MAT-255– NUMBER THEORY   SPRING 2024   IN CLASS WORK MARCH 27

Your Name: ____________________ Group Members: ____________________ ____________________

From class March 20:

Modulus	Quadratic residues	Quadratic nonresidues
2	1	None
3	1	2
5	$1, 4$	$2, 3$
7	$1, 2, 4$	$3, 5, 6$

Proposition (Proposition 4.5)**.** *Let p be an odd prime number and $a, b \in \mathbb{Z}$ with $p \nmid a$ and $p \nmid b$. Then*

(a) $\left(\dfrac{a^2}{p}\right) = 1$

(b) If $a \equiv b \pmod{p}$ *then* $\left(\dfrac{a}{p}\right) = \left(\dfrac{b}{p}\right)$

(c) $\left(\dfrac{ab}{p}\right) = \left(\dfrac{a}{p}\right)\left(\dfrac{b}{p}\right)$

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

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

Theorem (Quadratic reciprocity)**.** *Let p and q be distinct primes.*

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

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

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.*

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

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

Proof (a) Since $3 \equiv$ ____________ $\pmod{4}$,[1] we need two cases for Quadratic reciprocity.

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

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

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

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

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

(i) If $p \equiv 1 \pmod 4$, then $\left(\frac{-1}{p}\right) =$ __________ by Theorem 4.6 and $\left(\frac{3}{p}\right) =$ __________ by Quadratic reciprocity. Thus, $\left(\frac{-3}{p}\right) =$ __________ $= 1$ if and only if $p \equiv$ __________. Then $p \equiv$ __________ (mod 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 $\left(\frac{-1}{p}\right) =$ __________ by Theorem 4.6 and $\left(\frac{3}{p}\right) =$ __________ by Quadratic reciprocity. Thus, $\left(\frac{-3}{p}\right) =$ __________ $= 1$ if and only if $p \equiv$ __________. Then $p \equiv$ __________ (mod 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 $p \equiv$ __________ (mod 12), which is equivalent to $p \equiv 1 \pmod 6$.

■

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.

(a) 5

(b) -5

(c) 7

(d) -7

Proof (a) *Since* $5 \equiv$ __________ (mod 4), ________________ *by* Quadratic reciprocity. *Then* $\left(\frac{5}{p}\right) =$ _____ $=$ 1 *if and only if* ________________.

■