通信情報保護學會誌
第2卷 第3號, 1992. 9

初等 整數論과 暗號學
(2)

朴 勝 安*

이 글은 第1卷, 第2號에 揭載된 '初等 整數論과 暗號學 (1)'의 계속이다.

제5절에서는 位數와 原始根에 대하여 간단히 논하고 제6절에서는 이에 대한 응용문제로서 이른바 $1/p$ 生成子에 대한 定理와 몇 가지 예를 논하기로 한다.

5. 原 始 根

앞으로 n은 1 보다 큰 양의 정수를 나타낸다.

定義 5.1 정수 n ($n \geq 2$)과 서로 素인 정수 a에 대하여

$$a^r \equiv 1 \pmod{n}$$

를 만족시키는 가장 작은 양의 정수 r를 法 n에 관한 a 의 **位數**(order)라 하고 r 를 $\mathrm{ord}_n a$ 로 나타낸다.

Euler의 정리(定理 2.1)에 의하면

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

이므로 법 n에 관한 a의 位數는 $\varphi(n)$ 보다 크지 않다. 이 절에서 논하는 定理의 증명에 대해서는 다음 책을 참조하기 바란다.

金應泰·朴勝安, 整數論, 제3판, 京文社, 1991.

定理 5.2 법 n 에 관한 정수 a 의 位數가 일 때 다음이 성립한다.

(1) 음이 아닌 정수 k 에 대하여

$$a^k \equiv 1 \pmod{n} \iff r \mid k$$

특히, $\quad r \mid \varphi(n)$

(2) 음이 아닌 정수 i, j 에 대하여

$$a^i \equiv a^j \pmod{n} \iff r \mid (i-j)$$

定理 5.3 법 n 에 관한 정수 a 의 位數가 r 일 때, 음이 아닌 정수 k에 대하여 다음이 성립한다.

(1) a^k의 位數는 $\dfrac{r}{\gcd(k,r)}$ 이다.

(2) a^k 의 位數가 r 이기 위한 필요충분조건은 $\gcd(k, r) = 1$ 인 것이다.

定義 5.4 법 n에 관한 정수 g의 位數가 $\varphi(n)$일때, g를 법 n에 관한 **原始根**(primitive root)이라고 한다.

모든 양의 정수 n에 대하여 원시근이 존재하는 것은 아니다. 실제로, 양의 정수 n이 다음과 같은 정수일 때 그리고 이때에만 법 n에 관한 원시근이 존재한다.

2, 4,

p^k (p는 홀수인 素數, k는 양의 정수),

$2p^k$ (p는 홀수인 素數, k는 양의 정수)

* 종신회원, 서강대학교 이공대학 수학과 교수

보기 5.1 n=7, g=3에 대하여

$$g \equiv 3 \pmod 7$$
$$g^2 \equiv 9 \equiv 2 \pmod 7$$
$$g^3 \equiv 2 \cdot 3 \equiv 6 \pmod 7$$
$$g^4 \equiv 18 \equiv 4 \pmod 7$$
$$g^5 \equiv 12 \equiv 5 \pmod 7$$
$$g^6 \equiv 15 \equiv 1 \pmod 7$$

따라서 법 7에 관한 3의 位數는 6이고 또

$$\varphi(n) = \varphi(7) = 6$$

이므로 3은 법 7에 관한 원시근이다.

보기 5.2 n=15일 때,

$$\varphi(n)=\varphi(15)=\varphi(3)\varphi(5)=2 \cdot 4=8$$

이고 법 15에 관한 원시근은 존재하지 않는다.

실제로 다음 표가 성립한다.

정 수	1	2	4	7	8	11	13	14
位 數	1	4	2	4	4	2	4	2

정의와 정리 5.2, 5.3에 의하여 다음이 성립한다.

보기 5.5 법 n에 관한 원시근 g가 존재할 때, 음이 아닌 정수 k에 대하여 다음이 성립한다.

(1) $g^k \equiv 1 \pmod n \iff \varphi(n) | k$

(2) $g^i \equiv g^j \pmod n \iff i \equiv j \pmod{\varphi(n)}$

(3) $\{g^0, g^1, g^2, \cdots, g^{\varphi(n)-1}\}$ 는 법 n 에 관한 既約剩餘系이다.

(4) g^k 가 법 n에 관한 원시근이기 위한 필요충분조건은 $\gcd(k, \varphi(n)) = 1$ 인 것이다.

定義 5.6 양의 정수 n 이 原始根 g 를 가질때, n과 서로 소인 정수 a에 대하여

$$a \equiv g^i \pmod n, \qquad 0 \le i \le \varphi(n)-1$$

인 정수 i 가 단 하나 존재한다(정리 5.5 참조).

이와 같은 정수 i를 법 n에 관한 (g를 밑으로 가지는) a의 **離散로그**(discrete logarithm) 또는 **指數**(index)라 하고 이것을 간단히

$\text{ind}_g\, a$ 또는 $\text{ind}\, a$

로 나타낸다. 즉,

$$i=\text{ind}_g\, a \iff a \equiv g^i \pmod n, \quad 0 \le i \le \varphi(n)-1$$

보기 5.3 보기 5.1에 의하여

$$3 \equiv 3 \pmod 7$$
$$3^2 \equiv 2 \pmod 7$$
$$3^3 \equiv 6 \pmod 7$$
$$3^4 \equiv 4 \pmod 7$$
$$3^5 \equiv 5 \pmod 7$$
$$3^6 \equiv 1 \pmod 7$$

따라서 3을 밑으로 가지는 법 7에 관한 離散로그表는 다음과 같다.

a	1	2	3	4	5	6
$ind^a\, a$	0	2	1	4	5	3

離散로그는 널리 이용된다. 이에 대해서는 다음과 같은 법칙이 성립한다.

定理 5.7 양의 정수 n 이 原始根 g 를 가질 때 다음이 성립한다

(1) $\text{ind}_g\, a = \text{ind}_g\, b \iff a \equiv b \pmod n$

(2) $\text{ind}_g\, ab \equiv \text{ind}_g\, a + \text{ind}_g\, b \pmod{\varphi(n)}$

(3) $\text{ind}_g\, a^m = m\ \text{ind}_g\, a \pmod{\varphi(n)}$

위의 정리에 의하여, 법 n에 관한 곱의 문제를 법 $\varphi(n)$ 에 관한 합의 문제로 고쳐 쓸 수 있다. 따라서 위의 정리는 合同式에 대한 여러가지 문제를 푸는데 이용된다.

6. $1/p$ 生成子

이 절에서는 이른바 $1/p$ 生成子(generator)에 대한 이론을 一般化하여 소개하기로 한다.

이제 $a(a \ge 2)$를 고정된 양의 정수라고 할 때, 양의 유리수 u가 다음과 같이 나타내어진다고 하자.

$$u = r_m a^m + r_{m-1} a^{m-1} + \cdots + r_1 a + r_0 a^0 + s_1 a^{-1} + s_2 a^{-2} + \cdots + s_n a^{-n}$$
$$(1 \le r_m < a,\ \cdots,\ 0 \le r_0 < a,\ 0 \le s_1 < a,\ \cdots,\ 0 \le s_n < a)$$

이 때, u를 a 進法으로

$$u = r_m r_{m-1} \cdots r_1 r_0,\ s_1 s_2 \cdots s_{n(a)}$$

으로 나타낸다.

보기 6.1 양의 정수 c 에 대하여

$$c = r_{m-1} a^{m-1} + r_{m-2} a^{m-2} + \cdots + r_1 a + r_0 a^0$$

일 때, $\frac{c}{a^m} = 0.r_{m-1} r_{m-2} \cdots r_1 r_{0(a)}$ 이다.

마찬가지로, 양의 유리수 u가

$$u = r_m a^m + r_{m-1} a^{m-1} + \cdots + r_1 a + r_0 a^0 + s_1 a^{-1} + s_2 a^{-2} + \cdots + s_n a^{-n}$$
$$(1 \le r_m < a,\ \cdots,\ 0 \le r_0 < a,\ 0 \le s_1 < a,\ \cdots,\ 0 \le s_n < a)$$

와 같이 나타내어질 때, u를 a 進法으로

$$u = r_m r_{m-1} \cdots r_1 r_0 . s_1 s_2 \cdots s_n \cdots_{(a)}$$

으로 나타낸다.

특히, $0 < u < 1$인 유리수 u에 대하여

$$u = 0.s_1 s_2 \cdots s_r s_1 s_2 \cdots s_r s_1 s_2 \cdots s_r \cdots_{(a)}$$

와 같이 r 개의 항 $s_1,\ s_2,\ \cdots,\ s_r$가 이 순서대로 한없이 되풀이될 때, 즉

$$s_{n+r} = s_n \qquad (n = 1, 2, \cdots)$$

일 때, u를 '循環小數'

$$u = 0.\overline{s_1 s_2 \cdots s_r}_{(a)}$$

로 나타낸다.

여기서 r가 이와 같은 정수 중에서 가장 작은 양의 정수일 때, $s_1,\ s_2,\ \cdots,\ s_r$를 **循環마디**라 하고 r를 **週期**(period)라고 한다.

유리수를 10진법으로 나타내는 경우에는 밑 10을 생략한다.

보기 6.2 $a = 10$ 일 때,

$$\frac{1}{33} = \frac{3}{99} = \frac{3}{10^2 - 1} = \frac{3}{10^2} \frac{1}{1 - 10^{-2}}$$
$$= \frac{3}{10^2} \{1 + 10^{-2} + (10^{-2})^2 + \cdots\},$$
$$= 0.030303\cdots = 0.\overline{03}$$

定理 6.1 양의 정수 a $(a \ge 2)$와 유리수

$$u = \frac{c}{q} \quad (1 \le c < q,\ (c, q) = 1)$$

에 대하여 $\gcd(a, q) = 1$일 때, 法 q 에 관한 a 의 位數를 r 라 하고

$$s = \frac{a^r - 1}{q}$$

이라고 하면 다음이 성립한다.

(1) 양의 정수 cs는

$$cs = s_1 a^{r-1} + s_2 a^{r-2} + \cdots + s_{r-1} a + s_r$$
$$0 \le s_1 < a,\ 0 \le s_2 < a,\ \cdots,\ 0 \le s_r < a$$

의 꼴로 나타내어지고 이때

$$u = 0.\overline{s_1 s_2 \cdots s_{r-1} s_r}_{(a)}$$

이고 그 주기는 r이다.

(2) 음이 아닌 정수 a에 대하여

$$c_m \equiv a^m c \pmod q,\ 1 \le c_m < q,$$
$$u = 0.s_1 s_2 \cdots s_n \cdots_{(a)}$$

이라고 놓으면,

$$s_{n+r} = s_n \ (n = 1, 2, \cdots),$$
$$\frac{c_m}{q} = 0.\overline{s_{m+1} \cdots s_{m+1}}_{(a)},$$
$$c_m = c_n \iff m \equiv n \pmod r$$

(3) $a^{n-1} < q < a^n$ 일 때, 즉 $n = 1 + [\log_a q]$ 일 때,

$$s = q_1 a^{r-1} + q_2 a^{r-2} + \cdots + q_r$$
$$(0 \le q_1 < a,\ 0 \le q_2 < a,\ \cdots,\ 0 \le q_r < a)$$

이면

$$0 \le n < r,\ q_1 = q_2 = \cdots = q_{n-1} = 0,$$
$$\frac{1}{q} = 0.\overline{q_1 q_2 \cdots q_r}_{(a)}$$

證 明 (1) 양의 정수 r는 $a^r \equiv 1 \pmod q$인 가장 작은 양의 정수이므로, s 는 정수이고 $qs = a^r-1$ 이다. 또, $1 \le c < q$이므로

$$1 \le cs = \frac{c(a^r-1)}{q} < a^r-1 < a^r$$

이고, 따라서 cs 는

$$cs = s_1 a^{r-1}+s_2 a^{r-2}+\cdots+s_r$$
$$(0 \le s_1 < a,\ 0 \le s_2 < a,\ \cdots,\ 0 \le s_r < a)$$

의 꼴로 나타내어진다. 이 때,

$$u = \frac{c}{q}\frac{cs}{qs} = \frac{cs}{a^r-1} = \frac{cs}{a^r}\frac{1}{1-a^{-r}}$$
$$= \frac{cs}{a^r}(1+a^{-r}+a^{-2r}+a^{-3r}+\cdots)$$
$$= (s_1 a^{-1}+s_2 a^{-2}+\cdots+s_r a^{-r})\cdot$$
$$(1+a^{-r}+a^{-2r}+a^{-3r}+\cdots).$$

따라서

$$u = 0.s_1 s_2 \cdots s_r s_1 s_2 \cdots s_r s_1 s_2 \cdots s_r \cdots (a)$$
$$= 0.\overline{s_1 s_2 \cdots s_r}(a)$$

이제 음이 아닌 정수 m에 대하여

$$c_m \equiv a^m c \pmod q,\ 1 \le c_m < q,$$
$$u = s_1 a^{-1}+s_2 a^{-2}+\cdots+s_n a^{-n}+\cdots$$

이라고 하면,

$$s_{n+r} = s_n \quad (n=1,\ 2,\ \cdots),$$

$$c_m = c_n \iff a^m c \equiv a^n c \pmod q$$
$$\iff a^m \equiv a^n \pmod q$$
$$\iff m \equiv n \pmod r$$

$$\frac{a^m c}{q} = a^m u = s_1 a^{m-1} + s_2 a^{m-2}+\cdots+s_m a^0$$
$$+s_{m+1}a^{-1}+s_{m+2}a^{-2}+\cdots$$
$$= s_1 s_2 \cdots s_m . s_{m+1} s_{m+2} \cdots (a)$$

$$\frac{c_m}{q} = 0.s_{m+1} s_{m+2} \cdots (a)$$
$$= 0.\overline{s_{m+1} \cdots s_{m+r}}(a)$$

한편, $u = 0.\overline{s_1 s_2 \cdots s_m}(a)$이라고 가정하면,

$$s_i = s_{m+i} \qquad (i=1,\ 2,\ 3,\ \cdots)$$

이므로

$$\frac{c_0}{q} = u = 0.s_1 s_2 \cdots s_m s_{m+1} s_{m+2} \cdots s_n (a)$$
$$= 0.s_{m+1} s_{m+2} \cdots s_{2m} s_{2m+1} \cdots s_n \cdots (a) = \frac{c_m}{q}$$

즉 $c_0 = c_m$이고 따라서 $m \equiv 0 \pmod r$이다. 그러므로 $= 0.\overline{s_1 s_2 \cdots s_r}(a)$의 주기는 r 이다. 더욱이 $a^{n-1} < q < a^n$일 때,

$$\frac{a^r-1}{a^n} < s = \frac{a^r-1}{q} < \frac{a^r-1}{a^{n-1}}$$

즉 $a^{r-n} = \frac{a^r}{a^n} \le s < a^{r-n+1}$

이므로 $r-n \ge 0$ 즉 $0 \le n < r$ 이고 또

$$s = q^1 a^{r-1}+q_2 a^{r-2}+\cdots+q_r$$
$$(0 \le q_1 < a,\ 0 \le q_2 < a,\ \cdots,\ 0 \le q_r < a)$$

이라고 하면 $q_1 = q_2 = \cdots = q_{n-1} = 0$, $q^n \ne 0$이다.

앞의 정리에 의한면, $(10, q) = 1$인 경우에 즉 2와 5가 q의 소인수가 아닐 때, 10진법으로 $1/q$ 는 순환소수로 나타내어진다. 그리고, $(2, q)=1$일 때, 2진법으로 $1/q$ 는 순환소수로 나타내어진다. 그리고 법 q에 관한 a의 위수는 $\varphi(q)$의 약수이고 또 다음이 성립한다.

$$a_{n-1} < q < a \iff n = 1 + [\log_a q]$$
$$\iff (a\text{진법으로 나타낼 때 } q\text{는 } n\text{자리의 수})$$

보기 6.3 $a=10$, $q = 7$일 때, $\varphi(7) = 6$이고 a는 法 7에 관한 원시근이다. 한편,

$$1 < 7 < 10,\ \frac{10^6-1}{7} = 142857$$

이므로

$$\frac{1}{7} = 0.\overline{142857}$$

이고 다음이 성립한다.

$10^0 \equiv 1 \pmod 7$, $\frac{1}{7} = 0.\overline{142857}$

$10^1 \equiv 3 \pmod 7$, $\frac{3}{7} = 0.\overline{428571}$

$10^2 \equiv 2 \pmod 7$, $\frac{2}{7} = 0.\overline{285714}$

$10^3 \equiv 6 \pmod 7$, $\frac{6}{7} = 0.\overline{857142}$

$10^4 \equiv 4 \pmod 7$, $\frac{4}{7} = 0.\overline{571428}$

$10^5 \equiv 5 \pmod 7$, $\frac{5}{7} = 0.\overline{71428}$

법 q에 관한 원시근 a가 존재할 때, 법 q에 관한 a 의 위수는 $\varphi(q)$ 이므로 a진법으로 $1/q$는 주기가 $\varphi(q)$인 순환소수로 나타내어진다.

예를 들어 素數 p가

7, 17, 19, 23, 29, 47, 59, 61, …, 503, …

일 때 10은 법 p에 관한 원시근이고, p가

3, 5, 9, 11, 13, 19, 25, 27, 29, 37, …

일 때 2는 법 p에 관한 원시근이다.

보기 6.4 $a=2$, $p=13$일 때, 2는 법 13에 관한 원시근이다. 한편,

$$2^3<13<2^4, \quad \frac{2^{12}-1}{13} = 100111011_{(2)}$$

이므로 다음이 성립한다.

$2^0 \equiv 1 \pmod{13}$, $2^1 \equiv 2 \pmod{13}$,

$2^2 \equiv 4 \pmod{13}$, $2^3 \equiv 8 \pmod{13}$,

$2^4 \equiv 3 \pmod{13}$, $2^5 \equiv 6 \pmod{13}$,

$2^6 \equiv 12 \pmod{13}$, $2^7 \equiv 11 \pmod{13}$,

$2^8 \equiv 9 \pmod{13}$, $2^9 \equiv 5 \pmod{13}$,

$2^{10} \equiv 10 \pmod{13}$, $2^{11} \equiv 7 \pmod{13}$,

$$\frac{1}{13} = 0.\overline{000100111011}_{(2)}$$
$$\frac{2}{13} = 0.\overline{001001110110}_{(2)}$$
$$\frac{4}{13} = 0.\overline{010011101100}_{(2)}$$
$$\frac{8}{13} = 0.\overline{100111011000}_{(2)}$$
$$\frac{3}{13} = 0.\overline{001110110001}_{(2)}$$
$$\frac{6}{13} = 0.\overline{011101100010}_{(2)}$$
$$\frac{12}{13} = 0.\overline{111011000100}_{(2)}$$
$$\frac{11}{13} = 0.\overline{110110001001}_{(2)}$$
$$\frac{9}{13} = 0.\overline{101100010011}_{(2)}$$
$$\frac{5}{13} = 0.\overline{011000100111}_{(2)}$$
$$\frac{10}{13} = 0.\overline{100010011101}_{(2)}$$
$$\frac{7}{13} = 0.\overline{100010011101}_{(2)}$$

다음 정리의 증명은 생략하기로 한다.

定理 6.2 p 가 홀수인 素數일 때, g 를 법 p 에 관한 원시근이라 하고

$$g^{n-1}<p<g^n \text{ 즉 } n = 1+[\log_g p]$$

이라고 하자. 이 때, $1 \le c \le p-1$인 정수 c에 대하여

$$\frac{c}{p} = 0.\overline{s_1 s_2 \cdots s_{p-1}}_{(g)}$$
$$= 0.s_1 s_2 \cdots s_p s_{p+1} \cdots s_n \cdots_{(a)}$$

이라고 하면 다음이 성립한다.

(1) 임의의 $n-1$개의 원소

$$a_1, a_2, \cdots, a_{n-1} \quad (0 \le a_i \le g-1)$$

에 대하여

$$a_1 = s_{m+1}, \ a_2 = s_{m+2}, \ \cdots, \ a_{n-1} = s_{m+n-1}$$

인 정수 m $(0 \le m \le p-2)$이 적어도 하나 존재한다.

(2) 임의의 n개의 원소

$$a_1, a_2, \cdots, a_n \quad (0 \le a_i \le g-1)$$

에 대하여

$$a_1 = s_{m+1}, \ a_2 = s_{m+2}, \ \cdots, \ a_{n-1} = s_{m+n-1}$$

인 정수 m $(0 \le m \le p-2)$은 많아야 하나 존재한다.

위의 定理의 無限數列

$$s_1, s_2, s_3 \cdots, s_{p-1}, \ s_1, s_2, s_3 \cdots, s_{p-1}, \ \cdots$$

이 위의 두 조건을 만족시킨다는 의미에서 이 수열을 g 를 밑으로 가지는 주기가 $p-1$ 인 de Bruijn 數

列이라고 한다.

보기 6.5 앞의 보기 6.3에 의하여

1, 4, 2, 8, 5, 7, 1, 4, 2, 8, 5, 7, …

는 10을 밑으로 가지는 주기 6인 de Bruijn 수열이다. 또, 보기 6.4에 의하여

0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, …

는 2를 밑으로 가지는 주기 12인 de Bruijn 수열이다.

參 考 文 獻

1. Blum, L., Blum, M., and M. Shub, A simple secure pseudo-random generator, IEEE *Crypto* 82, 1982.

2. Desmedt, Y., Vandewalle, J. and R. Govaerts, Critical analysis of the Security of knapsack public key algorithms, in Proceeding of the IEEE *Internation Symposium on Information Theory* (1982), 115-116.

3. Koblitz, N., A coure in number theory and cryptography, *Springer-Verlag*, New York, 1987.

4. Kranakis, E., *Primality and cryptography*, John Wiley, New York, 1986.

5. Merkle, R.C. and M.E. Hellman, Hiding information and signature in trapdoor knapsacks, IEEE *Trans*. IT-24 (1978), 525-530.

6. Rivest, R.L., Shamir, A. and L.A. Adleman, A method for obtaining digital signatures and public key cryptosystems, *Comm. ACM 21*(1978), 120-126.

7. Shamir, A, Rivest, R.L., and L.A. Adleman, Mental poker, in the Mathematical Gardener, edited by Klarner, D., 1981, 37-43.

8. Shamir, A., A polynomial time algorithm for breaking Merkle-Hellman cryptosystems, *The Weizmann institute*, Rehovot, Israel.

9. Simmons, G.J., Contemporary cryptology, The science of information integrity, IEEE *Press*, New York, 1992.

10. 金應泰 · 朴勝安, **整數論**, 제 3 판, 경문사, 1991.

11. 金應泰 · 朴勝安, **線型代數學**, 청문각, 1991.

12. 朴勝安, GF(2)위의 고차다항식 및 이진수열에 관한 수학적 연구, 한국전자통신연구소, 1986.

13. 박승안 · 이민섭 · 이재학 · 신현용, **代數的符號理論**, 체신부, 1991.

14. 박승안 · 이민섭 · 이재학 · 신현용, Trapdoor one way function인 hard computational 문제에 관한 연구, 한국전자통신연구소 연구보고서, 1991.

□ 著者紹介

朴 勝 安(正會員)

서울대학교 師範大學 數學科(理學士)
서울대학교 大學院 數學科(理學碩士)
University of Illinois at Urbana 大學院 數學科(理學碩士, 理學博士)
西江大學校 이공대학 數學科, 조교수, 부교수, 교수
大韓數學會 편집이사, 무임소 이사
University of Illinois at Urbana, 방문교수
現 西江大學校 理工大學 數學科 教授
韓國通信情報保護學會 교육·호보 이사