Math 315; Homework # 5

Due March 4, 2015

1. (Exercise 18.1) Decode the following message, which was sent using the modulus $m = 7081$ and the exponent $k = 1789$. (Note that you will first need to factor m.)

$$5192, \quad 2604, \quad 4222$$

2. (Exercise 20.3) A number a is called a cubic residue modulo p if it is congruent to a cube modulo p [that is, if there is a number b so that $a \equiv b^3 \pmod{p}$].

(1) Make a list of all of the cubic residues modulo 5, modulo 7, and modulo 11.
(2) Find two numbers a_1 and b_1 so that neither a_1 nor b_1 is a cubic residue modulo 19, but $a_1 b_1$ is a cubic residue modulo 19. Similarly, find two numbers a_2 and b_2 so that none of the three numbers a_2, b_2 or $a_2 b_2$ is a cubic residue modulo 19.
(3) If $p \equiv 2 \pmod{3}$, make a conjecture as to which a's are cubic residues. Prove that your conjecture is correct.

3. (Exercise 21.1 (a,d)) Determine whether or not each of the following congruences has a solution. (All of the moduli are primes.)

(1) $x^2 \equiv -1 \pmod{5987}$
(2) $x^2 - 64x + 943 \equiv 0 \pmod{3011}$

(For (2), use the quadratic formula to find out what number you need to take the square root of modulo 3011.)

4. (Exercise 21.3, slightly different formulation) For which primes p is 3 a quadratic residue modulo p, namely, when does $x^2 \equiv 3 \pmod{p}$ have a solution? [Hint: use Quadratic reciprocity law, namely, $(\frac{3}{p}) = (\frac{p}{3})(-1)^{\frac{p-1}{2}}$ if $p \neq 2, 3$.]

5. (Exercise 21.5 (b)) Use the same ideas we used to verify Quadratic Reciprocity (Part II) to verify the following assertion: (b) If p is congruent to 2 modulo 5, then 5 is a nonresidue modulo p. [Hint: Reduce the numbers 5,10,15,..., $\frac{5}{2}(p-1)$ so that they lie in the range from $-\frac{1}{2}(p-1)$ to $\frac{1}{2}(p-1)$ and check how many of them are negative.]

6. (Exercise 22.3) Show that there are infinitely many primes congruent to 1 modulo 3. [Hint: See the proof of the "1 (Modulo 4) Theorem" in Chapter 21, use $A = (2p_1p_2 \cdots p_r)^2 + 3$, and try to pick out a good prime dividing A.]