Math 223 Number Theory, Spring ’07
Homework 10 Solutions

(1) Find all quadratic residues modulo 31. (Hint: Find a primitive root modulo 31.)
   Solution: It is not hard to see that, for example, 3 is a primitive root modulo 31. Then all the quadratic residues modulo 31 are \(3^2, 3^4, ..., 3^{30} \pmod{31}\).

(2) Determine whether each of the following congruences has a solution. All of the moduli are primes.
(a) \((24.1(a)) \ x^2 \equiv -1 \pmod{5987}\)
(b) \((24.1(b)) \ x^2 \equiv 6780 \pmod{6781}\)
(c) \(x^2 \equiv 8 \pmod{53}\)
(d) \(x^2 + 14x + 47 \equiv 0 \pmod{337}\) (Hint: Complete the square.)
   Solution:
(a) Since 5987 \(\equiv 3 \pmod{4}\), this congruence does not have a solution by Quadratic Reciprocity Part 1.
(b) This congruence can be rewritten as \(x^2 \equiv -1 \pmod{6781}\). Since 6781 \(\equiv 1 \pmod{4}\), there is a solution by Quadratic Reciprocity Part 1.
(c) Since 53 \(\equiv 5 \pmod{8}\), we have
   \[
   \left(\frac{8}{53}\right) = \left(\frac{2^3}{53}\right) = \left(\frac{2}{53}\right)^3 \left(\frac{2}{53}\right) = \left(\frac{2}{53}\right) \cdot 1 = \left(\frac{2}{53}\right) = -1
   \]
   so the congruence has no solutions by Quadratic Reciprocity Part 2.
(d) Since \(x^2 + 14x + 47 = (x + 7)^2 - 2\), the question is whether the congruence \((x + 7)^2 \equiv 2 \pmod{337}\) has a solution \(x + 7\). Since 337 \(\equiv 1 \pmod{8}\), the solution exists by Quadratic Reciprocity Part 2. Subtracting 7 from this solution gives a solution \(x\) to the original congruence.

(3) (parts of 25.1) Use the Law of Quadratic Reciprocity to compute the following Legendre symbols.
   (a) \(\left(\frac{85}{101}\right)\)
   (b) \(\left(\frac{29}{541}\right)\)
   Solution:
   (a) Since 85 factors as 5 \(\cdot\) 17 and since 101 \(\equiv 1 \pmod{4}\), we have
   \[
   \left(\frac{85}{101}\right) = \left(\frac{5}{101}\right) \left(\frac{17}{101}\right) = \left(\frac{101}{5}\right) \left(\frac{101}{17}\right) = \left(\frac{1}{5}\right) \left(\frac{16}{17}\right) = 1 \cdot \left(\frac{16}{17}\right) = \left(\frac{16}{17}\right).
   \]
   But since 17 \(\equiv 1 \pmod{4}\), we have
   \[
   \left(\frac{85}{101}\right) = \left(\frac{16}{17}\right) = \left(\frac{17}{16}\right) = \left(\frac{1}{16}\right) = 1.
   \]
   (b) Both 29 and 541 are primes. Since 29 \(\equiv 1 \pmod{4}\), we have
   \[
   \left(\frac{29}{541}\right) = \left(\frac{541}{29}\right) = \left(\frac{19}{29}\right) = \left(\frac{29}{19}\right) = \left(\frac{10}{19}\right) = \left(\frac{2}{19}\right) \left(\frac{5}{19}\right).
   \]
   Since 19 \(\equiv 3 \pmod{8}\), and since 5 \(\equiv 1 \pmod{4}\), we get
   \[
   \left(\frac{29}{541}\right) = -1 \cdot \left(\frac{19}{5}\right) = - \left(\frac{4}{5}\right) = - \left(\frac{5}{4}\right) = - \left(\frac{1}{4}\right) = -1.
   \]

(4) Let \(p\) be an odd prime and let \(a, b \in \mathbb{Z}\) be inverses modulo \(p\). Prove that if \(a\) is a quadratic residue modulo \(p\), then so is \(b\).
Solution: Suppose that \( \left( \frac{a}{p} \right) = 1 \). Then if \( ab \equiv 1 \pmod{p} \), we have
\[
1 = \left( \frac{1}{p} \right) = \left( \frac{ab}{p} \right) = \left( \frac{a}{p} \right) \left( \frac{b}{p} \right) = \left( \frac{b}{p} \right)
\]
as desired. The first equality is true since 1 is always a quadratic residue.

(5) Suppose \( p \) is a Mersenne prime greater than or equal to 5. Prove that \( \left( \frac{3}{p} \right) = -1 \).

Solution: Let \( p = 2^q - 1 \) be a Mersenne prime for some prime \( q \geq 3 \). Note that \( p \equiv 3 \pmod{4} \). Thus
\[
\left( \frac{3}{p} \right) = -\left( \frac{p}{3} \right) = -\left( \frac{2^q - 1}{3} \right) = -\left( \frac{(-1)^q - 1}{3} \right) = -\left( \frac{-1 - 1}{3} \right) = -\left( \frac{-2}{3} \right) = -\left( \frac{1}{3} \right) = -1.
\]

(6) Let \( p \) be a prime. Prove that, if \( p \equiv 3 \pmod{8} \) and \( \frac{p-1}{2} \) is a prime, then \( \frac{p-1}{2} \) is a quadratic residue mod \( p \).

Solution: Since \( p \equiv 3 \pmod{8} \), then \( \frac{p-1}{2} \equiv 1 \pmod{4} \) and \( p \equiv 1 \pmod{\frac{p-1}{2}} \), so
\[
\left( \frac{\frac{p-1}{2}}{p} \right) = \left( \frac{p}{\frac{p-1}{2}} \right) = \left( \frac{1}{\frac{p-1}{2}} \right) = 1.
\]

(7) Let \( p \) be a prime with \( p \geq 5 \) and let \( k = \frac{p-1}{2} \). Let \( a_1, a_2, ..., a_k \in \{1, 2, ..., p - 1\} \) be the quadratic residues mod \( p \). Prove that \( p \) divides \( \sum_{i=1}^{k} a_i \).

Solution: It suffices to show that this sum is congruent to 0 mod \( p \). If \( g \) is a primitive root mod \( p \), then the quadratic residues are given by \( g^2, g^4, ..., g^{p-1} \). Let \( M = g^2 + g^4 + \cdots + g^{p-1} \). Note that \( g^2 M \equiv M \pmod{p} \), so \( (g^2 - 1)M \equiv 0 \pmod{p} \). However, since \( p > 3 \), we have \( g^2 \not\equiv 1 \pmod{p} \) since \( g \) is a primitive root, so it must be that \( M \equiv 0 \pmod{p} \).