Euler's theorem

Leonard Euler published a proof of Fermat's little theorem in 1736. Fermat's theorem is stated for prime number. In 1760, Euler generalized Fermat's little theorem, which holds for composite number n. In other words, if n is prime, Euler's theorem reduces to Fermat's little theorem. Euler's theorem uses totient function $\emptyset(n)$ of the composite number n. (https://www.savitagandhi.com/articles/totient-function). Euler's theorem being generalization of Fermat's little theorem is also known as Fermat–Euler theorem or Euler's totient theorem. We now state Euler's theorem for any integer n .

Euler's theorem: If a and n are relatively prime than $a^{\emptyset(n)} \equiv 1(mod\ n)$.

The proof is on very similar lines as given for Fermat's theorem (https://www.savitagandhi.com/articles/fermats-little-theorem). Recall, $\emptyset(n)$ is number of positive integers less than or equal to n, that are relatively prime to n. It is clear that if n is prime, say $n = p$, then $\emptyset(n) = p - 1$ and Euler's theorem simplifies to $a^{p-1} \equiv 1(mod\ p)$, which is nothing but Fermat's little theorem. So, Fermat's little theorem is a special case of Euler's theorem with n as prime. We now prove, Euler's theorem for any integer n .

Proof: Let S be the set of such integers, $x_i, 1 \leq x_i \leq n$, relatively prime to n. Thus, $S = \{x_1, x_2, \dots, x_{\emptyset(n)}\}$. Obtain the set T from S by performing following two steps, one after other as follows:

(i) First multiply each element of S by a giving $\{ax_1, ax_2, \dots, ax_{\emptyset(n)}\}$

(ii) Then, do *modulo* n for each element giving, $T = \{ax_1(mod\ n), ax_2\ (mod\ n), \dots, ax_{\emptyset(n)}(mod\ n)\} = \{ax_i(\ mod\ n) |\ 1 \leq i \leq \emptyset(n)\}$

We claim that T is a permutation of S, that is, elements of T are the same as that of S, only order of elements appearing in the sequence could be different. Let us establish it.

Firstly, we show that $T \subseteq S$. Since $a\ and\ x_i$ are relatively prime to n, it follows that $a \cdot x_i$ is also relatively prime to n, for $i = 1, 2, \dots, \emptyset(n)$. Elements of T being $mod\ n$, we can say that elements of $T$are positive integers $< n$ and they are relatively prime to n. Thus,$T \subseteq S$.

Secondly, we prove that all elements of T are distinct. Let if possible, some two of the elements of T are equal. That is, $a \cdot x_i\ (mod\ n) = a \cdot x_j\ (mod\ n)$ for some $i \neq j, where\ 1 \leq i, j \leq \emptyset(n)$. Therefore, $(a \cdot x_i - a \cdot x_j)$ is a multiple of n. In other words $a \cdot (x_i - x_j)$ is divisible by n , with $(x_i - x_j) \neq 0$. As n does not divide a, n must divide $(x_i - x_j)$. But that is not possible, as $\left(x_i - x_j\right) < n$, and x_i, x_j are relatively prime to n. Thus, our assumption that some two of the elements of are T are equal cannot hold true. We can conclude, all elements of T are distinct. Therefore, order of T is $\emptyset(n)$, which is same as that of S. $T \subseteq S$ and number of elements in T being being equal to that in S yields $T = S$.

As $T = S$, product of all element of S and that of T is same. Taking product of all the elements in each of the sets S and T and equating them, gives us:

$$\prod_{i=1}^{\emptyset(n)} x_i = \prod_{i=1}^{\emptyset(n)} (ax_i(mod\ n))$$

$$\equiv \left(\prod_{i=1}^{\emptyset(n)} ax_i\right)(mod\ n)$$

$$\equiv \left(a^{\emptyset(n)}\left(\prod_{i=1}^{\emptyset(n)} x_i\right)\right)(mod\ n)$$

Since, $x_1, x_2, \dots, x_{\emptyset(n)}$ are relatively prime to n, it follows that $\prod_{i=1}^{\emptyset(n)} x_i$ is relatively prime to n. Thus, preceding congruence equation is equivalent to:

$1 \equiv a^{\emptyset(n)}(mod\ n)$, which is same as $a^{\emptyset(n)} \equiv 1(mod\ n)$. This proves the Euler's theorem.

****