FERMAT'S THEOREM

Ⓣ Let $a \in GF(q)$ $\quad a \neq 0$, q prime

Then $\boxed{a^{q-1} \equiv 1 \pmod{q}}$

Example: 1) $q = 7$, $a = 2$

$$2^6 = 64 \equiv 1 \pmod{7}$$

2) $q = 5$ $\quad a = 3$

$$3^4 = 81 \equiv 1 \pmod{5}$$

a not neccerely primitive !

Proof of Fermat's Theorem

by the binomial formula

$$(\underbrace{a+a+\dots+a}_{a})^{q} = (a\cdot a)^{q} = a^{2q} \equiv$$

$$\underbrace{a^{q}+a^{q}+\dots+a^{q}}_{a} = a\cdot a^{q} \quad (\bmod\ q)$$

Thus $a^{2q} = a\cdot a^{q}$ or

$$\boxed{a^{q} = a} \quad \text{or}$$

$$\boxed{a^{q-1} = 1} \quad (\bmod\ q)$$