

Section 11.1 - Quadratic Residues and Nonresidues

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

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

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

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

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

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

$$\text{QR: } p = 11, 13, 23, 37, 47, 59, 61, 71, 73, 83, 97, 107, 109$$

$$\text{NR: } p = 5, 7, 17, 19, 29, 31, 41, 43, 53, 67, 79, 89, 101, 103, 113, 127$$

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.

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.