

HOMEWORK 6: MATH 124 (NUMBER THEORY)

1. EXERCISES

Exercise 1.1. Determine which of the following congruences have a solution. Show your work.

- (1) $x^2 \cong 5 \pmod{227}$ (2 pts)
- (2) $x^2 \cong 7 \pmod{1009}$ (2 pts)
- (3) $x^2 \cong -7 \pmod{1009}$ (3 pts)
- (4) $x^2 \cong 150 \pmod{1009}$ (3 pts)
- (5) $x^2 \cong 73 \pmod{173}$ (3 pts)
- (6) $x^2 \cong 42 \pmod{97}$ (3 pts)

Exercise 1.2. Use quadratic reciprocity to show that 757 is a prime number. (Hint: Consider $55^2 + 3$). (4 pts).

Exercise 1.3. Find all the primes q for which the following equations have a solution.

- (1) $x^2 \cong 5 \pmod{q}$ (4 pts)
- (2) $x^2 \cong 15 \pmod{q}$ (4 pts)

Exercise 1.4. Let p be an odd prime and a a quadratic residue $\pmod{p}$. Show the following.

- (1) Prove that $x^2 \cong a \pmod{p^2}$ has exactly two solutions $\pmod{p^2}$. (Hint: Write a possible solution as $x_1 + py$, where x_1 is a solution to $x^2 \cong a \pmod{p}$.) (4 pts)
- (2) Using the reasoning in (1) and mathematical induction, show that $x^2 \cong a \pmod{p^k}$ always has exactly two solutions. (3 pts).

Exercise 1.5. Let p be an odd prime and $(a, p) = 1$ and $b \in \mathbb{Z}$. Show the following.

(1)

$$\sum_{j=1}^{p-1} \left(\frac{j}{p}\right) = 0$$

Conclude that half of the numbers in $(\mathbb{Z}/p\mathbb{Z})^*$ are quadratic residues and the other half are not quadratic residues. (Hint: use $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.) (3 pts)

(2)

$$\sum_{j=1}^p \left(\frac{aj+b}{p}\right) = 0$$

(3 pts)

Exercise 1.6. One of the crowning achievements of early analytic number theory is Dirichlet's theorem. This states that if $(a, m) = 1$ are relatively prime positive integers, then there are infinitely many primes

$$p \equiv a \pmod{m}.$$

The proof of Dirichlet's theorem is beyond the scope of the course. However, it uses Dirichlet characters (which are built from the Legendre symbol) and L-functions. To illustrate the utility of the Legendre symbol in proving such a result, we prove the special case when $m = 3$ using quadratic reciprocity and the ideas we used in showing that there are infinitely many prime numbers.

- (1) Determine the primes p for which $x^2 \cong -3 \pmod{p}$ has a solution. (3 pts).

- (2) Suppose, for contradiction, that there are only finitely many primes congruent to 1 (mod 3), say

$$p_1, \dots, p_r.$$

Set

$$P = p_1 p_2 \cdots p_r$$

and consider

$$N = 4P^2 + 3.$$

Consider a prime divisor q of N and show that $q \not\equiv 1 \pmod{3}$ and $q \neq p_i$. Conclude that there are infinitely many primes of the form

$$3n + 1.$$

(3 pts).

- (3) Argue as in Part (2), where we assume the finitely many $p_1, \dots, p_r$ are congruent to $-1 \pmod{3}$. Consider

$$M = 3p_1 p_2 \cdots p_r - 1,$$

and show that it has a prime divisor q distinct from the p_i and congruent to $-1 \pmod{3}$.

Conclude that there are infinitely many primes $p \not\equiv -1 \pmod{3}$. (4 pts)

Thus, Dirichlet's theorem holds for both reduced residue classes modulo 3.