MATH 301: Problem Set 7

1. Recall Euler's Theorem, which states that if $\gcd(a, m) = 1$, then

$$a^{\varphi(m)} \equiv 1 \pmod{m},$$

where $\varphi(m)$ is the number of positive integers less than m that are coprime to m.

   (a) Compute $\varphi(9)$.

   (b) Use Euler's Theorem to help compute $5^{123} \pmod 9$.

2. Without doing any calculations, the true statement

$$179^{492} \equiv 373 \pmod{493}$$

allows you to conclude something interesting about one of the numbers in the equation. Which number, and what is the conclusion? (Hint: what would Fermat's theorem say about this?)

3. Numbers like 11, 1111111, or 1111 that contain only the digit 1 are called **repunits**. Prove that *every* prime aside from 2 and 5 occurs as a factor of some repunit.

4. The **multiplicative order** of an integer a modulo m is the *smallest* positive integer exponent k so that $a^k \equiv 1 \pmod{m}$, if it exists.

   (a) The multiplicative order is only defined for those integers a that are coprime to the modulus m. Why?

   (b) Find the multiplicative orders of each element of $\mathbb{Z}/9\mathbb{Z}$ for which it is defined.

   (c) Find the multiplicative orders of each element of $\mathbb{Z}/8\mathbb{Z}$ for which it is defined. Do your findings contradict Euler's Theorem?

5. Prove that the multiplicative order of a modulo m divides $\varphi(m)$.

6. (★) Compute the last two digits of $3 \uparrow\uparrow 2000$. The notation $3 \uparrow\uparrow 2000$ is called "Knuth's up-arrow notation" and it means $3^{3^{3^{3^{\cdots^{3^3}}}}}$ (2000 3's total!!)