$\boxed{p \text{ premier}}$

$p-1 = \varphi(p)$ # inversibles mod p

$a < p$ tq. $\gcd(a;p) = 1$

$a^{p-1} \equiv 1 \mod p$ Fermat

si $\gcd(a;p) = 1$

$\mathbb{Z}^*_{17} = \{1;2;3;\dots;16\}$

$\boxed{m \in \mathbb{N}}$

$\varphi(m) = \boxed{\text{\# inversibles mod } m}$

$2 \cdot k \equiv 1 \mod 10$

$m = 10$

$a^{\varphi(m)} \equiv 1 \mod m$

4 éléments

$\mathbb{Z}^*_{10} = \{1;3;7;9\}$

si $\gcd(a;m) = 1$

$\varphi(10) = 4$

Ordre de 9 modulo 10 :

ordre$(9) = 2$ dans $\mathbb{Z}_{10}$

car $9^2 \equiv 1 \mod 10$

$9, 9^2, 9^3, 9^4 = 1$

$9^k \equiv 1 \mod 10$

la plus petite puissance, notée k, tq.

$\boxed{p \text{ est premier, } a \text{ tq. } \gcd(a;p) = 1 \Rightarrow \text{ordre}(a) \mid \overset{\varphi(p)}{p-1}}$

$\boxed{m \text{ entier, } a \text{ tq. } \gcd(a;m) = 1 \Rightarrow \text{ordre}(a) \mid \varphi(m)}$

$\mathbb{Z}_9^* = \{1; 2; 4; 5; 7; 8\}$ $\quad |\mathbb{Z}_9^*| = 6 = 2 \cdot 3$

$5^2, 5^3, 5^6$ $\quad \mathrm{ord}(5) = 6$ dans $\mathbb{Z}_9$

$\mathbb{Z}_5$

ordre(1) = 1 $\quad$ ordre(4) = 2

ordre(2) = 4

ordre(3) = 4

$\mathbb{Z}_5^* = \boxed{\{1; 2; 3; 4\}}$

4 éléments

$\mathbb{Z}_5 = \{1; 2; 3; 4\}$

$5 - 1 = 4$ # inversibles mod 5

$$\boxed{1^1 \equiv 1 \mod 5 \Rightarrow \text{ordre}_5(1) = 1}$$

$2^1 = 2 \not\equiv 1 \mod 5$

$2^2 = 4 \not\equiv 1 \mod 5$

$\cancel{2^3} = 8 \not\equiv 1 \mod 5$

$2^4 = 16 \equiv 1 \mod 5 \Rightarrow \text{ordre}_5(2) = 4$

$\boxed{2.6.10}$

$\boxed{a^8 \equiv 1 \mod 15}$

$3 \cdot 5$

$\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$

$8 = |\mathbb{Z}_{15}^*| = \varphi(15)$

$a \in \mathbb{Z}_{15}^*$

$\{a, 2a, 4a, 7a, 8a, 11a, 13a, 14a\} = \mathbb{Z}_{15}^*$

$a \cdot 2a \cdot 4a \cdot 7a \cdot 8a \cdot 11a \cdot 13a \cdot 14a \equiv 1 \cdot 2 \cdot 4 \cdot 7 \cdot 8 \cdot 11 \cdot 13 \cdot 14 \mod 15$

$a^8 \cdot 1 \cdot \cancel{2} \cdot \cancel{4} \cdot \cancel{7} \cdot \cancel{8} \cdot \cancel{11} \cdot \cancel{13} \cdot \cancel{14} \equiv 1 \cdot \cancel{2} \cdot \cancel{4} \cdot \cancel{7} \cdot \cancel{8} \cdot \cancel{11} \cdot \cancel{13} \cdot \cancel{14} \mod 15$

$\boxed{a^8 \equiv 1 \mod 15}$

$$c = m^{e} \bmod n$$

$$\boxed{ed \equiv 1 \bmod \varphi(n)}$$

$$c^{d} \bmod n = (m^{e})^{d} \bmod n$$

$$= m^{ed} \bmod n$$

$$= m^{1+k\cdot\varphi(n)} \bmod n = m^{1} \cdot \underbrace{(m^{\varphi(n)})^{k}}_{1} \bmod n$$