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:** Many functions can be made algebraic by restricting them, for example $f(x) = x^2$ certainly works on positive integers and is therefore arithmetic. The function $f(x) = \frac{1}{x^3}$ is not, however.
   
   Most functions are not multiplicative or even completely multiplicative, for example $f(x) = x + 1$ is not, since $f(3 \cdot 5) \neq f(3)f(5)$.
   
   It’s difficult to think of a function which is multiplicative but not completely multiplicative. For example $f(x) = x^2$ is multiplicative since $f(mn) = (mn)^2 = m^2n^2 = f(m)f(n)$ when $\gcd(m,n) = 1$ but in fact it works even when $\gcd(m,n) \neq 1$ so it’s completely multiplicative too.

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

   $$f(n) = f(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = f(p_1^{\alpha_1}) \cdots f(p_k^{\alpha_k})$$

   **Proof:** Follows from the definition of multiplicative. $\quad \square$

4. **All About $\phi$**

   (a) **Theorem:** For a prime $p$ we have $\phi(p) = p - 1$.
   
   **Proof:** All of $1, 2, \ldots, p - 1$ are coprime to $p$. $\quad \square$

   (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 $1, 2, 3, \ldots, p^\alpha$ the only ones not coprime to $p$ are the multiples of $p$ itself. Those are $p, 2p, 3p, \ldots, p^{\alpha - 1}p$ and so there are $p^{\alpha - 1}$ of these. The remaining ones are coprime and there are $p^\alpha - p^{\alpha - 1}$ of these. $\quad \square$

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

   **Example:** We have $\phi(256) = \phi(2^8) = 2^8 - 2^7 = 256 - 128 = 128$. 
Theorem: The Euler Phi function 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 $1, 2, 3, \ldots, mn$ are coprime to $mn$. To do this let’s write these numbers out as a table:

\[
\begin{array}{cccc}
1 & m + 1 & 2m + 1 & \ldots & (n-1)m + 1 \\
2 & m + 2 & 2m + 2 & \ldots & (n-1)m + 2 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
m & m + m & 2m + m & \ldots & (n-1)m + m = mn
\end{array}
\]

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

$$r, m + r, 2m + r, \ldots, (n-1)m + r$$

First note that all of these have the form $km + r$ for $0 \leq k \leq n - 1$ and since we know that $\gcd(km + r, m) = \gcd(r, m)$, the entire of row $r$ (every entry) is coprime to $m$ if and only if $\gcd(r, m) = 1$. If an integer is not coprime to $m$ then it is not coprime to $mn$ and so we can ignore all rows with $\gcd(r, m) \neq 1$.

There are $\phi(m)$ rows with $\gcd(r, m) = 1$. In such a row $r$ with $\gcd(r, m) = 1$ consider that the set $\{0, 1, 2, \ldots, n-1\}$ forms a complete set of residues mod $n$ and since $\gcd(m,n) = 1$ so does the set $\{0m + r, 1m + r, 2m + r, \ldots, (n-1)m + r\}$. 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 $\phi(mn) = \phi(m) \phi(n)$. QED

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

$$\phi(n) = \prod_{i=1}^{k} \left( p_i^{\alpha_i - 1} - p_i^{\alpha_i - 2} \right) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i - 1} (p_i - 1)}{p_i} = \frac{n \prod_{i=1}^{k} \left( 1 - \frac{1}{p_i} \right)}{(i)}$$

$$\phi(n) = \prod_{i=1}^{k} \left( 1 - \frac{1}{p_i} \right)$$

Proof: Follows immediately by calculation. 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 $p^a$ appears in the prime factorization of $n$ then by (i) we have $p - 1 \mid \phi(n)$ and $p^{a-1} \mid \phi(n)$. Since $\phi(n) = 6$ in order to have $p - 1 \mid 6$ we can only have $p - 1 = 1, 2, 3, 4, 6$ 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:

\[
\begin{align*}
\phi(2^0 \cdot 3^0 \cdot 7^0) &= 1 \\
\phi(2^0 \cdot 3^0 \cdot 7^1) &= 6 \\
\phi(2^0 \cdot 3^1 \cdot 7^0) &= 2 \\
\phi(2^0 \cdot 3^1 \cdot 7^1) &= 12 \\
\phi(2^0 \cdot 3^2 \cdot 7^0) &= 6 \\
\phi(2^0 \cdot 3^2 \cdot 7^1) &= 36 \\
\phi(2^1 \cdot 3^0 \cdot 7^0) &= 1 \\
\phi(2^1 \cdot 3^0 \cdot 7^1) &= 6 \\
\phi(2^1 \cdot 3^1 \cdot 7^0) &= 2 \\
\phi(2^1 \cdot 3^1 \cdot 7^1) &= 12 \\
\phi(2^1 \cdot 3^2 \cdot 7^0) &= 6 \\
\phi(2^1 \cdot 3^2 \cdot 7^1) &= 36 \\
\phi(2^2 \cdot 3^0 \cdot 7^0) &= 2 \\
\phi(2^2 \cdot 3^0 \cdot 7^1) &= 12 \\
\phi(2^2 \cdot 3^1 \cdot 7^0) &= 4 \\
\phi(2^2 \cdot 3^1 \cdot 7^1) &= 24 \\
\phi(2^2 \cdot 3^2 \cdot 7^0) &= 12 \\
\phi(2^2 \cdot 3^2 \cdot 7^1) &= 28 
\end{align*}
\]

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

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

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

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 $\Phi$ is the divisor summatory function for $\phi$ then $\Phi(n) = n$.

Proof: 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

$$n = \sum_{d \mid n} |C_d| = \sum_{d \mid n} \phi(n/d)$$
However as $d$ runs over all divisors of $n$ so does $n/d$ and so:

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

QED