Math 4400 Homework 8
Due: Friday, July 28th, 2017

Feel free to work with your classmates, but everyone must turn in their own assignment. Please make a note of who you worked with on each problem. Let me know if you find a typo, or you're stuck on any of the problems.

1. Answer the following:
   (a) (5 points) Is 123 a square modulo 137?
   (b) (5 points) Is 168 a square modulo 179?
   (c) (5 points) Is 8 a square modulo 73?
2. (5 points) Prove that an integer of the form $n^5 - n + 3, n \in \mathbb{Z}$ is never a square number (Hint: reduce modulo 5)
3. (10 points) Prove that $(\mathbb{Z}/p\mathbb{Z})^\times$ has an element of order 4 if and only if $p \equiv 1 \mod 4$.
4. (10 points) Let p be an odd prime. In class, we learned that 2 is a square modulo p if and only if $p \equiv 1$ or $p \equiv 7 \mod 8$. Use quadratic reciprocity to find a similar law for determining when 3 is a square modulo p. In other words, find a number n such that the value of $\left(\frac{3}{p}\right)$ depends only on the equivalence class of p modulo n. For which equivalence classes is 3 a square modulo p? (Hint: your notes from our lecture on the chinese remainder theorem might be helpful, here)
5. (5 points) Let p be an odd prime. Suppose there exist $x, y \in \mathbb{Z}$ with $x^2 + y^2 = p$. Show that $p \equiv 1 \mod 4$. (In fact, the converse holds as well: if $p \equiv 1 \mod 4$, then there exist such x and y. Try some examples yourself!)
6. Suppose Alice's public key for RSA encryption is $(m = 703, e = 5)$.
   (a) (5 points) Encrypt the message 2017 to send to Alice.
   (b) (5 points) You're talking to someone who claims to be Alice, but you're suspicious! You ask this person to send a message to you signed by Alice's private key. The person writes back with the message, $12, 34$, followed by the signed message, $255, 231$. Verify that this person really is Alice.
   (c) (5 points) Is $(m = 65, e = 10)$ a valid public key? Why or why not?
7. Your public key for RSA is $(m = 299, e = 5)$
   (a) (10 points) Find your private key, using the fact that $299 = 13 \cdot 23$.
   (b) (5 points) Someone sends you the message $(169, 129)$. Decrypt this message using your private key.
8. You're Varis and you're intercepting communications between Catelyn Stark and Brianne of Tarth. Here's a transcript of what you're able to read:

```
Catelyn: Let's use a Caesar cipher and do Diffie-Hellman to
         establish our secret key
Brianne: Sounds good
Catelyn: Ok, let's use p = 17 and g=10
Catelyn: X = 5
Brianne: Y = 11
Catelyn: ZHGGLQJ LV JRLQJ JUHDW
```

   (a) (10 points) Find either x or y. What is their shared secret?
   (b) (2 points) What does the message say?