① 배경지식

- 페르마 소정리

p가 소수이고, a와 p가 서로소이면

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

- 오일러 정리

a와 n이 서로소인 양의 정수인 때 ($gcd(a,n)=1$)

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$ ※ n이 소수면 $\varphi(n) = n-1$

$\varphi(n)$: 1부터 n까지 정수 중 n과 서로소인 정수의 개수

※ m, n이 서로소면 $\varphi(m \times n) = \varphi(m) \times \varphi(n)$

② 문제풀이

유형 1) modular inverse

$3^{-1} \bmod 7$?

Ⅰ 페르마 소정리 활용

$a^{p-1} \equiv 1 \pmod{p}$ 에서 양변에 a^{-1}을 곱함

$a^{p-2} \equiv a^{-1} \pmod{p}$

예시에 적용하면 $3^5 \equiv 3^{-1} \pmod{7}$

Ⅱ 오일러 정리 활용

$a^{\varphi(n)} \equiv 1 \pmod{n}$ 의 양변에 a^{-1} 곱함

$a^{\varphi(n)-1} \equiv a^{-1} \pmod{n}$

예시에 적용하면 $3^{6-1} \equiv 3^{-1} \pmod{7}$

③ EEA 활용 $3^{-1} \bmod 7$

$3^{-1} \bmod 7 = s$라고 하면, $3 \cdot s \equiv 1 \pmod 7$

또, 3과 7의 최대공약수 $\gcd(3,7) = 3 \cdot s + 7 \cdot t = 1$

$3 \cdot s = 1 - 7 \cdot (t)$ 에서

$\Rightarrow 3 \cdot s \equiv 1 \pmod 7$ 가 성립하므로 3, 7에 EEA 적용.

r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
3	7	3	1	0	1	0	1	0
7	3	1	0	1	-2	1	0	1
3	1	0	1	-2	7	0	1	-3
1	0		**-2**	7		**1**	-3	

$\gcd(3,7) = 3 \cdot (-2) + 7 \cdot (1) = 1$

$s = -2$ 인데 나머지는 양수여야 하므로

$-2 + 7 = 5$. 따라서 답은 5.

① 페르마 소정리 문제풀이

$9^{150} \pmod{13}$

$= 3^{300} \pmod{13}$

$= 3^{12 \times 25} \pmod{13}$

$\equiv 1 \pmod{13}$ $\quad (\because 3^{12} \equiv 1 \pmod{13})$

② 오일러 정리 문제풀이

$7^{10} \pmod{18}$

$\varphi(18) = 6$ $\{1, 5, 7, 11, 13, 17\}$

$= 7^6 \times 7^4 \bmod 18$

$= 7^4 \bmod 18$

$= 2401 \bmod 18$

$\equiv 7 \bmod 18$

③ 제곱-곱 연산 방법

$a^{13} = a^{1101_{(2)}}$

① 1
② 10 ⇒ 11 ↙ left bitshift.
③ 110 ↙
④ 1100 ⇒ 1101

1. $a^{10} = (a^1)^2 \Rightarrow a^{11} = (a^1)^2 \times a$
2. $a^{110} = (a^{10})^2$
3. $a^{1100} = (a^{110})^2 \Rightarrow a^{1101} = (a^{110})^2 \times a$.

예시) $13^{17} \bmod 37$.

$17_{(10)} = 10001_{(2)}$ 이므로 $13^{17} \bmod 37 = 13^{10001_{(2)}} \bmod 37$ 이다.

MSB → $a_5 = 1$, $y \equiv 13 \bmod 37$

$a_4 = 0$, $y \equiv 13^2 \equiv 21 \bmod 37$

$a_3 = 0$, $y \equiv 21^2 \equiv 34 \bmod 37$

$a_2 = 0$, $y \equiv 34^2 \equiv 9 \bmod 37$

$a_1 = 1$, $y \equiv 9^2 \times 13 \equiv 17 \bmod 37$.

$\therefore 13^{17} \equiv 17 \bmod 37$.