Math 580/780I Notes 10

Euler's Phi Function Revisited:

- Recall $\phi(n)$ is the number of positive integers $\le n$ that are relatively prime to n.
- **Lemma 1.** *For every prime p and every positive integer k, $\phi(p^k) = p^k - p^{k-1}$.*
- **Proof.** The number of multiples of p which are $\le p^k$ is p^{k-1}. The result follows.
- **Lemma 2.** *For relatively prime positive integers m and n, $\phi(mn) = \phi(m)\phi(n)$.*
- **Proof.** If $m = 1$ or $n = 1$, then the result is clear; so we suppose both $m > 1$ and $n > 1$. Let $a_1, \dots, a_{\phi(m)}$ denote the positive integers $\le m$ which are relatively prime to m, and let $b_1, \dots, b_{\phi(n)}$ denote the positive integers $\le n$ which are relatively prime to n. Suppose now that $k \in \{1, 2, \dots, mn\}$ and $(k, mn) = 1$. Define a and b by

$$k \equiv a \pmod m, \quad 0 \le a < m, \quad k \equiv b \pmod n, \quad \text{and} \quad 0 \le b < n.$$

Since $k = a + tm$ for some integer t and since $(k, m) = 1$, we deduce that $(a, m) = 1$. Similarly, $(b, n) = 1$. Hence, there are $i \in \{1, 2, \dots, \phi(m)\}$ and $j \in \{1, 2, \dots, \phi(n)\}$ such that

$$k \equiv a_i \pmod m \qquad \text{and} \qquad k \equiv b_j \pmod n.$$

Since there are $\phi(m)\phi(n)$ choices of pairs (i, j) and k is uniquely determined by the above congruences (i.e., because of the Chinese Remainder Theorem), we get $\phi(mn) \le \phi(m)\phi(n)$.

Now, fix a pair (i, j) with $i \in \{1, 2, \dots, \phi(m)\}$ and $j \in \{1, 2, \dots, \phi(n)\}$, and consider the integer $k \in \{1, 2, \dots, mn\}$ (that exists by the Chinese Remainder Theorem) which satisfies $k \equiv a_i \pmod m$ and $k \equiv b_j \pmod n$. There exists an integer t such that $k = a_i + tm$ so that, since $(a_i, m) = 1$, we obtain $(k, m) = 1$. Also, $(k, n) = 1$. Hence, $(k, mn) = 1$. Therefore, since each pair (i, j) corresponds to a different k, $\phi(mn) \ge \phi(m)\phi(n)$. Combining the inequalities, we get $\phi(mn) = \phi(m)\phi(n)$.

- **Theorem 15.** *Suppose $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, where $e_1, \dots, e_r$, and r are positive integers and $p_1, \dots, p_r$ are distinct primes. Then*

$$\phi(n) = \prod_{j=1}^{r} (p_j^{e_j} - p_j^{e_j - 1}) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right).$$

- **Proof.** The first equality follows from Lemma 1 and Lemma 2 (using $\phi(n) = \phi(p_1^{e_1}) \cdots \phi(p_r^{e_r})$). To get the second equality, factor out $p_j^{e_j}$ for each $j \in \{1, 2, \dots, r\}$ to get

$$\prod_{j=1}^{r} (p_j^{e_j} - p_j^{e_j - 1}) = \prod_{j=1}^{r} p_j^{e_j} \cdot \prod_{j=1}^{r} \left(1 - \frac{1}{p_j}\right) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right).$$

- **Examples.** Use the theorem to show that $\phi(100) = 40$ and $\phi(140) = 48$.
- A "sieve" proof (or a proof using the inclusion-exclusion principle) of Theorem 15 can be given that doesn't make use of the lemmas. Observe that a positive integer m is not relatively

prime to n if and only if m is divisible by some p_j with $j \in \{1, 2, \dots, r\}$. For distinct $j_1, \dots, j_k$ in $\{1, 2, \dots, r\}$, the number of positive multiples of $p_{j_1} \cdots p_{j_k}$ which are $\le n$ is $n/(p_{j_1} \cdots p_{j_k})$. The inclusion-exclusion principle implies that the number of positive integers $\le n$ which are not divisible by $p_1, \dots, p_{r-1}$, or p_r is

$$n - \sum_{j=1}^{r} \frac{n}{p_j} + \sum_{j_1 < j_2 \le r} \frac{n}{p_{j_1} p_{j_2}} - \sum_{j_1 < j_2 < j_3 \le r} \frac{n}{p_{j_1} p_{j_2} p_{j_3}} + \cdots + (-1)^r \frac{n}{p_1 p_2 \dots p_r} = n \prod_{j=1}^{r} \left(1 - \frac{1}{p_j}\right).$$

The theorem follows.

- **Comments:** An open problem due to Carmichael is to determine whether or not there is a positive integer n such that if m is a positive integer different from n then $\phi(m) \neq \phi(n)$. If such an n exists, it is known that if must be $> 10^{1000}$. Some result in this direction can be obtained as follows. Observe that $n \equiv 0 \pmod 2$ since otherwise $\phi(n) = \phi(2n)$. Now, $n \equiv 0 \pmod 4$ since otherwise $\phi(n) = \phi(n/2)$. Now, $n \equiv 0 \pmod 3$ since otherwise $\phi(n) = \phi(3n/2)$; and $n \equiv 0 \pmod 9$ since otherwise $\phi(n) = \phi(2n/3)$. This approach can be extended (apparently indefinitely as long as one is willing to consider branching off into different cases).

Homework:

(1) Calculate each of the following:

(a) $\phi(98)$

(b) $\phi(120)$

(c) $\phi(180)$

(2) Note that $2010 = 2 \cdot 3 \cdot 5 \cdot 67$. What is the value of $\phi(2010)$?

(3) What is the remainder when 2^{165} is divided by 165?

(4) Show that the remainder when 2^{2010} is divided by 825 is 199?

(5) There are two positive integers n such that $\phi(n) = 2010$. What are they?

(6) Explain why $\phi(1) = \phi(2) = 1$ is the only odd value of $\phi(n)$ as n varies over the positive integers.

(7) Find all positive integers $n \le 50$ for which $\phi(n)$ is twice an odd number. Try to do this without computing all values of $\phi(n)$ for $n \le 50$. (There should be 18.)

(8) Find all positive integers $n \le 50$ for which $\phi(n)$ has no odd prime divisor. Try to do this without computing all values of $\phi(n)$ for $n \le 50$. (There should be 19.)

Challenge Problem:

Prove that if n is a positive integer as in the comment above, then $n > 10^{30}$. (Hint: Eventually consider two cases depending on whether $13|n$ or $13 \nmid n$.)