Math 322 Fall 2019
Number Theory HW 7 Solutions
Due Friday, October 18

You may *not* discuss the starred problem with classmates, though you should of course feel free to discuss it with me as much as you like. Linguistic precision is important for this problem.

($\star$) **Starred Problem:** Show that if n is odd, then $\phi(4n) = 2\phi(n)$.

For the remainder of these problems, I encourage you to collaborate with your classmates, as well as to discuss them with me.

1. Let m be a natural number. Find a reduced residue system modulo 2^m.

   Solution: One reduced residue system modulo 2^m is the set of all numbers which are relatively prime to 2^m and less than 2^m. A number d is relatively prime to 2^m if and only if d is odd. thus a reduced residue system modulo 2^m is

   $$\{1, 3, 5, 7, \ldots, 2^m - 1\} = \{n \in \mathbb{N} : (n, 2) = 1, n \leq 2^m\} = \{2n + 1 : 0 \leq n \leq 2^{m-1} - 1\}.$$

2. Use Euler's theorem to find the last decimal digit of:

   (a) 3^{1000}

   Solution: We know $\phi(10) = 4$ so $3^{1000} = (3^4)^{250} \equiv 1 \mod 10$, so the last decimal digit of 3^{1000} is 1.

   (b) $7^{999,999}$

   Solution: We know $\phi(10) = 4$ so $7^{999,999} = (7^4)^{249,999} \cdot 7^3 \equiv 7^3 \equiv 3 \mod 10$.

3. Let n be a natural number. Prove that $\phi(n) = n - 1$ if and only if n is prime.

   Solution: Suppose n is prime. Then if $n \not| d$ we know that $(n, d) = 1$, and thus every number less than n is relatively prime to n. Since $(n, n) = n > 1$, there are $n - 1$ numbers $\leq n$ and relatively prime to n.

   Conversely, suppose $\phi(n) = n - 1$. Then $n > 1$ since if $n = 1$ then $\phi(n) = 1 \neq n - 1$. Then $(n, n) = n > 1$, so if there are $n - 1$ numbers $\leq n$ and relatively prime to n this means that every number less than n is relatively prime to n. Thus n can have no factors except itself and 1, so n is prime by definition.

4. Let a, b be relatively prime natural numbers. Show that $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \mod ab$.

   Solution: By Euler's theorem, we know that $a^{\phi(b)} \equiv 1 \mod b$ and $b^{\phi(a)} \equiv 1 \mod a$. But clearly $a^{\phi(b)} \equiv 0 \mod a$ and $b^{\phi(a)} \equiv 0 \mod b$, so we have $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \mod a$ and $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \mod b$. Then by the Chinese Remainder Theorem, we have $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \mod ab$.

5. Let $c_1, c_2, \ldots, c_{\phi(m)}$ be a reduced residue system modulo m, where $m > 2$. Show that $c_1 + c_2 + \cdots + c_{\phi(m)} \equiv 0 \mod m$.

   Solution:

   First notice that, as with our proof of Euler's theorem in class, we know that the set $\{c_1, c_2, \ldots, c_{\phi(m)}\}$ has exactly one representative from every equivalence class modulo m that is relatively prime to m. Thus if $R = \{r_1, r_2, \ldots, r_{\phi(m)}\}$ is the reduced residue system of integers which are $\leq m$ and relatively prime to m, we know that

   $$c_1 + c_2 + \cdots + c_{\phi(m)} \equiv r_1 + r_2 + \cdots + r_{\phi(m)} \mod m.$$

   So we just need to prove the result for this particular reduced residue system.

   We observe that if $(r_i, m) = 1$, then $(m - r_i, m) = 1$, so every element of R has an additive inverse modulo m that is also in R. Further, suppose that $r_i \equiv -r_i \mod m$; then $m|2r_i$ and since $m \neq 2$ this implies that $(m, r_i) > 1$, which is a contradiction, so each element has a distinct additive inverse. Thus we can uniquely pair each element with its additive inverse, and we have

   $$r_1 + r_2 + \cdots + r_{\phi(m)} \equiv (r_1 - r_1) + (r_2 - r_2) + \cdots \equiv 0 \mod m.$$

6. Determine whether each of the following functions is multiplicative, completely multiplicative, or neither.

   (a) $f(n) = 0$

   Solution: Completely multiplicative, since $f(mn) = 0 = 0 \cdot 0 = f(m)f(n)$.

   (b) $\gcd(n, k)$ for some fixed integer k.

   Solution: Multiplicative. We see it is not completely multiplicative since $\gcd(4, 2) = 2 \neq 2 \cdot 2 = \gcd(2, 2) \cdot \gcd(2, 2)$.

   To prove that it's multiplicative: fix k and suppose $(m, n) = 1$. Suppose $d|mn, k$. Then we can write $d = d_1 d_2$ where $d_1|m, k$ and $d_2|n, k$. Thus $\gcd(mn, k) \leq \gcd(m, k) \cdot \gcd(n, k)$.

   Conversely, suppose $d_1|m, k$ and $d_2|n, k$. Then $d_1 d_2|mn$, and since $(m, n) = 1$ we know that $d_1 d_2|k$. Thus $\gcd(m, k)\gcd(n, k) \leq \gcd(mn, k)$. Therefore $\gcd(mn, k) = \gcd(m, k)\gcd(n, k)$ if $(m, n) = 1$.

   (c) $\log(n)$ **Solution:** Not multiplicative: $\log(6) = \log(2) + \log(3) \neq \log(2)\log(3)$.