Recall: (Fermat's Little Theorem) Let p be a prime, and let a be any number satisfying $a \not\equiv 0 \pmod{p}$. Then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Question: Is this true if we replace "p" with "m"?

Answer: Not necessarily.

(Counter) example: $m = 6 \quad a = 5$.

$$5^{6-1} = 3125 \equiv 5 \pmod{6}$$
$$\not\equiv 1 \pmod{6}.$$

To look at the general case, we define the following

Euler's Phi function:

$$\phi(m) := \#\{a : 1 \le a \le m \text{ and } \gcd(a, m) = 1\}$$

Example:

$$\phi(2) = \#\{a : 1 \le a \le 2, \gcd(a,2) = 1)\} = \#\{1\} = 1$$

$$\phi(3) = \#\{a : 1 \le a \le 3, \gcd(a,3) = 1)\} = \#\{1,2\} = 2$$

$$\phi(4) = \#\{a : 1 \le a \le 4, \gcd(a,4) = 1)\} = \#\{1,3\} = 2.$$

$$\phi(10) = \#\{a: 1 \le a \le 10, \gcd(a,10) = 1\}$$

$$= \#\{1, 3, 7, 9\} = 4$$

....

Note: $\phi(p) = p - 1$. since

$$\{a: 1 \le a \le p, \gcd(a,p) = 1\} = \{1, 2, \cdots p-1\}.$$

Theorem: (10.1 Euler's formula). If $\gcd(a,m) = 1$, then

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Remark: When $m = p$ is a prime, this is Fermat's Little Theorem.

The proof is quite similar to the prime case.

By the definition of $\phi(m)$, we can list all the numbers between 1 and m, and coprime to m:

$$b_1, b_2, \cdots b_{\phi(m)} \qquad 1 \le \cdots \le m$$

coprime to m.

$\{$ multiply by a.

$$ab_1, ab_2, \cdots, ab_{\phi(m)}$$

} reduce to (mod m) between $1 \leq \cdots \leq m$

$$ab_1 \pmod m,\ ab_2 \pmod m,\ \cdots\ ab_{\phi(m)} \pmod m$$

Lemma 10.2. If $\gcd(a, m) = 1$, then the numbers:

$$b_1,\ b_2,\ b_3 \cdots\ b_{\phi(m)} \pmod m$$

are the same as the numbers

$$ab_1,\ ab_2,\ ab_3, \cdots ab_{\phi(m)} \pmod m$$

Proof: Similar to the previous proof.

Proof of Euler's Formula:

By Lemma 10.2,

$$(ab_1)(ab_2) \cdots (ab_{\phi(m)}) \equiv b_1\, b_2 \cdots b_{\phi(m)} \pmod m$$

That is:

$$a^{\phi(m)} \cdot b_1 b_2 \cdots b_{\phi(m)} \equiv b_1\, b_2, \cdots b_{\phi(m)} \pmod m$$

By the definition of $b_1, b_2 \cdots b_{\phi(m)}$,

$$\gcd(b_1, m) = \gcd(b_2, m) = \cdots \gcd(b_{\phi(m)}, m) = 1$$

Therefore:

$$\gcd(b_1 \cdots b_{\phi(m)}, m) = 1.$$

(This uses a fact: if $\gcd(a,c) = \gcd(b,c) = 1$ then $\gcd(ab, c) = 1$.)

Then we can cancel $b_1 b_2 \cdots b_{\phi(m)}$ on each side:

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

□