**Math 461** **Spring 2015**
**Homework 5** **Drew Armstrong**

---

**1. Equivalence mod $n$.** Let $S$ be a set. For each pair $(x, y) \in S^2$ we define $x \sim y$ to be either true or false, and we will usually write $x \sim y$ as shorthand for "$x \sim y$ is true". We say that $\sim$ is an **equivalence relation** if

- $x \sim x$ for all $x \in S$,
- $x \sim y$ implies $y \sim x$ for all $x, y \in S$,
- $x \sim y$ and $y \sim z$ imply $x \sim z$ for all $x, y, z \in S$.

Now let $n \in \mathbb{Z}$ be a **nonzero** integer. For all $x, y \in \mathbb{Z}$ we will write $x \sim_n y$ to mean that $n$ divides $x - y$ (i.e., there exists $k \in \mathbb{Z}$ such that $x - y = nk$). Prove that $\sim_n$ is an equivalence relation on $\mathbb{Z}$.

**2. Primitive Roots of Unity.** Consider a positive integer $n \in \mathbb{Z}$ and let $\omega = e^{2\pi i/n}$.

(a) Prove that $\omega^k = \omega^\ell$ if and only if $k \sim_n \ell$ (as in Problem 1).
(b) Given an integer $k$, let $m$ be the smallest positive integer such that $(\omega^k)^m = 1$. Show that $m = \mathrm{lcm}(k, n)/k$.
(c) Prove that $\omega^k$ is a primitive $n$th root of 1 if and only if $\gcd(k, n) = 1$. [Hint: $\gcd(k, n) = kn/\mathrm{lcm}(k, n)$.]

**3. Euler's Totient Function.** Given a positive integer $n \in \mathbb{Z}$ we define

$$\varphi(n) := \#\{k : 0 \leq k \leq n-1, \gcd(k, n) = 1\}.$$

(a) Explain why $\varphi(n)$ is the degree of the cyclotomic polynomial $\Phi_n(x) \in \mathbb{Z}[x]$.
(b) If $p \in \mathbb{Z}$ is prime and $m$ is a positive integer, prove that $\varphi(p^m) = p^m - p^{m-1}$. [Hint: The only integers less than $p^m$ that are not coprime to $p^m$ are the multiples of $p$. How many of these are there?]
(c) Prove that for all positive integers $n$ we have

$$\varphi(n) = n \prod_{p|n} \frac{p-1}{p},$$

where the product is over prime numbers $p$ that divide $n$. [Hint: You can assume without proof that for all coprime $a, b \in \mathbb{Z}$ we have $\varphi(ab) = \varphi(a)\varphi(b)$. Now express $n$ as a product of primes $n = p_1^{m_1} p_2^{m_2} \cdots$.]
(d) Compute the degree of $\Phi_{120}(x)$. Do not compute $\Phi_{120}(x)$ itself.

**4. Fermat Primes.** In 1650, Pierre de Fermat conjectured that every number of the form $F(n) = 2^{2^n} + 1$ is prime. He based this conjecture on the fact that $F(0) = 3, F(1) = 5, F(2) = 17, F(3) = 257, F(4) = 65537$ are prime. However, Euler showed in 1732 that $F(5)$ is **not** prime, and to this day it is not known whether there exist **any** other "Fermat primes". D'oh!

(a) If $2^a + 1$ is a prime number, prove that $a$ must be a power of 2. [Hint: Suppose that $a = bc$ where $b$ is **odd**. Factor the polynomial $1 - x^b$ and then substitute $x = -2^c$.]
(b) Let $p$ be prime. If $\varphi(p)$ is a power of two, show that $p$ is a Fermat prime.