MATH 4573: HOMEWORK 7

INSTRUCTOR: TYLER GENAO

Due: March 29, 2024.

This homework has two sections: the first section has the problems that you'll turn in for credit. The second section contains recommended problems from the textbook, myself or other sources; you are not required to do these, but I recommend that you check them out.

For any problem in this assignment, **you must show all of your work in order to receive full credit.** Please do not use words such as "clear", "obvious" or "trivial" in your solutions.

Your solutions should not use theorems from sections which come after the day the homework was assigned. This HW should use up to what we've covered in class so far (including §3.1 – 3.3).

1. Problems to Submit

Exercise 1. We've used the following facts throughout this class, but have never proved them. Since these can help us with Legendre and Jacobi symbol calculations, we'll prove them once and for all.

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 a_0 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 $a_0 = 0$ or 5.

(*Hint:* for each of these parts, work with the base 10 expansion of k: i.e., write $k = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \ldots + a_r \cdot 10^r$, 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) $\left(\frac{1001}{9907}\right)$, where 9907 is prime.

Exercise 3. Prove that for any odd prime $p \in \mathbb{Z}^+$, if $a, b \in \mathbb{Z}$ are not squares modulo p then their product ab is a square modulo p.

Exercise 4.

a) List the squares modulo 7, and then the non-squares.

b) Determine all primes $p \in \mathbb{Z}^+$ such that $x^2 - 7$ has a root modulo p. (*Hint:* your final answer should include several different congruency conditions on p.)

Exercise 5. Using quadratic reciprocity and/or its supplemental laws, prove that for any odd prime $p \in \mathbb{Z}^+$, 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 $p \in \mathbb{Z}^+$ be an odd prime, and suppose that g is a primitive root modulo p.

a) 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 $k \in \mathbb{Z}$.
b) Use part a) to give a complete list of quadratic residues modulo 19; **write them using positive integers between 1 and 18, listed in increasing order.** (*Hint:* 2 is a primitive root modulo 19.)
c) How many quadratic residues are there modulo an odd prime $p \in \mathbb{Z}^+$? What about quadratic nonresidues?

Exercise 7. Determine 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 the textbook, pages $135 - 136$: $\#4, 5, 7 - 10$.
Pages $140 - 141$: $\#1 - 11$.
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. This exercise fills in some steps from our proof of quadratic reciprocity, which can be found on Carmen. Following the notation in our proof, let $p, q > 2$ be primes, and set $P := \frac{p-1}{2}$ and $Q := \frac{q-1}{2}$.

a) 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 $\frac{q-1}{2} < q - k$.)
b) 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 $\ell \geq 1$.)
c) Show that Pq is the greatest multiple of q below $\frac{pq}{2}$.

Bonus Exercise 11. Let $a \in \mathbb{Z}$ be an integer, and set $f(x) := x^2 - a$. Show that for any prime $p \in \mathbb{Z}^+$, the number of roots of $f(x)$ modulo p is $1 + \left(\frac{a}{p}\right)$.

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).