Fermat's little theorem:

Fermat's little theorem was discovered around 350 years back. Pierre de Fermat used to make observations about number theory results. Leonhard continued with his work. Fermat's Little Theorem is a special case of Euler Totient theorem, which was proved later by Euler. Fermat's little theorem simplifies the computation of exponents in modular arithmetic, plays important role in discovery of large prime numbers and public key cryptography.

Theorem: It states that, if p is prime and a is a positive number such that p does not divide a, then, $a^{p-1} \equiv 1(mod\ p)$

Many different methods for proving this theorem are available in literature. We just present one of them.

Proof: Let $S = \{1, 2, \dots, p-1\}$, where p is prime, and a be a natural number, such that p does not divide a. Construct a set T from S by performing two steps, in sequence as follows:

(i) First multiply each element of S by a giving $\{a, 2a, \dots, (p-1)a\}$

(ii) Then, do $modulo\ p$ for each element of the set thus obtained, giving, $T = \{a\ mod\ p, 2a\ mod\ p, \dots, (p-1)a\ mod\ p\}$

For example, if $p = 7$ and $a = 3$, then $S = \{1, 2, 3, 4, 5, 6\}$ and $T = \{(1 \cdot 3)\ mod\ 7, (2 \cdot 3)\ mod\ 7, (3 \cdot 3)\ mod\ 7, (4 \cdot 3) mod\ 7, (5 \cdot 3) mod\ 7, (6 \cdot 3)\ mod\ 7\}$ giving $T = \{3\ mod\ 7, 6\ mod\ 7, 9\ mod\ 7, 12\ mod\ 7, 15\ mod\ 7, 18\ mod\ 7\} = \{3, 6, 2, 5, 1, 4\} = \{1, 2, 3, 4, 5, 6\}$ = S. Here, we got $T = S$. Is it a coincidence? Well, it is not just a coincidence, it is true always. We shall prove that, $T = S$. Let us see, how?

We can express the set T as $T = \{i \cdot a\ (mod\ p) | 1 \le i \le p-1\}$. Since elements of T are $mod\ p$, it is clear that each and every element of T is $\le p-1$. Firstly, we claim that $0 \notin T$. As p does not divide a, and p does not divide i for $1 \le i \le p-1$; p being prime, it follows that p cannot divide $i \cdot a$ for $i = 1, 2, \dots, p-1$. ($p|ab \Rightarrow p|a\ or\ p|b$). Thus, $i \cdot a\ (mod\ p) \neq 0$ for $i = 1, 2, \dots, p-1$. So, no element of T is zero giving $T \subseteq S$, as elements of T are positive and $\le p-1$.

Next, we establish that all elements of T are distinct. We prove it by method of contradiction. Let if possible, some two of the elements are equal. That is, $i \cdot a\ (mod\ p) = j \cdot a\ (mod\ p)$ for some $i \neq j$, $where\ 1 \le i, j \le p-1$. Therefore, $(i \cdot a - j \cdot a)$ is a multiple of p. In other words $a \cdot (i-j)$ is divisible by p, with $(i-j) \neq 0$. As p does not divide a, p most divide $(i-j)$. But that is not possible, as $(i-j) < p$, and p is prime. Thus, our assumption that some two of the elements of T are equal can not hold true. We can

conclude, all elements of T are distinct. Therefore, order of T is $p-1$, which is same as that of S. $T \subseteq S$ and number of elements in T being equal to that in S yields $T = S$.

Therefore, product of all element of S and that of T are same. Taking product of all the elements in each of the sets S and T gives us:

$$1 \cdot 2 \cdot 3 \ldots . (p-1) = (a \bmod p)(2a \bmod p) \ldots ((p-1)a \bmod p)$$

$$= \left[1 \cdot 2 \cdot 3 \ldots . (p-1)a^{(p-1)}\right] (mod\ p)$$

$\therefore (p-1)!\ (a^{(p-1)} - 1)$ is divisible by p. As $(p-1)!$ is not divisible by p, we can say that $(a^{(p-1)} - 1)$ is divisible by p . That is, $a^{(p-1)} \equiv 1(mod\ p)$. This proves Fermat's little theorem.

****