Math 255 - Spring 2018
Homework 11

This homework is due on Monday, April 23.

1. What are the last two digits of 2018^{2018}?

2. Let $n \geq 2$ be an integer, and recall that $(\mathbb{Z}/n\mathbb{Z})^\times$ denotes the group of units in $\mathbb{Z}/n\mathbb{Z}$. Show that
$$\prod_{a \in (\mathbb{Z}/n\mathbb{Z})^\times} a \equiv \pm 1 \pmod{n}.$$
(In other words this product will always be either 1 or -1.)
Hint: This is similar to the proof of Wilson's Theorem, except that it is now false that $x^2 \equiv 1 \pmod{n}$ has exactly two solutions.

3. In this problem we will show how we can factor n given knowledge of the value of $\phi(n)$, under certain circumstances. This is a trick that it used to break the RSA cryptosystem when $\phi(n)$ is leaked or guessed. Throughout, suppose that n is a positive integer with $n = pq$, for p and q two distinct primes.
   (a) In this case what is $\phi(n)$?
   (b) From knowledge only of the values of n and $\phi(n)$, and knowledge of the fact that $n = pq$ is a product of two primes, explain how one can obtain the value of $p + q$.
   (c) From knowledge only of n and $\phi(n)$, and knowledge of the fact that $n = pq$ is a product of two primes, explain how one can obtain the values of p and q. Hint: What are the roots of the polynomial $x^2 - (p + q)x + n$?
   (d) Apply part (c) to factor the number $n = 4399$, which is of the form $n = pq$ for p and q two distinct primes, using the fact that $\phi(4399) = 4264$.

Extra problem for graduate credit:

4. In this problem we will prove that ϕ is multiplicative in a different way than the one we used in class.
   (a) Let m and n be positive integers with $(m, n) = 1$. Prove that there is a bijection
   $$(\mathbb{Z}/mn\mathbb{Z})^\times \leftrightarrow (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times.$$
   (b) Conclude from this bijection that when $(m, n) = 1$, $\phi(mn) = \phi(m)\phi(n)$.