Fermat's Little Theorem:

假設 $m \in \mathbb{Z}$ 且 $p$ 為質數，使得 $\gcd(m, p) = 1$，

則 $m^{p-1} \equiv 1 \pmod{p}$。

證明：

考慮 $p-1$ 個數 $x_1, x_2, \cdots, x_{p-1}$

$\Rightarrow x_1 = m \bmod p$，$x_2 = (2m) \bmod p$，$x_3 = (3m) \bmod p$，

$\cdots\ x_{p-1} = [(p-1)m] \bmod p$，

則 $x_1, x_2, \cdots, x_{p-1} \in \{0, 1, \cdots, p-1\}$.

因為 $\gcd(m, p) = 1$，所以 $p \nmid (km)$，$\forall k = 1, 2, \cdots, p-1$

$\Rightarrow x_i \neq 0$，$\forall i = 1, 2, \cdots, p-1$.

此外，$x_i \neq x_j$，$\forall i \neq j$，這是因為若 $x_i = x_j$，則 $im \equiv jm \pmod{p}$.

根據：

> 假設 $a, b, c, n \in \mathbb{Z}$，若 $\gcd(c, n) = 1$，則
>
> $$ac \equiv bc \pmod{n} \longleftrightarrow a \equiv b \pmod{n}$$

$i \equiv j \pmod{p}$，產生矛盾.

所以 $\{x_1, x_2, \cdots, x_{p-1}\} = \{1, 2, \cdots, p-1\}$

$\Rightarrow m(2m)(3m)\cdots[(p-1)m] \equiv x_1 x_2 \cdots x_{p-1} \equiv (p-1)! \pmod{p}$

$\Rightarrow (p-1)!\, m^{p-1} \equiv (p-1)! \pmod p$

因為 $\gcd((p-1)!, p) = 1$，所以 $m^{p-1} \equiv 1 \pmod p$.

---

Euler 對 Fermat's little theorem 的推廣，當 $n=p$ 為質數時，

$\phi(n) = p-1$ 滿足費瑪小定理 (Fermat's little theorem)

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

定理：(Euler 對 Fermat's little theorem 的解釋)

假設 $m \in \mathbb{Z}$，$n \in \mathbb{Z}^+$ 且 $\gcd(m,n)=1$，則 $m^{\phi(n)} \equiv 1 \pmod n$

證明：

假設小於 $n$ 且與 $n$ 互質的元素所成集合為 $R = \{x_1, x_2, \ldots, x_{\phi(n)}\}$

令 $S = \{(mx_1 \bmod n), (mx_2 \bmod n), \ldots, (mx_{\phi(n)} \bmod n)\}$.

首先證明 $\gcd(mx_i, n) = 1$，$\forall i = 1, 2, \ldots, \phi(n)$.

若 $\gcd(mx_i, n) \neq 1$, for some $1 \le i \le \phi(n)$，則 $\exists p$ 為質數使得

$p \mid \gcd(mx_i, n) \Rightarrow p \mid m$ 或 $p \mid x_i$ 此與 $\gcd(m,n) = 1 = \gcd(x_i, n)$

矛盾。

所以 $\gcd(mx_i, n) = 1$，$\forall i = 1, 2, \ldots, \phi(n)$.

因此 $S$ 中元素皆小於 $n$ 且與 $n$ 互質，即 $S \subseteq R$

接著證明S中的元素皆相異.

利用矛盾證法，若 $\exists i \neq j$ 使得

$(mx_i \bmod n) = (mx_j \bmod n)$

根據:

$$\boxed{\begin{array}{l}\text{假設 } a,b,c,n \in \mathbb{Z}\text{，若 } \gcd(c,n)=1\text{，則} \\ \quad ac \equiv bc \pmod{n} \longleftrightarrow a \equiv b \pmod{n}\end{array}}$$

$x_i = x_j$ 產生矛盾，因此 $|S| = \phi(n) = |R|$，再加上

$S \subseteq R$ 可得 $S = R$

所以

$$\prod_{i=1}^{\phi(n)} (mx_i \bmod n) = \prod_{i=1}^{\phi(n)} x_i$$

$$\Rightarrow \prod_{i=1}^{\phi(n)} mx_i \equiv \prod_{i=1}^{\phi(n)} x_i \pmod{n}$$

$$\Rightarrow m^{\phi(n)} \left[\prod_{i=1}^{\phi(n)} x_i\right] \equiv \left[\prod_{i=1}^{\phi(n)} x_i\right] \pmod{n}$$

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

衍生出 $\Rightarrow$ $m \in \mathbb{Z}$, $n \in \mathbb{Z}^+$, $\gcd(m, n) = 1$

$$m^{\phi(n)} \equiv 1 \pmod{n} \Rightarrow m^{\phi(n)-1} \cdot m \equiv 1 \pmod{n}$$

$m$ 為 $m^{\phi(n)-1}$ 在 mod $n$ 下的乘法反元素。