Math 115, Summer 2012
Homework 4
Due Tuesday, July 16th

NZM a.b.c refers to a problem in our text, 5th edition - these may differ slightly from the problems appearing in other editions, so use the version printed here to be safe).

(1) (NZM 3.1.7) Which of the following congruences have solutions?
  (a) $x^2 \equiv 2 \mod 61$
  (b) $x^2 \equiv -2 \mod 61$
  (c) $x^2 \equiv 2 \mod 59$
  (d) $x^2 \equiv -2 \mod 118$

(2) (NZM 3.1.13) Prove that if r is a quadratic residue mod $m > 2$, then $r^{\phi(m)/2} \equiv 1 \mod m$. [Hint in the book]

(3) (NZM 3.1.19) Prove that for all primes p, $x^8 \equiv 16 \mod p$ has a solution. [Hint in the book]

(4) (NZM 3.2.3) Prove that if a prime p has the form $4k+1$, and is a quadratic residue mod an odd prime q, then q is a quadratic residue mod p.

(5) (NZM 3.2.4) Which of the following congruences is solvable?
  (a) $x^2 \equiv 5 \mod 227$
  (b) $x^2 \equiv 5 \mod 229$
  (c) $x^2 \equiv -5 \mod 227$
  (d) $x^2 \equiv -5 \mod 229$
  (e) $x^2 \equiv 7 \mod 1009$
  (f) $x^2 \equiv -7 \mod 1009$

  [Hint: 227,229, and 1009 are primes]

(6) (NZM 3.2.6) Decide whether $x^2 \equiv 150 \mod 1009$ is solvable or not.

(7) (NZM 3.2.7) Find all primes such that $x^2 \equiv 13 \mod p$ has a solution.

(8) (NZM 3.2.9) Find all primes q such that $\left(\frac{5}{q}\right) = -1$.

(9) (NZM 3.2.13) Prove that there are infinitely many primes of the form $3n+1$.

  [Hint: Proceed just like in Euclid's proof that there are infinitely many primes, namely assume there are only finitely many, say $p_1, \ldots, p_r$. We want a contradiction. Let $a = p_1 \cdots p_r$ be their product. Note a has the form $3n+1$, too. Here's the trick: Look at $N = (2a)^2 + 3$. Now consider a prime q dividing n, and show it cannot be in our list $p_1, \ldots, p_r$, using quadratic reciprocity. Note the factor of 2 in the expression for N is to make sure that q is odd.]

(10) (NZM 3.2.14) Let p and q be twin primes, that is, primes satisfying $q = p+2$. Prove that there is an integer a such that $p|(a^2-q)$ if and only if there is an integer b such that $q|(b^2-p)$.