**Math 406 Section 6.3: Euler's Theorem**

1. **Introduction:** Fermat's Little Theorem tells us that if $p$ is a prime and if $p \nmid a$ then $a^{p-1} \equiv 1 \bmod p$. Since this is useful for reducing large powers of $a$ mod $p$ it might be helpful if we had a version for when the modulus is not prime.

2. **Preliminaries:**

   (a) **Definition:** Define the *Euler Phi-Function* $\phi : \mathbb{Z}^+ \to \mathbb{Z}$ by $\phi(1) = 1$ and otherwise $\phi(n)$ is the number of positive integers less than $n$ and coprime to $n$.

   **Example:** For example $\phi(10) = 4$ because 1,3,7,9 are coprime to 10 and $\phi(16) = 8$ because 1,3,5,7,9,11,13,15,17 are coprime to 16.

   **Example:** For a prime $p$ we have $\phi(p) = p - 1$.

   (b) **Definition:** A *reduced residue set* mod $m$ is a set of $\phi(m)$ integers all of which are coprime to $m$ and no two of which are congruent to each other mod $m$.

   **Note:** This differs from a complete residue set in terms of the number of integers and the coprimality.

   **Example:** If $m = 10$ then $\{1, 3, 7, 9\}$ is a reduced residue set. Another would be $\{11, -7, 57, -11\}$.

   (c) **Theorem:** Given a modulus $m$, if $\{r_1, r_2, ..., r_{\phi(m)}\}$ is a RRS mod $m$ and if $a \in \mathbb{Z}$ is such that $\gcd(a, m) = 1$ then $\{ar_1, ar_2, ..., ar_{\phi(m)}\}$ is also a RRS.

   **Proof:** First we show by contradiction that every element in the new set is coprime to $m$. If $\gcd(ar_i, m) \neq 1$ then some prime $p$ divides both $ar_i$ and $m$. Well, $p \mid ar_i$ implies $p \mid a$ or $p \mid r_i$. If $p \mid r_i$ then along with $p \mid m$ we get $\gcd(r_i, m) \neq 1$ which contradicts the fact that our original set is a reduced residue set mod $m$. Thus $p \mid a$ but this along with $p \mid m$ contradicts $\gcd(m, a) = 1$.

   Second we show by contradiction that no two elements in the new set are congruent to each other mod $m$. If $ar_i \equiv ar_j \bmod m$ then because $\gcd(a, m) = 1$ we may cancel to get $r_i \equiv r_j \bmod m$ which contradicts the fact that our original set is a reduced residue set mod $m$. $\mathcal{QED}$

3. **Euler's Theorem:** Suppose $m$ is a modulus and $a \in \mathbb{Z}$ with $\gcd(a, m) = 1$. Then $a^{\phi(m)} \equiv 1 \bmod m$.
**Note:** In the case when $m$ is prime we have $\phi(m) = m - 1$ and we get Fermat's Little Theorem.
**Proof:** Let $S = \{r_1, r_2, ..., r_{\phi(m)}\}$ be any RRS mod $m$, for example $S$ could be the set of positive integers less than $m$ and coprime to $m$. Then by the theorem above $S' = \{ar_1, ar_2, ..., ar_{\phi(m)}\}$ is also a RRS. It follows that $S$ and $S'$ consist of the same integers mod $m$, although probably in a different order. Thus we know:

$$
\begin{aligned}
(ar_1)(ar_2)...(ar_{\phi(m)}) &\equiv r_1 r_2 ... r_{\phi(m)} \bmod m \\
a^{\phi(m)} r_1 r_2 ... r_{\phi(m)} &\equiv r_1 r_2 ... r_{\phi(m)} \bmod m \\
a^{\phi(m)} &\equiv 1 \bmod m
\end{aligned}
$$

The reason we can cancel all the $r_i$ is that they are coprime to $m$ because $S$ is a RRS.

**Example:** To reduce $9^{453}$ mod 16 we note that $\gcd(9, 16) = 1$ so Euler's Theorem tells us that $9^{\phi(16)} \equiv 1 \bmod 16$. Since $\phi(16) = 8$ we have $9^8 \equiv 1 \bmod 16$ and so:

$$
9^{453} \equiv 9^{8(56)+5} \equiv 9^5 \equiv 9(81)(81) \equiv 9(1)(1) \equiv 9 \bmod 16
$$

**Corollary:** Suppose $m$ is a modulus and $a \in \mathbb{Z}$ with $\gcd(a, m) = 1$. Then $a^{\phi(m)-1}$ is an inverse of $a$ mod $m$.
**Proof:** Follows immediately.