Enoch Yu

Euler's Theorem

$\forall (a,n)=1, \quad a^{\varphi(n)} \equiv 1 \pmod{n}$

pf) $\varphi(n)$ = # of elements in reduced residue system of modulo n.

$1, 2, \ldots, n-2, n-1$

$RRS(n) = \{a_1, a_2, \ldots, a_k\}$

$\varphi(n) = k$

Assuming that $(a,n)=1$,

$RRS(n) = \{aa_1, aa_2, \ldots, aa_k\}$

$$aa_1 \cdot aa_2 \cdots aa_k \equiv a_1 \cdot a_2 \cdots a_k \pmod{n}$$

$$a^k(a_1 \cdots a_k) \equiv a_1 \cdots a_k \pmod{n} \qquad (a_i, n) = 1$$

$$\therefore a^k \equiv 1 \pmod{n}$$

$$a^{\varphi(n)} \equiv 1 \pmod{n} \quad \text{if } (a,n)=1.$$

$\square$

Find the remainder when 3^{804} is divided by 17.

Solution) Because $(3,17)=1$,

$$3^{\varphi(17)} \equiv 1 \pmod{17}$$

$$3^{16} \equiv 1 \pmod{17}$$

$$3^{800} \equiv 1 \pmod{17}$$

$$\therefore 3^{804} \equiv 81 \pmod{17}$$

$$\equiv 13 \pmod{17}$$

13

$\begin{array}{r} 2 \\ 17 \\ \times 4 \\ \hline 68 \end{array}$

If $(a,n)=1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Corollary (Fermat's Little Theorem)

For $\forall$ prime numbers p and a number a such that $p \nmid a$, $a^p \equiv a \pmod{p}$.

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

pf) Because $(a,p)=1$, by Euler's theorem,

$$a^{\varphi(p)} \equiv 1 \pmod{p},$$

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

$$a^p \equiv a \pmod{p}$$

$\square$