

1.1 Introduction	2
1.2 Divisibility	3
1.3 Primes	8
2.1 Congruences	13
2.2 Solutions of Congruences	21
2.3 The Chinese Remainder Theorem	22
2.5 Public-Key Cryptography	25
2.7 Prime Modulus	27
2.8 Primitive Roots and Power Residues	30
2.9 Congruences of Degree Two, Prime Modulus	42

Ch 01. Divisibility

1.1 Introduction

- ① irrational number : $\sqrt{2}$, π , ...
- ② Fermat's last theorem (not yet been proved)
(1601-1665)
 $x^n + y^n = z^n$ (n 은 3이상의 정수) 를 만족하는 자연수 x, y, z 는 없다.
- ③ Because it's relatively easy to make conjectures in number theory,
the person whose name gets attached to a problem has often made a lesser
contribution than the one who later solves it.
- ④ 2 basic principles
1st: 공집합이 아닌 모든 자연수 집합은 최소인 원소를 가지고 있다.
2nd: 1을 포함하고 있고, n 을 포함하고 있다면 $n+1$ 을 포함하고 있는
자연수 집합은 모든 자연수를 포함하고 있다.
- ⑤ Difficulty of Assertion and Proof
A simple statement "There is an integer with some particular property"
Not simple statement "All numbers possess a certain property"
- ⑥ \mathbb{Z} 정수집합 \mathbb{Q} 유리수집합 \mathbb{R} 실수집합 \mathbb{C} 복소수집합

1.2 Divisibility

Def 1.1 정수 b , 0 이 아닌 정수 a 에 대하여, $b = ax$ 를 만족하는
정수 x 가 존재한다면, 이를 ' b 가 a 로 나누어 떨어진다'고 하고,
 $a|b$ 라 나타낸다. 나누어 떨어지지 않는 경우는 $a \nmid b$ 로 나타낸다.
 $a|0$ 은 0 이 아닌 모든 정수 a 에 대하여 항상 성립.

$$a^k|b : a^k|b \text{ 이지만 } a^{k+1} \nmid b$$

- Thm 1.1
- (1) $a|b \rightarrow a|bc$
 - (2) $a|b \& b|c \rightarrow a|c$
 - (3) $a|b \& a|c \rightarrow a|(bx+cy)$
 - (4) $a|b \& b|a \rightarrow a = \pm b$
 - (5) $a|b \& a>0, b>0 \rightarrow a \leq b$
 - (6) $m \neq 0 \rightarrow (a|b \Leftrightarrow ma|m b)$

Thm 1.2 a, b 는 정수. $a > 0$.에 대하여
Division
Algorithm
 $b = qa + r$ ($0 \leq r < a$) 를 만족하는 유일한 정수 q 와 r 이 존재하고,
 $a \nmid b$ 인 경우에는 $0 < r < a$ 이다.

Def 1.2 $a|b$ & $a|c$ 일 때 a 를 b 와 c 의 공약수 (Common divisor) 라 한다.
 $b=c=0$ 인 case를 제외하고는 어떤 b,c 에 대해서도 유한 개의 공약수가 존재한다.
그 공약수들 중 가장 큰 수를 최대공약수 (gcd) 라 하고, (b,c) 라 표기한다.
 b_1, b_2, \dots, b_n 의 최대공약수는 (b_1, b_2, \dots, b_n) 이라 표기한다.
 $b=c=0$ 만 아니라면, $(b,c) \geq 1$ 이다.

Thm 1.3 $g = (b,c)$ 이면, $g = (b,c) = bx_0 + cy_0$ 를 만족하는 정수 x_0 와 y_0 가 존재한다.

Pf) l 을 $bx_0 + cy_0$ 꼴의 수들 중 가장 작은 자연수라 하자.
 $l \nmid b$ 라면 $b = lq + r$ ($0 < r < l$) 이다. 이때 $r = b - lq = b - (bx_0 + cy_0)q$ 이므로
 $r = b(1 - qx_0) + c(-y_0q)$ 이고, r 이 ' $bx_0 + cy_0$ ' 꼴이 된다.
 l 이 그런 꼴 중 가장 작은 자연수였으므로 이는 오순. 따라서 $l | b$. 같은 방식으로 $l | c$.
 $g = \text{gcd}(b,c)$ 라 하자. $b = gb'$, $c = gc'$ 라 할 수 있다.
이때 $l = bx_0 + cy_0 = gb'x_0 + gc'y_0 = g(b'x_0 + c'y_0)$ 이고, $g | l$ 이다.
 $g, l > 0$ 이고 $g | l$ 이므로 Thm 1.1의 (5)에 의해 $g \leq l$ 이다.
 $l | b$, $l | c$ 였으므로 l 은 b 와 c 의 공약수. 따라서 g 의 정의에 의해 $g < l$ 은 불가.
 $\therefore g = l = bx_0 + cy_0$. 즉, b 는 정수 x_0, y_0 에 대하여 $bx_0 + cy_0$ 꼴의 수들 중 가장 작은 자연수.

Thm 1.4 $g = (b,c)$ 인 g 를 다음과 같은 두 가지 방법으로 표현할 수 있다.

- (1) g 는 정수 x, y 로 만들 수 있는 $bx + cy$ 중 가장 작은 자연수이다.
- (2) g 는 모든 공약수들로 나누어지는 양의 공약수이다.

Thm 1.5 0이 아닌 정수 b_1, b_2, \dots, b_n 에 대하여, g 가 이들의 gcd 라면 다음을 만족하는 정수 d_1, d_2, \dots, d_n 이 존재한다.

$$g = (b_1, b_2, \dots, b_n) = \sum_{j=1}^n b_j d_j$$

또한, 이러한 g 는 모든 가능한 $\sum_{j=1}^n b_j d_j$ 의 수들 중 가장 작은 자연수이다.

Thm 1.6 양의 정수 m 에 대하여, $(ma, mb) = m(a, b)$ 이다.

$$\begin{aligned} \text{Pf)} \quad (ma, mb) &= \text{least positive value of } ma+mb \\ &= m \cdot \{ \text{least positive value of } ax+by \} \\ &= m(a, b) \end{aligned}$$

Thm 1.7 $d | a, d | b, d > 0$ 이면, $\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d}(a, b)$ 이다.

또한, $(a, b) = g$ 이면, $\left(\frac{a}{g}, \frac{b}{g}\right) = 1$ 이다.

Thm 1.8 $(a, m) = (b, m) = 1$ 이면, $(ab, m) = 1$ 이다.

$$\begin{aligned} \text{Pf)} \quad \left(\begin{array}{l} ax_0 + my_0 = 1 \\ bx_1 + my_1 = 1 \end{array} \right) &\Rightarrow \underline{ax_0 + my_0 = b x_1 + my_1 = 1} \\ \therefore ax_0 \times bx_1 &= (-my_0) \times (-my_1) = (-m(y_0 y_1)) + m^2 y_0 y_1 = (-m^2 y_0 y_1) \\ \therefore abx_0 x_1 + my_2 &= 1 \Rightarrow ab \square + m \square \text{의 수 중 가장 작은 자연수} \\ \therefore (ab, m) &= 1 \end{aligned}$$

Def 1.3 $(a, b) = 1$ 인 a 와 b 를 relatively prime (상수소) 이라 한다.

* Thm 1.9 $(a, b) = (b, a) = (a, -b) = (a, b+ax)$ (x 는 모든 정수)

Pf) $(a, b) = d, (a, b+ax) = g$

$$d = ax_0 + by_0 = ax_0 + by_0 - axy_0 + axy_0 = a(x_0 - xy_0) + (b+ax)y_0$$

$(a, b+ax) = g$ 이므로 $g | d$ ⑦

같은, $d | a, d | b$ 이므로 $d | b+ax$. $(a, b+ax) = g$ 이므로 $d | g$ ⑧

⑦과 ⑧에 의해 $g = \pm d$. $d, g > 0$ 이므로 $g = d$. ($\therefore (a, b) = (a, b+ax)$)

Thm 1.10 $c | ab \& (b, c) = 1 \rightarrow c | a$

* Thm 1.11 b, c 는 정수, $c > 0$ 에 대하여

$$\left\{ \begin{array}{ll} b = cq_1 + r_1 & (0 < r_1 < c) \\ c = r_1 q_2 + r_2 & (0 < r_2 < r_1) \\ r_1 = r_2 q_3 + r_3 & (0 < r_3 < r_2) \\ \vdots & \vdots \\ r_{j-2} = r_{j-1} q_j + r_j & (0 < r_j < r_{j-1}) \\ r_{j-1} = r_j q_{j+1} & \end{array} \right. \text{일 때, } (b, c) = r_j \text{ 이다.}$$

또한, 모든 r_i 는 b 와 c 의 linear combination이다.

↳ r_i 는 b 와 c 의 linear combination.

* Thm 1.11은 Thm 1.9의 따름정리.

r_1 도 “ ” .

r_i ($i \geq 3$)는 r_{i-2} 와 r_{i-1} 의 L.C.

$\therefore r_i$ ($i \geq 3$)는 b 와 c 의 L.C.

EX

$$42823 = 42823 \cdot (1) + 6404 \cdot (0)$$

$$6404 = 42823 \cdot (0) + 6404 \cdot (1)$$

$$g_1 = 6$$

$$4369 = 42823 \cdot (1) + 6404 \cdot (-6)$$

$$g_2 = 1$$

$$2040 = 42823 \cdot (-1) + 6404 \cdot (7)$$

$$g_3 = 2$$

$$289 = 42823 \cdot (3) + 6404 \cdot (-20)$$

$$g_4 = 1$$

$$M = 42823 \cdot (-22) + 6404 \cdot (147)$$

Def 1.4

0 이 아닌 정수 a_1, a_2, \dots, a_n 에 대하여, $a_i \mid b$ ($i=1, 2, \dots, n$)인 b 가 존재하고, 그 중 가장 작은 양의 정수를 lcm (least common multiple) 이라고 하되, $[a_1, a_2, \dots, a_n]$ 이라 쓴다.

Thm 1.(2) b 가 a_1, a_2, \dots, a_n 의 common multiple 이라면, $[a_1, a_2, \dots, a_n] \mid b$ 이다.

Thm 1.(3) (1) $m > 0$ 이면, $[ma, mb] = m[a, b]$ 이다.

(2) $[a, b] \cdot (a, b) = (ab)$ 이다.

Pf) (1) $[ma, mb] = H$, $[a, b] = h$ 가 정의된다.

$a \mid h$, $b \mid h$ 이므로 $ma \mid mh$, $mb \mid mh$ 이다.

$ma \mid H$, $mb \mid H$ 이므로 $a \mid \frac{H}{m}$, $b \mid \frac{H}{m}$ 이다.

따라서, $H \leq mh$ & $h \leq \frac{H}{m}$ 이고, $H = mh$ 이다.

(2) $(a, b) = 1$ 이라 하자. $a \mid [a, b]$ 이므로 $[a, b] = ma$ 가 표현할 수 있다.

이때 $b \mid ma$ 이므로, $(a, b) = 1$ 이면 $b \mid m$ 이다.

$[a, b] = [a, -b]$ 이므로 a, b 를 양의 정수라 두면 $b \leq m$ 이다. 양변에 a 를 곱해 $ab \leq ma$ 이다.

$[a, b] = ma$ 가 표현되었으므로 $ab \leq ma$ 라면, $(a, b) = 1$ 인 경우 $ab = [a, b]$ 가 될 수 있다.

이제 $(a, b) = g$ ($g > 1$)인 일반적인 경우를 가정하자,

$\left(\frac{a}{g}, \frac{b}{g}\right) = 1$ 이므로 $\left[\frac{a}{g}, \frac{b}{g}\right] \left(\frac{a}{g}, \frac{b}{g}\right) = \frac{a}{g} \cdot \frac{b}{g}$ 이다.

양변에 g^2 을 곱하면 $g \left[\frac{a}{g}, \frac{b}{g}\right] \cdot g \left(\frac{a}{g}, \frac{b}{g}\right) = ab$ 이다, $[a, b] \cdot (a, b) = ab$ 이다.

1.3 Primes

Def 1.5 1보다 큰 정수 P 에 대하여, $d|P$ ($1 < d < P$) 를 만족하는 d 가 있을 때
그러한 P 를 prime number, 소수라 한다. 1보다 큰 정수가 prime이 아닐 때,
그러한 수는 composite number, 합성수라 한다.

Thm 1.4 1보다 큰 모든 정수는 product of primes 로 표현할 수 있다.

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \quad (\text{canonical factoring of } n \text{ into prime powers})$$

"Unique factorization need not hold in a mathematical system."

ex) the class \mathcal{E} of positive even integers.

\mathcal{E} is a multiplicative system.

\Rightarrow product of any two elements in \mathcal{E} being again in \mathcal{E}

'The only numbers we know' are members of \mathcal{E} .

$\Rightarrow 8 = 2 \cdot 4$ is 'composite', 10 is 'prime'.

Thm 1.5 $\Sigma P \mid ab \rightarrow P \mid a \text{ or } P \mid b$

$P \mid a_1 a_2 \cdots a_n \rightarrow P \text{ divides at least one factor } a_i \text{ of the product.}$

Thm 1.6 "Fundamental theorem of arithmetic / Unique factorization theorem"

(1) The factoring of any integer $n > 1$ into primes is unique.

= 소인수 분해는 유일하다.

기호학

$$a = \prod_p p^{\alpha(p)}$$

$$(a, b) = \prod_p p^{\min(\alpha(p), \beta(p))}$$

$$[a, b] = \prod_p p^{\max(\alpha(p), \beta(p))}$$

(2) 어떤 수를 n^2 꼴로 나눌 수 있을 때, 이를 square라 한다.

어떤 수를 나눌 수 있는 가장 큰 square가 1 뿐인 때,

이런 수를 square-free라고 한다. 이는 모든 exponent $\alpha(p)$ 가 0 또는 1 뿐인 경우를 말한다.

여기서, P 가 소수라면 $p^k \mid a \Leftrightarrow k = \alpha(p)$ 이다.

Thm 1.11 Euclid. The number of primes is infinite.

Thm 1.12 There are arbitrarily large gaps in the series of primes.

어떤 양의 정수 n 에 대해서도, n 개의 연속된 짝수수가 존재한다.

pf)

임의의 양의 정수 k 에 대해 아래의 연속된 숫자들의 차를 고려하면,

$$(k+1)! + 2, (k+1)! + 3, (k+1)! + 4, \dots, (k+1)! + k+1$$

' $(k+1)! + j$ ' 꼴의 수 ($2 \leq j \leq k+1$)는 모두 j 로 나누어 떨어진다.

기호학

x 를 초과하지 않는 prime의 개수 $\Rightarrow \pi(x)$

Q. 이름이 왜 π ? Because of the irregular occurrence of the primes.

Thm 1.19 2보다 큰 모든 실수 y 에 대하여, 다음이 성립한다.

$$\sum_{p \leq y} \frac{1}{p} > \log \log y - 1$$

pf) $\prod_{p \leq y} \left(1 - \frac{1}{p}\right)^{-1} = \prod_{p \leq y} \frac{1}{1 - \frac{1}{p}}$ 에 대하여, 기하급수에 의해

$$\frac{1}{1 - \frac{1}{p}} = 1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \dots \text{ 이므로}$$

$\prod_{p \leq y} \frac{1}{1 - \frac{1}{p}} = \prod_{p \leq y} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \dots\right)$ 이다. 여기서 우변은

y 이하의 소수들로만 이루어진 모든 수들의 역수의 합 이므로

$$\prod_{p \leq y} \left(1 - \frac{1}{p}\right)^{-1} \geq \sum_{n=1}^{[y]} \frac{1}{n} \text{이다. } (\because \prod_{p \leq y} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \dots\right) \geq \sum_{n=1}^{[y]} \frac{1}{n})$$

$$\sum_{n=1}^{[y]} \frac{1}{n} = 1 + \frac{1}{2} + \frac{1}{3} + \dots > \int_1^{[y]+1} \frac{1}{x} dx = \ln([y]+1) \text{ 이고}$$

구불+천법

$$\ln([y]+1) > \ln[y] \text{ 이므로}$$

$$\therefore \prod_{p \leq y} \left(1 - \frac{1}{p}\right)^{-1} \geq \sum_{n=1}^{\lfloor y \rfloor} \frac{1}{n} > \ln[y] \quad \dots \quad (7)$$

⑦의 양변에 ln 취하면

$$\text{증명: } \ln\left(\prod_{p \leq y} \left(1 - \frac{1}{p}\right)^{-1}\right) = \sum_{p \leq y} \ln\left(1 - \frac{1}{p}\right)^{-1} = \sum_{p \leq y} \ln\left(\frac{1}{1 - \frac{1}{p}}\right)$$

$$\text{우변} = \ln(\ln[g])$$

$$\sum_{p \in y} \ln\left(\frac{1}{1-\frac{1}{p}}\right) > \ln(\ln[g])$$

$$\textcircled{B}: \ln\left(\frac{1}{1-\frac{t}{P}}\right) = \ln 1 - \ln\left(1 - \frac{t}{P}\right) = \int_{1-\frac{t}{P}}^1 \frac{1}{x} dx$$

∴ ①은 평균값 정의에 의해

$$\frac{1}{P} = \frac{1}{P} \cdot \frac{1}{1} < \int_{1-\frac{1}{P}}^1 \frac{1}{x} dx < \frac{1}{P} \cdot \frac{1}{1 - \frac{1}{P}} = \frac{1}{P-1}$$

일반
높이
일반
높이

따라서 $\sum_{p \leq y} \frac{1}{p} < \sum_{p \leq y} \ln\left(\frac{1}{1-\frac{1}{p}}\right) < \sum_{p \leq y} \frac{1}{p-1}$

이걸 ②에 다시 적용하면

$$\sum_{p \leq y} \frac{1}{p-1} > \sum_{p \leq y} \ln\left(\frac{1}{1-\frac{1}{p}}\right) > \ln(\ln[y])$$

$$\therefore \sum_{p \leq y} \frac{1}{p-1} > \ln(\ln[y])$$

$$\frac{1}{p-1} = \frac{p-1+1}{p(p-1)} = \frac{p-1}{p(p-1)} + \frac{1}{p(p-1)} = \frac{1}{p} + \frac{1}{p(p-1)}$$

$$\therefore \sum_{p \leq y} \frac{1}{p-1} = \sum_{p \leq y} \frac{1}{p} + \sum_{p \leq y} \frac{1}{p(p-1)}$$

$$\sum_{p \leq y} \frac{1}{p} + \left| \sum_{p \leq y} \frac{1}{p-1} - \sum_{p \leq y} \frac{1}{p} \right| > \ln \ln y + \ln(\ln[y]) - \ln \ln y$$

(1) > 0 0 > > -1

따라서, $\sum_{p \leq y} \frac{1}{p} > \log \log y - 1$

Ch02. Congruences

2.1 Congruences

Def 2.1 0이 아닌 정수 m 이 $a-b$ 를 나누는 때, 이를 a 는
 $a \equiv b \pmod{m}$ 이라 한다. m 이 $a-b$ 를 나누지 못할 때,
이를 a 는 $a \not\equiv b \pmod{m}$ 이라 한다.

Thm 2.1 $a, b, c, d \geq 0$ 정수.

- (1) $a \equiv b \pmod{m} \iff b \equiv a \pmod{m} \iff a-b \equiv 0 \pmod{m}$
- (2) $a \equiv b \pmod{m} \wedge b \equiv c \pmod{m} \rightarrow a \equiv c \pmod{m}$
- (3) $a \equiv b \pmod{m} \wedge c \equiv d \pmod{m} \rightarrow a+c \equiv b+d \pmod{m}$
- (4) $a \equiv b \pmod{m} \wedge c \equiv d \pmod{m} \rightarrow ac \equiv bd \pmod{m}$
- (5) $a \equiv b \pmod{m} \wedge d|m \wedge d > 0 \rightarrow a \equiv b \pmod{d}$
- (6) $a \equiv b \pmod{m} \wedge c > 0 \rightarrow ac \equiv bc \pmod{mc}$

Thm 2.2 모든 짜수가 짝수인 대량함수 $f(x)$ 에 대하여,
 $a \equiv b \pmod{m}$ 이면 $f(a) \equiv f(b) \pmod{m}$ 이다.

Thm 2.3 (1) $ax \equiv ay \pmod{m} \iff x \equiv y \pmod{\frac{m}{(a,m)}}$

(2) $ax \equiv ay \pmod{m} \wedge (a,m)=1 \rightarrow x \equiv y \pmod{m}$

(3) $x \equiv y \pmod{m_1} \wedge x \equiv y \pmod{m_2} \wedge \dots \wedge x \equiv y \pmod{m_r}$
 $\iff x \equiv y \pmod{[m_1, m_2, \dots, m_r]}$

~~Def~~

Def 2.2 $x \equiv y \pmod{m} \Leftrightarrow y$ is a residue of x modulo m .

$y \equiv x_i \pmod{m}$ 을 만족하는 x_i 가 $\{x_1, x_2, \dots, x_m\}$ 라는 집합에

만 1개 빼면 없을 때, 이러한 집합 $\{x_1, x_2, \dots, x_m\}$ 을

Complete Residue System이라 한다.

완전 잉여계

Thm 2.4 $b \equiv c \pmod{m} \rightarrow (b, m) = (c, m)$

Pf) $c = b + mx \rightarrow (b, m) = (b + mx, m)$

~~Def~~

Def 2.3 다음 조건을 만족하는 정수 r_i 들의 집합 $\{r_1, r_2, \dots, r_k\}$ 을 Reduced Residue System이라 한다.

① 모든 r_i 는 m 과 서로소. $(r_i, m) = 1$.

기약잉여계

② 모든 r_i 는 서로 합동이 아님. $r_i \not\equiv r_j \pmod{m}$

③ Complete Residue System 내에서 m 과 서로소인 모든 수가

집합 내 어떤 r_i 를 m 에 대하여 합동.

~~Def~~

R.R.S는 C.R.S에서 m 과 서로소가 아닌 수들을 제외하여 얻을 수 있다.

m 에 대한 모든 R.R.S는 원소 개수가 같고, $\phi(m)$ 으로 표기한다.

Thm 2.5

R.R.S의 원소 개수를 뜻하는 $\phi(m)$ 은 'm 이하의 m과 서로소인 정수의 개수'와 같다.

* Thm 2.6 $(a, m) = 1$ 인 임의의 a 에 대하여, $\{r_1, r_2, \dots, r_n\}$ 이 C.R.S / R.R.S 인 경우,
 $\{a \cdot r_1, a \cdot r_2, \dots, a \cdot r_n\}$ 도 ~~또한~~ C.R.S / R.R.S이다.

* Thm 2.1 [Fermat's Theorem]

소수 p , 정수 a 가 주어지면, $p \nmid a$ 이면 $a^{p-1} \equiv 1 \pmod{p}$ 이다.

\rightarrow Thm 2.8에 의해 자동 증명

* Thm 2.8 [Euler's Generalization]

$(a, m) = 1$ 이면, $a^{\phi(m)} \equiv 1 \pmod{m}$ 이다.

pf) modulo m 에 대하여 정합 $\{r_1, r_2, \dots, r_{\phi(m)}\}$ 을 R.R.S가 할 때, $(a, m) = 1$ 이면
 Thm 2.6의 $\{a \cdot r_1, a \cdot r_2, \dots, a \cdot r_{\phi(m)}\}$ 도 R.R.S이다. 이에 대해 설명한다.

$$\prod_{j=1}^{\phi(m)} (a \cdot r_j) \equiv \prod_{i=1}^{\phi(m)} r_i \pmod{m}$$

$$\Leftrightarrow a^{\phi(m)} \cdot \prod_{j=1}^{\phi(m)} r_j \equiv \prod_{i=1}^{\phi(m)} r_i \pmod{m}$$

$$\Leftrightarrow a^{\phi(m)} \equiv 1 \pmod{m} \quad (\because \gcd(\prod_{i=1}^{\phi(m)} r_i, m) = 1)$$

Thm 2.3 (\Rightarrow)

Thm 2.6 증명

① C.R.S

보여야 하는 것

$$\{r_1, r_2, \dots, r_n\} \text{이 C.R.S} \rightarrow \{a \cdot r_1, a \cdot r_2, \dots, a \cdot r_n\} \text{이 C.R.S}$$

$\{r_1, r_2, \dots, r_n\}$ 이 C.R.S 이므로, $a \cdot r_i$ 는 집합 Y 에 임의의 r_j 와 합동.

(\because CRS는 임의의 정수 y 에 대하여 합동인 원소가 무한 (개 존재하는 집합)

$$\begin{array}{c} X \\ \left(\begin{array}{l} r_1 \\ r_2 \\ \vdots \\ r_n \end{array} \right) \\ \xrightarrow{f} Y \\ \left(\begin{array}{l} a \cdot r_1 \\ a \cdot r_2 \\ \vdots \\ a \cdot r_n \end{array} \right) \end{array}$$

$a \cdot r_i \equiv r_j \pmod{m}$ 이므로 외측 그림과 같이
집합 X 에서 집합 Y 로의 함수 f 를 정의할 수 있음.
 $f: X \rightarrow Y, f(x) \equiv x \pmod{m}$

i) $a \cdot r_i \equiv a \cdot r_j \pmod{m}$ 이면 $\gcd(a, m) = 1$ 이므로 양변에 a^{-1} 곱셈.

$$a^{-1} \cdot a \cdot r_i \equiv a^{-1} \cdot a \cdot r_j \pmod{m} \Leftrightarrow r_i \equiv r_j \pmod{m}$$

$\therefore r_i \not\equiv r_j \pmod{m}$ 이면 $a \cdot r_i \not\equiv a \cdot r_j \pmod{m}$ 이다. (대우명제)

$\therefore f$ 는 단사함수 (일대일함수)

ii) X 와 Y 의 원소 개수 동일 & f 는 단사함수

$\rightarrow f$ 는 전사함수. (f 는 전단사, 일대일 대응)

$\therefore f$ 가 전단사함수이므로 X 가 CRS라면 Y 도 CRS.

결론

② R.R.S

보여야 하는 것

$$\{r_1, r_2, \dots, r_n\} \text{의 R.R.S} \rightarrow \{a \cdot r_1, a \cdot r_2, \dots, a \cdot r_n\} \text{의 R.R.S}$$

$\{r_1, r_2, \dots, r_n\}$ 의 R.R.S 이면 $(r_i, m) = 1$.

\gcd 가 1이므로 아래와 같이 나타낼 수 있음.

$$\begin{cases} (a, m) = 1 \\ (r_i, m) = 1 \end{cases} \Rightarrow \begin{cases} ax_0 + my_0 = 1 \\ r_i x_i + my_i = 1 \end{cases}$$

$$\Rightarrow ax_0 \cdot r_i x_i = (1 - my_0) \cdot (1 - my_i) = 1 - m(y_0 + y_i) + m^2 y_0 y_i = (-my_2)$$

$$\therefore ax_0 \cdot r_i x_i = (-my_2) \Leftrightarrow \underbrace{ar_i(x_0 x_i) + my_2}_\text{선호정수의 least positive integer} = 1.$$

$$\therefore (ar_i, m) = 1.$$

모든 r_i 에 대하여 $(a \cdot r_i, m) = 1$ 이므로,

CRL에서와 마찬가지로 함수 f 를 정의하면

$$\{a \cdot r_1, a \cdot r_2, \dots, a \cdot r_n\} \text{도 R.R.S}$$

결론

Thm 2.9 $(a, m) = 1$ 이면 $a \not\equiv 1 \pmod{m}$ 인 x 가 C.R.S에 오직 1개 풀이 존재한다.
 $(a, m) > 1$ 이면, 그런 x 가 존재하지 않는다. (해의 존재 및 유일성)
 만약 m 이 소수라면? $1 \leq a \leq p-1$ 인 a 에 대해 풀이 $(a, p) = 1$ 이므로
 이때 $a \not\equiv 1 \pmod{p}$ 를 만족하는 x 가 C.R.S에 유일하다. (역법의 유일성)

Pf) $(a, m) = 1$ 이면 $ax + my = 1$ 을 만족하는 x 와 y 가 존재한다.
 $ax - 1 = my$ 이므로 $a \not\equiv 1 \pmod{m}$ 인 x 가 존재한다.
 만약 그런 x 가 C.R.S에 x_1, x_2 외에 존재한다면,
 $a x_1 \equiv 1 \pmod{m}$ & $a x_2 \equiv 1 \pmod{m}$ 이므로
 $a x_1 \equiv a x_2 \pmod{m}$ 이고, $(a, m) = 1$ 이므로 $x_1 \equiv x_2 \pmod{m}$ 이다.

기호화 $a \not\equiv 1 \pmod{m}$ 은 a 의 mod m 에서의 곱의 역원이
 x 의 residue임을 의미한다. 이때는 역원을 \bar{a} 라 표기한다.

Lemma 2.10 소수 p 에 대하여, $x^2 \equiv 1 \pmod{p} \iff x \equiv \pm 1 \pmod{p}$
 (= 자기 자신을 역원으로 가지는 것 (또는 -1 배에 같다.)

Thm 2.11

[Wilson's theorem]

p 가 소수이면 $(p-1)! \equiv -1 \pmod{p}$ 이다.

pf)

$1 \leq a \leq p-1$ 인 a 를 고려하자. $(a, p) = 1$ 이므로
 $a \not\equiv 1 \pmod{p}$ 인 x 가 $\{1, 2, \dots, p-1\}$ 에 오직 1개 존재한다.

이때, \pmod{p} 에 대해 자기자신을 역원으로 갖는 원소는

$$\begin{aligned} x^2 &\equiv 1 \pmod{p} \\ \Leftrightarrow x^2 - 1 &\equiv 0 \pmod{p} \\ \Leftrightarrow (x+1)(x-1) &\equiv 0 \pmod{p} \\ \Leftrightarrow P &\mid (x+1) \text{ or } P \mid (x-1) \\ \Leftrightarrow x &\equiv 1 \text{ or } x \equiv p-1 \pmod{p} \end{aligned} \quad \left. \begin{array}{l} \text{이므로} \\ \text{1과 } p-1 \text{ 뿐이다.} \end{array} \right\}$$

이때, 나머지 원소들 $\{2, 3, \dots, p-2\}$ 은

① 자기자신이 역원이 아니면서 ② 서로 역원 관계로 짝을 이룬다.

$$\begin{aligned} \text{따라서, } (p-1)! &= (1 \times 2 \times 3 \times \cdots \times (p-2) \times (p-1)) \\ &= 1 \times [\text{역원 관계인 쌍들의 곱}] \times (p-1) \\ &= p-1 \\ &\equiv -1 \pmod{p} \end{aligned}$$

Thm 2.12 p 가 소수일 때, $x^2 \equiv -1 \pmod{p}$ 는 $p=2$ or $p \equiv 1 \pmod{4}$ 일 경우에만 해를 가진다.

pf) $p=2$ 일 때는 $x=1$ 로 해를 가짐.

p 가 odd prime 이라면, Wilson's theorem을 다음과 같이 증명 가능.

$$\left(1 \times 2 \times \cdots \times \frac{p-1}{2}\right) \times \left(\frac{p+1}{2} \times \frac{p+3}{2} \times \cdots \times (p-2) \times (p-1)\right) \equiv -1 \pmod{p}$$

$$\Leftrightarrow \prod_{j=1}^{\frac{p-1}{2}} j(p-j) \equiv -1 \pmod{p}$$

$$\Leftrightarrow \prod_{j=1}^{\frac{p-1}{2}} (-j^2) \equiv -1 \pmod{p}$$

$$\Leftrightarrow (-1)^{\frac{p-1}{2}} \cdot \left(\prod_{j=1}^{\frac{p-1}{2}} j\right)^2 \equiv -1 \pmod{p}$$

이때 $\frac{p-1}{2}$ 이 even 이라면, 즉 $\frac{p-1}{2} = 2k \Leftrightarrow p = 4k+1$ 이라면

$\left(\prod_{j=1}^{\frac{p-1}{2}} j\right)^2 \equiv -1 \pmod{p}$ 가 되고, $x = \prod_{j=1}^{\frac{p-1}{2}} j$ 라는 해를 가짐.

거꾸로, $x^2 \equiv -1 \pmod{p}$ 의 양변에 $\frac{p-1}{2}$ 제곱을 해서 증명하면,

$$(x^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod{p} \Leftrightarrow x^{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod{p} \text{이다.}$$

$$x^{p-1} \equiv 1 \pmod{p} \text{ 이므로 } 1 \equiv (-1)^{\frac{p-1}{2}} \pmod{p} \text{이다.}$$

주어진 식의 해 x 가 존재한다면, 그 해에서 주어진 식이 성립하고,

$1 \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$ 는 주어진 식과 동치 이므로 이것도 성립해야 한다.

따라서, $x^2 \equiv -1 \pmod{p}$ 가 해를 가진다면 $p=2$ or $p \equiv 1 \pmod{4}$ 이다.

2.2 Solutions of Congruences

Def

Def 2.4

$\{r_1, r_2, \dots, r_m\}$ 을 mod m에 대한 C.R.S라 할 때,

$f(x) \equiv 0 \pmod{m}$ 의 해의 수는 $f(r_i) \equiv 0 \pmod{m}$ 인 r_i 의 수와 같다.
modulo equation의 해는 CRS 내에서 선택.

$$\text{ex)} \quad x^2 + 1 \equiv 0 \pmod{1} \rightarrow 3\text{개 } 0, 1, -1$$

$$x^2 + 1 \equiv 0 \pmod{5} \rightarrow 3\text{개 } 2, 3, 4$$

$$x^2 - 1 \equiv 0 \pmod{8} \rightarrow 3\text{개 } 1, 3, 5$$

Def 2.5

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 \text{ 를 } \text{정의},$$

$a_n \not\equiv 0 \pmod{m}$ 인 경우 $f(x) \equiv 0 \pmod{m}$ 의 degree는 n이다.

Thm 2.16

$d | m, d > 0$ 이고 $f(x) \equiv 0 \pmod{m}$ 의 해가 u 일 때,

u 는 $f(x) \equiv 0 \pmod{d}$ 의 해이다.

Thm 2.17

$a, b, m (m > 0)$ 이 정수일 때, $g = (a, m)$ 이면

$ax \equiv b \pmod{m}$ 은 $g(b)$ 이면 해를 갖는다.

pf)

$$ax \equiv b \pmod{m} \Leftrightarrow ax - b = my \Leftrightarrow \underbrace{ax + m(-y)}_g = b$$

$g = (a, m) = \text{least positive integer}$

의 배수이면 식 성립!

2.3 The Chinese Remainder Theorem

Thm 2.18

[The Chinese Remainder Theorem]

$\{m_1, m_2, m_3, \dots, m_r\}$ 을 모두 각각 서로소라 하면,
 $\{a_1, a_2, a_3, \dots, a_r\}$ 을 r 개의 임의의 정수라 하면.
 이때, 다음의 연립방정식을 만족하는 해가 존재한다.

$$\begin{aligned}x &\equiv a_1 \pmod{m_1} \\x &\equiv a_2 \pmod{m_2} \\x &\equiv a_3 \pmod{m_3} \\&\vdots \quad \vdots \\x &\equiv a_r \pmod{m_r}\end{aligned}$$

pf)

$\{m_1, m_2, \dots, m_r\}$ 모두 각각 서로소이므로,

$M = m_1 \times m_2 \times \dots \times m_r$ 이 때 하면 $\gcd\left(\frac{M}{m_j}, m_j\right) = 1$ 이다.

여기서 서로소인 두 수 $\frac{M}{m_j}$ 과 m_j 에 대하여

$\frac{M}{m_j} \times y_j \equiv 1 \pmod{m_j}$ 를 만족하는 $\frac{M}{m_j}$ 의 역원 y_j 가 무조건 단 1개 있다.

이때 $x = \sum_{j=1}^r \frac{M}{m_j} \cdot y_j \cdot a_j$ 라 하면, 임의의 j ($1 \leq j \leq r$)에 대해

$\sum_{j=1}^r \frac{M}{m_j} \cdot y_j \cdot a_j \equiv a_j \pmod{m_j}$ 가 성립한다.

$$\text{ex1) } \begin{array}{l} x \equiv 5 \pmod{7} \\ x \equiv 1 \pmod{11} \\ x \equiv 3 \pmod{13} \end{array} \Rightarrow M = \underbrace{7 \times 11 \times 13}_{\text{수식}}$$

$$\therefore x = \sum_{j=1}^3 \frac{M}{m_j} \cdot y_j \cdot a_j$$

$$= \frac{7 \cdot 11 \cdot 13}{7} \cdot 5 \cdot 5 + \frac{7 \cdot 11 \cdot 13}{11} \cdot 4 \cdot 1 + \frac{7 \cdot 11 \cdot 13}{13} \cdot 12 \cdot 3$$

$$= 143 \cdot 25 + 91 \cdot 28 + 11 \cdot 3$$

$$= 889 \pmod{7 \times 11 \times 13}$$

One-to-One Correspondence Between the r-tuples and C.R.S modulo M

$$\begin{aligned}x &\equiv a_1 \pmod{m_1} \\x &\equiv a_2 \pmod{m_2} \\x &\equiv a_3 \pmod{m_3} \\&\vdots \quad \vdots \\x &\equiv a_r \pmod{m_r}\end{aligned}$$

연립합동식에서, $1 \leq i \leq r$ 인 i 에 대해
 a_i 를 $\{1, 2, \dots, m_i\}$ 중 하나,
즉 m_i 에 대한 C.R.S의 원소라 하면,
주어진 연립합동식에서 가능한 (a_1, a_2, \dots, a_r) 의
조합은 총 $m_1 \times m_2 \times \dots \times m_r = M$ 가지이다.

(a_1, a_2, \dots, a_r) 조합을 r -tuple이라 하면, Thm 2.18 CRT에 의해
서로 다른 r -tuple에 대해 서로 다른 해가 존재한다.
즉, m 개의 r -tuple에서 M 개의 서로 다른 해 $(\text{mod } M)$ 가 존재한다.

$$\left[\begin{array}{l} (a_1, a_2, \dots, a_i, \dots, a_r) \text{ } r\text{-tuple A} \\ (a_1, a_2, \dots, a'_i, \dots, a_r) \text{ } r\text{-tuple B} \end{array} \right]$$

하나의 원소만 다른 두개의 r -tuple A와 B가 있다고 하면,
 i 를 제외한 나머지에 대해서는 두 개의 서로 다른 연립합동식에서
 $x \equiv a_k \pmod{m_k}$ 가 같은 해를 가질 수 있음.
하지만 i 에서 $x \equiv a_i \pmod{m_i}$ 와 $x \equiv a'_i \pmod{m_i}$ 는
서로 같은 해를 가질 수 없음.

⇒ 즉, 하나의 a_k 만 다르더라도 해가 달라짐.

큰수 $x \pmod{M}$ 을 표현하는 또 다른 방법!

$M = m_1 \times m_2 \times \dots \times m_r$ 를 두고

x 를 합동인 유일한 연립합동식 시스템으로 표현하는 것!

Thm 2.19 (1) 서로소인 두 정수 m_1 과 m_2 에 대해, 다음이 성립한다.

$$\phi(m_1 \cdot m_2) = \phi(m_1) \cdot \phi(m_2)$$

(2) m 을 $m = \prod_{p|m} p^k$ 으로 소인수 분해할 수 있을 때, 다음이 성립한다.

$$\phi(m) = \prod_{p|m} (p^k - p^{k-1}) = m \prod_{p|m} \left(1 - \frac{1}{p}\right)$$

Pf) $M = m_1 \times m_2$ 를 하자. $(d, M) = 1$ 인 d 를 가정하면,

$$(d, m_1 \cdot m_2) = 1 \text{ 이므로 } (d, m_1) = 1 \& (d, m_2) = 1 \text{ 이다.}$$

$$(d, m_1) = 1 \text{ 이면 } (m_1, d \bmod m_1) = 1 \text{ 이고, 마찬가지로 } (m_2, d \bmod m_2) = 1 \text{ 이다.}$$

여기서 $f: A \rightarrow B$, $f(x) = (x \bmod m_1, x \bmod m_2)$ 인 f 를 정의하면,

$(m_1, m_2) = 1$ 이므로 CRT에 의해 서로 다른 $(x \bmod m_1, x \bmod m_2)$ 조합에 대하여 각각 서로 다른 residue를 가지므로 (\because one-to-one correspondence)

f 는 단사함수이다. ($f(x_1) = f(x_2)$ 이면 $x_1 = x_2$ 이다.)

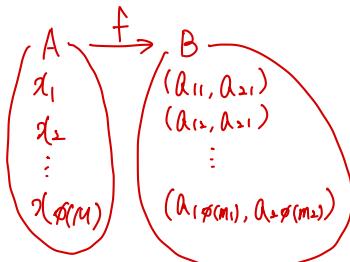
또한 임의의 $(a_1, a_2) \in B$ 에 대해, $(a_1, m_1) = 1 \& (a_2, m_2) = 1$ 이므로

CRT에 의해 $x \equiv a_1 \pmod{m_1}$ & $x \equiv a_2 \pmod{m_2}$ 인 x 가 존재한다.

이 x 는 $x \equiv a_1 \pmod{m_1}$ & $(a_1, m_1) = 1$ 이므로 $(x, m_1) = 1$ 이다.

마찬가지로 $(x, m_2) = 1$ 이므로 $(x, m_1 \cdot m_2) = 1$ 이고, $x \in A$ 이다.

따라서 f 는 전사함수.



$f: A \rightarrow B$ 가 전사함수이므로

$$\phi(m_1 \cdot m_2) = \underbrace{\phi(m_1)}_{x \text{의 개수}} \cdot \underbrace{\phi(m_2)}_{a_1 \text{의 개수}} \cdot \underbrace{\phi(m_2)}_{a_2 \text{의 개수}}$$

2.5 Public-key Cryptography

Lemma 2.22 양의 정수 $m \neq 1$, $(a, m) = 1$ 을 만족하는 a 가 있을 때,
 $\frac{a^k}{a} \equiv 1 \pmod{\phi(m)}$ 을 만족하는 양의 정수 k, \overline{k} 가 있다면
 $a^{\frac{a^k}{a}} \equiv a \pmod{m}$ 이다.

pf) $a\overline{x} \equiv a\overline{y} \pmod{m}$ 이라 하면 다음과 성립한다.

$$m \mid a\overline{x} - a\overline{y} \iff m \mid a(\overline{x} - \overline{y}).$$

$(a, m) = d$ 라 하면, $a = da'$ & $m = dm'$ (while $(a', m') = 1$) 이므로
 위 식에 대입해서 정리하면 아래와 같다.

$$dm' \mid da'(\overline{x} - \overline{y}) \iff m' \mid a'(\overline{x} - \overline{y}) \iff m' \mid \overline{x} - \overline{y} \iff \overline{x} \equiv \overline{y} \pmod{m'}$$

$$m' = \frac{m}{d} = \frac{m}{(a, m)} \text{ 이므로 } \boxed{\overline{x} \equiv \overline{y} \pmod{\frac{m}{(a, m)}}}.$$

\therefore if $(a, m) = 1$ 인 경우, $a\overline{x} \equiv a\overline{y} \pmod{m}$ 이라면 $\overline{x} \equiv \overline{y} \pmod{m}$ 이다.

Thm 2.6의 의해, $(a, m) = 1$ 인 a 에 대하여 $\prod_{j=1}^{\phi(m)} r_j \equiv \prod_{i=1}^{\phi(m)} a \cdot r_i \pmod{m}$ 이다.

$$\prod_{j=1}^{\phi(m)} r_j \equiv a^{\phi(m)} \cdot \prod_{i=1}^{\phi(m)} r_i \pmod{m} \text{ 이고, } \left(\prod_{i=1}^{\phi(m)} r_i, m \right) = 1 \text{ 이므로 } \boxed{a^{\phi(m)} \equiv 1 \pmod{m}} \text{이다.}$$

$$\frac{a^k}{a} \equiv 1 \pmod{\phi(m)} \text{ 이므로 } \frac{a^k}{a} - 1 = r \cdot \phi(m) \text{ 이다.}$$

$r \geq 0, \phi(m) > 0$ 이므로 $r \geq 0$ 이다. 이때, 다음과 성립한다.

$$\boxed{a^{\frac{a^k}{a}} = a \cdot a^{\frac{a^k}{a}-1} \equiv a \cdot a^{r\phi(m)} = a \cdot (a^{\phi(m)})^r \equiv a \cdot 1^r = a \pmod{m}}$$

Public-Key Cryptography with Thm 2.19 & Lemma 2.22

two distinct large primes P_1, P_2 . $m = P_1 \times P_2$

$$\Rightarrow \phi(m) = \phi(P_1 \cdot P_2) = \phi(P_1) \cdot \phi(P_2) = (P_1 - 1)(P_2 - 1) \quad (\because \text{Thm 2.19})$$

$0 < k < \phi(m)$ & $(k, \phi(m)) = 1$ 인 k 에 대하여,

m 과 k 를 공개키로, $P_1, P_2, \phi(m)$ 을 비밀키로 한다.

보내고자 하는 메세지가 있으려고 하자. "Gauss was a genius!"

ASCII 코드를 가지고 G는 011, a는 091, ⋯, !는 033 등으로 변환.

그렇게 변환된 메세지는 $a = 01109111 \dots 115033$ 이 된다.

P_1 과 P_2 가 각각 100자리 짜리를이라고 하면, m 은 200자리 짜릴 것이다. ($\because m = P_1 \times P_2$)

보내고자 하는 메세지 a 는 56자리이기에 $0 < a < m$ 이다.

a 를 보낼 때, 공개키 m 과 k 를 이용해 암호화를 할 수 있다.

보내고자 하는 a 를 k 제곱하여 $a^k \equiv b \pmod{m}$ 인 b 를 보낸다.

b 를 받은 사람은, $k \cdot k \equiv 1 \pmod{\phi(m)}$ 인 양수 k' 를 찾어서,

$0 \leq c < m$ 인 $c \equiv b^{k'} \pmod{m}$ 를 계산한다.

Lemma 2.22에 의해, $c \equiv (a^k)^{k'} \equiv a \pmod{m}$ 이다.

m 을 소인수분해하여야 $\phi(m)$ 을 구할 수 있다.

$\phi(m)$ 은 $\phi(P_1) \times \phi(P_2)$ 를 통해 간접적으로 구해야 하기 때문이다.

200자리 소인수분해는 현실적으로 불가능하므로, 보안성이 흥복된다.

2.7 Prime Modulus

Thm 2.25

$f(x) \equiv 0 \pmod{p}$ 에서 $f(x)$ 의 차수 n 이 $n \geq p$ 이면,

$f(x) = (x^p - x) f(x) + r(x)$ ($r(x)$ 의 차수 $\leq p-1$)가 할 때

$f(x) \equiv 0 \pmod{p}$ 는 '정수 전체'를 해로 가지거나

$r(x) \equiv 0 \pmod{p}$ 와 동일한 해 집합을 가진다.

pf)

페르마의 소정리 (Thm 2.1)에 의해 $x^p - x \equiv 0 \pmod{p}$ 는 모든 정수에 대해 성립한다. 따라서 $f(x)$ 가 만약 $(x^p - x)$ 를 인자로 가진다면 $r(x) = 0$ 이 되어 $f(x) \equiv 0 \pmod{p}$ 는 정수 전체에 대해 성립하게 된다.

$x^p - x \nmid f(x)$ 인 경우, $(x^p - x)g(x) + r(x) \equiv 0 \pmod{p}$ 는 $r(x) \equiv 0 \pmod{p}$ 와 동일한 해를 공유하게 된다.

Thm 2.26

n 차 합동식 $f(x) \equiv 0 \pmod{p}$ 은 최대 n 개의 해를 갖는다.

pf)

i) $n=1$ 일 때

$f(x) = ax+b$ 라 하면 $ax+b \equiv 0 \pmod{p}$ 는

$x \equiv (-b) \cdot a^{-1} \pmod{p}$ 라는 유일한 해를 가짐. 해 개수 $\leq n$.

ii) $n=k$ 일 때 성립한라 가정. \Rightarrow n 차 합동식 $f(x) \equiv 0 \pmod{p}$ 은 최대 n 개의 해.

iii) $n=k+1$ 일 때

① $f(x) \equiv 0 \pmod{p}$ 가 해를 갖지 않을 경우: $0 \leq n \leq k$ 이므로 성립

② $f(x) \equiv 0 \pmod{p}$ 가 해 r 을 가질 경우:

$f(x) \equiv (x-r)g(x) \pmod{p}$ 라 하면 $g(x)$ 의 차수는 k .

$f(x)$ 의 도약을 해를 s 라 하면 $f(s) \equiv (s-r)g(s) \equiv 0 \pmod{p}$ 이면, 이는 $s-r \equiv 0 \pmod{p}$ 이거나 $g(s) \equiv 0 \pmod{p}$.

$s-r \equiv 0 \pmod{p}$ 이면 '도약을 해'가 아닌 거고, $g(s) \equiv 0 \pmod{p}$ 이면

iii)에 의해 그런 s 는 최대 n 개 존재한다. 따라서 이 경우 해는 최대 $k+1$ 개.

Thm 2.29 차수가 n 이고 최고차항의 계수가 1인 합동식 $f(x) \equiv 0 \pmod{p}$ 가

$$\boxed{\text{정학이 } n\text{ 개의 해를 가진다}} \quad \xleftarrow{\text{동치}} \quad \boxed{f(x) \mid x^p - x}$$

i) 정학이 n 개의 해를 가진다 $\rightarrow f(x) \mid x^p - x$

$f(x) \equiv 0 \pmod{p}$ 가 정학히 n 개의 해를 가지므로

$$f(x) \equiv (x - k_1)(x - k_2) \cdots (x - k_n) \pmod{p}$$

Thm 2.1 페르마의 소정리에 의해 모든 정수 x 에 대해 $x^p - x \equiv 0 \pmod{p}$.

$$k_1^p - k_1 \equiv k_2^p - k_2 \equiv \cdots \equiv k_n^p - k_n \equiv 0 \pmod{p} \text{ 이므로}$$

$$f(x) \equiv (x - k_1)(x - k_2) \cdots (x - k_n) \mid x^p - x \quad (\because k_1, k_2, \dots, k_n \text{은 모두 } x^p - x \equiv 0 \pmod{p} \text{의 해})$$

ii) $f(x) \mid x^p - x \rightarrow$ 정학히 n 개의 해를 가진다.

일단 Thm 2.1 페르마의 소정리에 의해 $x^p - x \equiv 0 \pmod{p}$ 는

$$x^p - x \equiv x(x-1)(x-2) \cdots (x-(p-1)) \pmod{p} \text{ 이다.} \quad (\because \text{모든 원소가 해})$$

Thm 2.26에 의해 최대 n 개의 해를 가지는 n 차 합동식 $f(x)$ 는 $x^p - x$ 의 인수이므로

$$f(x) \equiv (x - r_1)(x - r_2) \cdots (x - r_n) \equiv 0 \pmod{n} \text{ 은 정학히 } n \text{개의 해를 가진다.}$$

($\because n$ 차 합동식이 n 개보다 적은 개수의 해를 가지면 $f(x) \mid x^p - x$ 일 수 없다.)

$\Rightarrow 'x^p - x'$ 는 모든 원소 $\{0, 1, \dots, p-1\}$ 을 해로 갖는 특별한 다항식이고,

그런 $x^p - x$ 의 인수인 n 차 다항식 $f(x)$ ($n \leq p$)는 정학히 n 개의 해를 갖는다.

Cor 2.30 $d \mid p-1$ 이면, $x^d \equiv 1 \pmod{p}$ 는 d 개의 해를 가진다.

$d \mid p-1$ 이므로 $dk = p-1$ 인 k 존재.

$x^p - x = x(x^{p-1} - 1) = x(x^{dk} - 1)$ 이고, 인수분해 공식에 의해

$x(x^{dk} - 1) = x(x^d - 1) \{ (x^d)^{k-1} + (x^d)^{k-2} + \dots + (x^d)^1 + (x^d)^0 \}$ 이다.

따라서 $x^d - 1 \mid x^p - x$ 이고, ' $x^p - x$ '의 인수인 d 차 다항식 ' $x^d - 1$ '은, Thm 2.9에 의해 $x^d - 1 \equiv 0 \pmod{p}$ 에서 정확히 d 개의 해를 갖는다.

2.8 Primitive Roots and Power Residues

Def 2.6 $(a, m) = 1$ 을 만족하는 서로소인 두 수 a 와 m 에 대하여,
위수의 정의
 $a^h \equiv 1 \pmod{m}$ 을 만족하는 가장 작은 양의 정수 h 를
' a 의 mod m 에 대한 위수' 라고 한다.

Lemma 2.31 a 가 m 에 서로소여서, mod m 에 대하여 위수 h 를 가지면,

위수의
법에 대한 설명
 $a^k \equiv 1 \pmod{m}$ 을 만족하는 양의 정수 k 는 위수 h 의 배수이다.

$h | k$ 라 하면 $k = h \cdot g$ 라 할 수 있고, h 가 위수라면

$$a^{kg} = (a^h)^g \equiv 1^g \equiv 1 \pmod{m} \text{ 이다.}$$

반대로 $a^k \equiv 1 \pmod{m}$ 이라면, $k = gh + r$ 라 할 때

$$a^k = a^{gh+r} = (a^h)^g \cdot a^r \equiv a^r \pmod{m} \text{ 이고,}$$

$a^r \equiv 1 \pmod{m}$ 이어야 하는데 위수가 h 이므로 $0 \leq r < h$ 인 범위에서 $r=0$ 이다.

따라서 $k = gh + 0$ 이고, $h | k$ 이다.

Cor 2.32 $(a, m) = 1$ 이어서 a 가 m 에 대한 위수 h 를 가지면,

정리 2.8 오일러의 정리에 의해 $a^{\varphi(m)} \equiv 1 \pmod{m}$ 이므로
위한 활용
 h 는 $\varphi(m)$ 의 약수가 된다.

Lemma 2.33 $a^k \bmod m$ 에 대해 위수 h 를 가지면, a^k 는 $\bmod m$ 에 대해 $\frac{h}{(h,k)}$ 를 위수로 갖는다.

pf)

$$(h,k) = d \text{ 가 } \Rightarrow \text{면 } h = dh', k = dk'.$$

$$\left(a^k\right)^{\frac{h}{d}} = \left(a^{dk'}\right)^{h'} = \left(a^{dh'}\right)^{k'} = \left(a^h\right)^{k'} \equiv 1^{k'} \equiv 1 \pmod{m}$$

$(a^k)^{\frac{h}{d}} \equiv 1 \pmod{m}$ 이면, a 의 위수가 h 이므로 $h \mid k$.

$(h,k) = d$ 가 하면 $h = dh'$, $k = dk'$ 이고, $dh' \mid dk'$.

$dh' \mid dk'$ 이면 $h' \nmid k'$ 이고, $(h',k') = 1$ 이며 $h' \mid t$

$h' \mid t \Leftrightarrow \frac{h}{d} \mid t$ 이므로, a^k 을 $\bmod p$ 에 대해 1과 합동이 되게 만드는

모든 t 는 $\frac{h}{d}$ 의 배수.

$\therefore a^k$ 의 $\bmod m$ 에 대한 위수는 $\frac{h}{d}$.

Lemma 2.34 a 의 $\bmod m$ 에 대한 위수가 h , b 의 $\bmod m$ 에 대한 위수가 k , $(h,k) = 1$ 이면 ab 는 $\bmod m$ 에 대한 hk 를 위수로 갖는다.

pf)

$$\begin{aligned} a^h &\equiv 1 \pmod{m} \\ b^k &\equiv 1 \pmod{m} \end{aligned} \Rightarrow \begin{aligned} a^{hk} &\equiv 1 \pmod{m} \\ b^{hk} &\equiv 1 \pmod{m} \end{aligned} \Rightarrow (ab)^{hk} \equiv 1 \pmod{m}$$

따라서 ab 의 $\bmod m$ 에 대한 위수가 r , 즉 $(ab)^r \equiv 1 \pmod{m}$ 이라면 $r \mid hk$.

$a^h \equiv 1 \pmod{m}$ 이므로, $b^{rh} \equiv a^h \cdot b^{rh} \pmod{m}$ 이고, $b^{rh} \equiv (ab)^r \cdot b^{rh} \pmod{m}$ 이다.

$b^{rh} \equiv (ab)^r \cdot b^{rh} \pmod{m}$ 일때, r 은 ab 의 위수 hk 으로 $b^{rh} \equiv 1 \pmod{m}$ 이다.

b 의 $\bmod m$ 에 대한 위수가 rk 으로 $b^{rh} \equiv 1 \pmod{m}$ 이면 $k \mid rh$.

$(h,k) = 1$ 이므로 $k \mid rh$ 에서 $k \mid r$. 같은 방식으로 $a^{rk} \equiv 1 \pmod{m}$ 에서 $h \mid r$.

$k \mid r \& h \mid r \rightarrow hk \mid r$ 이므로, $r \mid hk$ 이자 $hk \mid r$ 인 $r = hk$.

Def 2.1 mod m에 대해 g의 위수가 $\phi(m)$ 일 경우, 그런 g를 m의 원시근이라 한다.
원시근의 정의

Lemma 2.35 소수 p와 q에 대해 $\alpha \geq 1$ 에서 $q^\alpha | (p-1)$ 일 경우, mod p에 대해
 q^α 을 위수로 갖는 원소가 RR에 정확히 $q^\alpha - q^{\alpha-1}$ 개 존재한다.

Pf)

페르마의 소정리에 의해 $x^{p-1} \equiv 1 \pmod{p}$. $q^\alpha | (p-1)$ 이라면 $q^\alpha \cdot k = p-1$ 이므로,
 $x^{p-1} - 1 = x^{q^\alpha \cdot k} - 1 = (x^{q^\alpha} - 1) \{ (x^{q^\alpha})^{k-1} + (x^{q^\alpha})^{k-2} + \dots + (x^{q^\alpha})^1 + (x^{q^\alpha})^0 \}$
 위와 같이 인수분해가 된다고 할 때 $f(x) = x^{q^\alpha} - 1$ 이라고 보면 $f(x) | x^{p-1} - 1$ 이다.
 따라서 $f(x) = x^{q^\alpha} - 1 \equiv 0 \pmod{p}$ 는 Thm 2.29에 의해 정확히 q^α 개의 해를
 가진다.

그 말은, q^α 개의 해는 $x^{q^\alpha} \equiv 1 \pmod{p}$ 라는 합동식을 성립되게 하므로,
 그 해들의 위수는 q^α 의 약수라 할 수 있다. ... ①

마찬가지 방식으로, $q^\alpha | (p-1)$ 이라면, $q^{\alpha+1} | (p-1)$ 이기도 하므로, $q^{\alpha+1} \cdot k = p-1$ 이면 $x^{p-1} - 1 = x^{q^{\alpha+1} \cdot k} - 1 = (x^{q^{\alpha+1}} - 1) \{ t^{k-1} + t^{k-2} + \dots + t^1 + t^0 \}$ 로 인수분해가 가능하고,
 $f(x) = x^{q^{\alpha+1}} - 1$ 이라고 하면 $f(x) | x^{p-1} - 1$ 이되어 $f(x) = x^{q^{\alpha+1}} - 1 \equiv 0 \pmod{p}$ 의 해가
 정확히 $q^{\alpha+1}$ 개 존재하게 된다.

여기서도 이 $q^{\alpha+1}$ 개의 해는 $x^{q^{\alpha+1}} \equiv 1 \pmod{p}$ 의 해인것이므로, 모두 $q^{\alpha+1}$ 의 약수를
 위수로 갖는다. ... ②

$$x^{q^\alpha} = (x^{q^{\alpha+1}})^{\frac{1}{q}} \equiv 1^{\frac{1}{q}} \equiv 1 \pmod{p} \text{ 이므로}$$

$x^{q^{\alpha+1}} \equiv 1 \pmod{p}$ 의 해는 모두 $x^{q^\alpha} \equiv 1 \pmod{p}$ 의 해이다.

①과 ②에 의해, q^α 의 약수를 위수로 갖는 q^α 개의 해를 중,
 $q^{\alpha+1}$ 의 약수를 위수로 갖는 $q^{\alpha+1}$ 개의 해를 제외하면,
 $'q^\alpha - q^{\alpha+1}'$ 개의 해는 모두 위수가 q^α 인 것들이다.

Thm 2.36 P 가 소수일 때, $\mod P$ 에 대해 $\phi(p-1)$ 개의 원시근이 존재한다.

pf) $P-1$ 의 Canonical factorization은 $P-1 = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots \cdot p_j^{\alpha_j}$ 라 하자.

P 의 원시근은, P 의 CRS에서 $\phi(P)$, 즉 $P-1$ 을 위수로 갖는 수를 말한다.

$i=1, 2, \dots, j$ 에 대하여 $p_i^{\alpha_i} | P-1$ 이므로, Lemma 2.35에 의해

$\mod p_i$ 에 대해 $p_i^{\alpha_i}$ 를 위수로 갖는 원소가 정확히 ' $p_i^{\alpha_i} - p_i^{\alpha_i-1}$ ' 개 존재한다.

이어, $p_i^{\alpha_i}$ 를 위수로 갖는 임의의 원소 r_i 를 가정하면,

$g = r_1 \times r_2 \times \cdots \times r_j$ 라 할 때, Lemma 2.34에 의해 g 는 $P-1$ 을 위수로 갖는다.

($\because r_i$ 는 $\mod p_i$ 에서 위수 $p_i^{\alpha_i}$ 를 갖고, r_j 는 위수 $p_j^{\alpha_j}$ 를 가짐.)

$p_i^{\alpha_i}$ 과 $p_j^{\alpha_j}$ 는 소인수분해 결과의 일부로서 모두 각각 서로소.)

$\mod P$ 에 대해 $P-1$ 을 위수로 갖는 $g = r_1 \times r_2 \times \cdots \times r_j$ 가 존재함이 증명되었다.

이어 P 의 한 원시근을 g 라 하면, $\{g^1, g^2, \dots, g^{p-2}, g^{p-1}\}$ 라는 집합은 $\mod P$ 에 대해 P 의 RRJ가 된다. (\because 원시근의 정의)

Lemma 2.33에 의해, g 가 $\mod P$ 에 대해 위수 $P-1$ 을 가지면,

g^k 은 $\mod P$ 에 대해 $\frac{P-1}{(P-1, k)}$ 을 위수로 가진다.

P 의 $RRJ = \{g^1, g^2, \dots, g^{p-1}\}$ 의 원소들 중 위수가 $P-1$ 인 수는

g^k 에서 $(P-1, k)=1$ 인 수들, 즉 $P-1$ 과 서로소인 k 를 차수로 갖는 g^k 들의 개수라

할 수 있다. $P-1$ 과 서로소인 수의 개수는 $\phi(p-1)$ 이므로, 원시근의 개수는 $\phi(p-1)$ 개.

Thm 2.36

Pf 2)

정학히 α 개의 해가 존재하는 합동식 $x^k \equiv 1 \pmod{P}$ 의 해들은 모두 위수로 α 의 약수(divisor)를 가짐. 따라서, \pmod{P} 에 대해 α 의 약수를 위수로 가지는 수의 개수는 정학히 α 개.

만약 $P-1 = P_1^{K_1} \cdot P_2^{K_2} \cdots \cdot P_r^{K_r}$ 로 소인수분해를 한다치면, 여기서 $\alpha | P-1$ 인 α 를 $\alpha = P_j^{K_j}$ 라 했을 때 $x^{\alpha} \equiv 1 \pmod{P}$ 가 정학히 α 개의 해를 가진다는 점에 임각하여 $x^{P_j^{K_j}} \equiv 1 \pmod{P}$ 가 정학히 $P_j^{K_j}$ 개의 해를 가지게 됨. 그러나 이런 비단 $\alpha = P_j^{K_j}$ 뿐만 아니라 $P_j^{(K_j-1)}$ 이 α 일 때도 마찬가지로 성립하므로 $x^{P_j^{(K_j-1)}} \equiv 1 \pmod{P}$ 는 정학히 $P_j^{(K_j-1)}$ 개의 해를 갖게 됨. $x^{P_j^{K_j}} \equiv 1 \pmod{P}$ 의 해는 모두 '위수가 $P_j^{K_j}$ 의 약수인 수'들 이었으므로, $P_j^{K_j}$ 의 약수는 $1, P_j, P_j^2, P_j^3, \dots, P_j^{(K_j-1)}, P_j^K$ 이라는 점에서, 같은 원리로 $P_j^{(K_j-1)}$ 의 약수가 $1, P_j, P_j^2, P_j^3, \dots, P_j^{(K_j-1)}$ 라고 할 수 있고, 통합하면 $x^{P_j^K} \equiv 1 \pmod{P}$ 의 해 P_j^K 개 중 $P_j^{(K_j-1)}$ 개의 해를 빼면 만큼이 정학히 '위수가 $P_j^{K_j}$ 인 수'가 됨.
 $\Rightarrow \pmod{P}$ 에 대해 P_j^K 를 위수로 가지는 수의 개수: $P_j^K - P_j^{(K_j-1)}$

P 의 원시근을 g 라 하면, $g^1, g^2, g^3, \dots, g^{P-1}$ 은 모두 \pmod{P} 에 대해 서로 다른 수. 즉 $\{g^1, g^2, \dots, g^{P-1}\}$ 은 P 의 RRSL. g^k 의 위수는, g 의 위수를 h 라 할 때 $\frac{h}{(h, k)}$ 이다. $h = P-1$ 이므로 $\frac{P-1}{(P-1, k)}$ 이 g^k 의 위수.
 g^k 의 위수가 $P-1$ 이 되면 g^k 도 g 와 같은 또래의 원시근이 되는데.
그렇게 되다면 $(P-1, k) = 1$ 이어야 한다. 즉, $P-1$ 과 서로소인 수들은 모두 위수로 $P-1$ 을 가지는 것. 그런 수들의 개수는 $\varphi(P-1)$.
따라서 $\varphi(P-1)$ 의 원시근의 개수는 $\varphi(P-1)$.

Thm 2.31
n 차 합동식이
해를 가질 조건

소수 P 와 서로소인 a 에 대하여, \Rightarrow 위수가 정의될 조건

합동식 $x^n \equiv a \pmod{P}$ 는

$$a^{\frac{P-1}{(n, P-1)}} \equiv 1 \pmod{P} \text{ 의 여부에 따라}$$

$(n, P-1)$ 개의 해를 가지거나 해가 없다.

pf)

P 는 원시근을 가정. 원시근을 g 라 하면,

어떤 정수 i 를 차수로하여 $g^i \equiv a \pmod{P}$ 라고 표현 가능.

만약 합동식 $x^n \equiv a \pmod{P}$ 가 해를 갖는다면 그 해는 P 와 서로소일 것.

그러서 그런 x 를 임의의 정수 u 에 대해 $g^u \equiv x \pmod{P}$ 라 표현할 수 있게 된다.

그리면 최종적으로 주어진 합동식이 $g^{un} \equiv g^i \pmod{P}$ 가 되고,

이 합동식은 $un \equiv i \pmod{P-1}$ 과 동치가 된다.

$un \equiv i \pmod{P-1}$ 은 $d = (n, P-1)$ 에 대해 $d | i$ 일 때에만
해를 가지며, 해가 존재한다면 정확히 d 개의 해가 존재한다. (u 값이 d 개 \rightarrow x 값도 d 개)

$d | i$ 라는 조건은 $i = dk$ (k 는 정수)로 바꿔쓸 수 있고, 이 조건을 아래 식에 적용하면

$$a^{\frac{P-1}{(n, P-1)}} = a^{\frac{P-1}{d}} = g^{i(\frac{P-1}{d})} \pmod{P} = g^{dk(\frac{P-1}{d})} = g^{k(P-1)} = (g^{P-1})^k \equiv 1 \pmod{P}$$

$$\Rightarrow a^{\frac{P-1}{(n, P-1)}} \equiv 1 \pmod{P} \text{ 이다. (이게 조건이 됨)}$$

따라서 주어진 합동식은 $a^{\frac{P-1}{(n, P-1)}} \equiv 1 \pmod{P}$ 이면 d 개의 해를 갖고,
아니면 없다.

Thm 2.39 p 가 소수일 때, $\mod p^2$ 에 대응하여

p^2 의
원시근의 개수

$$\phi(\phi(p^2)) = (p-1)\phi(p-1) > 1$$
의 원시근이 존재한다.

$$\phi(p^2) = p^2 - p = p(p-1) \Rightarrow p^2$$
의 원시근? 위수가 $p(p-1)$ 인 수.

$$\phi(\phi(p^2)) = \phi(p(p-1)) = \phi(p) \times \phi(p-1) = (p-1)\phi(p-1) (\because \text{Thm 2.19 (i)})$$

g 가 소수 p 의 원시근이라 해보자. $g^{p-1} \equiv 1 \pmod{p}$

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

p^2 에서 g 의 위수를 d 라 하면, $g^d \equiv 1 \pmod{p^2}$ 이다.

$g^{d-1} = p^2k$ 이면, $g^{d-1} = p(pk)$ 이므로 $g^d \equiv 1 \pmod{p}$ 이다.

$\mod p^2$ 에서 g 의 위수는 $p-1$ 이었으므로, $p-1 | d$ 이다.

즉, p^2 에서의 g 의 위수는 $p-1$ 의 배수이다.

하지만 지금은 $g^{p-1} \not\equiv 1 \pmod{p^2}$ 이라는 가정상태 이므로 p^2 에서의

g 의 위수 d 는 $p-1$ 은 아닌 배수이다.

p 는 소수, g 는 그걸 p 의 원시근이므로 $(g, p) = 1$ 이다. 이에, 다음이 성립.

$$g^{\phi(p^2)} \equiv 1 \pmod{p^2} (\because \text{Thm 2.39 B 일려 정리})$$

$g^{\phi(p^2)} = g^{p(p-1)} \equiv 1 \pmod{p^2}$ 이므로, d 는 $p(p-1)$ 의 약수여야 한다.

$(p-1)$ 의 배수이면서 $p(p-1)$ 의 약수이고 $p-1$ 은 아닌 d 로 가능한 것 $p(p-1)$ 뿐.

따라서 소수 p 의 원시근을 g 라 하면, p^2 에 대한 g 의 위수는 $p(p-1)$.

\therefore i)의 경우, g 가 p^2 의 원시근.

$$ii) g^{p-1} \equiv 1 \pmod{p}$$

→ h 는 p 의 원시근

$h = g + p$ 가 하면, $h \equiv g \pmod{p}$ 이므로 h 의 p 에 대한 위수는 $p-1$.

$$h^{p-1} = (g+p)^{p-1} = g^{p-1} + (p-1)g^{p-2} \cdot p + \cdots + (p-1)g \cdot p^{p-2} + p^{p-1}$$

h^{p-1} 의 앞 두 항은 뺀 나머지는 $\pmod{p^2}$ 에 대해서 0. ($\because p^2$ 를 포함)

$$\therefore h^{p-1} \equiv g^{p-1} + (p-1)g^{p-2} \cdot p \pmod{p^2}$$

ii)의 가정에 따라 $g^{p-1} \equiv 1 \pmod{p^2}$ 이므로

$$h^{p-1} \equiv 1 + (p-1)g^{p-2} \cdot p \pmod{p^2} \quad \Rightarrow h^{p-1} \not\equiv 1 \pmod{p^2}$$

$(g, p) = 1$ 이므로 $(p-1)g^{p-2} \cdot p \not\equiv 0 \pmod{p^2}$.

따라서 p 의 또 다른 원시근인 h 는 p^2 에서 $p-1$ 의 배수를 위수로 가지고,
위수가 $p-1$ 은 아니며, $(h, p) = 1$ 이기에 위수가 $p(p-1)$ 의 약수여야 한다.

↳ i)과 같은 상황.

따라서 ii)의 경우에도 p^2 에 대한 h 의 위수가 $p(p-1)$ 로
 h 가 p^2 의 원시근.

중간결론

i)과 ii)의 결론: 소수 p 의 원시근을 g 라 가정하면 p^2 의 원시근이 존재!

소수는 Thm 2.36에 의해 무한원 원시근이 존재하므로 p^2 의 원시근도 무한존재.

g 와 $g+p$ 중 하나는 p^2 의 원시근!

소수 p 에 대해 p^2 의 원시근이 무조건 존재함이 증명되었으므로
 p^2 의 원시근을 g 가 하면, $g^k \equiv 1 \pmod{p^2}$ 을 만족하는
최초의 k 가 $\phi(p^2)$ 이므로 집합 $\{g^1, g^2, \dots, g^{\phi(p^2)}\}$ 의 원소들은
 $\pmod{p^2}$ 에 대해 모두 다른 값이다.

p^2 의 RR는 $\phi(p^2)$ 개의 원소를 가지고 있으므로 위 집합이 RRS.

Lemma 2.33에 의해

$g \not\equiv 1 \pmod{p^2}$ 에 대해 위수 $\phi(p^2)$ 을 가지면, g^k 는 $(\phi(p^2), k) = 1$ 일 경우
 $\phi(p^2)$ 을 위수로 가진다. 그런 g^k 의 개수는, $\phi(\phi(p^2))$ 이고,
계산하면 $(p-1)\phi(p-1)$.

정리: p 가 소수일 때, p^2 은 원시근이 무조건 존재하고
하나의 원시근을 g 로 두면 $\phi(p^2)$ 과 서로소인 k 에 대하여
 g^k 도 위수를 $\phi(p^2)$ 으로 가지는 원시근이 된다.
그런 k 의 개수는 $\phi(\phi(p^2))$ 이므로
“ p 가 소수일 때 p^2 은 $\phi(\phi(p^2))$ 개의 원시근을 가진다.”

결론

Thm 240
P의 원시근의
성질

P: odd prime
g: P^{α} 의 원시근 \Rightarrow g는 P^{α} 의 원시근 ($\alpha = 3, 4, 5, \dots$)

① g가 P^{α} 의 원시근

1) g의 P^{α} 에 대한 위수는 $\phi(P^{\alpha}) = P(P-1)$

2) g는 P과 서로소 \rightarrow g는 P^{α} 과 서로소 \rightarrow P^{α} 에 대한 g의 위수 존재

② g의 P^{α} 에 대한 위수를 h라 하면,

1) 오일러의 정리에 의해 $h | \phi(P^{\alpha}) = P^{\alpha-1}(P-1)$

2) $g^h \equiv 1 \pmod{P^{\alpha}}$ $\rightarrow P^{\alpha} | g^h - 1 \rightarrow P^{\alpha} | g^h - 1 \rightarrow g^h \equiv 1 \pmod{P^{\alpha}}$

③ g의 P^{α} 에 대한 위수가 $\phi(P^{\alpha}) = P(P-1)$ 이었으므로 $g^h \equiv 1 \pmod{P^{\alpha}}$ 에서 $P(P-1) | h$.

④ $h | P^{\alpha-1}(P-1)$ 이고 $P(P-1) | h$ 이므로 $h = P^{\beta}(P-1)$ ($1 \leq \beta \leq \alpha-1$)

⑤ $P^{\beta}(P-1) \sim P^{\alpha-2}(P-1)$ 은 P^{α} 에 대한 g의 위수 아님.

⑥ $h = P^{\alpha-1}(P-1) = \phi(P^{\alpha})$ 이므로 P^{α} 에 대한 g의 위수는 $\phi(P^{\alpha})$.

Thm 2.41
원시근이
존재할 조건

'mod m에 대해 원시근이 존재한다'는 것은,
odd prime P 에 대해 $m = 1, 2, 4, P^\alpha, 2P^\alpha$ 이라는 것과 같다.

i) m 이 $1, 2, 4, P^\alpha, 2P^\alpha$ 중 한 형태 $\rightarrow m$ 의 원시근이 존재

CASE 1: $m = 1$

모든 정수가 원시근

CASE 2: $m = 2$

1이 원시근

CASE 3: $m = 4$

3이 원시근

CASE 4: $m = P^\alpha$ (P 는 홀수인 소수)

Thm 2.39, Thm 2.40에 의해 원시근 존재

CASE 5: $m = 2 \cdot P^\alpha$ (P 는 홀수인 소수)

P^α 의 홀수의 원시근을 갖자 하면,

z 의 $2P^\alpha$ 에 대한 위수를 d 가 가질 때,

$$\varphi(P^\alpha) | d \quad \& \quad d | \varphi(2 \cdot P^\alpha) \rightarrow d = \varphi(2 \cdot P^\alpha)$$

ii) 어떤 수 m 의 원시근이 존재 $\rightarrow m$ 이 $1, 2, 4, P^\alpha, 2P^\alpha$ 중 한 형태

CASE 1: $m = 2^\alpha$ ($\alpha = 3, 4, 5, \dots$)

원시근이 존재한다 가정 \rightarrow 모순!

$\rightarrow \alpha \geq 3$ 인 α 에 대해 $m = 2^\alpha$ 에서 원시근이 존재하지 않음.

CASE 2: $m = 2^\alpha \times P^\alpha$ ($\alpha \geq 2, \alpha \geq 1$)

이 경우 원시근이 없음.

CASE 3: $m = 2^\alpha \times P_1^{\alpha_1} \times P_2^{\alpha_2} \times \dots \times P_r^{\alpha_r}$ ($r \geq 2$)

원시근이 존재한다 가정 \rightarrow 모순!

CASE 4: $m = 2^0, 2^1, 2^2, P^\alpha, 2P^\alpha$

이 경우에만 모순 없음.

Cor 2.42 odd prime p 에 대해 $m = 1, 2, 4, p^\alpha, 2p^\alpha$ 이라 하자. \Rightarrow 원시근이 존재할 조건

$(a, m) = 1$ 이면 \Rightarrow 원시근이 있는 조건

합동식 $x^n \equiv a \pmod{m}$ 은

$a^{\frac{\phi(m)}{(n, \phi(m))}} \equiv 1 \pmod{m}$ 의 성립 여부에 따라

$(n, \phi(m))$ 개의 해를 갖거나 해가 없다.

Pf) 원시근을 갖는 m 에 대해 Thm 2.39의 증명을 일반화.

Ex) $x^4 \equiv 61 \pmod{11}$ 의 해의 개수

$11 = 3^2 \times 13 \Rightarrow 3^2$ 과 13 으로 분해.

$$\textcircled{1} \quad \frac{\phi(3^2)}{(n, \phi(3^2))} = \frac{3^2 - 3}{(4, 3^2 - 3)} = 3 \Rightarrow 61^3 \equiv (-2)^3 \equiv 1 \pmod{3^2}$$

$\therefore x^4 \equiv 61 \pmod{3^2}$ 의 해의 개수: $(4, 3^2 - 3) = 2$ 개

$$\textcircled{2} \quad \frac{\phi(13)}{(n, \phi(13))} = \frac{12}{(4, 12)} = 3 \Rightarrow 61^3 \equiv (-4)^3 \equiv 1 \pmod{13}$$

$\therefore x^4 \equiv 61 \pmod{13}$ 의 해의 개수: $(4, 12) = 4$ 개

CRT에 의해 $x^4 \equiv 61 \pmod{3^2 \cdot 13}$ 의 해의 개수: $2 \times 4 = 8$ 개.

2.9 Congruences of Degree Two, Prime Modulus.

2.9절 intro $f(x) = ax^2 + bx + c$. 차수는 2, $a \neq 0 \pmod{P}$.

소수 P 를
방법으로 하는
오차 합동식의
해 구하기 문제

$$4a f(x) = 4a(ax^2 + bx + c) \equiv 0 \pmod{P}$$

$$\text{정리하면 } 4a f(x) = (2ax + b)^2 - (b^2 - 4ac) \text{ 가 됨.}$$

$(2ax + b)^2 - (b^2 - 4ac) \equiv 0 \pmod{P}$ 의 해를 구하는 것은,

$$b^2 - 4ac = V^2 \pmod{P} \text{ 할 때}$$

$x^2 \equiv b^2 - 4ac \pmod{P}$ 를 V 를 찾는 문제와 동일.

LH? V 만 찾으면 $2ax + b = \pm V$ 로 x 를 결정할 수 있으니까.

Thm 2.45 a 와 b 가 서로소이고 P 가 소수일 때,

a 와 b 가 \pmod{P} 에 대해 2^j 은 원수로 가지면,

ab 는 \pmod{P} 에 대해 우조건 j 보다 작은 어떤 j' 으로 $2^{j'}$ 은 원수로 가진다.

PF) $x = a^{2^{j'-1}} \circ (2^j \text{를 하면},$

$$x^2 = (a^{2^{j'-1}})^2 = a^{2^{j'}} \equiv 1 \pmod{P}$$

a 의 \pmod{P} 에 대한 원수가 2^j 였으므로 $a^{2^{j'-1}} \not\equiv 1 \pmod{P}$.

따라서 $x^2 \equiv 1 \pmod{P}$ 를 만족하는 것은 $x \equiv -1 \pmod{P}$ 뿐.

(\because Lemma 2.10에 의해).

같은 방식으로 $x = b^{2^{j'-1}}$ 이라 하면 $x \equiv -1 \pmod{P}$.

$$a^{2^{j'-1}} \times b^{2^{j'-1}} \equiv (-1) \times (-1) \equiv 1 \pmod{P}.$$

$(ab)^{2^{j'-1}} \equiv 1 \pmod{P}$ 이므로 ab 의 원수는 $2^{j'-1}$ 의 약수 (divisor).