Math 406 Section 7.1: Multiplicative Functions and ϕ

1. **Introduction:** We see that Euler's Theorem is useful for doing modular exponentiation but it relies upon us calculating $\phi(m)$ and it may not be clear how we can do this easily.

2. **Function Definitions:**

   (a) **Definition:** A function is *arithmetic* if it is defined for all positive integers.

   (b) **Definition:** An arithmetic function f is *multiplicative* if $f(mn) = f(m)f(n)$ whenever $\gcd(m, n) = 1$.

   (c) **Definition:** An arithmetic function f is *completely multiplicative* if $f(mn) = f(m)f(n)$ for all m, n.

   Obviously a completely multiplicative function is multiplicative.

   (d) **Notes and Examples:**

   The function $f(x) = x$ is completely multiplicative and hence multiplicative as is $f(x) = x^r$ for any r. For example if $f(x) = x^3$ then $f(mn) = (mn)^3 = m^3n^3 = f(m)f(n)$.

   Most functions are not multiplicative or even completely multiplicative, for example $f(x) = x + 1$ is not, since $f(3 \cdot 5) \neq f(3)f(5)$.

   Consider that it is difficult to think of a function which is multiplicative but not completely multiplicative.

3. **Theorem:** If f is multiplicative then if $n = p_1^{\alpha_1} ... p_k^{\alpha_k}$ is the prime factorization of n then

$$f(n) = f\left(p_1^{\alpha_1} ... p_k^{\alpha_k}\right) = f\left(p_1^{\alpha_1}\right) ... f\left(p_k^{\alpha_k}\right)$$

   Proof: Follows from the definition of multiplicative. $\mathcal{QED}$

4. **All About ϕ**

   (a) **Theorem:** For a prime p we have $\phi(p) = p - 1$.
   Proof: All of $1, 2, ..., p - 1$ are coprime to p. $\mathcal{QED}$

   (b) **Theorem:** For a prime p we have $\phi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha \left(1 - \frac{1}{p}\right)$.
   Proof: Out of the integers $1, 2, 3, ..., p^\alpha$ the only ones not coprime to p are the multiples of p itself. Those are $p, 2p, 3p, ..., p^{\alpha-1}p$ and so there are $p^{\alpha-1}$ of these. The remaining ones are coprime and there are $p^\alpha - p^{\alpha-1}$ of these. $\mathcal{QED}$

   Example: We have $\phi(125) = \phi(5^3) = 5^3 - 5^2 = 100$.

   Example: We have $\phi(256) = \phi(2^8) = 2^8 - 2^7 = 256 - 128 = 128$.

(c) **Theorem:** ϕ is multiplicative.

Proof: We wish to show that $\phi(mn) = \phi(m)\phi(n)$ when $\gcd(m,n) = 1$. Basically what we'll do is count which of $1, 2, 3, ..., mn$ are coprime to mn. To do this let's write these numbers out as a table:

$$\begin{array}{llllll}
\text{Row } 1 \Longrightarrow & 0m+1 & 1m+1 & 2m+1 & \dots & (n-1)m+1 \\
\text{Row } 2 \Longrightarrow & 0m+2 & 1m+2 & 2m+2 & \dots & (n-1)m+2 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
\text{Row m} \Longrightarrow & 0m+m & 1m+m & 2m+m & \dots & (n-1)m+m = mn
\end{array}$$

Consider a particular row, say row r with $1 \leq r \leq m$:

$$\text{Row } r \Longrightarrow \quad 0m + r, 1m + r, 2m + r, ..., (n-1)m + r$$

An entry in this row looks like $km + r$ for $0 \leq k \leq n - 1$.

If $\gcd(r,m) \neq 1$ then $\gcd(km + r, m) = \gcd(r, m) \neq 1$ and then $\gcd(km + r, mn) \neq 1$. This means if $\gcd(r,m) \neq 1$ we would not count any entry in that row since none of them are coprime to mn.

Thus we can ignore all rows with $\gcd(r,m) \neq 1$.

Let R with $1 \leq R \leq m$ be a row with $\gcd(R,m) = 1$. Notice that every entry in such a row is coprime to m since $\gcd(km + R, m) = \gcd(R, m) = 1$.

There are $\phi(m)$ such rows with $\gcd(R,m) = 1$

In such a row R consider that the set $\{0, 1, 2, ..., n-1\}$ forms a complete set of residues mod n and since $\gcd(m,n) = 1$ so does the set $\{0m+R, 1m+R, 2m+R, ..., (n-1)m+R\}$ by a Theorem from class. It follows that out of these n integers $\phi(n)$ of them are coprime to n. Since (by being in this row) they are coprime to m as well, they are coprime to mn.

In conclusion $\phi(m)$ rows with $\phi(n)$ entries per row gives us a total number coprime to mn of $\phi(m)\phi(n)$ and thus $\phi(mn) = \phi(m)\phi(n)$. $\mathcal{QED}$

(d) **Corollary:** If $n = p_1^{\alpha_1} ... p_k^{\alpha_k}$ then:

$$\phi(n) = \prod_{i=1}^{k} \left(p_i^{\alpha} - p_i^{\alpha-1}\right) = \underbrace{\prod_{i=1}^{k} p_i^{\alpha-1}(p_i - 1)}_{\text{(i)}} = \prod_{i=1}^{k} p^{\alpha}\left(1 - \frac{1}{p_i}\right) = \underbrace{n\prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right)}_{\text{(ii)}}$$

Proof: Follows immediately by calculation. $\mathcal{QED}$

Note: Each of these forms is useful in its own way, especially (i) and (ii).

Example: To find $\phi(432)$ we find $432 = 2^4 \cdot 3^3$ and so by (ii):

$$\phi(432) = 432\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 144$$

Example: To find $\phi(45375)$ we find $45375 = 3 \cdot 5^3 \cdot 11^2$ and so by (ii):

$$\phi(45375) = 45375\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{11}\right) = 22000$$

Example: Let's find all n with $\phi(n) = 6$. If p^α appears in the prime factorization of n then by (i) we have $p - 1 \mid \phi(n)$ and $p^{\alpha-1} \mid \phi(n)$. Since $\phi(n) = 6$ in order to have $p - 1 \mid 6$ we can only have $p - 1 = 1, 2, 3, 6$ with p prime so only $p = 2, 3, 7$. Thus we have $n = 2^a \cdot 3^b \cdot 7^c$.

- Since $2^a \mid n$ if $a > 0$ then we have $2^{a-1} \mid \phi(n) = 6$ and so possibilities are $a = 0, 1, 2$.
- Since $3^b \mid n$ if $b > 0$ then we have $3^{b-1} \mid \phi(n) = 6$ and so possibilities are $b = 0, 1, 2$.
- Since $7^c \mid n$ if $c > 0$ then we have $7^{c-1} \mid \phi(n) = 6$ and so possibilities are $c = 0, 1$.

Now then, not all of these will work since they're necessary but not sufficient. it's possible to argue further but it's easier to just check the cases now:

$$
\begin{gathered}
\phi(2^0 \cdot 3^0 \cdot 7^0) = 1 \\
\phi(2^0 \cdot 3^0 \cdot 7^1) = 6 \\
\phi(2^0 \cdot 3^1 \cdot 7^0) = 2 \\
\phi(2^0 \cdot 3^1 \cdot 7^1) = 12 \\
\phi(2^0 \cdot 3^2 \cdot 7^0) = 6 \\
\phi(2^0 \cdot 3^2 \cdot 7^1) = 36 \\
\phi(2^1 \cdot 3^0 \cdot 7^0) = 1 \\
\phi(2^1 \cdot 3^0 \cdot 7^1) = 6 \\
\phi(2^1 \cdot 3^1 \cdot 7^0) = 2 \\
\phi(2^1 \cdot 3^1 \cdot 7^1) = 12 \\
\phi(2^1 \cdot 3^2 \cdot 7^0) = 6 \\
\phi(2^1 \cdot 3^1 \cdot 7^1) = 36 \\
\phi(2^2 \cdot 3^0 \cdot 7^0) = 2 \\
\phi(2^2 \cdot 3^0 \cdot 7^1) = 12 \\
\phi(2^2 \cdot 3^1 \cdot 7^0) = 4 \\
\phi(2^2 \cdot 3^1 \cdot 7^1) = 24 \\
\phi(2^2 \cdot 3^2 \cdot 7^0) = 12 \\
\phi(2^2 \cdot 3^1 \cdot 7^1) = 28
\end{gathered}
$$

Thus $n = 7, 9, 14, 18$ are all that work.

5. **Definition:** For an arithmetic function f we define the *divisor summatory function*

$$F(n) = \sum_{d|n} f(d)$$

Example: For a function f we would have $f(12) = f(1) + f(2) + f(3) + f(4) + f(6) + f(12)$.

6. **Theorem:** If Φ is the divisor summatory function for ϕ:

$$\Phi(n) = \sum_{d|n} \phi(d)$$

then $\Phi(n) = n$.

Proof: For each $d \mid n$ we define:

$$C_d = \{m \mid 1 \leq m \leq n, \gcd(m, n) = d\}$$

By definition each $1 \leq m \leq n$ is in one and only one C_d and in fact $m \in C_d$ iff $\gcd(m, n) = d$ iff $\gcd(m/d, n/d) = 1$ and hence $|C_d| = \phi(n/d)$ and so:

$$n = \sum_{d|n} |C_d| = \sum d \mid n\phi(n/d)$$

However as d runs over all divisors of n so does n/d and so:

$$n = \sum d \mid n\phi(n/d) = \sum d \mid n\phi(d) = \Phi(n)$$

$\mathcal{QED}$

This is less confusing than it may look. Consider $n = 20$. The divisors of 20 are $1, 2, 4, 5, 10, 20$. If we take all of $1, 2, 3, ..., 20$ and separate them according to their gcd with 20 into divisor buckets:

Divisor d	C_d	$\phi(20/d)$
1	$C_1 = \{1, 3, 7, 9, 11, 13, 17, 19\}$	$\phi(20/1) = \phi(20) = 8$
2	$C_2 = \{2, 6, 14, 18\}$	$\phi(20/2) = \phi(10) = 4$
4	$C_4 = \{4, 8, 12, 16\}$	$\phi(20/4) = \phi(5) = 4$
5	$C_5 = \{5, 15\}$	$\phi(20/5) = \phi(4) = 2$
10	$C_{10} = \{10\}$	$\phi(20/10) = \phi(2) = 1$
20	$C_{20} = \{20\}$	$\phi(20/20) = \phi(1) = 1$
		$\Phi(20) = \text{Total} = 20$