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

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

$k = 0, \cdots, g-1$ (∵ g번 이상 더하면 같은 값이 나오면서 순환한다.

정수 : $-\infty, \cdots, \infty$ ⇒ 무한집합 $a+a+a+a+\cdots \equiv$?

합동식 $(\bmod m)$: $0, \cdots, m-1$ ⇒ m개의 숫자 ⇒ 유한집합

$a+a+\cdots+a \equiv$? $\pmod m$

$a + (\underbrace{a+\cdots+a}_{m개}) \equiv a \pmod m$

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

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

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

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

$m \mid ka$

$a \cdot a \cdot \cdots \cdot a \equiv a \pmod m$

$a^n \equiv a \pmod m$ $\qquad a^2 \equiv 1 \pmod m$

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

↳ $?+1$

* 페르마의 소정리

$a^{p-1} \equiv 1 \pmod p$ 단, p는 소수이고, $a \not\equiv 0 \pmod p$

pf) * Thm. p를 소수, a를 $a \not\equiv 0 \pmod p$ 인 정수라고 할 때,

$a, 2a, 3a, 4a, \cdots, (p-1)a \pmod p$ 와

$1, 2, 3, 4, \cdots, (p-1)$ 은

순서를 무시하면 같은 목록이다.

ex) $p=7$, $a=3$

$9 \equiv 2 \pmod 7$ $\quad 12 \equiv 7+5 \equiv 0+5 \equiv 5 \pmod 7$

$3, 2\cdot 3, 3\cdot 3, 4\cdot 3, 5\cdot 3, 6\cdot 3 \pmod 7$

$3, 6, 2, 5, 1, 4$

$p=2$

pf) $0a$ $2a$ $\cdots$ $(p-1)a$ ⇒ 총 $p-1$ 개

$a \not\equiv 0$ $ka \equiv 0 \pmod p$ ⇒ $p \mid ka$ $\quad p \nmid k$ or $p \mid a$

$a \not\equiv 0 \pmod p \Rightarrow p \nmid a$ $\quad p \mid ka$

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

$1, \sim, p-1$ ⇒ $p-1$ 개 $\quad 1 \le i, j \le p-1$

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

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

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

* 페르마의 소정리
$a \not\equiv 0 \pmod p$, $a^{p-1} \equiv 1 \pmod p$

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

$\Rightarrow 1 \quad 2 \quad 3 \quad \cdots \quad (p-1)$ $\quad \equiv 1 \cdot 2 \cdot \cdots \cdot (p-1) \pmod p$

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

$\equiv 1 \cdot 2 \cdots (p-1) \pmod p$ $\quad a^{p-1} \equiv 1 \pmod p$

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

$a \cdot X \equiv 1 \pmod p$

$\gcd(a, p) = 1 \mid 1 \Rightarrow$ 해가 존재

p는 소수 $\quad a \not\equiv p \not\equiv 0 \pmod p$

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

$2^{p-1} \not\equiv 1 \pmod p$

$\Rightarrow$ ✿암호 (나) (상대)