Study guide

- Know the notation $\left(\frac{a}{p}\right)$ for the Legendre symbol.
- Understand Euler's criterion: a is a quadratic residue modulo p iff $a^{(p-1)/2} \equiv 1 \bmod p$.
- How do you evaluate $\left(\frac{-1}{p}\right)$?
- How do you evaluate $\left(\frac{2}{p}\right)$?
- Understand the proof of the formula for $\left(\frac{2}{p}\right)$.
- Know the *statement* (but not a full proof) of the law of quadratic reciprocity. How can you use it to evaluate $\left(\frac{a}{p}\right)$?

1. (Textbook 21.1(a,b,c))
   For each congruence, determine whether or not a solution exists. You do not need to find the solution. (*Note.* Each modulus is prime.)

   (a) $x^2 \equiv -1 \pmod{5987}$

   (b) $x^2 \equiv 6780 \pmod{6781}$

   (c) $x^2 + 14x - 35 \equiv 0 \pmod{337}$

2. (Textbook 21.5)
   Use the same ideas we used to verify Quadratic Reciprocity (Part II) to verify the following two assertions. **For this problem, you should not use the full law of quadratic reciprocity, which implies both statements easily. The purpose of the problem is to see a glimpse of how the full law of quadratic reciprocity is proved.**

   (a) If p is congruent to 1 modulo 5 , then 5 is a quadratic residue modulo p.

   (b) If p is congruent to 2 modulo 5 , then 5 is a nonresidue modulo p.

   Hint Reduce the numbers $5, 10, 15, \ldots, \frac{5}{2}(p-1)$ so that they lie in the range from $-\frac{1}{2}(p-1)$ to $\frac{1}{2}(p-1)$ and check how many of them are negative.

   Note For all subsequent problems, you may, and should, use the full law of quadratic reciprocity, even though we didn't give a full proof of it.

3. Evaluate each of the following Legendre symbols.

   (a) $\left(\frac{85}{101}\right)$

   (b) $\left(\frac{29}{541}\right)$

   (c) $\left(\frac{101}{1987}\right)$

   (d) $\left(\frac{31706}{43789}\right)$

4. Let n be an number such that $n + 5$ is a perfect square. Prove that every prime factor of n, besides possibly 2 and possibly 5, is congruent to 1 or 4 modulo 5.

5. (a) Prove that if n is an even number that is not divisible by 3, then all of the prime factors of $n^2 + 3$ are congruent $1 \pmod 3$.

   (b) Prove that there are infinitely many primes congruent to 1 modulo 3.

   Note Both theorem 21.3 and the result of part (b) are special cases of Dirichlet's theorem on primes in arithmetic progressions.