Math 250 – Number Theory – Homework 5

Due: Friday March 24th

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)
   $$x \equiv 2 \bmod 5,\ x \equiv 3 \bmod 7,\ x \equiv 10 \bmod 11.$$

   (b)
   $$3x \equiv 6 \bmod 12,\ 2x \equiv 5 \bmod 7,\ 3x \equiv 1 \bmod 5.$$

   (c)
   $$x \equiv 13 \bmod 40,\ x \equiv 5 \bmod 44,\ x \equiv 38 \bmod 275.$$

   (d)
   $$x \equiv 6 \bmod 8,\ 5x \equiv 10 \bmod 12,\ 3x \equiv 86 \bmod 100.$$

2. Consider the simultaneous congruences
   $$3x \equiv b \bmod 28,\ 4x \equiv c \bmod 35.$$
   (a) Find *two* different pairs of integers b, c for which these congruences have a solution. Give the most general solution in each case.
   (b) Find *two* different pairs of integers b, c for which these congruences *do not* have a solution. Explain why no solution exists in each case.

3. (a) Let p and q be coprime positive integers, and let $n = pq$. Explain why x is a solution to the linear congruence $ax \equiv b \bmod n$ if and only if
   $$ax \equiv b \bmod p \text{ and } ax \equiv b \bmod q.$$
   (b) Hence find a solution to the congruence $91x \equiv 419 \bmod 440$ without using a calculator.
   (c) Is the statement from part a) still true if p and q are not coprime? Why or why not?

4. (a) Prove that there are infinitely many primes that divide some integer of the form $m^2 + m + 1$ (Hint: use the same idea as Euclid's proof that there are infinitely many primes).
   (b) Let n be a natural number. Use Sunzi's theorem to show that there exists an integer m so that $m^2 + m + 1$ has at least n different prime factors.
   (c) Hence deduce that there exist n different numbers $k_1, \ldots, k_n$, all coprime to one another, so that $k_1 k_2 \cdots k_n - 1$ is the product of two consecutive integers.