

# 15강 연속제곱법 (Successive Squaring)

\* 오일러 피 함수

$$a^{\phi(m)} \equiv 1 \pmod{m} \quad \gcd(a, m) = 1$$

ex)  $3083 \cdot 4283 = 13,204,489 = m$

$$\phi(m) = \phi(3083) \cdot \phi(4283) = 3082 \cdot 4282 = 13,197,124$$

$$a^{13197124} \equiv 1 \pmod{m}$$

$$a^{1000,000,000,000} \equiv a^{\phi(m) \times 75774 + 1126024} \equiv (a^{\phi(m)})^{75774} \cdot a^{1126024} \pmod{m}$$

$$\left( \begin{aligned} 1000,000,000,000 &= \phi(m) \times 75774 + 1126024 \\ &\quad \text{몫} \quad \text{나머지} \\ &\Rightarrow a^{1126024} \pmod{m} \end{aligned} \right) \quad m = 13204489$$

$$a = 7 \quad 7^{1000,000,000,000} \equiv 7^{1126024} \pmod{m}$$

\* 연속제곱법 (Successive Squaring)

23번  $7 \equiv 7 \pmod{m}$

$$7^2 \equiv 49 \pmod{m}$$

$$7^4 \equiv 49^2 \equiv 2401 \pmod{m}$$

$$7^8 \equiv 2401^2 \equiv 5764801 \pmod{m}$$

ex) 701 숫

$$7^{283} \equiv ? \pmod{701}$$

$$\begin{aligned} 7^2 &\equiv 7 \\ 7^2 &\equiv 49 \pmod{701} \\ 7^2 &\equiv 49^2 \equiv 2401 \pmod{701} \\ 7^2 &\equiv 2401^2 \equiv 478 \\ 7^4 &\equiv 478^2 \equiv 659 \\ 7^5 &\equiv 659^2 \equiv 362 \pmod{701} \\ 7^6 &\equiv 362^2 \equiv 658 \pmod{701} \\ 7^{2^7} &\equiv 658^2 \equiv 447 \pmod{701} \\ 7^{2^8} &\equiv 447^2 \equiv 24 \pmod{701} \end{aligned}$$

$$\begin{aligned} 2 \overline{) 283} &= 100011011_2 \\ 2 \overline{) 141} &1 \\ 2 \overline{) 70} &1 \\ 2 \overline{) 35} &0 \\ 2 \overline{) 17} &1 \\ 2 \overline{) 8} &1 \\ 2 \overline{) 4} &0 \\ 2 \overline{) 2} &0 \\ 2 \overline{) 1} &0 \end{aligned}$$

$$\begin{aligned} 7^{283} &\equiv 7^{2^8 + 2^4 + 2^3 + 2^1 + 2^0} \equiv 7^{2^8} \cdot 7^{2^4} \cdot 7^{2^3} \cdot 7^{2^1} \cdot 7^{2^0} \\ &\equiv 24 \cdot 659 \cdot 478 \cdot 49 \cdot 7 \equiv 25 \pmod{701} \end{aligned}$$

ex)  $283 = 100011011_2$

$$7^0 = 1 \quad (7^0)^2 = 1 \cdot 7 = 7$$

$$\begin{aligned} \text{num} &= 7 \\ a &= 1 \\ a &= a^2 \end{aligned}$$

$$(7^{2^0})^2 = 7^{2^1}$$

$$(7^{2^1})^2 = 7^{2^2}$$

$$(7^{2^2})^2 = 7^{2^3}$$

$$(7^{2^3})^2 = 7^{2^4} \cdot 7 = 7^{2^4+2^0}$$

$$(7^{2^4+2^0})^2 = 7^{2^5+2^1} \cdot 7 = 7^{2^5+2^1+2^0}$$

$$(7^{2^5+2^4+2^0})^2 = 7^{2^6+2^2+2^1}$$

$$(7^{2^6+2^2+2^1})^2 = 7^{2^7+2^3+2^2} \cdot 7 = 7^{2^7+2^3+2^2+2^0}$$

$$(7^{2^7+2^3+2^2+2^0})^2 = 7^{2^8+2^4+2^3+2^1+2^0}$$

$$\begin{cases} \text{if } (\text{cur} == 1) \\ a = a \cdot \text{num} \\ a = a \% m \end{cases}$$