MATH 567 NUMBER THEORY I, PROBLEMS 7

To be submitted by Tuesday, October 14th

Throughout this problem sheet, \( p \) denotes an odd prime number.

**Easier problems**

1. Let \( g \) be a primitive root modulo \( p \). Prove that the quadratic residues are precisely the residue classes \( g^{2k} \) with \( 0 \leq k < \frac{1}{2}(p-1) \). Show that, if \( p > 3 \), then the sum of the quadratic residues modulo \( p \) is the 0 residue.

2. Show that if \( p \equiv \pm 1 \pmod{8} \), then 2 is a quadratic residue and otherwise 2 is a quadratic non-residue. By considering the polynomial \( x^2 - 2 \), or otherwise, show that there are infinitely many primes in the residue class 7 \( \pmod{8} \).

3. Of which primes is \(-2\) a quadratic residue?

4. Decide whether \( x^2 \equiv 150 \pmod{1009} \) is soluble or not.

5. Find all primes \( p \) such that \( x^2 \equiv 13 \pmod{p} \) has a solution.

**Harder problems**

6. Prove that every quadratic non-residue modulo \( p \) is a primitive root modulo \( p \) if and only if \( p = 2^{2n} + 1 \) for some non-negative integer \( n \).

7. Show that \((x^2 - 2)/(2y^2 + 3)\) is never an integer when \( x \) and \( y \) are integers.