Math 250 – Number Theory – Homework 6

Due: Friday March 31st

Please explain your answers carefully using full sentences, not only symbols. You may use the textbook and your notes, and you're welcome to discuss the problems with one another or with me. However, your final answers should be written on your own and in your own words.

At the top of the first page, please list any classmates you collaborated with while working on these exercises (so that we know to expect similar solutions).

1. Find all solutions to the following simultaneous congruences.

   (a)
   $$x^2 \equiv 1 \bmod 8,\ 5x \equiv 15 \bmod 20,\ 5x \equiv -1 \bmod 6.$$

   (b)
   $$x^2 \equiv 9 \bmod 10,\ 7x \equiv 19 \bmod 24,\ 2x \equiv -1 \bmod 45.$$

   (c)
   $$x^2 \equiv 3 \bmod 6,\ x^3 \equiv 3 \bmod 5.$$

2. (a) Find all solutions to the congruence $x^2 \equiv -1 \mod p$ for all primes $p \leq 17$.
   (b) Make a conjecture about how many solutions the congruence $x^2 \equiv -1 \mod p$ for any prime p (you do not need to prove your conjecture! We'll learn a general method for doing this by the end of the semester).

3. (a) How many solutions are there in $\mathbb{Z}/n$ to the congruence $x^2 \equiv 1 \mod n$ when $n = 1300$?
   (b) Find all the solutions to the congruence from part a).
   (c) Prove that the congruence $x^2 \equiv 1 \mod 2^a$ has exactly 4 solutions modulo 2^a whenever a is an integer greater than 2.

4. (a) Find $128^{129} \mod 17$. Express your answer as the least positive residue.
   (b) What day of the week will it be in one googolplex (i.e. $10^{10^{100}}$) days? Today is Friday.

5. Let p, q be two different primes. Suppose that $a^p \equiv a \mod q$ and $a^q \equiv a \mod p$. Prove that $a^{pq} \equiv a \mod pq$.