116 - Number Theory
Spring 2007

Homework 10

Name: _____
Instructor: Travis Kelm

## Section 11.1 - Quadratic Residues and Nonresidues

**1. Quadratic Congurences:** Determine which of the following congruences have a solution. (All of the moduli are primes.)

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

*Solution*: Since $5987 \equiv -1 \pmod 4$ there is no solution. □

(b) $x^2 \equiv 6780 \pmod{5987}$

*Solution*: There is no solution as the following computation reveals:

$$\begin{aligned}\left(\frac{6780}{5987}\right) &= \left(\frac{793}{5987}\right)\\ &= \left(\frac{5987}{793}\right)\\ &= \left(\frac{436}{793}\right)\\ &= \left(\frac{4}{793}\right)\left(\frac{109}{793}\right)\\ &= \left(\frac{793}{109}\right)\\ &= \left(\frac{30}{109}\right)\\ &= \left(\frac{2}{109}\right)\left(\frac{3}{109}\right)\left(\frac{5}{109}\right)\\ &= (-1)\left(\frac{109}{3}\right)\left(\frac{109}{5}\right)\\ &= (-1)\left(\frac{1}{3}\right)\left(\frac{4}{5}\right) = \boxed{-1}\end{aligned}$$

□

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

*Solution*: Using the quadratic formula we get

$$x = \frac{-14 \pm \sqrt{196 - 4(-35)}}{2} = \frac{-14 \pm \sqrt{-1}}{2} \pmod{337}$$

This means that we have a solution so long as there is a $\sqrt{-1}$, in other words, so long as $x^2 \equiv -1 \pmod{337}$ has a solution. By the Law of Quadratic Reciprocity, the congruence $x^2 \equiv -1 \pmod{337}$ does have a solution, and hence, $x^2 + 14x - 35 \equiv 0 \pmod{337}$ has a solution. □

(d) $x^2 - 94x + 943 \equiv 0 \pmod{3011}$

*Solution*: Using the quadratic formula we get

$$x = \frac{94 \pm \sqrt{(-94)^2 - 4(943)}}{2} = \frac{94 \pm \sqrt{5064}}{2} \pmod{3011}$$

This means that we have a solution so long as there is a $\sqrt{5064}$, in other words, so long as $x^2 \equiv 5064 \pmod{3011}$ has a solution. One can compute $\left(\frac{5064}{3011}\right) = -1$ and thus the congruence $x^2 - 94x + 943 \equiv 0 \pmod{3011}$ has no solution. □

**2. When is 3 a Quadratic Residue:** The first few primes for which 3 is a quadratic residue and a nonresidue are

$$\begin{aligned} \text{QR:} &\quad p = 11, 13, 23, 37, 47, 59, 61, 71, 73, 83, 97, 107, 109 \\ \text{NR:} &\quad p = 5, 7, 17, 19, 29, 31, 41, 43, 53, 67, 79, 89, 101, 103, 113, 127 \end{aligned}$$

Try reducing the list modulo $m$ for various $m$'s until you see a pattern and make a conjecture identifying which primes have 3 as a quadratic residue.

*Solution*: Try reducing modulo 12. This gives

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{12} \\ -1 & \text{if } p \equiv \pm 5 \pmod{12} \end{cases} \qquad \square$$

## Section 11.2 - The Law of Quadratic Reciprocity

**3. When is 5 a Quadratic Residue:** Find a congruence describing all primes for which 5 is a quadratic residue.

*Solution*: The first few primes for which 5 is a quadratic residue and a nonresidue are

$$\begin{aligned} \text{QR:} &\quad p = 11, 19, 29, 31, 41, 59, 61, 71, 79, 89, 101, 109 \\ \text{NR:} &\quad p = 7, 13, 17, 23, 37, 43, 47, 53, 67, 73, 83, 97, 103, 107, 113, 127 \end{aligned}$$

If you put on your mod 5 glasses you will see

$$\left(\frac{5}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{5} \\ -1 & \text{if } p \equiv \pm 2 \pmod{5} \end{cases}$$

Perhaps easier to see is if you try mod 10 glasses you get

$$\left(\frac{5}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 9 \pmod{10} \\ -1 & \text{if } p \equiv 3, 7 \pmod{10} \end{cases} \qquad \square$$