MATH 3320, HOMEWORK #7

DUE MONDAY, OCTOBER 15

Note the due date of Monday October 15!

To ensure that you get full credit, be sure to *show your work* in the problems that require calculations. Very little credit is given for answers without justification. Please write in complete sentences to help us understand what you are doing.

You may collaborate with classmates in solving the problems, including the extra credit problems. If you do so, please list their names on your assignment. However, you should not consult *any* other people (except the instructors or TAs), or use online resources. (Seriously, it's very obvious to us when this occurs, and there are drastic consequences, so don't do it!) If you use results that were not proved in class, please provide your own proof.

1. (15 points) Use Euler's criterion to determine if 2 and 3 are squares modulo 79.

2. (15 points) We know that if p is a prime, then there exists a primitive root modulo p. Use this fact to give a direct proof that $(\frac{-3}{p}) = 1$ when $p \equiv 1 \pmod 3$. (Hint: There is an element $m \in (\mathbf{Z}/p\mathbf{Z})^\times$ of order 3. Show that $(2m+1)^2 \equiv -3$.)

3.

(a) (10 points) Fix a prime $p \equiv 3 \pmod 4$ and an integer a that is a quadratic residue modulo p. Prove that $a^{(p+1)/4}$ is a solution to the congruence

$$x^2 \equiv a \pmod p.$$

(b) (10 points) Use part (a) to solve the equation $x^2 \equiv 37 \pmod{127}$.

4. (20 points) Fix an odd prime p. Let n be the smallest positive integer that is not a square modulo p. Prove that n is a prime.

5. (Extra Credit) Suppose that a teacher proposes to his n students at recess that they play the following game. The n children are to sit in a circle, and are numbered $0, \ldots, n-1$ clockwise. Their teacher walks clockwise around the children and hands out gumballs from a seemingly inexhaustible bag according to the following rule:

The teacher first select one child ("0") and gives them a gumball. Then he skips a child ("1") and gives a gumball to the next child ("2"). Then he skips 2 children ("3" and "4") and gives a gumball to the next one ("5"). Then he skips 3... etc.

(a) (5 points) What are the values of n for which eventually (maybe after many rounds) each child ends up with at least one gumball? Furthermore, for such an n, how many gumballs need to be passed out? (Hint: Turn into a problem modulo n. What is $\sum_{k=1}^{m} k$ for various values of m?)

(b) (5 points) Suppose you already know about this game (you're a transfer student and they played it at your old school), know that a total of n students will be playing, and know that your teacher will always start by giving the person closest to the door a gumball. What position (of $\{0, 1, \ldots, n-1\}$) should you pick, if you want to get the most gumballs? Does

it depend on how many gumballs are passed out? (e.g. if the teacher stops after n gumballs, or after $\frac{n}{10}$ gumballs, or stops after everybody gets one, or hands out gumballs forever?)