

MATH 4573: HOMEWORK 7

INSTRUCTOR: TYLER GENAO

Due: March 13, 2026.

This homework has two sections: the first section has the assigned problems that you will turn in to Gradescope for credit. The second section contains recommended and bonus problems, either from myself, the textbook or other sources. These latter problems are not graded for credit, but you may find them to be useful practice and/or interesting!

For any assigned problem in this homework, **you must show all of your work in order to receive full credit. Your solutions can only cite up to §3.3 of our notes. Everything else must be proven.**

1. PROBLEMS TO SUBMIT

Exercise 1. The following exercise has the flavor of a HW 3 problem, but can be useful for simplifying Legendre symbol calculations. Show that for any integer $k \in \mathbb{Z}^+$, one has the following.

- a) k is congruent to its unit digit a_0 modulo 2, and thus $2 \mid k$ if and only if $a_0 = 0, 2, 4, 6$ or 8 .
- b) k is congruent to the sum of its digits modulo 3, and thus $3 \mid k$ if and only if 3 divides this sum.
- c) k is congruent to its unit digit a_0 modulo 5, and thus $5 \mid k$ if and only if $a_0 = 0, 5$.

(*Hint:* for each of these parts, work with the base 10 expansion of k : write $k = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \dots + a_r \cdot 10^r$, where each $0 \leq a_i < 10$ and $a_r \neq 0$.)

Exercise 2. Compute the following Legendre/Jacobi symbols.

- a) $\left(\frac{51}{71}\right)$.
- b) $\left(\frac{-35}{97}\right)$.
- c) $\left(\frac{1011}{9907}\right)$, where 9907 is prime.

Exercise 3. Prove that for a prime $p > 2$, if $a, b \in \mathbb{Z}$ are not squares modulo p then ab is a square modulo p .

Exercise 4.

- a) List the squares modulo 7, and then the non-squares.
- b) Determine all primes p such that $x^2 - 7$ has a root modulo p . Your final answer should include several different congruence conditions on p .

Exercise 5. Using Quadratic Reciprocity and/or its supplemental laws, prove that for any prime $p > 2$ one has

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

Exercise 6. Let $p > 2$ be prime, and suppose that g is a primitive root modulo p .

- Prove that for any $a \in \mathbb{Z}$ coprime to p , one has that a is a quadratic residue modulo p if and only if $a \equiv g^{2k} \pmod{p}$ for some $k \in \mathbb{Z}$.
- Use part a) to give a complete list of quadratic residues modulo 19; **write them as positive integers in $[1, 18]$, listed in increasing order.**
- How many quadratic residues are there modulo any odd prime p ? What about quadratic nonresidues?

Exercise 7. Determine with proof whether the polynomial $x^4 - 36$ has a root modulo the prime $p = 5077$.

Exercise 8. Who did you consult for this assignment? What resources did you use?

2. OTHER RECOMMENDED PROBLEMS

From [NZM91, §3.1], pages 135 – 136: #4 – 5, 7 – 10.

From [NZM91, §3.2], pages 140 – 141: #1 – 11.

From [NZM91, §3.3], page 147: #2 – 4.

Bonus Exercise 9. Show that $5^{1500} \equiv 1 \pmod{3001}$. (*Hint:* you may assume that 3001 is prime.)

Bonus Exercise 10. Let a be an integer, and set $f(x) := x^2 - a$. Show that for any prime p , the number of solutions to $f(x) \equiv 0 \pmod{p}$ is $1 + \left(\frac{a}{p}\right)$.

Bonus Exercise 11. This exercise fills in some steps from our proof of Quadratic Reciprocity. Following the notation from the proof, let $p, q > 2$ be distinct primes, and set $P := \frac{p-1}{2}$ and $Q := \frac{q-1}{2}$.

- Show that

$$\left(\frac{q-1}{2}\right)!^2 \equiv (-1)^{\frac{q-1}{2}} \cdot (q-1)! \pmod{q}.$$

(*Hint:* for each integer $1 \leq k < q$, one has $k \leq \frac{q-1}{2}$ if and only if $\frac{q-1}{2} < q - k$.)

- Show that

$$\prod_{Qp < k < \frac{pq}{2}} k \equiv P! \pmod{p}.$$

(*Hint:* observe that each term of this product has the form $k = \ell + Qp$ where $\ell \geq 1$.)

- Show that Pq is the greatest multiple of q below $\frac{pq}{2}$.

REFERENCES

- [NZM91] I. Niven, H.S. Zuckerman and H.L. Montgomery, *An introduction to the theory of numbers*, 5th Ed., John Wiley & Sons, Inc., New York (1991).