Petit thm de Fermat

p premier

(1) $\gcd(a; p) = 1 \Rightarrow \boxed{a^{p-1} \equiv 1} \mod p$

(2) $\boxed{a^p \equiv a} \mod p$

$48^{322} \mod 25$ $\quad$ $48 \mod 25 = 23$ $\quad$ $\gcd(23; 25) = 1$

$25 = 5 \cdot 5$ $\quad$ $\varphi(25) = \varphi(5^2) = 5 \cdot (5-1) = 5 \cdot 4 = 20$

1 2 3 4 $\cancel{5}$ 6 7 8 9 $\cancel{10}$ 11 12 13 14 $\cancel{15}$ 16 17 18 19 $\cancel{20}$ 21 22 23 24

$322 = 16 \cdot 20 + 2$ $\quad$ $48^{20} \mod 25 = 1$

$$48^{16 \cdot 20 + 2} = 48^{16 \cdot 20} \cdot 48^2 = \left(48^{20}\right)^{16} \cdot 48^2$$

$48 \equiv 23 \mod 25$

$$\left(48^{20}\right)^{16} \cdot 48^2 \mod 25 = 1 \cdot 23^2 \mod 25$$

$\boxed{2.6.12}$

$$a^{p-1} = a \cdot a^{p-2} \equiv 1 \mod p \qquad \text{si } \gcd(a;p)=1$$

mod 23

Inverse de 3 mod 23

$$3^{22} \equiv 1 \mod 23$$

$$3 \cdot 3^{21} \equiv 1 \mod 23$$

$$3^{21} \mod 23$$

$$\underbrace{3^{16+4+1} \mod 23}_{\underbrace{3 \cdot 12 \cdot 13 \mod 23}_{8}}$$

3	3
3^2	9
3^4	12
3^8	6
3^{16}	13

$$\boxed{\varphi(p\cdot q) = (p-1)(q-1)}$$

si p, q sont premiers et que $p \neq q$

$$\mathbb{Z}_{15} = \mathbb{Z}_{3\cdot 5}$$

$$\varphi(15) = 2 \cdot 4 = 8$$

$$1 \quad 2 \quad \cancel{3} \quad 4 \quad \cancel{5} \quad \cancel{6} \quad 7 \quad 8 \quad \cancel{9} \quad \cancel{10} \quad 11 \quad \cancel{12} \quad 13 \quad 14$$

$$\{1;\ 2;\ 4;\ 5;\ 8;\ 10;\ 11;\ 13;\ 16;\ 17;\ 19;\ 20\} = \mathbb{Z}_{21}^*$$

$$|\mathbb{Z}_{21}^*| = 12$$

$a \in \mathbb{Z}_{21}^*$ $\qquad a^{12} \equiv 1 \mod 21$

$$\{a;\ 2a;\ 4a;\ 5a;\ 8a;\ 10a;\ 11a;\ 13a;\ 16a;\ 17a;\ 19a;\ 20a\} = \mathbb{Z}_{21}^*$$

commutativité

$$a \cdot 2a \cdot 4a \cdot 5a \cdot 8a \cdot 10a \cdot 11a \cdot 13a \cdot 16a \cdot 17a \cdot 19a \cdot 20a \equiv 1 \cdot 2 \cdot 4 \cdot 5 \cdot 8 \cdot 10 \cdot 11 \cdot 13 \cdot 16 \cdot 17 \cdot 19 \cdot 20 \mod 21$$

$$1 \cdot \cancel{2} \cdot \cancel{4} \cdot \cancel{5} \cdot \cancel{8} \cdot \cancel{10} \cdot \cancel{11} \cdot \cancel{13} \cdot \cancel{16} \cdot \cancel{17} \cdot \cancel{19} \cdot \cancel{20} \cdot a^{12} \equiv 1 \cdot \cancel{2} \cdot \cancel{4} \cdot \cancel{5} \cdot \cancel{8} \cdot \cancel{10} \cdot \cancel{11} \cdot \cancel{13} \cdot \cancel{16} \cdot \cancel{17} \cdot \cancel{19} \cdot \cancel{20} \mod 21$$

$$a^{12} \equiv 1 \mod 21$$

$$\underbrace{1}_{a} z^2 \underbrace{-3(1+i)}_{b} \cdot z + \underbrace{6+7i}_{c} = 0$$

$a = 1 \qquad b = -3(1+i) \qquad c = 6+7i$

$$\Delta = b^2 - 4ac = 9(1+i)^2 - 4(6+7i) = 9(\cancel{1}+2i-\cancel{1}) - 24 - 28i$$

$$= 18i - 24 - 28i$$

$$= -24 - 10i$$

$$z_1 = \frac{-b+\sqrt{\Delta}}{2a} \qquad z_2 = \frac{-b-\sqrt{\Delta}}{2a}$$

$1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad \cancel{7} \quad 8 \quad 9 \quad 10 \quad 11 \quad 12 \quad 13 \quad \cancel{14} \quad \ldots \qquad 7 \cdot 7^4$

7^5

$$|(a+bi)^2| = |-24-10i| \qquad a^2+b^2 = \sqrt{24^2+10^2} = \sqrt{26^2} = 26$$

$$a^2 + 2abi + (bi)^2 = -24 - 10i$$

$$a^2 - b^2 + 2abi = -24 - 10i$$

$$\boxed{\begin{aligned} &a^2 - b^2 = -24 \qquad a^2 + b^2 = 26 \\ &2ab = -10 \end{aligned}}$$

$$a = \pm 1$$

$$b = \mp 5$$

$$w_1 = 1 - 5i$$

$$w_2 = -1 + 5i$$

$a \in \mathbb{Z}_m$ tq. $\gcd(a; m) = 1$

Euler

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

$m = 10$

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

$3^4 \equiv ? \mod 10$

$9^4 \equiv ? \mod 10$

$7^4 \equiv ? \mod 10$

$$\boxed{\varphi(p \cdot q) = (p-1)(q-1)}$$ si p, q premiers

$$\boxed{\varphi(p^n) = (p-1)\,p^{n-1} = p^n - p^{n-1}}$$

$$\varphi(8) = \varphi(2^3) = 1 \cdot 2^2 = 4$$

$$\{1; 3; 5; 7\} = \mathbb{Z}_8^* \Rightarrow \varphi(8) = |\mathbb{Z}_8^*| = 4$$

$1 \quad 7 \quad 14 \quad 7 \cdot 7^4$

$$7^5 - 7^4 = 7^4(7-1)$$

$$\varphi(p^n) = (p-1)p^{n-1} = p^n - p^{n-1}$$

$48^{322} \bmod 25 = 23^{322} \bmod 25$ $\qquad \varphi(5^2) = (5-1)\cdot 5^{2-1}$

$\varphi(25) = 5 \cdot 4 = 20$

$1\ 2\ 3\ 4\ \cancel{5}\ 6\ 7\ 8\ 9\ \cancel{10}\ 11$

$$23^{\varphi(25)} = \boxed{23^{20} \equiv 1 \mod 25}$$ Euler

$$23^{322} = 23^{(320+2)} = 23^{\overbrace{16\cdot 20}^{320}} \cdot 23^2 = \left(23^{20}\right)^{16} \cdot 23^2$$

$$\equiv 1^{16} \cdot 23^2 \mod 25$$

$$\equiv 23^2 \mod 25$$

$$\equiv 4 \mod 25$$