Your Name: ____________ Group Members: ____________ ____________

Results

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

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

Theorem 2 (Theorem 4.6)**.** *Let p be an odd prime number. Then*

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

Theorem 3 (Quadratic reciprocity)**.** *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 $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$

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*

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

Problems

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:

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

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

Learning outcomes:

Author(s): Claire Merriman

(b) Factor into $\left(\frac{-6}{11}\right) = \left(\frac{-1}{11}\right)\left(\frac{2}{11}\right)\left(\frac{3}{11}\right) = (\underline{\qquad})\left(\frac{2}{11}\right)\left(\frac{3}{11}\right)$. 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 the specified method:

- Using Euler's Criterion.

- Using Gauss's Lemma.

(ii) Find $\left(\frac{3}{11}\right)$ using the specified method:

- Using Euler's Criterion.

- Using Quadratic reciprocity

- Using Gauss's Lemma.

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

(c) Use that $-6 \equiv 5 \pmod{11}$, so $\left(\frac{-6}{11}\right) = \left(\frac{5}{11}\right)$. Then find $\left(\frac{5}{11}\right)$ the specified method:

(i) Using Euler's Criterion.

(ii) Using Quadratic reciprocity

(iii) Using Gauss's Lemma.

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 $k <$ ______. Thus, $\frac{p-1}{2} - \lfloor \_\_\_\_\_\_ \rfloor$ of $2, 2(2), 3(2), \ldots, 2(\frac{p-1}{2})$ are greater than $\frac{p}{2}$.

Now complete this table

p	$\lfloor \_\_\_\_\_\_ \rfloor$	$\frac{p-1}{2} - \lfloor \_\_\_\_\_\_ \rfloor$	$2, 2(2), 3(2), \ldots, 2(\frac{p-1}{2})$	$\left(\frac{2}{p}\right)$
3			Less than $\frac{3}{2}$: Greater than $\frac{3}{2}$:	
5			Less than $\frac{5}{2}$: Greater than $\frac{5}{2}$:	
7			Less than $\frac{7}{2}$: Greater than $\frac{7}{2}$:	
11			Less than $\frac{11}{2}$: Greater than $\frac{11}{2}$:	
13			Less than $\frac{13}{2}$: Greater than $\frac{13}{2}$:	
17			Less than $\frac{17}{2}$: Greater than $\frac{17}{2}$:	
19			Less than $\frac{19}{2}$: Greater than $\frac{17}{2}$:	
p			Less than $\frac{17}{2}$: Greater than $\frac{17}{2}$:	