通信情報保護學會誌
第1卷, 第2號, 1991. 8

初等 整數論과 暗號學
(1)

朴 勝 安*

1. 서 론

抽象代數學 및 整數論의 이론은 수학의 모든 분야에 이용될 뿐만이 아니라, 自然科學, 人文科學, 社會科學에 이용되며 근래에 와서는 電子計算學, 情報通信學 및 暗號學에 널리 이용되고 있다.

특히, 암호학과 정보통신학에 쓰이는 알고리즘은 수준 높은 代數學에 대한 이론을 그 바탕으로 하고 있다. 예를 들어, stream cipher 체계에 사용되는 二進數列에 대한 이론을 연구하는 데에는 有限體(finite field) 및 그 곱셈 群의 대수적 구조에 관한 이론과 多項式論에 대한 이론을 필요로 하고, 정수 및 특정한 다항식의 因數分解 알고리즘을 개발하는 데에는 有限群論, 射影幾何學에 대한 지식과 旣約基底(reduced basis)에 대한 지식이 요구된다. 또, 符號理論(coding theory)을 이해하는 데에는 有限體, 有限群, 環, 行列에 대한 이론에 대한 이해가 필요하다[14, 15, 16]. 또, 素數 判定法, 公開 열쇠 暗號體系의 연구에는 고급의 정수론과 確率論이 이용된다[4, 5].

이 논문에서는 初等 整數論에서 다루는 合同式에 대한 이론을 소개하고 이들 이론이 암호학에 어떻게 이용되는지를 논하기로 한다.

初等 整數論은 정수의 因數分解, 素數 判定法, 公開 열쇠 暗號體系(public key cryptosystem), 디지탈 署名(digital sinature), 認證, knapsack 문제 등에 대한 알고리즘을 이해하는 데 필요한 수학적 이론을 제공해 준다. 실제로, 초등 정수론에서 다루는 논제로서 암호학과 정보통신학에 응용되는 것으로서는

여러가지 유형의 合同式(congruence),
位數(order), 原始根(primitive root),
離散로그(discrete logarithm),
二次剩餘(quadratic residue)와 Legendre 기호,
二次體, 連分數(continued fraction),
여러가지 不定方程式(Diophantine equation)

등이 있다.

이 논문의 제2절에서는 合同式에 대한 기초사항과 Euler의 정리, 중국인의 나머지 정리 등을 간단히 논하고 제3절과 제4절에서는 다음 사항에 근거가 되는 정리를 증명하여 이를 실제로 적용하는 방법을 다루기로 한다.

(1) 중국인의 나머지 정리의 응용,
(2) 公開 열쇠 暗號體系,
(3) knapsack 문제
(4) 디지탈 署名, 認證과 관련된 문제

* 정회원, 서강대학교 이공대학 수학과 교수

2. 合同式

두 정수 a, b의 최대공약수를 $\gcd(a, b)$ 또는 (a, b)로 나타낸다. 특히, $\gcd(a, b)=1$ 일 때 두 정수 a와 b는 서로 素(relatively prime)라고 한다. Euclid의 互除法(Euclidean algorithm)에 의하면 두 정수 a, b의 최대공약수가 d일 때

$$d = as + bt$$

인 정수 s, t가 존재한다.

고정된 양의 정수 n에 대하여 두 정수 a, b의 차 $a-b$가 n의 倍數일 때, a와 b는 法(modulus) n에 관하여 서로 合同(congruent)이라 하고 이 사실을

$$a \equiv b \pmod{n}$$

으로 나타낸다.

정수 a를 n으로 나누었을 때의 몫과 나머지를 각각 q, r라고 하면

$$a \equiv nq + r, \qquad 0 \leq r < n$$

이고 이때 $a \equiv r \pmod{n}$이다. 따라서 임의의 정수 a는 집합 $\mathbf{Z}_n=\{0, 1, \cdots, n-1\}$에 속하는 한 정수와 법 n에 관하여 합동이다. 예를 들면,

$$12 \equiv 0 \pmod 4, \qquad 13 \equiv 1 \pmod 4$$

$$14 \equiv 2 \pmod 4 \qquad 15 \equiv 3 \pmod 4$$

정수에 대한 等式의 경우와 마찬가지로 合同式에 대해서는 다음이 성립한다.

(1) $a \equiv a \pmod n$

(2) $a \equiv b \pmod n$이면, $b \equiv a \pmod n$

(3) $a \equiv b \pmod n$, $b \equiv c \pmod n$이면, $a \equiv c \pmod n$

(4) $a \equiv b \pmod n$, $c \equiv d \pmod n$이면,
$a \pm c \equiv b \pm d \pmod n$,
$ac \equiv bd \pmod n$
$a^m \equiv b^m \pmod n$

이 밖에도 합동식에 대해서는 다음이 성립한다.

(5) $ac \equiv bc \pmod n$일 때, $\gcd(c, n) = 1$이면 $a \equiv b \pmod n$

(6) $a \equiv b \pmod n$이면, $\gcd(a, n) = \gcd(b, n)$

양의 정수 $1, 2, \cdots, n$ 중에서 n과 서로 소인 정수의 개수를 $\varphi(n)$으로 나타낸다. 예를 들면,

$\varphi(1)=1$, $\varphi(2)=1$, $\varphi(3)=2$,
$\varphi(4)=2$, $\varphi(5)=4$, $\varphi(6)=2$,
p가 素數일 때, $\varphi(p^k)=p^k-p^{k-1}$

定理 2.1 (Euler의 정리) $\gcd(a, n) = 1$이면

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

따름定理 2.2 (Fermat의 정리) p가 素數일 때, $\gcd(a, p) = 1$이면, $a^{p-1} \equiv 1 \pmod p$이다.

따름定理 2.3 p가 素數일 때,

(1) 임의의 정수 a 대하여
$a^p \equiv 1 \pmod p$

(2) 임의의 정수 a, b에 대하여
$(a+b)^p \equiv a^p + b^p \pmod p$
$(ab)^p \equiv a^p b^p \pmod p$

Euler의 정리에서 '$\gcd(a, n)=1$'이라는 조건은 반드시 있어야 한다. 예를 들어

$$\varphi(4)=2, \qquad 3^2 \equiv 9 \equiv 1 \pmod 4$$

이지만, $2^2 \equiv 4 \equiv 0 \pmod 4$이다.

정수를 계수로 가지는 다항식

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$

에 대하여 $a_n \not\equiv 0 \pmod n$인 경우에 합동식

$$f(x) \equiv 0 \pmod n$$

을 n차의 **合同式**이라고 한다.

한 정수 u에 대하여 $f(u) \equiv 0 \pmod n$일 때,

$$x \equiv u \pmod n$$

를 합동식 $f(x) \equiv 0 \pmod n$의 解(solution)라고 한다. 예를 들면

$$0^2 \equiv 0 \pmod 4, \qquad 1^2 \equiv 1 \pmod 4$$

$$2^2 \equiv 0 \pmod 4, \qquad 3^2 \equiv 1 \pmod 4$$

이므로, 합동식 $x^2 \equiv 1 \pmod 4$은 두개의 해

$$x \equiv 1 \pmod 4, \quad x \equiv 3 \pmod 4$$

를 갖지만 합동식 $x^2 \equiv 2 \pmod 4$의 해는 없다.

定理 2.4 양의 정수 n에 대하여 $\gcd(a,n)=1$일 때, 일차합동식

$$ax \equiv b \pmod{n}$$

는 단 한개의 해를 가진다.

특히, $\gcd(a,n)=1$이면, $ac \equiv 1 \pmod{n}$인 정수 c가 존재한다.

실제로 $\gcd(a,n)=1$인 경우에 $as+nt=1$인 정수 s,t가 존재하고 이때 합동식 $ax \equiv b \pmod{n}$의 해는 $x \equiv sb \pmod{n}$이다. Euler의 정리를 이용하여 이 합동식의 해를 구하면 다음과 같다.

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

定理 2.5 (中國人의 나머지 정리, Chinese Remainder Theorem) 양의 정수 $n_1, n_2, \cdots, n_r$가 쌍마다 서로 소일 때, 즉 $\gcd(n_i,n_j)=1$, $i \neq j$일 때, 聯立一次合同式

$$\begin{cases} x \equiv c_1 \pmod{n_1} \\ x \equiv c_2 \pmod{n_2} \\ \cdots\cdots \\ x \equiv c_r \pmod{n_r} \end{cases}$$

는 법 $n_1 n_2 \cdots n_r$에 관하여 단 하나의 해를 가진다.

예를 들어, 연립일차합동식

$$\begin{cases} x \equiv c_1 \pmod{n_1} \\ x \equiv c_2 \pmod{n_2} \end{cases}$$

에 대하여 N_1과 N_2를

$$N_1 n_2 \equiv 1 \pmod{n_1},\ N_2 n_1 \equiv 1 \pmod{n_2}$$

인 정수라고 할 때,

$$x \equiv c_1 N_1 n_2 + c_2 N_2 n_1 \pmod{n_1 n_2}$$

은 이 연립일차합동식의 해이다.

定理 2.6 두 양의 정수 m, n이 서로 소이면

$$\varphi(mn) = \varphi(m)\varphi(n)$$

또 정수 n의 표준분해가 $n = p_1^{e_1} \cdots p_r^{e_r}$이면,

$$\varphi(n) = (p_1^{e_1} - p_1^{e_1-1}) \cdots (p_r^{e_r} - p_r^{e_r-1})$$

3. Euler의 定理의 應用

이 절에서는 중국인의 나머지 정리와 Euler의 정리가 暗號學에 어떻게 이용되는지를 살펴보기로 한다.

중국인의 나머지 정리(정리 2.5)는 서로 소인 두 양의 정수 n_1, n_2를 법으로 택하여 만든 두 가지 체계의 부호를 결합하는 경우에 이용된다.

그리고, 일반적인 體(field)의 원소를 계수로 가지는 다항식에 대해서도 이 정리와 비슷한 정리가 성립하며, 이 정리는 특히 有限體 위의 다항식을 既約다항식의 곱으로 인수분해하는 알고리즘에 이용된다[14].

서로 소인 두 양의 정수 n_1, n_2가 있을 때, 임의의 정수 c_1, c_2에 대하여 연립일차합동식

$$\begin{cases} x \equiv c_1 \pmod{n_1} \\ x \equiv c_2 \pmod{n_2} \end{cases}$$

의 해 $x \equiv a \pmod{n_1 n_2}$를 다음과 같이 간편하게 나타낼 수 있다.

실제로, 한 정수 a에 대하여

$$a \equiv c_1 \pmod{n_1},$$
$$a \equiv c_2 \pmod{n_2},$$

일 때, 이 사실을

$$a \equiv (c_1, c_2) \pmod{n_1 n_2}$$

으로 나타내면 주어진 연립일차합동식의 해는 다음과 같다.

$$x \equiv a \equiv (c_1, c_2) \pmod{n_1 n_2}$$

예를 들면,

$$51 \equiv 16 \equiv 1 \pmod{5}$$
$$51 \equiv 16 \equiv 2 \pmod{7}$$

이므로,

$$51 \equiv 16 \equiv (1,2) \pmod{35}$$

이고 연립일차합동식

$$\begin{cases} x \equiv 1 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

의 해는 $x \equiv 16 \pmod{35}$이다.

아래 표는 $n_1=5$, $n_2=7$인 경우에 대한 표이다.

c_1 \ c_2	0	1	2	3	4	5	6
0	**0**	15	30	10	25	**5**	20
1	21	**1**	16	31	11	26	**6**
2	**7**	22	**2**	17	32	12	27
3	28	**8**	23	**3**	18	33	13
4	14	29	**9**	24	**4**	19	34

위의 표에서 첫째 열의 맨 위에 0부터 시작하여 $-45°$ 방향으로 내려가면서 0, 1, 2, 3, 4가 차례로 나타나고 이어서 다음 열의 맨 위에 5부터 시작하여 $-45°$ 방향으로 내려가면서 5, 6이 차례로 나타나며, 첫째 열의 셋째 칸에 7이 나타난다.

일반적으로 서로 소인 두 양의 정수 n_1, n_2에 대한 표를 만들 때에는 c_1, c_2를

$$0 \leq c_1 < n_1, \quad 0 \leq c_2 < n_2$$

로 제한하고, 0에서 n_1n_2-1까지의 정수를 위의 표에서와 같이 늘어 놓으면 된다. 또한,

$$a \equiv (c_1, c_2) \pmod{n_1n_2},$$

$$b \equiv (d_1, d_2) \pmod{n_1n_2}$$

일 때, 다음이 성립함을 쉽게 알 수 있다.

$$a+b \equiv (c_1+d_1, c_2+d_2) \pmod{n_1n_2}$$

$$ab \equiv (c_1d_1, c_2d_2) \pmod{n_1n_2}$$

여기서 첫째 성분과 둘째 성분은 법 n_1, n_2에 관하여 계산한다. 예를 들면,

$$19 \equiv (4, 5) \pmod{35}$$

$$32 \equiv (2, 4) \pmod{35}$$

이므로

$$19+32 \equiv (6, 9) = (1, 2) \pmod{35}$$

$$19 \cdot 32 \equiv (8, 20) = (3, 6) \pmod{35}$$

다음에는 Euler의 정리의 응용에 대하여 생각하기로 한다. 비밀을 요하는 傳文을 상대방에게 송신하는 경우에는 먼저 보내려는 전문을 특정한 수 또는 수열로 나타낸 다음에 이 수열을 暗號文으로 바꾸어 보낸다. 公開 열쇠를 이용한 암호문의 전송에서는 덫문(trap door)과 같은 안전장치가 마련되어 있어야 한다. 예를 들면, 전자계산기를 이용하여 500자리의 두 素數를 곱하는 일은 쉬우나 500자리의 두 素數의 곱인 정수를 정당한 시간내에 인수분해하는 일은 거의 불가능하다. 또, 주어진 양의 정수 a, a, s에 대하여 $a^s \equiv b \pmod n$인 양의 정수 b를 구하는 일은 쉬우나, 주어진 양의 정수 n, s, b에 대하여 위의 합동식을 만족시키는 양의 정수 a를 구하는 일은 쉽지 않다.

定理 3.1 양의 정수 n, a, s에 대하여 다음 두 조건이 성립한다고 가정하자.

(i) $\gcd(a, n)=1$ (ii) $\gcd(s, \varphi(n))=1$

이 조건 아래에서 $a^s \equiv b \pmod n$일 때, t를

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

으로 정하면 $a \equiv b^t \pmod n$이다.

실제로 조건 (ii)와 Euler의 정리에 의하여

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

이므로, $st = 1+\varphi(n)k$인 정수 k가 존재한다.

한편, 조건 (i)와 Euler의 정리에 의하여

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

따라서 $a^s \equiv b \pmod n$일 때

$$b^t \equiv a^{st} = a^{1+\varphi(n)k} = aa^{\varphi(n)k} \equiv a \pmod n$$

보 기 $p=7$, $q=17$, $n=pq=187$일 때,

$$\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1) = 160$$

$$\varphi(\varphi(n)) = \varphi(160) = \varphi(2^5 \cdot 5) = 2^4 \cdot 4 = 64$$

이제 $a=3$, $s=7$로 택하면,

$$t \equiv s^{\varphi(\varphi(n))-1} \equiv 7^{63} \equiv 23 \pmod{160}$$

$$b \equiv a^s \equiv 3^7 \equiv 130 \pmod{187}$$

$$a \equiv b^t \equiv 130^{23} \equiv 3 \pmod{187}$$

앞에서 증명한 정리 3.1의 결과를 이용하면, 열쇠 관리센터 C가 비밀전문을 여러 사용자 $A_1, \cdots, A_n$에게 개별적으로 송신하는 공개 열쇠 암호체계를 논할 수 있다.

(1) 사용자 A는 대단히 큰 두 素數 p, q를 택하여

$$n = pq$$

의 값을 구한 다음에 p와 q의 값은 공개하지 않고 n의 값만을 공개한다.

(2) A는

$$\gcd(s, \varphi(n)) = 1, \qquad 0 < s < \varphi(n)$$

인 정수 s를 택하여 s의 값을 공개한다.

(3) A는

$$t \equiv s^{\varphi(\varphi(n))-1} \pmod{\varphi(n)},$$
$$0 < t < \varphi(n)$$

인 정수 t를 구하고 t의 값은 공개하지 않는다.

(4) 열쇠 관리센터 C는 A에게 송신하고자 하는 비밀전문을 양의 정수 $a\ (0 < a < n)$로 나타내고, A가 공개한 s를 이용하여

$$b \equiv a^s \pmod{n}, \qquad 0 < b < n$$

인 b를 계산하여 b의 값을 A에게 전송한다.

(5) A는 본인만이 알고 있는 t의 값을 이용하여

$$a \equiv b^t \pmod{n}, \qquad 0 < a < n$$

를 계산한다. 이로서 A는 C로부터 수신한 a의 값을 알 수 있다.

위의 단계 (1)에서 A가 상당한 큰 素數 p, q를 책하면 제삼의 解讀者가 n을 인수분해하는 일은 거의 불가능하고 따라서 $\varphi(n)$의 값을 구하기가 대단히 어렵다.

한편, 정리 3.1을 이용하려면 단계 (4)에서 a와 n이 서로 소이어야 한다. 그런데

$$\frac{\varphi(n)}{n} = \frac{(p-1)(q-1)}{pq} = \frac{p-1}{p}\,\frac{q-1}{q}$$

이고, 또 p와 q는 상당히 큰 素數이므로 C가 택한 정수 a와 n이 서로 소일 확률은 대단히 크고 따라서 이 사실은 무시하여도 좋다.

단계 (3)에서 t의 값을 구하려면

$$\varphi(\varphi(n)) = \varphi(\varphi(pq)) = \varphi((p-1)(q-1))$$

의 값을 구하여야 하고 이를 위해서는 $p-1$, $q-1$를 인수분해하여야 하나, 이 두 정수는 상당히 큰 정수이므로 이 정수를 인수분해하는 일은 대단히 어렵거나 불가능하다. 이러한 난점을 극복하려면 이미 알고 있는 素數를 이용하여 p, q를 정하는 것이 좋다. 예를 들면,

$$p - 1 = 2 \cdot 3 \cdot 11 = 66$$

다음에서는 Merkle－Hellman의 공개 열쇠 암호체계 중에서 간단한 체계를 소개한다.

임의의 양의 정수 a는 2의 거듭제곱인 정수

$$2^0, 2^1, 2^2, 2^3, 2^4, 2^5, \cdots$$

의 합으로 나타낼 수 있다. 실제로, 양의 정수 a에 대하여

$$a = a_r 2^r + a_{r-1} 2^{r-1} + \cdots + a_1 2^1 + a_0 2^0$$
$$(a_r, a_{r-1}, \cdots, a_1, a_0 \text{는 } 0 \text{ 또는 } 1)$$

일 때, a를 二進法으로

$$a = a_r a_{r-1} \cdots a_1 a_{0(2)}$$

으로 나타낸다. 예를 들어

$$53 = 32 + 16 + 4 + 1$$

이므로 $53 = 110101_{(2)}$이다.

한편,

$$2^{r-1} + \cdots + 2^1 + 2^0 = 2^{r-1} < 2^r$$

일반적으로 양의 정수로 이루어진 수열

$$c_0, c_1, c_2, \cdots, c_r, \cdots$$

에서 임의의 양의 정수 r에 대하여

$$c_0 + c_1 + c_2 + \cdots + c_{r-1} < c_r$$

일 때 수열 $\{c_r\}$를 超增加(super increasing) 수열이라고 한다. 수열 $\{2^r\}$는 超增加 수열이다.

定理 3.2 양의 정수 n, a, w 에 대하여 다음 세 조건이 성립한다고 가정하자.

(i) $\gcd(w,n)=1$

(ii) 적당한 超增加 수열 $\{c_r\}$에 대하여

$$a=a_rc_r+a_{r-1}c_{r-1}+\cdots+a_1c_1+a_0c_0$$

(iii) $w_i \equiv c_iw \pmod n$ $(i=0,1,2,\cdots,r)$

이 조건 아래에서

$$b \equiv a_rw_r+a_{r-1}w_{r-1}+\cdots+a_1w_1+a_0w_0 \pmod n$$

인 경우에, 정수 t 를 $wt \equiv 1 \pmod n$으로 정하면 $a \equiv bt \pmod n$이다.

실제로 $w_it \equiv c_iwt \equiv c_i \pmod n$이므로

$$bt \equiv \sum_{i=0}^{r} a_iw_it \equiv \sum_{i=0}^{r} a_ic_i \equiv a \pmod n$$

다음과 같이 knapsack을 이용한 공개 열쇠 암호 체계는 정리 3.2의 결과를 이용한 것이다.

불행하게도 이 방법이 안전하지 못하다는 사실이 밝혀졌다.

(1) 사용자 A는 먼저 超增加 수열

$$c_0,\ c_1,\ c_2,\ \cdots,\ c_r,\ \cdots$$

를 임의로 택하고 이를 공개하지 않는다.

(2) A는 상당히 큰 양의 정수 n 과

$$\gcd(w,n)=1,\quad 0<w<n$$

인 양의 정수 w 를 택하고, 또

$$wt \equiv 1 \pmod n,\quad 0<t<n$$

인 양의 정수 t 를 구한 다음에 n, w, t 의 값을 공개하지 않는다.

(2) A는 w 의 값을 이용하여

$$w_i \equiv c_iw \pmod n,$$
$$0<w_i<n \quad (i=0,1,2,\cdots)$$

인 정수 w_0, w_1, w_2, … 를 계산하여 이들 정수를 공개한다.

(3) C는 A에게 전송하고자 하는 비밀전문을 정수 a $(0<a<n)$로 나타낸 다음에 a 를 다음과 같이 나타낸다.

$$a=a_rc_r+a_{r-1}c_{r-1}+\cdots+a_1c_2+a_0c_0$$

다음에 C는 A가 공개한 w_0, w_1, w_2, …, w_r 를 이용하여

$$b=a_rw_r+a_{r-1}w_{r-1}+\cdots+a_1w_1+a_0w_0$$

를 계산하여 b 의 값을 A에게 송신한다.

(4) A는 본인만이 알고 있는 t 의 값을 이용하여

$$a \equiv bt \pmod n,\quad 0<a<n$$

를 계산한다.

이로서 A는 C로부터 수신한 a 의 값을 알수 있다.

4. 二次合同式의 應用

이 절에서는 특수한 유형의 二次合同式의 해들 사이의 관계를 논하고 그 응용문제를 논한다.

定理 4.1 p, q 가 서로 다른 홀수인 素數이고 또 $\gcd(a,pq)=1$일 때, 二次合同式

$$x^2 \equiv a \pmod{pq}$$

가 해를 가진다면 그 해는

$$x \equiv \pm x_0 \pmod{pq},\quad 1 \leq x_0 < pq$$
$$x \equiv \pm y_0 \pmod{pq},\quad 1 \leq y_0 < pq$$

의 꼴이며,

$$\gcd(x_0+y_0,\ pq),$$
$$\gcd(x_0-y_0,\ pq)$$

중 하나는 p 이고 다른 하나는 q 이다.

실제로 주어진 合同式이 解를 가지려면 합동식

$$x^2 \equiv a \pmod p,$$
$$x^2 \equiv a \pmod q$$

가 모두 解를 가져야 한다. 이 두 합동식은 각각

$$x \equiv \pm b \pmod p,$$
$$x \equiv \pm c \pmod q$$

의 꼴의 해를 가지며, 이 경우에 주어진 합동식의 해는 다음과 같은 4개의 聯立合同式의 해와 같다.

$$\begin{cases} x \equiv b \pmod{p} \\ x \equiv c \pmod{q} \end{cases}$$

$$\begin{cases} x \equiv -b \pmod{p} \\ x \equiv c \pmod{q} \end{cases}$$

$$\begin{cases} x \equiv b \pmod{p} \\ x \equiv -c \pmod{q} \end{cases}$$

$$\begin{cases} x \equiv -b \pmod{p} \\ x \equiv -c \pmod{q} \end{cases}$$

이제 정리 2.5를 이용하기 위하여

$$qN_1 \equiv 1 \pmod{p},$$

$$pN_2 \equiv 1 \pmod{q}$$

인 두 정수 N_1, N_2를 택하고 또

$$x_0 = bqN_1 + cpN_2,$$

$$y_0 = bqN_1 + cpN_2$$

이라고 놓으면 이들 연립합동식의 해는 각각 다음과 같다.

$$x \equiv x_0 \pmod{pq},$$

$$x \equiv y_0 \pmod{pq},$$

$$x \equiv -y_0 \pmod{pq},$$

$$x \equiv -x_0 \pmod{pq}$$

그런데,

$$\begin{aligned} x_0 + y_0 &= bqN_1 + cpN_2 - bqN_1 + cpN_2 \\ &= 2cpN_2, \end{aligned}$$

$$\begin{aligned} x_0 - y_0 &= bqN_1 + cpN_2 + bqN_1 - cpN_2 \\ &= 2bqN_1 \end{aligned}$$

이므로,

$$\gcd(x_0 + y_0,\ pq) = p,$$

$$\gcd(x_0 - y_0,\ pq) = q,$$

$$\gcd(-x_0 - y_0,\ pq) = p,$$

$$\gcd(-x_0 + y_0,\ pq) = q$$

한편, 가정에 의하여 $a \not\equiv 0 \pmod{pq}$이므로

$$x_0 \equiv 0 \pmod{pq},\quad y_0 \equiv 0 \pmod{pq}$$

이고, x_0, $-x_0$ 그리고 y_0, $-y_0$ 중에서 하나는 양의 정수이다. 따라서 정리가 성립한다.

서로 다른 두 홀수인 素數 p, q의 곱으로 인수분해되리라고 예상되는 양의 정수 n이 있을 때, 이차합동식

$$x^2 \equiv 1 \pmod{n}$$

을 만족시키는 두 정수

$$x_0 = 1,$$

$$y_0 \quad (1 < y_0 < n-1)$$

를 구하면 앞의 定理 4.1에 의하여

$$\gcd(x_0 + y_0,\ n),\quad \frac{n}{\gcd(x_0 + y_0,\ n)}$$

은 n의 두 素因數이다.

보 기 $x^2 \equiv 1 \pmod{341}$에 대하여 생각해 보자. 먼저, $341 = 11 \cdot 31$이며, 두 합동식

$$x^2 \equiv 1 \pmod{11},$$

$$x^2 \equiv 1 \pmod{31}$$

의 해는 각각 다음과 같다.

$$x \equiv \pm 1 \pmod{11},$$

$$x \equiv \pm 1 \pmod{31}$$

따라서 주어진 이차합동식의 해는 다음과 같다.

$$x \equiv \pm 1 \pmod{341},$$

$$x \equiv \pm 32 \pmod{341}$$

정리 4.1의 결과는 의사결정 문제나, 디지탈 署名 또는 認證 등에 이용된다.

서로 멀리 떨어져 있는 두 단체의 대표 A, B가 전화를 이용하여 동전던지기로 可否를 결정하여야 하는 경우를 생각해 보자. 이 때, A가 동전을 던지고 그 결과를 B에게 알려주기로 한다면 A가 속일 수도 있고, B가 이를 믿지 않을 수도 있다. 이러한 경우에 定理 4.1의 결과를 이용하여 다음과 같이 하면 이러한 여러가지 어려움을 쉽게 해결할 수 있다.

(1) A는 상당히 큰 홀수인 素數 p,q 를 택하여

$$n=pq$$

를 계산하고 B에게 n 의 값만을 알려준다.

(2) B는 n 보다 작은 양의 정수 x_0 를 임의로 택하고, $a \equiv x_0 \pmod{n}$, $1<a<n$인 양의 정수 a 를 구하여 A에게 a 의 값만을 알려준다.

(3) A는 이미 알고 있는 두 素數 p,q 를 이용하여 이차합동식 $x^2 \equiv a \pmod{n}$ 의 해

$$x \equiv \pm x_0 \pmod{n}, \quad 1<x_0<n$$

$$x \equiv \pm y_0 \pmod{n}, \quad 1<y_0<n$$

를 구한 다음에 B에게 x_0 또는 y_0 의 값을 알려준다.

(4) B는 A가 알려준 정수의 제곱을 n 으로 나누었을 때의 나머지가 a 인지를 조사한다.

이와 같이 함으로써 B는 A가 잘못 계산하였는지 또는 속이고 있는지를 확인할 수 있다.

(5) A가 B에게 x_0 를 통보한 경우에 A가 이기는 것으로 하고, 반대로 y_0를 통보한 경우에는 B가 이기는 것으로 정한다.

(6) A가 B에게 y_0 를 통보한 경우에 B는 y_0 의 값과 이미 알고 있는 x_0 의 값을 이용하여

$$\gcd(x_0+y_0,\ n), \quad \frac{n}{\gcd(x_0+y_0,\ n)}$$

를 계산하면 B는 n 의 두 素因數 p,q 를 구할 수 있다. B는 p,q 의 값을 A에게 알려줌으로써 B가 이겼음을 A에게 확인시킨다.

參 考 文 獻

1. 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.

2. Diffie, W. and M.E. Hellman, *New Directions in Cryptography*, IEEE Trans. on Information Theory, IT-22(1976), 644-465.

3. Goldwasser, S. and S. Micali, *Probabilistic Encryption and how to play mental poker*, in Proceedings of the 4th ACM Symposium on the Thoery of Computing, 1982, 365-372.

4. Koblitz, N., *A Coure in Number Theory and Cryptography*, Springer-Verlag, New York, 1987.

5. Kranaskis, E., *Primality and Cryptography*, John Wiley, New York, 1986.

6. Merkle, R.C. and M.E. Hellman, *Hinding Information and Signature in Trapdoor Knapsacks*, IEEE Trans. IT-24(1978), 525-530.

7. Rivest, R.L., Shamir, A. and L.A. Adleman, A Method for obtaining Digital Signatures and Public Key Cryptosystems, Comm. ACM, 21(1878), 120-126.

8. Schroeder, M.R., *Number Theory in Science and Communications*, Springer-Verlag, New York, 1984.

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

10. Shamir, A., *A Polynomial Time Algorithm for breaking Merkle-Hellman Cryptosystems*, Internal Report Applied Math., The Weizmann Institute, Rehovot, Israel.

11. 金應泰·朴勝安, 現代代數學, 제 3 판, 경문사, 1991.

12. 金應泰·朴勝安, 整數論, 제 3 판, 경문사, 1991.

13. 金應泰·朴勝安, 線型代數學, 청문각, 1991.

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

15. 朴勝安, 타원곡선을 이용한 정수의 인수분해 알고리즘과 Basis reduction 알고리즘에 관한 연구, 한국전자통신연구소, 1987.

16. 朴勝安·이민섭·이재학·신현용, 代數的 符號理論, 세신부, 1991.

□ 著者紹介

朴 勝 安(正會員)

서울大學校 師範大學 數學科(理學科)
서울大學校 大學院 數學科(理學碩士)
University of Illinois at Urabana 大學院 數學科(理學碩士, 理學博士)
西江大學校 理工大學 數學科 助教授, 副教授, 教授
大韓數學會 編輯理事, 무임소 이사
University of Illinois at Urabana, 數學科 訪問教授
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 教育·弘報 理事