Math 351 Homework 3

Due Wednesday, September 28

Solutions should be written LaTeX or Markdown and converted to a PDF. You are encouraged to work with others on the assignment, but you should write up your own solutions independently. This means no copy pasting. You should reference all of your sources, including your collaborators.

1. Let $n \in \mathbb{N}$ and $x \in \mathbb{Z}$ and suppose that $\gcd(x, n) = 1$. The **order** of x modulo n is the smallest $m \in \mathbb{N}$ such that $x^m = 1 \pmod{n}$. What is the order of 2 modulo 17?

2. Let p be a prime. Prove that $\mathbb{Z}/p\mathbb{Z}$ is a field.

3. Show that multiplication in $\mathbb{Z}/p\mathbb{Z}$ is well-defined.

4. Use Wilson's Theorem (Proposition 2.1.22) to prove that if $n > 4$ is composite then

$$(n-1)! \equiv 0 \pmod{n}.$$

5. Euler's φ function is defined as follows: for $n \in \mathbb{N}$, let

$$\varphi(n) = |\{a \in \mathbb{N} \mid a \leqslant n \text{ and } \gcd(a, n) = 1\}|.$$

For what values of n is $\varphi(n)$ odd?