

## 정수론 12강 페르마의 소정리 (Fermat's Little Theorem)

$$a \cdot x \equiv c \pmod{m} \quad \gcd(a, m) = g \mid c \Rightarrow x \equiv x_0 + k \cdot \frac{m}{g} \pmod{m}$$

$k = 0, \dots, g-1$  ( $\because$   $g$ 번 이상 더하면 같은 값이 나오면서 순환한다.)

정수:  $-\infty, \dots, \infty \Rightarrow$  무한집합  $a + a + a + \dots \equiv \boxed{?}$

합동식  $\pmod{m}$ :  $0, \dots, m-1 \Rightarrow m$ 개의 숫자  $\Rightarrow$  유한집합

$$a + a + \dots + a \equiv \boxed{?} \pmod{m}$$

$$a + (\underbrace{a + \dots + a}_{m \text{ 개}}) \equiv a \pmod{m}$$

$$a + m \cdot a \equiv a + 0 \cdot a \equiv a \pmod{m}$$

$$4 + \underbrace{4 + 4 + 4}_{4 \times 3} \equiv 4 \pmod{12}$$

$$4 \times 3 \equiv 0 \pmod{12}$$

$$a + k \cdot a \equiv a \pmod{m}$$

$$m \mid ka$$

$$a \cdot a \cdot \dots \cdot a \equiv a \pmod{m}$$

$$\underline{a^n} \equiv \underline{a} \pmod{m}$$

$$a^2 \equiv 1 \pmod{m}$$

$$\Rightarrow a^{2+1} \equiv a \pmod{m}$$

$$\downarrow$$

$$2+1$$

\* 페르마의 소정리

$$\underline{a^{p-1} \equiv 1 \pmod{p}} \quad \text{단, } p \text{는 소수이고, } a \not\equiv 0 \pmod{p}$$

pf) \* Thm.  $p$ 는 소수,  $a$ 를  $a \not\equiv 0 \pmod{p}$ 인 정수라고 할 때,

$$a, 2a, 3a, 4a, \dots, (p-1)a \pmod{p} \text{ 와}$$

순서를 무시하면 같은 목록이다.

ex)  $p=7, a=3$

$$9 \equiv 2 \pmod{7} \quad 12 \equiv 5 \pmod{7} \Rightarrow 0+5=5 \pmod{7}$$

$$3, \underline{2 \cdot 3}, \underline{3 \cdot 3}, \underline{4 \cdot 3}, \underline{5 \cdot 3}, \underline{6 \cdot 3} \pmod{7}$$

$$\underline{3}, \underline{6}, \underline{2}, \underline{5}, \underline{1}, \underline{4}$$

pf)  $0a, 2a, \dots, \underline{(p-1)a} \Rightarrow$  총  $p-1$  개  $p=2$

$$a \not\equiv 0 \quad \underline{ka} \equiv 0 \pmod{p} \Rightarrow \underline{p \mid ka} \quad \underline{p \nmid k} \text{ or } \underline{p \mid a}$$

$$a \not\equiv 0 \pmod{p} \Rightarrow \underline{p \nmid a} \quad \underline{p \nmid ka}$$

$$\pmod{p} \quad \underline{ia} \not\equiv \underline{ja} \pmod{p} \quad i \neq j$$

$$1, \dots, p-1 \Rightarrow p-1 \text{ 개} \quad 1 \leq i, j \leq p-1$$

$$i \cdot a - j \cdot a \equiv 0 \pmod{p}$$

$$\Rightarrow p \mid i \cdot a - j \cdot a = a \cdot (i - j)$$

$$\Rightarrow p \mid i - j \quad |i - j| < p-1 \quad i - j = 0 \quad (i = j)$$

\* 페르마의 소정리

$$a \not\equiv 0 \pmod{p}, \quad a^{p-1} \equiv 1 \pmod{p}$$

pf)  $a \quad 2a \quad 3a \quad \dots \quad (p-1)a \quad a \cdot 2a \cdot \dots \cdot (p-1)a$

$$\Rightarrow 1 \quad 2 \quad 3 \quad \dots \quad (p-1) \quad \equiv 1 \cdot 2 \cdot \dots \cdot (p-1) \pmod{p}$$

$$a \cdot 2a \cdot \dots \cdot (p-1)a \equiv \{1 \cdot 2 \cdot \dots \cdot (p-1)\} a^{p-1}$$

$$\equiv \{1 \cdot 2 \cdot \dots \cdot (p-1)\} \pmod{p}$$

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

\* 역원

\* 소수 p에 대해  $a^{-1}$ 는 존재한다.  $a \not\equiv 0 \pmod{p}$

$$a \cdot \textcircled{x} \equiv \textcircled{1} \pmod{p}$$

$$\gcd(a, p) = 1 \Rightarrow \text{해가 존재}$$

$$p \text{는 소수} \quad a \not\equiv p \not\equiv 0 \pmod{p}$$

$$2^{123456788} \equiv 1 \pmod{123456789}$$

$$2^{\textcircled{p-1}} \not\equiv 1 \pmod{\textcircled{p}} \quad \text{소수}$$

$$\Rightarrow \text{양호} \quad (\text{나}) \quad (\text{상대})$$