Math 4400 Homework 7
Due: Monday, July 17th, 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. Solve the following equations:
   (a) (5 points) $x^{11} \equiv 13 \mod 35$
   (b) (5 points) $x^5 \equiv 3 \mod 64$
2. (10 points) Find all the 6^{th} roots of unity in $\mathbb{Z}/13\mathbb{Z}$. Which roots are primitive? (A calculator might be helpful, here).
3. (a) (5 points) Let p be a prime. Show that $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + 1$.
   (b) (5 points) Compute $\Phi_8(X)$ and $\Phi_9(X)$.
   (c) (2 points) Conjecture a formula for $\Phi_{p^n}(x)$, where p is prime and n is an integer.
4. (5 points) Let p be a prime. Prove that $\mathbb{Z}/p\mathbb{Z}$ has a primitive $(p-1)^{\text{th}}$ root of unity.
5. Let p be a prime and α a primitive $(p-1)^{\text{th}}$ root of unity in $\mathbb{Z}/p\mathbb{Z}$.
   (a) (10 points) Let $x \in (\mathbb{Z}/p\mathbb{Z})^\times$. Prove that x can be written as α^n for some unique n in $\{1, 2, \ldots, p-1\}$. This number n is usually denoted $I(x)$, and is called the *index* of x modulo p, with respect to α. It's also called the *discrete logarithm* of x modulo p, with respect to α.
   (b) (5 points) Show that the function $I : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{Z}/(p-1)\mathbb{Z}$ is a homomorphism.
6. (10 points) Let $n > 1$ be an integer. Show that $\displaystyle\sum_{\zeta \in \mu_n(\mathbb{C})} \zeta = 0$. (Hint: what happens when you multiply that sum by any $\zeta \in \mu_n(\mathbb{C})$?)
7. (a) (10 points) Let p be an odd prime. Prove that exactly $(p-1)/2$ elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ are squares.
   (b) (5 points) Use part (a) to show that, for each odd prime p, there exists a field of order p^2.
8. (5 points) Use Euler's criterion to determine if the following are squares:
   (a) 3 modulo 31
   (b) 7 modulo 29
9. (5 points) Let n be a positive integer. Let p be a prime divisor of $n^2 + 1$. Prove that $p \equiv 1 \mod 4$ (Hint: use proposition 23).
10. (10 points) Use the above to show that there are infinitely many primes congruent to 1 modulo 4. (Hint: come up with infinitely many numbers of the form $n^2 + 1$ that are all relatively prime to one-another).