WORKSHEET #5 – MATH 2200
SPRING 2018

DUE WEDNESDAY, MARCH 28TH

You may work in groups of up to 4 people. Only one assignment needs to be turned in per group, but make sure everyone's name is on it.

Therefore, we should take great care not to accept as true such properties of the numbers which we have discovered by observation and which are supported by induction alone. – Leonhard Euler

Consider a number n (such as $n = 15$). A natural question is

How many integers are there, between 1 and n, which are relatively prime to n?

The answer to this question is denoted by $\varphi(n)$. The function φ is called *Euler's φ function.*

1. For each of the following numbers n, compute $\varphi(n)$. You can divide up the work among people in your group, but make sure to write your answers down carefully.

(a) 10
(b) 9
(c) 11
(d) 37
(e) 15
(f) 45
(g) 22
(h) 27
(i) 30
(j) 32
(k) 49
(l) 50

2. Make some general predictions about what $\varphi(n)$ is. At least for special kinds of n. Some particular cases to consider.

(a) What if n is prime.
(b) What if $n = 2p$ for p prime?
(c) What if $n = p^2$ for p prime?
(d) What if $n = p^3$ for p prime?
(e) What if $n = p^n$ for p prime?
(f) What if $n = pq$ for p and q different, but both odd primes?
(h) What if $n = p^2q^2$ for p and q different, but both odd primes?

3. Prove that if m, n are relatively prime positive integers, then $\varphi(mn) = \varphi(m)\varphi(n)$.

Hint: For any integer $k > 1$, consider the set of numbers $T_k = \{x \in \mathbb{Z} \mid 1 \leq x \leq k, \gcd(x, k) = 1\}$. For instance, $T_{10} = \{1, 3, 7, 9\}$. Prove that $|T_k| = \varphi(k)$. What is $|T_m \times T_n|$? Now, construct a function $f : T_{mn} \longrightarrow T_m \times T_n$ defined by $x \mapsto \big(x \pmod{m}, x \pmod{n}\big)$. Show that this function is bijective by using the full force of the Chinese Remainder Theorem.

4. Find a general algorithm or strategy for computing $\varphi(n)$. You should be able to do this by combining **2.(e)** and **3.**. You don't need to prove that your algorithm is correct, however you must explain it carefully and correctly.

A more general form of Fermat's Little Theorem (due to Euler) is the following. Suppose $a > 0$ and n are integers and that $\gcd(a, n) = 1$. Then

$$a^{\varphi(n)} \equiv 1 (\text{mod } n)$$

5. Verify that Euler's generalization of Fermat's Little Theorem is true in the following examples (note this is not a proof). Write up your computations carefully.

(a) $a = 5, n = 12.$

(b) $a = 3, n = 10.$

(c) $a = 5, n = 16.$

(d) $a = 2, n = 21.$

(e) $a = 8, n = 21.$

(f) $a = 8, n = 15.$