Math 255 - Spring 2018
Homework 12

This homework is due on Monday, April 30.

1. Let $m > 1$ be an integer. Show that if there is a an integer with $(a, m) = 1$ and the order of a modulo m is $m - 1$, then m is prime.

2. Let p be an odd prime and g and h be primitive roots of p. Show that $g \equiv h^k \pmod{p}$ for some k, and that in this case k is odd.

3. Let p be an odd prime. Show that if a has order 3 modulo p, then $a + 1$ has order 6 modulo p.
   Hint: You may use the following result without proof: If $a \not\equiv 1 \pmod{p}$ and a has order t modulo p, then
   $$a^{t-1} + a^{t-2} + \ldots + a + 1 \equiv 0 \pmod{p}.$$

4. In this problem we will show that if $n > 2$, then $\phi(n)$ is even in two different ways.
   (a) Show this directly, using the explicit formula we have for $\phi(n)$.
   (b) Show this by first showing that if $n > 2$, then there is a with $(a, n) = 1$ and a has order 2 modulo n. Then apply Theorem 2 of Section 10 to conclude.

Extra problem for graduate credit:

5. Let m be any integer that has a primitive root. Show that in this case
   $$\prod_{a \in (\mathbb{Z}/m\mathbb{Z})^\times} a \equiv -1 \pmod{m}.$$