* $\frac{3}{2}$: $\boxed{2}$	$\boxed{(-1)^1 = -1}$
5	$\boxed{1}$	$\boxed{1}$	*Less than* $\frac{5}{2}$: $\boxed{2}$ *Greater than* $\frac{5}{2}$: $\boxed{4}$	$\boxed{(-1)^1 = -1}$
7	$\boxed{1}$	$\boxed{2}$	*Less than* $\frac{7}{2}$: $\boxed{2}$ *Greater than* $\frac{7}{2}$: $\boxed{4, 6}$	$\boxed{(-1)^2 = 1}$
11	$\boxed{2}$	$\boxed{3}$	*Less than* $\frac{11}{2}$: $\boxed{2, 4}$ *Greater than* $\frac{11}{2}$: $\boxed{6, 8, 10}$	$\boxed{(-1)^3 = -1}$
13	$\boxed{3}$	$\boxed{3}$	*Less than* $\frac{13}{2}$: $\boxed{2, 4, 6}$ *Greater than* $\frac{13}{2}$: $\boxed{8, 10, 12}$	$\boxed{(-1)^3 = -1}$
17	$\boxed{4}$	$\boxed{4}$	*Less than* $\frac{17}{2}$: $\boxed{2, 4, 6, 8}$ *Greater than* $\frac{17}{2}$: $\boxed{10, 12, 14, 16}$	$\boxed{(-1)^4 = 1}$
19	$\boxed{4}$	$\boxed{5}$	*Less than* $\frac{19}{2}$: $\boxed{2, 4, 6, 8}$ *Greater than* $\frac{17}{2}$: $\boxed{10, 12, 14, 16, 18}$	$\boxed{(-1)^5 = -1}$
23	$\boxed{5}$	$\boxed{6}$	*Less than* $\frac{17}{2}$: $\boxed{2, 4, 6, 8, 10}$ *Greater than* $\frac{17}{2}$: $\boxed{12, 14, 16, 18, 20, 22}$	$\boxed{(-1)^6 = 1}$

Wednesday, April 3: Proving Gauss's Lemma and the Quadratic Residue of 2