通信情報保護學會誌
第2卷 第2號, 1992.3

Legendre 기호와 암호학

오정환*, 김 철**

1. 서 론

본 논제에서는 원시근과 이차 잉여류를 중심으로 관련되는 암호학에 이용을 언급하기로 한다. 이외에도 이산로그(discrete logarithm), 연분수(continued fraction), 여러 부정 방정식(diophantine equation)의 이론등이 암호학에서 빈번히 사용되는 알고리즘의 근간을 이루는 이론들로 알려져 있다. 또한, 유사임의 수열(pseudo-random number sequence)을 만들기 위한 생성자(generator)들 중에는 정수론에 기초하고 있는 것들이 많이 있다.

제 2 절에서는 정수의 위수와 원시근에 대한 성질을 논하고, 제 3 절에서는 2 차 잉여류와 Legendre 기호를 소개한 후, 제 4절에서 이들이 주로 사용되는 암호학의 분야를 논하기로 한다.

2. 위수(order)와 원시근(primitive root)

이 절에서는 정수 a의 법 p에 관한 위수와 원시근에 대한 이론과 이를 이용하는 합동식의 해를 위한 필요충분조건을 소개한다.

정의 2.1 p는 소수, $a \not\equiv 0 \pmod p$인 정수일 때, $a^k \equiv 1 \pmod p$를 만족하는 최소의 양의 정수 k를 a의 법 p에 관한 위수(order of a, mod p)라 하고, $\mathrm{ord}_p a = k$로 나타낸다.

예컨데, $\mathrm{ord}_7 2 = 3$, $\mathrm{ord}_7 3 = 6$, $\mathrm{ord}_7 6 = 2$ 이다. 또한, Fermat의 정리에 의하여 $\mathrm{ord}_p a$는 $1 \le \mathrm{ord}_p a \le p-1$를 만족하는 정수이다.

정의 2.1 정수 a가 소수 p와 서로 소일때, 위수에 관한 다음과 같은 기본적인 세 가지 성질이 있다.

(i) $\mathrm{ord}_p a \mid p-1$,

(ii) $a^b \equiv 1 \pmod p \Leftrightarrow \mathrm{ord}_p a \mid b$,

(iii) $\mathrm{ord}_p a^m = \dfrac{\mathrm{ord}_p a}{\gcd(m, \mathrm{ord}_p a)}$.

증명 [Bu]의 184쪽 참고. ■

$p \nmid a$이고, a^*가 법 p에 관한 a의 역원 (즉, $aa^* \equiv 1 \pmod p$)이면, $\mathrm{ord}_p a = \mathrm{ord}_p a^*$이다. 이 성질을 이용하여 p가 소수이고, 정수 $a_1, a_2, \cdots\cdots, a_r$이 p와 서로 소이며, $\mathrm{ord}_p a_i = k_i$ 이고, 또, $\gcd(k_i, k_j) = 1, i \neq j$ 이면, $\mathrm{ord}_p (a_1 a_2 \cdots\cdots a_r) = k_1 k_2 \cdots\cdots k_r$ 이 됨을 쉽게 보일 수 있다.

* 연세대학교 수학과 교수
** 광운대학교 수학과 조교수

정의 2.2 어떤 정수 g에 대하여,

$$g^0 = 1,\ g^1,\ g^2,\ \cdots,\ g^{p-2}$$

가 법 p의 기약 잉여계(reduced set of residues, mod p)를 이룰때, 이 g를 법 p의 원시근(primitive root, mod p)이라 한다. g가 법 p의 원시근이 되기 위한 필요충분조건은 $\mathrm{ord}_p g = p-1$이다.

이상에서 기술한 한 법 p의 원시근이나, 위수의 정의 및 그 성질과, $k \mid p-1$ (p는 소수)이면, 합동식 $x^k - 1 \equiv 0 \pmod p$는 명확히 k개의 근을 갖는다는 성질 ([Bu]의 192쪽 참고)로부터 법 p의 원시근이 존재함을 보일 수 있다.

보기 p=23의 원시근을 구하려면, $p-1 = 22 = 2 \cdot 11$ 이므로, $\mathrm{ord}_{23} g_1 = 2$, $\mathrm{ord}_{23} g_2 = 11$을 만족하는 g_1과 g_2를 구하여 그 곱을 만들면, 그것이 법 p의 원시근이다. 계산에 의하면, $g_1 = -1$, $g_2 = 2$가 되므로, -2가 법 p=23의 하나의 원시근이다.

원시근의 용도를 좀더 자세히 살펴보기 위하여, 이제 g를 법 p의 원시근이라 하자. 그러면 $g^0,\ g^1,\ \cdots,\ g^{p-2}$는 법 p의 기약 잉여계가 된다. 따라서 이들 중 어느 두개도 법 p에 관하여 합동이 아니다. 그렇다면 일반적으로 언제 법 p에 관하여

임의의 $i < j$에 대하여, $g^i \equiv g^j \pmod p$

가 성립하는가를 조사해 보자. 즉, 윗 식은 $g^{j-i} \equiv 1 \pmod p$와 같으므로,

$\mathrm{ord}_p g = p-1 \Rightarrow p-1 \mid j-i$이며, 역으로,
$p-1 \mid j-i \Rightarrow j = i + k(p-1)$이 되어
$g^j = g^{i+k(p-1)} = g^i (g^{p-1})^k \equiv g^i 1^k = g^i \pmod p$이다.

이상에서 우리는 다음과 같은 결론을 얻을 수 있다.

정리 2.2 g가 법 p의 원시근이면, $g^i \equiv g^j \pmod p$가 되기 위한 필요충분조건은 $i \equiv j \pmod{p-1}$이다.

이와 같이 원시근을 이용하면, 마치 logarithm의 경우와 비슷하게, 법 p에 관한 곱셈의 문제를 법 p-1에 관한 덧셈의 문제로 바꿀 수가 있다. 하나의 보기로 다음 문제를 상세히 연구해 보기로 한다.

정수 $n > 0$, a에 대한 다음 합동식의 해의 존재에 대하여 생각하여 보자.

$$x^n \equiv a \pmod p \qquad (1)$$

이 합동식에서 $p \mid a$이면, $a \equiv 0 \pmod p$이고, 따라서 $x^n \equiv 0 \pmod p$, 즉, $x \equiv 0 \pmod p$와 같으므로, 앞으로는 $p \nmid a$라 하자. (1)의 해가 항상 존재하는 것은 아니다. 예컨대,

$$x^2 \equiv 2 \pmod 2$$

는 해가 없다. 왜냐하면, $x \equiv 1,2,3,4 \pmod 5$의 각각을 제곱하면, $x^2 \equiv 1,4,4,1 \pmod 5$로 되기 때문이다.

이제 합동식 (1)에 해를 가지기 위한 조건을 조사해 보자. 법 p의 한 원시근 g를 고정하고, $g^0, g^1, \cdots, g^{p-2}$를 법 p의 기약 잉여계라 하자. $p \nmid a$이므로 정수 b가 존재하여 다음 식을 만족한다.

$$a \equiv g^b \pmod p \qquad (2)$$

(1)의 해 x는 p로 나누어지지 않으므로, $x \equiv g^y \pmod p$의 꼴로 쓸 수 있다. 이 x와 (2)를 (1)에 대입하면,

$$g^{ny} \equiv g^b \pmod p$$

로 되어 결국은 $ny \equiv b \pmod{p-1}$과 같은 1차 합동식으로 변형된다. 잘 알려져 있는 바대로 이 합동식이 해 y를 가지기 위한 필요충분조건은 $\gcd(n, p-1) \mid b$이다. 이상을 요약하면 다음과 같다.

정리 2.3 정수 p와 정수 a에 대하여, $p \nmid a$라 하고 정수 g를 법 p의 원시근이라 하자. 또, $a \equiv g^b \pmod p$라 하면, 합동식 $x^n \equiv a \pmod p$가 해를 갖기 위한 필요충분조건은 $\gcd(n, p-1) \mid b$이다.

보기 p=23일 때를 생각하자. -2가 법 23의 원시근임을 이용하여, $a \equiv (-2)^b \pmod{23}$라 놓을 때, $x^n \equiv a \pmod{23}$이 해를 갖기 위해서는 $\gcd(n, 22) \mid b$가 성립하여야 한다. 따라서, n=2이면, b는 짝수여야 하고, n=11이면, b는 11의 배수가

되어야 한다. 또 $2 \nmid n$이고, $11 \nmid n$이면, b는 임의의 정수라도 해를 가진다.

보기 법 p=23의 원시근 $g = -2$의 제곱표,

b	0	1	2	3	4	5	6	7
g^b	1	21	4	14	16	14	18	10

8	9	10	11	12	13	14
3	17	12	22	2	19	8

15	16	17	18	19	20	21
7	9	5	13	20	6	11

를 이용하여 합동식 $x^7 \equiv 17 \pmod{23}$을 풀어보자. 위의 표에서 $17 \equiv (-2)^9 \pmod{23}$이고, $x \equiv (-2)^y \pmod{23}$이라고 놓으면, 합동식 $x^7 \equiv 17 \pmod{23}$은 다음과 같이 쓸 수 있다.

$$(-2)^{7y} \equiv (-2)^9 \pmod{23}.$$

이 식은 $7y \equiv 9 \pmod{22}$와 동치이므로, $y \equiv 17 \pmod{22}$를 얻고, x의 식에 대입하면 $x \equiv 5(-2)^{17} \equiv \pmod{23}$이 본래 합동식의 해가 된다.

Euler의 판정식 p는 소수이고, a는 $\gcd(p, a)=1$인 정수, n은 양의 정수라 할 때, $s=\gcd(n, p-1)$이라 하면, 합동식 $x^n \equiv a \pmod{p}$가 해를 갖기 위한 필요충분조건은 $a^{\frac{(p-1)}{s}} \equiv 1 \pmod{p}$이다.

보기 소수 p가 3이 아닌 홀수이며, a는 $3 \nmid a$을 만족한다고 하자. 그러면 합동식 $x^3 \equiv a \pmod{p}$는 $p \equiv 2 \pmod{3}$이면, 언제나 해를 가지고, $p \equiv 1 \pmod{3}$일 때에는 $a^{\frac{(p-1)}{3}} \equiv 1 \pmod{p}$일 때에만 해를 가진다.

3. 2차 합동식과 Legendre기호

이 절에서는 2차 잉여류와 Legendre기호, 그리고 이차 잉여의 상호법칙에 대하여 언급한다. 일반적인 2차 합동식 $ax^2 + bx + c \equiv 0 \pmod{n}$은 n의 소인수 p를 법으로 하는 합동식으로, 즉, $ax^2 + bx + c \equiv 0 \pmod{p}$로 변환하고, 이 합동식은 다시 일반 2차 방정식의 근의 공식을 유도할 때와 비슷한 방법에 의하여 결과적으로는 $x^2 \equiv a \pmod{p}$를 푸는 문제로 귀착한다.

정의 3.1 $x^2 \equiv a \pmod{p}$가 해를 가질때, a를 법 p의 2차 잉여류(quadratic residue, mod p)라 하고, 해를 가지지 않을 때, a를 법 p의 2차 비 잉여류(quadratic non-residue, mod p)라 한다.

p가 소수이고 a가 법 p의 2차 잉여류이면, $p \nmid a$이고, 어떤 x가 존재하여 $a \equiv x^2 \pmod{p}$가 성립한다. 그런데 이 임의의 정수 x는 $0, 1, 2, \cdots\cdots, p-1 \pmod{p}$ 중의 어느 하나와 합동하므로, a는

$$1^2, 2^2, \cdots\cdots, (p-1)^2 \pmod{p}$$

의 어느 하나와 합동이다. 실제로는 $p-x \equiv -x \pmod{p}$이므로, $(p-x)^2 \equiv (-x)^2 \pmod{p}$, 즉, $(p-x)^2 \equiv (x)^2 \pmod{p}$가 성립한다. 따라서, a가 법 p의 2차 잉여류가 되기 위해서는 a는

$$1^2, 2^2, \cdots\cdots, (\tfrac{p-1}{2})^2 \pmod{p}$$

중의 어느 하나와 합동이다. 그리고 이들은 어느 두 정수도 법 p에 관하여 합동이 되지 않는다. 따라서 정수 $1, 2, \cdots\cdots, p-1$중에는 꼭 $(\frac{p-1}{2})$개의 2차 잉여류와, 꼭 $(\frac{p-1}{2})$개의 2차 비 잉여류가 있다.

정의 3.2 소수 p가 홀수이고, $p \nmid a$일때, Legendre의 기호$(\frac{a}{p})$는 다음과 같이 정의한다.

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & a\text{가 법 p의 2차 잉여류인 경우} \\ -1, & a\text{가 법 p의 2차 비잉여류인 경우} \end{cases}$$

보기 p=13 일 때의 2차 잉여류와 2차 비 잉여류를 구하고, 해당되는 Legendre의 기호를 계산해 보자. $(\frac{p-1}{2}) = 6$이므로, 법 13의 2차 잉여류는 $1^2, 2^2, 3^2, 4^2, 5^2, 6^2$ 즉, 1, 4, 9, 3, 12, 10이고, 2차 비 잉여류는 2, 5, 6, 7, 8, 11이다. 따라서 다음과 같은 Legendre의 기호의 값을 얻는다. $(\frac{2}{13}) = -1$, $(\frac{3}{13}) = 1$, $(\frac{4}{13}) = 1$, $(\frac{5}{13}) = -1$. 또한, $18 \equiv 5 \pmod{13}$이고, 5가 2차

비 잉여류이므로, 18도 비 잉여류가 된다. 즉, $(\frac{18}{13}) = -1$.

Legendre의 기호는 18세기, 2차 잉여류를 계산하기 위해서 불란서의 수학자 Legendre가 처음 소개한 것이다. 이 Legendre기호를 법이 합성수가 되는 경우에 확장할 수 있도록 한 것이 Jacobi의 기호이다. 그 정의는 $n > 1$이고, $n = p_1 p_2 \cdots p_r$로 소인수분해 될 때, n과 서로소인 정수 a에 대해, $(\frac{a}{n})$은 Legendre의 기호를 사용하여 $(\frac{a}{p_1})(\frac{a}{p_2}) \cdots (\frac{a}{p_r})$이 된다.

Legendre의 기호의 정의로부터 쉽게 얻어지는 몇 가지 성질은 다음과 같다.

(i) $(\frac{a^2}{p}) = 1$,
(ii) $(\frac{1}{p}) = 1$,
(iii) $a \equiv b \pmod p$이면, $(\frac{a}{p}) = (\frac{b}{p})$.

가 성립하고, 보다 일반적으로는, 다음의 Euler의 판정식이 있다.

정리 3.1 (Euler의 판정식) 소수 p가 홀수이고, $p \nmid a$이면, 다음 식이 성립한다.

$$(\frac{a}{p}) = a^{\frac{(p-1)}{2}} \pmod p.$$

증명 [Bu]의 216쪽 참고. ■

또 이 판정식으로부터 다음의 따름 정리를 얻는다. 즉,

따름정리 소수 p가 홀수이고, $p \nmid a$, $p \nmid b$이면,

$$(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p}).$$

Euler의 판정식으로부터 $(\frac{-1}{p}) = (-1)^{\frac{(p-1)}{2}} \pmod p$이므로, 이것은 다음과 같이 풀어서 알아두는 것이 더 유용하다. 즉,

$$\left(\frac{-1}{p}\right) = \begin{cases} +1, & p \equiv 1 \pmod 4 \\ -1, & p \equiv 3 \pmod 4 \end{cases}$$

보기 합동식 $x^2 \equiv 19 \pmod{23}$이 해를 가지는지의 여부를 살펴보자. $19 \equiv -4 \pmod{23}$이므로,

$$\left(\frac{19}{23}\right) = \left(\frac{-4}{23}\right) = \left(\frac{-1}{23}\right)\left(\frac{2}{23}\right)^2 = -1.$$

따라서 위의 합동식은 해를 갖지 않는다.

정리 3.2 (Gauss의 보조정리) 소수 p가 홀수이고, $p \nmid a$라 하고, a, 2a, 3a, ……, $\frac{(p-1)}{2}$ a를 법 p에 대하여 $-\frac{(p-1)}{2}$와 $\frac{(p-1)}{2}$에 들어있는 잉여로 대치시켰을 때, 그 중에 포함된 음수 잉여의 개수를 n이라 하면, Legendre의 기호 $(\frac{a}{p})$는 $(-1)^n$과 같다.

증명[Bu]의 226쪽 참고. ■

정리 3.3 (2차 잉여류의 상호법칙, Quadratic Reciprocity Law) 소수 p와 q가 서로 다른 홀수이면 다음 등식이 성립한다.

$$(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{(p-1)}{2}\frac{(q-1)}{2}}$$

증명[Bu]의 235쪽 참고. ■

보기 $(\frac{7}{61})$을 구하여 보자.

$$\left(\frac{7}{61}\right) = (-1)^{\frac{60}{2}\frac{6}{2}}\left(\frac{61}{7}\right) = \left(\frac{5}{7}\right)$$
$$= (-1)^{\frac{6}{2}\frac{4}{2}}\left(\frac{7}{5}\right) = \left(\frac{2}{5}\right) = -1.$$

마지막으로 제 2절의 원시근과의 관계를 살펴보자.

참고 p와 2p+1이 각각 홀수인 소수일때, 정수 $(-1)^{\frac{(p-1)}{2}}2$는 2p+1의 원시근이다.

예컨대, 소수 11, 59, 107, 179 등은 2를 원시근으로 갖고, -2는 7, 23, 47, 167 등의 원시근이 된다.

4. 암호학에의 응용

이 절에서는 2절과 3절에서 소개된 정수론의 여러 성질들을 이용하는 암호학의 분야를 언급하고자 한다. 다음과 같은 크게 구분된 두 부분을 다룬다.

(i) 유사 임의 수열 생성자와 Rabin암호시스템.
(ii) Jacobi기호에 의한 암호화 프로토콜.

유사임의 수열 생성자와 Rabin 암호 시스템

유사 임의 수열은 0과 1만을 사용하는 수열로 축소하여 생각할 수 있으므로, 보통 유사 임의 이진수열(Pseudo Random Bit Sequence, 또는 Random Bit)을 일컫는다. 이 Random Bit는 생성자(Generator)에 씨(Seed)라 불리우는 몇 개의 작은 초기 입력 이진수에 의해서 만들어진다. 따라서, 이러한

Random Bit를 위한 생성자를 어떻게 만들 것인가 하는 문제와 만들어진 Random Bit들이 암호학에 사용될 수 있는 조건을 만족하는가 하는 문제가 중요시 되어 왔다. 정수론에 기초하는 많은 생성자들 중 Power Generator에 대하여 살펴본다.

먼저 사용할 기호는 다음과 같다. $\{0,1\}^+$는 (이것은 Automata Theory에서의 Kleene의 닫힘(closure)의 하나이다. [Ho]의 28쪽 참고.) 0과 1에 의해서 만들어지는 수열들의 집합, 즉, {0, 1, 00, 01, 10, 11, 000, 001, …}을 말한다. 이 $\{0,1\}^+$의 한 원소 x_i에 대하여, 그 x_i에 사용된 0과 1의 개수를 x_i의 길이(length)라 하며, $|x_i|$으로 표시한다. $\{0,1\}^k$는 $\{0,1\}^+$에서 길이가 k인 Random Bit들의 집합을 말한다. 따라서 $\{0,1\}^+ = \bigcup_{k=1,2,\cdots} \{0,1\}^k$ 이다. 이제 $\{0,1\}^+$의 한 원소 x_i을 잡자. 물론 이 $\{0,1\}^+$가 길이가 작은 순으로 순서대로 나열되어 있는 것은 아니다. 이 x_i을 이용하여 $\{0,1\}^+$에서 그 다음으로 생성되는 원소 x_{i+1}을 만드는 관계식은 다음과 같다. x_0를 씨라 하였을 때,

$$x_{i+1} \equiv (x_i)^d \pmod{n}.$$

특히 n이 서로 다른 두 홀수 소수 p_1과 p_2의 곱이라 할때, 다음의 두 가지 경우를 살펴보자.

첫째 경우는 $\phi(n) = (p_1-1)(p_2-1)$과 d가 서로소인 경우이다. 법 n에서의 사상 $x \to x^d$는 기약잉여계 Z_n^*에서 1대 1 대응하고, 이는 RSA공개키 체계에서 암호화 수단으로 사용된다. ([Ri]참고.) d와 n이 공개되는 것으로 이러한 생성자를 RSA 생성자라 부르기도 한다.

다음 경우는 제곱 생성자(Square Generator)라 불리우는 것으로 d=2, $p_1 \equiv p_2 \equiv 3 \pmod 4$인 경우이다. 이 경우,

$$x_{i+1} \equiv (x_i)^2 \pmod{n}$$

는 Z_n^*에서 4대 1 대응한다. n과 서로소인 2차 잉여류 a는 꼭 4개의 해를 가진다. 물론 $p_1 \equiv p_2 \equiv 3 \pmod 4$라는 조건 때문에 -1은 법 p_1, p_2에 대하여 2차 비잉여류가 된다. 따라서 이 4개의 해중 꼭 하나가 2차 잉여류가 된다. 이 제곱 생성자의 정의역을 n과 서로소인 2차 잉여류 a들의 집합으로 제한하면, 1대 1 대응을 얻게 되어 유사 임의 수열 생성자로 사용할 수 있다. ([Ra]참고)

이것은 또한 Rabin의 암호 시스템([Ra]참고)에도 응용되고 있는 것으로, 이 Rabin의 암호 시스템은 RSA 공개키 암호 시스템의 변형으로, 다른 RSA 공개키 암호 시스템과는 달리, 그 비도가 n의 소인수분해의 어려움과 같다는 것이 증명되었다. (참고 [Ti]의 90쪽)

RSA에서 공개되는 키로 사용되는 d는 $\phi(n)$과 서로소인 정수였으나, 여기 Rabin의 암호시스템에서는 위와 같이 d를 2로 잡는다. $\gcd(2, \phi(n)) = 2$이므로 다시 복호화 할 때, 법 p_1으로 2개, 법 p_2로 2개, 모두 4개의 평문이 구해지는 단점이 있다. 이 암호 시스템은 다음과 같이 구성되어 진다.

1. 임의로 n보다 작은 정수 b를 선택하여, n과 b를 공개키로 한다.

2. p_1과 p_2는 비밀키이다.

3. 평문 $x \in P$를 법 n에서 $x(x+b) \in C$로 하여 암호화 한다.

4. 이차 합동식 $x^2 + bx - C$의 근을 법 p_1과 법 p_2에서 각각 구한 다음 중국인의 나머지 정리를 이용하여 평문 P를 계산한다.

Jacobi 기호에 의한 암호화 프로토콜

제 3절에서 $(\frac{7}{61})$을 구하는 과정이 보여주듯이 $(\frac{a}{p})$를 $O(log^2 p)$의 시간에 구할 수 있다. Jacobi 기호를 계산하는 알고리즘은 [Sh]에 설명되어 있다. n이 p_i들의 곱으로 소인수분해 된다고 하자. a가 법 n의 2차 잉여류라면, n을 나누는 모든 소수 p_i들에 대하여서도 a는 2차 잉여류이다.

$(\frac{a}{n}) = -1$이라면, $(\frac{a}{p_i}) = -1$이고, a는 법 n에 대하여 2차 비 잉여류이다. 한편, $(\frac{a}{n}) = 1$임에도 a는 법 n에 대하여 2차 비 잉여류일 수 있다. 2차 잉여류인가를 결정하는 유일한 방법은 n을 먼저 인수분해 하여야 하는 것이기 때문에 암호화 프로토콜에 사용이 될 수 있다.

이제 그 예를 하나 들자. 일반적으로는 A와 B 사이의 동전던지기(Coin Flipping)로 알려진 것으로 그 프로토콜은 다음과 같이 이루어 진다.

1. B는 충분히 큰 두 소수 p와 q의 곱인 n과

$(\frac{a}{n}) = 1$이 되는 임의의 수 a를 A에게 알려준다.

2. A는 이 a가 법 n에 대하여 2차 잉여류인가, 아닌가를 추측하여 B에게 알려준다.

3. B는 A에게 그 추측이 옳은지 그른지를 알려준다.

4. 후에, B는 p와 q를 A에게 알려준다.

여기서 A는 밝혀진 p와 q가 소수인지를 확인하여야 한다. 왜냐하면 B가 다음과 같이 속일 수 있기 때문이다.

위의 1단계에서 B는 세 소수 p_1, p_2, q_1 과 $(\frac{a}{p_1}) = (\frac{a}{p_2}) = -1, (\frac{a}{q_1}) = 1$을 만족하는 수 a를 선택한다. A의 옳은 추측이 앞면이고 그른 추측이 뒷면이라 가정하자. 만약 B가 앞면이기를 원한다면, A가 잉여류라 말할 때는, B는 p로서 $p_1 \cdot p_2$ 를 q로서 q_1을 밝힐 것이고, A가 비 잉여류라 말할 때는, B는 p로서 p_1 을 q로서 $p_2 \cdot q_1$을 밝힐 것이고, 만약 B가 뒷면이기를 원한다면, A가 잉여류라 말할 때는, B는 p로서 p_1을 q로서 $p_2 \cdot q_1$을 밝힐 것이고, A가 비 잉여류라 말할 때는, B는 p로서 $p_1 p_2$ 를 q로서 q_1을 밝힐 것이기 때문이다.

참 고 문 헌

[Bl] L. Blum, M. Blum, and M. Shub, *A Simple Unpredictable Pseudorqudom Number Operator*, SIAM J. Comput. 15(1986), 364-383.

[Bu] D.M. Burton, *Elementary Number Thoery*, Wm. C. Brown, Dubuque, Iowa, 1989.

[Ho] J.E. Hopcroft and J.D. Ullman, *Introduction to Automata Theory, Languages, and Computation*, Addison Wesley, Reading, Massachusetts, 1979.

[Ra] M.O. Rabin, *Digitalized Signatures and Public-key Functions as Intractable as Factorization*, Tech. Report MIT/LCS/TR-212 (1979).

[Ri] R.L. Rievest, A. Shamir, and L.M. Adleman, *A Method for Obtaining Digital Signatures and Public-key Cryptosystems*, Comm. of the ACM 21(1978), 120-126.

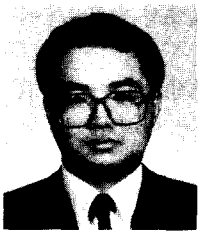
[Sh] J. Shallit, *On the Worst Case of Three Algorithms of Computing the Jacobi Symbol*, J. of Symbolic Computation, to appear.

[Ti] H. van Tilborg, *An Introduction to Cryptology*, Kluwer Academic Publishers, Norwell, Massachusetts, 1989.

□ 著者紹介

오 정 환

연세대학교 수학과(이학석사 · 박사)
1972년~1974년 미국 Pennsylvania State University
1986년~1987년 미국 University of Illinois at Urabana 방문교수
1964년~현 재 연세대학교 수학과 교수
연구관심분야 : 대수적 수론



김 철

미국 North Carolina 주립대학 수학과(이학석사 · 박사)
1990년~1991년 미국 University of South Dakota 수학과 조교수
1991년~현 재 광운대학교 수학과 조교수
연구관심분야 : 응용대수학, 암호이론