[UCI]I804:24011-200000239567

2010년 2월
교육학석사(수학교육)학위논문

中國人의 나머지 정리에 관한 硏究

조선대학교 교육대학원

수학교육전공

신 현 철

中國人의 나머지 정리에 관한 研究

A study on the Chinese Remainder Theorem.

2010 년 2 월

조선대학교 교육대학원

수학교육전공

신 현 철

中國人의 나머지 정리에 관한 研究

지도교수 박 순 철

이 논문을 교육학석사학위 청구논문으로 제출합니다.

2009 년 10 월

조선대학교 교육대학원

수학교육전공

신 현 철

신현철의 교육학 석사학위 논문을 인준함.

심사위원장 조선대학교 교수 인

심사위원 조선대학교 교수 인

심사위원 조선대학교 교수 인

2009 년 12 월

조선대학교 교육대학원

목 차

ABSTRACT

A study on the Chinese Remainder Theorem.

Shin Hyun-cheol

Advisor : Prof. Park Soon-cheol, Ph. D.

Major in Mathematics Education

Graduate School of Education, Chosun University

In this dissertation, I'll comment on the Chinese Remainder theorem, one of the best-known propositions in the Number theory.

This theorem deals with ways to figure out values from the simultaneous linear equations.

After arguing fundamental natures that the Number theory and the Ring has, I'll look into the verifications of the Chinese Remainder theorem in a different point of view.

I'm also going to show how it has been applied to the cryptology.

I 서 론

연립 1차 합동식의 해를 구하는 문제로 잘 알려진 중국인의 나머지 정리는 정수론 자체에서도 매우 중요하지만 최근에는 전자계산학, 정보통신 및 암호학에 널리 이용되고 있다.

중국인의 나머지 정리 자체도 매우 중요하지만 이 논문에서는 다른 증명 방법을 살펴보고 중국인의 나머지 정리가 정수론과 현대대수학에서 어떠한 역할을 하고 있는지 살펴보며, 또한 어떻게 이용되고 있는지 그 응용을 다루어 볼 것이다.

본 논문에서는 정수론에서의 합동관계와 기본성질, 정수론에서의 중국인의 나머지 정리를 설명하고 대수학에서의 정수환, 다항식환, 일반적인 환에서의 중국인의 나머지 정리를 설명하여 그 응용을 다룬다.

≪ 중국인의 나머지 정리에 관한 수학사 ≫

17세기 이전

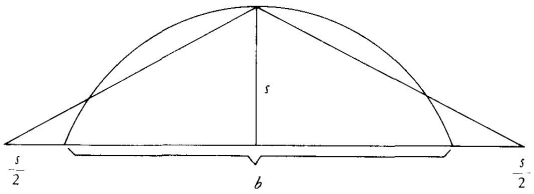

그림 1

중국, 인도, 아라비아의 수학

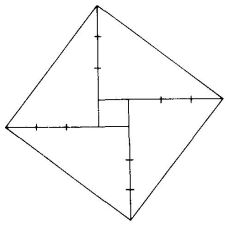

그림 2

고대 중국의 수학책 중에서 가장 중요한 <구장산술, 九章算術>은 한(漢)대에서 쓰여진 것으로서 한대 훨씬 이전의 내용도 담고 있다. <구장산술>은 농업, 상업, 공업, 측량, 방정식의 해법, 직각 삼각형의 성질 등에 관한 246개의 문제를 싣고 있다. 그 곳에는 해법이 주어지긴 했지만 그리스식의 어떤 증명도 찾아볼 수 없다.

1장의 문제 36에는 밑변이 b 이고 호의 높이 (sagitta : 원호의 중점에서 그 현의 중점까지의 길이)가 s 인 원호의 면적이 경험공식인 $s(b+s)/2$ 로 주어지고 있다. 이는 아마 그림1 으로 부터 추정되었을 것이다. 즉 그림의 할선이 이등변 삼각형의 면적과 원호의 면적이 같아 보이게끔 그려졌을 때 할선은 각각 밑변을 양쪽으로 $s/2$만큼 연장시킨 곳을 자르고 있는 것처럼 보인다. 반원에 대한 이 경험공식은 π 를 3으로 취하게 만든다. 또한 이 책에는 연립 1차 방정식을 푸는 문제들도 나오는데, 이것은 오늘날 행렬법으로 불리는 방식에 의하여 풀렸다.

<구장산술>보다 더 오래된 것으로 추정되는 또 하나의 유명한 고전으로 <주비산경, 周髀算經>이 있다. 이 책은 일부만 수학적 내용을 담고 있는데 가장 흥미로운 것은 그림2 을 바탕으로 한 피타고라스 정리에 대한 논의이다. (그러나 증명은 없다.)

그 뒤를 이어 한대가 낳은 수학자 순체(筍彘)가 구장산술에 나오는 것과 유사한 내용을 담고 있는 책을 한 권 저술했다. 이 책에서 부정(不定) 해석에 관한 최초의 중국문제가 등장한다.

연립1차 합동 방정식

$$a_1 x \equiv b_1 \pmod{m_1} \quad a_2 x \equiv b_2 \pmod{m_2} \quad \cdots \quad a_r x \equiv b_r \pmod{m_r}$$

에서 법 m_k 가 쌍마다 서로소라 가정하자.

분명히 연립합동식은 각 개별 합동식을 풀 수 없으면 해가 존재하지 않는다.

즉 각 k 에 대하여

$d_k = (a_k, m_k)$ 일 때 $d_k \mid b_k$ 가 아니면 해가 존재하지 않는다.

이 조건을 만족할 때 인수 d_k 는 k 번째 합동식에서 소거하여

원래의 해집합과 같은 해 집합을 갖는 새로운 연립합동식을 얻는다.

$$a_1{}' x \equiv b_1{}' \pmod{m_1} \quad a_2{}' x \equiv b_2{}' \pmod{m_2} \cdots \quad a_r{}' x \equiv b_r{}' \pmod{m_r}$$

여기서 $n_k = \dfrac{m_k}{d_k}$ 이고 $i \neq j$ 에 대해 $(n_i, n_j) = 1$ 이다.

더욱이 $(a_i, n_j) = 1$ 이다.

개별합동식의 해를 다음과 같은 형태라 가정하자.

$$x \equiv c_1 \pmod{n_1} \quad x \equiv c_2 \pmod{n_2} \quad \cdots \quad x \equiv c_r \pmod{n_r}$$

그러므로 문제는 이와 같은 간단한 형태의 연립합동식의 해를 찾는 문제로 바꾸어진다.

연립합동식에 의해 해결될 수 있는 문제는 기원 후 1세기 정도만큼 일찍 중국문화에 나타나는 긴 역사를 가지고 있다.

순츄(Sun - Tsu) 는 “3, 5, 7로 각각 나누었을 때 나머지가 2, 3, 2가 남는 수를 구하라”라고 물었다. 그러한 수학적 수수께끼는 결코 단 하나의 문화적 분위기로 제한되지 않는다. 사실상 같은 문제는 그리스 수학자 니코마쿠스(Nichomachus)의 『산술입문』(Introductio Arithemeticae)에 나타난다.

약 100년경이나 이른 그들의 기여를 기리기 위해 1차 합동식 해를 구하는 규칙을 보통 중국인의 나머지 정리(Chinese Remainder Theorem)라 부른다.

$$x \equiv 2 \pmod 3, \quad x \equiv 3 \pmod 5, \quad x \equiv 2 \pmod 7$$

위의 세 합동식을 동시에 만족시키는 해를 모두 구하는 문제는 1세기 경부터 고대 중국인들에게 널리 알려졌던 수수께끼 문제로서 중국수학자 Ch'in Chiu - Shao (1202 ~ 1261)가 1247년에 출간한 책인 '구장산술'에 그 풀이법이 실려 있다.

Ⅱ 기본적인 성질

【 Definition 2-1 】

주어진 정수 $m \geq 1$ 에 대하여, 주 정수 a 와 b 사이에 $m \mid (a-b)$ 인 관계가 있을 때 'a 는 法(modulus) m 에 관하여 b 에 합동이다.' (a is congruent to b modulo m) 라 하고 이것을 $a \equiv b \pmod{m}$ 으로 나타낸다.

$$a \equiv b \pmod{m} \quad \Leftrightarrow \quad m \mid (a-b)$$

합동기호 $\equiv$ 가 들어있는 식을 합동식(congruence) 이라고 한다.

≪ Theorem 2-1 ≫

정수 a, b, m 에 대하여 다음이 성립한다.

$$(a, m) = (b, m) = 1 \quad \Leftrightarrow \quad (ab, m) = 1$$

$(proof)$ 먼저 $(a, m) = (b, m) = 1$ 이면

$as + mt = 1$, $bu + mv = 1$

인 정수 s, t, u, v 가 존재하고 이때 $(as+mt)(bu+mv) = 1$ 이다.

$ab(su) + m(asv + but + mtv) = 1$ 이므로

$(ab, m) = 1$ 이다.

역으로, $(ab, m) = 1$ 이면

$(ab)s + mt = 1$ 인 정수 s, t 가 존재하고 이때

$a(bs) + mt = 1$, $b(as) + mt = 1$ 이므로

$(a, m) = (b, m) = 1$ 이다. ∎

≪ Corollary 2-1 ≫

정수 $a_1, a_2, \ldots, a_n, m$ 에 대하여 다음이 성립한다.

$(a_1, m) = (a_2, m) = \ldots = (a_n, m) = 1 \quad \Leftrightarrow \quad (a_1 \cdot a_2 \cdot \ldots a_n \cdot m) = 1$

≪ Theorem 2-2 ≫

정수 a, b, c 에 대하여 $(a, b) = 1$ 일때 $a \mid bc \quad \Leftrightarrow \quad a \mid c$ 이다.

$(proof)$ $(a, b) = 1$ 이므로 $as + bt = 1$ 인 정수 s, t 가 존재한다.

c 를 양변에 곱하면 $a(cs) + (bc)t = c$ 이다.

따라서 $a \mid bc$ 이면, $a \mid c$ 이다.

역으로 $a \mid c$ 이면 분명히 $a \mid bc$ 이다. ∎

≪ Theorem 2-3 ≫

정수 a, b, c 에 대하여 $a \mid b$, $a \mid c$ 일 때

임의의 정수 x, y 에 대하여 $a \mid (bx + cy)$ 이다.

$(proof)$ $a \mid b$, $a \mid c$ 이면 적당한 정수 d, e 에 대하여

$b = ad$, $c = ae$ 이고,

따라서 임의의 정수 x, y 에 대하여

$bx + cy = adx + aey = a(dx + ey)$ 이므로

$a \mid (bx + cy)$ 이다. ∎

≪ Theorem 2-4 ≫

0이 아닌 정수 a, b 에 대하여 $(a,b)[a,b] = |ab|$ 이다.

$(proof)$ 이제 $d = (a,b)$, $l = [a,b]$ 라 하고 적당한 정수 x, y 에 대하여
$a = dx$, $b = dy$ 라고 하자
이때 $ay = (dx)y = x(dy) = xb$ 이므로 $a \mid ay$, $b \mid ay$ 이고
따라서 최소공배수의 정의에 의하여 $[a,b] \mid ay$ 이다.
즉 $l \mid ay$ 이다.
다음에 $a \mid c$, $b \mid c$ 라고 가정하고
$c = az$ 이라고 하면 $b \mid az$ 이므로 $dy \mid xdz$ 즉 $y \mid xz$ 이고
$(x,y) = 1$ 이므로 $y \mid z$ 이고 따라서 $ay \mid az$ 즉 $ay \mid c$ 이다.
따라서 최소공배수 정의에 의하여
$l = dxy$, $dl = dxdy = |ab|$ 이다. ∎

(다른증명) $(a,b) = d$ 라 하고 적당한 정수 r, s 에 대하여
$a = dr$, $b = ds$ 라고 하자
이때 $\dfrac{ab}{d} = m$ 이라고 하면 $m = as = br$ 이다.
즉 $a \mid m$, $b \mid m$ 이고 m은 a 와 b의 공배수이다.
a, b의 임의의 공배수를 c라 하면, 즉 $a \mid c$, $b \mid c$ 이다.
적당한 정수 u, v에 대하여 $c = au$, $c = bv$ 가 성립한다.
그런데 $(a,b) = d = ax + by$ 이고

$$\frac{c}{m} = \frac{c}{\frac{ab}{d}} = \frac{cd}{ab} = \frac{c(ax+by)}{ab} = (\frac{c}{b})x + (\frac{c}{a})y = vx + uy$$

즉 $c = m(vx + uy)$ 이고 $m \mid c$ 이다.
최소공배수 정의에 의하여 $m = [a,b]$ 이다.
따라서 $ab = md = [a,b](a,b)$ 이다.

(다른증명) $a = p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}$, $b = p_1^{s_1} p_2^{s_2} \dots p_t^{s_t}$ $(k_i, s_i \geq 0)$ (단 p_i는 소수)

이라고 놓자. $(a, b) = d$ 라고 하자. $d \mid a$, $d \mid b$ 이고

d는 $p_1, p_2, \dots, p_t$의 소인수를 가지고 있다.

$d = p_1^{r_1} p_2^{r_2} \dots p_t^{r_t}$, $r_i = \min(k_i, s_i)$ 이다.

$[a, b] = l$ 이라고 하자. $a \mid l$, $b \mid l$ 이고

l는 $p_1, p_2, \dots, p_t$의 소인수를 가지고 있다.

$l = p_1^{u_1} p_2^{u_2} \dots p_t^{u_t}$, $u_i = \max(k_i, s_i)$ 이다.

$$
\begin{aligned}
(a, b)[a, b] &= d\,l \\
&= (p_1^{r_1} \dots p_t^{r_t})(p_1^{u_1} \dots p_t^{u_t}) \\
&= p_1^{\max(k_1, s_1) + \min(k_1, s_1)} \dots p_t^{\max(k_t, s_t) + \min(k_t, s_t)} \\
&= p_1^{k_1 + s_1} p_2^{k_2 + s_2} \dots p_t^{k_t + s_t} \\
&= (p_1^{k_1} p_2^{k_2} \dots p_t^{k_t})(p_1^{s_1} p_2^{s_2} \dots p_t^{s_t}) \\
&= a\,b \quad \blacksquare
\end{aligned}
$$

≪ Theorem 2-5 ≫

양의정수 m 과 임의의 정수 a, b 사이에 다음이 성립한다.

$$a \equiv b \pmod{m} \quad \Rightarrow \quad (a, m) = (b, m)$$

$(proof)$ $a \equiv b \pmod{m}$ 이므로 $a = mk + b$ 인 정수 k가 존재한다.

정수 d, e 에 대하여 $d = (a, m)$, $e = (b, m)$ 이라 하자.

$e = (b, m)$ 에서 $e \mid b$, $e \mid m$ 이다

$a = mk + b$ 이므로 $e \mid a$ 이고

따라서 $e \mid m$ 에 의하여 $e \mid (a, m)$ 가 된다.

그러므로 $e \mid d$ 이다.

또 $d = (a, m)$ 에서 $d \mid a$, $d \mid m$ 이고

$a = mk + b$ 에서 $b = a + m(-k)$ 이다.

$d \mid \{a + m(-k)\}$ 가 성립한다.

따라서 $d \mid b$ 이고 $d \mid m$ 이다.

$d \mid (b, m)$ 이므로 $d \mid e$ 이다.

$e \mid d$ 이고 $d \mid e$ 이므로 $d = e$ 이다.

따라서 $(a, m) = (b, m)$ 이다. ∎

≪ Theorem 2-6 ≫

양의정수 $m_1, m_2, \ldots\ldots, m_n$ $(n \geq 2)$과 정수 a, b 에 대하여 다음이 성립한다.

$$\begin{cases} a \equiv b \pmod{m_1} \\ a \equiv b \pmod{m_2} \\ \quad\vdots \\ a \equiv b \pmod{m_n} \end{cases} \iff a \equiv b \pmod{[m_1, m_2, \ldots, m_n]}$$

$(proof)$ 양의정수 $m_1, m_2, \ldots\ldots, m_n$ $(n \geq 2)$과 정수 a, b 에 대하여

$a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, $\cdots$, $a \equiv b \pmod{m_n}$

이므로 $m_1 \mid (a-b)$, $m_2 \mid (a-b)$, $\cdots$, $m_n \mid (a-b)$ 이다.

최소공배수 정의에 의하여 $[m_1, m_2, \ldots, m_n] \mid a-b$ 이다.

따라서 $a \equiv b \pmod{[m_1, m_2, \ldots, m_n]}$ 이다.

역으로 $a \equiv b \pmod{[m_1, m_2, \ldots, m_n]}$ 이라고 하자.

$[m_1, m_2, \ldots, m_n] \mid (a-b)$ 이고

$m_1 \mid [m_1, m_2, \ldots, m_n]$, $m_2 \mid [m_1, m_2, \ldots, m_n]$

$\cdots$ $m_n \mid [m_1, m_2, \ldots, m_n]$ 이므로

$m_1 \mid (a-b)$, $m_2 \mid (a-b)$, $\cdots$, $m_n \mid (a-b)$ 이다.

$\therefore$ $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, $\cdots$, $a \equiv b \pmod{m_n}$ ∎

≪ Corollary 2-2 ≫

특히 $m_1, m_2, \ldots, m_n$ $(n \geq 2)$이 쌍마다 서로소 일 때 다음이 성립한다.

$$\begin{cases} a \equiv b \pmod{m_1} \\ a \equiv b \pmod{m_2} \\ \quad\vdots \\ a \equiv b \pmod{m_n} \end{cases} \iff a \equiv b \pmod{m_1 m_2 \ldots m_n}$$

【 Definition 2-2 】

합동관계 $a \equiv b \pmod{m}$ 은 정수전체의 집합 Z 위의 동치관계이다.

이 동치관계로부터 얻어지는 동치류를 법 m에 관한 잉여류(residue class modulo m)

라고 한다. 이 때 $a \in Z$ 에 의하여 결정되는 잉여류를 $\overline{a}$ 로 나타내면

$\overline{a} = \{x \in Z \mid x \equiv a \pmod{m}\} = \{a + km \mid k \in Z\}$ 이다.

【 Definition 2-3 】

$(R, +, \cdot)$ 을 환$(ring)$ 이라 하고 R의 부분집합 $I\ (\neq \varnothing)$가

다음 두 조건이 성립할 때 I 를 R 의 이데알(ideal) 이라고 한다.

(i) I 는 덧셈군 $(R, +)$의 부분군이다.

즉 $a, b \in I \quad \Rightarrow \quad a - b \in I$

(ii) $a \in I,\ r \in R \quad \Rightarrow \quad ra \in I,\ ar \in I$

【 Definition 2-4 】

환 R에서 I가 이데알 일 때

집합 $R/I = \{a+I \mid a \in R\}$ 는 다음과 같이 정의된 상등관계와

덧셈 및 곱셈에 관하여 환을 이룬다.

$$a+I = b+I \quad \Leftrightarrow \quad a-b \in I$$

$$(a+I)+(b+I) = (a+b)+I$$

$$(a+I)\cdot(b+I) = ab+I$$

이와 같이 정의된 환 R/I를 환 R의 이데알 I에 의한

잉여환(residue ring) 또는 인자환(factor ring) 또는 상환(quotient ring) 이라고

한다.

※ 환 R에서 R과 $\{0\}$은 이데알이고 $R/R \cong \{0\}$, $R/\{0\} \cong R$ 이다.

【 Definition 2-5 】

환 R에서 환 R'으로의 사상 $f: R \to R'$ 가 환의 두 연산을 보존시킬 때,

즉 임의의 원소 $a, b \in R$ 에 대하여

$f(a+b) = f(a) + f(b)$, $f(ab) = f(a)f(b)$ 일 때

f 를 R 에서 R'으로의 환 준동형사상(ring - homomorphism) 이라고 한다.

또, 준동형사상 $f: R \to R'$ 가 일대일대응 일 때

f 를 R 에서 R'으로의 환 동형사상(ring - isomorphism) 이라고 한다.

그리고, 환 동형사상 $f: R \to R'$ 가 존재할 때 환 R 와 환 R'은

서로 동형(isomorphism) 인 환이라 하고

이 사실을 $R \cong R'$ 으로 나타낸다.

≪ Theorem 2-7 ≫

사상 $f : R \to R'$ 가 환 준동형사상 일 때 R의 부분환 S에 대하여

$f(S) = \{ f(a) \mid a \in S \}$ 는 R'의 부분환이고

특히 $im\, f = f(R) = \{ f(a) \mid a \in R \}$ 는 R'의 부분환이고

따라서 $f(S)$는 $f(R)$의 부분환이다

그리고 I 가 R의 이데알이면, $f(I)$는 환 $f(R)$의 이데알이다.

$(proof)$ 임의의 $a, b \in S$ 에 대하여

$a - b,\ ab \in S$ 이므로

$f(a) - f(b) = f(a-b) \in f(S)$

$f(a)f(b) = f(ab) \in f(S)$

이고 따라서 $f(S)$는 R'의 부분환이다

이제 I 를 R의 이데알이라고 하자

이 때, $f(I)$는 환 $f(R)$의 부분환이고

임의의 $a, b \in I$ 와 $r \in R$에 대하여

$a - b \in I,\quad ra \in I,\quad ar \in I$ 이므로

$f(a) - f(b) = f(a-b) \in f(I)$

$f(r)f(a) = f(ra) \in f(I)$

$f(a)f(r) = f(ar) \in f(I)$ 이다

따라서 $f(I)$는 환 $f(R)$의 이데알이다. ∎

≪ Theorem 2-8 ≫

사상 $f : R \to R'$ 가 환 준동형사상 일 때

$\ker f = \{ a \in R \mid f(a) = 0' \}$ 이라고 하면 $\ker f$ 는 R 의 이데알이다.

여기서 $\ker f$ 를 f 의 핵(kernel) 이라고 한다.

$(proof)$ 먼저 $f(0) = 0'$ 이므로 $0 \in \ker f \neq \varnothing$ 이다.

따라서 임의의 $a, b \in \ker f$ 와 $r \in R$ 에 대하여

$f(a-b) = f(a) - f(b) = 0' - 0' = 0'$,

$f(ra) = f(r)f(a) = f(r)0' = 0'$,

$f(ar) = f(a)f(r) = 0'f(r) = 0'$ 이므로

$a-b$, ra, ar 는 $\ker f$ 에 속한다.

따라서 $\ker f$ 는 R 의 이데알이다. ∎

≪ Theorem 2-9 ≫

사상 $f : R \to R'$ 가 환 R 에서 R'으로의 환 준동형사상 이라고 하자.

(1) f가 일대일 준동형사상 일 때, 그리고 이때에만 $\ker f = \{0\}$ 이다.

(2) $I = \ker f$ 라고 할 때 임의의 $a, b \in R$에 대하여

$$f(a) = f(b) \Leftrightarrow a - b \in I$$
$$\Leftrightarrow a + I = b + I$$

$(proof)$ (1) f 가 일대일 준동형사상 일 때 $a \in \ker f$ 이면

$f(a) = 0' = f(0)$ 이므로 $a = 0$ 이고,

따라서 $\ker f = \{0\}$ 이다.

역으로 $\ker f = \{0\}$ 이라고 가정하면

$$f(a) = f(b) \Leftrightarrow f(a) - f(b) = 0'$$
$$\Leftrightarrow f(a - b) = 0'$$
$$\Leftrightarrow a - b \in \ker f$$
$$\Leftrightarrow a - b = 0 \quad \text{즉} \quad a = b$$

이므로 f는 일대일 준동형사상이다.

(2) $f(a) = f(b)$

$$\Leftrightarrow f(a) - f(b) = 0'$$
$$\Leftrightarrow f(a - b) = 0'$$
$$\Leftrightarrow a - b \in \ker f = I$$
$$\Leftrightarrow a + I = b + I \text{ 이다. ∎}$$

≪ Theorem 2-10 ≫ (제 1동형정리)

사상 $f : R \to R'$ 를 환 준동형사상 이라 할 때

$I = \ker f$ 라고 하면 I 는 R 의 이데알(ideal)이고 다음이 성립한다.

$$R/I \cong im f = f(R)$$

실제로 $\phi : R/I \to im f$, $\phi(a+I) = f(a)$ 는 동형사상이다.

$(proof)$ $a+I = b+I \Leftrightarrow f(a) = f(b)$

$\Leftrightarrow \phi(a+I) = \phi(b+I)$ 이므로

$\phi : R/I \to im f$, $\phi(a+I) = f(a)$

는 잘 정의된 일대일 사상이다.

한편 임의의 $a, b \in R$ 에 대하여

$$\begin{aligned}\phi((a+I)+(b+I)) &= \phi((a+b)+I) \\ &= f(a+b) \\ &= f(a)+f(b) \\ &= \phi(a+I)+\phi(b+I)\end{aligned}$$

$$\begin{aligned}\phi((a+I)(b+I)) &= \phi(ab+I) \\ &= f(ab) = f(a)f(b) \\ &= \phi(a+I)\,\phi(b+I)\end{aligned}$$

$im\,\phi = \{\phi(a+I) \mid a \in R\} = \{f(a) \mid a \in R\} = im f$

이므로, ϕ는 동형사상이고

따라서 $R/I \cong im f$ 이다. ∎

【 Definition 2-6 】 (Ring의 직합)

환 $R_1, \ldots, R_n$ 에 대하여, 곱집합

$R_1 \times \ldots \times R_n = \{(x_1, \ldots, x_n) \mid x_1 \in R_1, \ldots, x_n \in R_n\}$는

다음과 같이 정의된 덧셈과 곱셈에 관하여 환을 이룬다.

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$$

$$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = (a_1 b_1, \ldots, a_n b_n)$$

이 환을 $R_1, \ldots, R_n$ 의 외적인 직합(external direct sum) 이라고 하고

이 환을 $R_1 \oplus \ldots \oplus R_n$ 으로 나타낸다.

【 Definition 2-7 】

환 R 의 이데알 I_1, I_2 에 대하여

$R = I_1 + I_2$, $I_1 \cap I_2 = \{0\}$ 일 때

R 를 두 이데알 I_1, I_2 의 내적인 직합(internal direct sum)이라 하고

이 사실을 $R = I_1 \dot{+} I_2$ 또는 $R = I_1 \oplus I_2$ 로 나타낸다.

그리고 이 경우에 R 는 두 이데알 I_1, I_2의 직합으로 분해된다고 하고

I_1, I_2 를 R 의 직합인자(direct summand) 라고 한다.

$R = I_1 \dot{+} I_2 = I_2 \dot{+} I_1$ 이고 또 $R = \{0\} \dot{+} R = R \dot{+} \{0\}$ 이다.

그리고 $R = I_1 \dot{+} I_2$ 이면 덧셈군 $(R, +)$ 는 부분군 I_1, I_2 의 직합이기도 하다.

≪ Theorem 2-11 ≫

환 R 에서 R 의 두 이데알 I_1, I_2 에 대하여

$R = I_1 + I_2$, $I_1 \cap I_2 = \{0\}$ 일 때

I_1, I_2 의 외적인 직합 $I_1 \oplus I_2$ 에서 R 로의 사상

$f : I_1 \oplus I_2 \to R$, $f(a_1, a_2) = a_1 + a_2$ 는

환 동형사상이고 따라서 $R \cong I_1 \oplus I_2$ 이다.

$(proof)$ 먼저 $im\, f = \{a_1 + a_2 \mid a_1 \in I_1, a_2 \in I_2\} = I_1 + I_2 = R$

이므로 f 는 위로의 사상이다.

그리고 $I_1 \cap I_2 = \{0\}$ 이므로

모든 원소 $a_1 \in I_1$, $a_2 \in I_2$ 에 대하여 $a_1 a_2 = a_2 a_1 = 0$ 이다.

따라서 임의의 두 원소 (a_1, a_2), $(b_1, b_2) \in I_1 \oplus I_2$ 에 대하여

$$\begin{aligned} f((a_1, a_2) + (b_1, b_2)) &= f(a_1 + b_1, a_2 + b_2) \\ &= a_1 + b_1 + a_2 + b_2 \\ &= a_1 + a_2 + b_1 + b_2 \\ &= f(a_1, a_2) + f(b_1, b_2) \end{aligned}$$

$$\begin{aligned} f((a_1, a_2)(b_1, b_2)) &= f(a_1 b_1, a_2 b_2) \\ &= a_1 b_1 + a_1 b_2 + a_2 b_1 + a_2 b_2 \\ &= (a_1 + a_2)(b_1 + b_2) \\ &= f(a_1, a_2) f(b_1, b_2) \end{aligned}$$

이므로 f 는 환 준동형사상이다. 그리고 $I_1 \cap I_2 = \{0\}$ 이므로

$$\begin{aligned} (a_1, a_2) \in \ker f &\Rightarrow f(a_1, a_2) = 0 \\ &\Rightarrow a_1 + a_2 = 0 \\ &\Rightarrow a_1 = -a_2 \in I_1 \cap I_2 \\ &\Rightarrow a_1 = a_2 = 0 \end{aligned}$$

이고 따라서 $\ker f = \{(0, 0)\}$ 이다.

그러므로 f 는 환 동형사상이고, 따라서 $R \cong I_1 \oplus I_2$ 이다. ∎

【 Definition 2-8 】

$\{R_i\}_{i \in I}$ 를 환의 족이라고 하자.

$R = \Pi R_i = \{(\lambda_1, \lambda_2, \ldots, \lambda_n, \ldots) \mid \lambda_i \in R_i$ 유한개를 제외한 모든 i에 대하여 $\lambda_i = 0\}$

이제 이 집합 ΠR_i 에 환의 구조를 주기 위해 다음 연산을 정의한다.

i) 상 등

$(\lambda_1, \lambda_2, \ldots) = (\mu_1, \mu_2, \ldots) \Leftrightarrow$모든 i 에 대하여 $\lambda_i = \mu_i$

ii) 덧 셈 (addition)

$(\lambda_1, \lambda_2, \ldots) + (\mu_1, \mu_2, \ldots) = (\lambda_1 + \mu_1, \lambda_2 + \mu_2, \ldots)$

iii) 곱 셈 (multiplication)

$(\lambda_1, \lambda_2, \ldots)(\mu_1, \mu_2, \ldots) = (\lambda_1 \mu_1, \lambda_2 \mu_2, \ldots)$

이 연산에 관해 $(\Pi R_i, +, \cdot)$ 은 환을 이룬다.

이 환을 환 R_i 의 직적(direct product) 이라 하고

첨수집합 I 가 유한집합(finite set) 일 때

$\oplus R_i = \Pi R_i = \{(\lambda_1, \lambda_2, \ldots, \lambda_n) \mid \forall i,\ \lambda_i \in R_i\}$ 으로 표시한다.

첨수집합 I 가 무한집합(infinite set) 일 때

$\oplus R_i = \Pi R_i = \{(\ldots, \lambda_i, \ldots) \mid \forall i,\ \lambda_i \in R_i\}$이다.

【 Definition 2-9 】

$I_1, I_2, \ldots, I_n$ 을 R 의 이데알이라 하자.

$\forall i \neq j$, $I_i + I_j = R$ 이면 I_i 와 I_j 를 여극대(comaximal) 또는 서로소 (coprime) 이라 한다.

≪ Lemma 2-1 ≫

I 와 $I_1, I_2, \ldots, I_n$ 이 comaximal 이면 $I + (\bigcap_{i=1}^{n} I_i) = R$ 이다.

$$(proof) \quad R = R^n = (I + I_1)(I + I_2) \ldots (I + I_n)$$

$$= I + (I_1 I_2 \ldots I_n) \subseteq I + \bigcap_{i=1}^{n} I_i \subseteq R$$

$$\therefore \; I + \bigcap_{i=1}^{n} I_i = R$$

【 Definition 2-10 】

정수 전체의 집합 Z 위에서의 합동관계 $a \equiv b \pmod{m}$ 에 의하여 결정되는 동치류를 법 m 에 관한 잉여류(residue class)라고 한다.

$\overline{a}$ 를 a 를 포함하는 법 m 에 관한 잉여류라 하고 $\overline{Z_m}$ 를 법 m 에 관한 잉여류 집합이라 하고 Z_m 를 최소양의 완전잉여계라고 한다.

$$\overline{a} = \{x \in Z \mid x \equiv a \pmod{m}\} = \{a + mk \mid k \in Z\}$$

$$\overline{Z_m} = \{\overline{a} \mid a \in Z\} = \{\overline{0}, \overline{1}, \cdots, \overline{m-1}\}$$

$$Z_m = \{0, 1, \cdots, m-1\}, \qquad |\overline{Z_m}| = |Z_m| = m$$

【 Definition 2-11 】

임의의 정수 a를 양의 정수 m으로 나누었을 때의 나머지를 $<a>_m$ 으로 나타내기로 한다. 즉

$a \equiv <a>_m \pmod{m}$, $0 \le <a>_m < m$ 즉 $<a>_m \in Z_m$ 이다.

【 Definition 2-12 】

서로소인 양의 정수 m_1, m_2 에 대하여

(1) $(<a_1>_{m_1}, <a_2>_{m_2}) + (<b_1>_{m_1}, <b_2>_{m_2})$

$$= (<a_1+b_1>_{m_1}, <a_2+b_2>_{m_2})$$

(2) $(<a_1>_{m_1}, <a_2>_{m_2})(<b_1>_{m_1}, <b_2>_{m_2})$

$$= (<a_1 b_1>_{m_1}, <a_2 b_2>_{m_2})$$

으로 정의한다.

【 Definition 2-13 】

함수 $f: Z_{m_1 m_2} \rightarrow Z_{m_1} \times Z_{m_2}$ 을 $f(\overline{a}) = (<a>_{m_1}, <a>_{m_2})$ 으로 정의하고 이 함수를 $Z_{m_1 m_2}$ 에서 $Z_{m_1} \times Z_{m_2}$으로 대응되는 표준함수(*canonical map*) 라 부른다.

이 함수는 $Z_{m_1 m_2}$ 의 원소 $\overline{a}$는 a를 m_1으로 나눈 나머지를 포함하는 법 m_1에 관한 잉여류와 a를 m_2로 나눈 나머지를 포함하는 법 m_2에 관한 잉여류의 상으로 대응시킨다.

Ⅲ 주 정 리

Ⅲ-1 정수론에서 중국인의 나머지 정리

≪ Theorem 3-1 ≫ (중국인의 나머지 정리, Chinese Remainder Theorem)

양의정수 $m_1, m_2, \ldots, m_n$ $(n \geq 2)$ 이 쌍마다 서로소 일 때

$M = m_1, m_2, \ldots, m_n$ 이라고 하면

임의의 정수 $c_1, c_2, \ldots, c_n$ 에 대하여 연립일차 합동식

$$\begin{cases} x \equiv c_1 \pmod{m_1} \\ x \equiv c_2 \pmod{m_2} \\ \quad \vdots \qquad\qquad \vdots \\ x \equiv c_n \pmod{m_n} \end{cases}$$

은 법 M 에 관하여 단 한개의 해 $x \equiv u \pmod{M}$ 를 가진다.

$(proof\ 1)$ $M_i = \dfrac{M}{m_i} = m_1 \ldots m_{i-1} m_{i+1} \ldots m_n \quad (1 \leq i \leq n)$

이라고 놓으면 $1 \leq i \neq j \leq n$ 일때 $(m_i, m_j) = 1$ 이므로

$(M_i, m_i) = 1 \qquad (1 \leq i \leq n)$ 이고

따라서 $M_i N_i \equiv 1 \pmod{m_i} \qquad (1 \leq i \leq n)$ 인

정수 N_i 가 존재한다.

이제 $u = M_1 N_1 c_1 + M_2 N_2 c_2 + \ldots + M_n N_n c_n$ 이라고 놓으면

$1 \leq i \neq j \leq n$ 일 때 $M_j \equiv 0 \pmod{m_i}$

$u \equiv M_i N_i c_i \equiv c_i \pmod{m_i} \qquad (1 \leq i \leq n)$ 이고

따라서 주어진 연립합동식은 다음과 같이 고쳐 쓸 수 있다.

$$\begin{cases} x \equiv u \pmod{m_1} \\ x \equiv u \pmod{m_2} \\ \quad \vdots \qquad\qquad \vdots \\ x \equiv u \pmod{m_n} \end{cases}$$

한편 정리 2.6에 의하여 위의 연립합동식은

$x \equiv u \pmod{M}$ 과 동치이므로 주어진 연립합동식은

단 한개의 해 $x \equiv u \pmod{M}$ 를 가진다.

유일성 주장에 대해서는 u' 를 이 합동식의 또 다른 해라고 가정하면

$u \equiv c_i \equiv u' \pmod{m_i}$ $(1 \leq i \leq n)$ 이고

그래서 각 i 값에 대하여 $m_i \mid (u - u')$ 이다

$(m_i, m_j) = 1$ 이므로 $m_1 m_2 \ldots m_n \mid (u - u')$ 이다.

따라서 $u \equiv u' \pmod{M}$ 이다. ∎

(*proof* 2) $m_1, m_2, \ldots, m_n$ 가 쌍마다 서로소이므로

함수 $f : Z_{m_1 \ldots m_n} \rightarrow Z_{m_1} \times Z_{m_2} \times \ldots \times Z_{m_n}$ 을

$f(\bar{a}) = (<a>_{m_1}, <a>_{m_2}, \ldots, <a>_{m_n})$ 로 정의하면

f 는 전단사함수이다.

실제로 $f(\bar{a}) = f(\bar{b})$ 라 가정하면

$(<a>_{m_1}, \ldots, <a>_{m_n}) = (<b>_{m_1}, \ldots, <b>_{m_n})$이다.

그러므로 $<a>_{m_1} = <b>_{m_1}, \ldots, <a>_{m_n} = <b>_{m_n}$ 이다.

따라서 $m_1 \mid (b-a), \ldots, m_n \mid (b-a)$ 이다.

$(m_1, m_2, \ldots, m_n) = 1$ 이므로 $m_1 m_2 \ldots m_n \mid (b-a)$ 이다.

그러므로 $\bar{a} = \bar{b}$ 이고 따라서 f 는 단사함수이다.

한편 $Z_{m_1 \ldots m_n}$ 와 $Z_{m_1} \times \ldots \times Z_{m_n}$ 이 모두 원소 $m_1 \ldots m_n$ 개

가지고 있으므로 f 는 전사함수이다.

따라서 f 는 전단사함수이고,

$(<c_1>_{m_1}, \ldots, <c_n>_{m_n}) \in Z_{m_1} \times \ldots \times Z_{m_n}$에 대하여

$f(\bar{a}) = (<a>_{m_1}, \ldots, <a>_{m_n}) = (<c_1>_{m_1}, \ldots, <c_n>_{m_n})$을

만족하는 $\bar{a} \in Z_{m_1 \ldots m_n}$ 가 단 하나 존재한다.

따라서 $<a>_{m_1} = <c_1>_{m_1}, \ldots, <a>_{m_n} = <c_n>_{m_n}$,

즉 $a \equiv c_1 \pmod{m_1}, \ldots, a \equiv c_n \pmod{m_n}$ 인

유일한 해 $x \equiv a \pmod{m_1 \ldots m_n}$ 가 존재한다. ∎

≪ Corollary 3-1 ≫

두 양의 정수 m_1, m_2 가 서로소 일 때, 즉 $(m_1, m_2) = 1$ 일 때

임의의 두 정수 c_1, c_2 에 대하여 연립일차합동식

$$\begin{cases} x \equiv c_1 \pmod{m_1} \\ x \equiv c_2 \pmod{m_2} \end{cases}$$

은 법 $M = m_1 m_2$ 에 관하여 단 한 개의 해를 가진다.

(*proof* 1) m_1, m_2 가 서로소인 양의 정수이므로 $(m_1, m_2) = 1$ 이고

$M = m_1 m_2$ 이라 하고 $M_i = \dfrac{M}{m_i}$ 이라 놓자.

$M_1 = m_2$, $M_2 = m_1$ 이다.

$(M_i, m_i) = 1$ 이고 $M_i N_i \equiv 1 \pmod{m_i}$ 인 정수 N_i 가 존재

이제 $u = M_1 N_1 c_1 + M_2 N_2 c_2$ 이라고 놓으면

$i \neq j$ 일 때 $M_j \equiv 0 \pmod{m_i}$ 이므로

$u \equiv M_i N_i c_i \equiv c_i \pmod{m_i}$ 이고

따라서 주어진 연립 합동식은 다음과 같이 고쳐 쓸 수 있다.

$$\begin{cases} x \equiv u \pmod{m_1} \\ x \equiv u \pmod{m_2} \end{cases}$$

위의 연립합동식은 $x \equiv u \pmod{m_1 m_2}$ 와 동치이므로

주어진 연립 합동식은 단 한 개의 해

$x \equiv u \pmod{m_1 m_2}$ 를 가진다

유일성 주장에 대해서는 u' 를 이 합동식의 또 다른 해라고 가정하면

$u \equiv c_i \equiv u' \pmod{m_i}$

그래서 각 i 값에 대하서 $m_i \mid u - u'$ 이다.

$(m_1, m_2) = 1$ 이므로 $m_1 m_2 \mid u - u'$ 이다.

따라서 $u \equiv u' \pmod{m_1 m_2}$ 이다. ∎

(*proof* 2) m_1, m_2 가 서로소인 양의 정수이므로

함수 $f: Z_{m_1 m_2} \rightarrow Z_{m_1} \times Z_{m_2}$ 은 전단사 함수이다

실제로 $f(\overline{a}) = f(\overline{b})$ 라 가정하면

$(<a_1>_{m_1}, <a_2>_{m_2}) = (<b_1>_{m_1}, <b_2>_{m_2})$ 이다.

그러므로 $<a>_{m_1} = <b>_{m_1}$ 이고 $<a>_{m_2} = <b>_{m_2}$ 이다

따라서 $m_1 \mid (b-a)$ 이고 $m_2 \mid (b-a)$ 이다.

$(m_1, m_2) = 1$ 이므로 $m_1, m_2 \mid (b-a)$ 이다.

그러므로 $\overline{a} = \overline{b}$ 이고 따라서 f 는 단사함수이다.

한편 $Z_{m_1 m_2}$ 와 $Z_{m_1} \times Z_{m_2}$ 이 모두 원소 $m_1 m_2$ 개

가지고 있으므로 f 는 전사함수이다.

따라서 f 는 전단사함수이다.

$(<c_1>_{m_1}, <c_2>_{m_2}) \in Z_{m_1} \times Z_{m_2}$ 에 대하여

$f(\overline{a}) = (<a>_{m_1}, <a>_{m_2}) = (<c_1>_{m_1}, <c_2>_{m_2})$ 을

만족하는 $\overline{a} \in Z_{m_1 m_2}$ 가 단 하나 존재한다.

따라서 $<a>_{m_1} = <c_1>_{m_1}$ 이고 $<a>_{m_2} = <c_2>_{m_2}$ 이다.

즉 $a \equiv c_1 \pmod{m_1}$, $a \equiv c_2 \pmod{m_2}$ 이다.

그러므로 $x \equiv a \pmod{m_1 m_2}$ 이 한개의 해이다. ∎

Ⅲ-2 대수학에서 중국인의 나머지 정리

≪ Theorem 3-2 ≫ (환에서 중국인의 나머지 정리)

단위원 1을 가진 환 R 에서 R의 이데알 $I_1, I_2, \ldots, I_n$ 에 대하여

$R = I_1 + I_2 + \ldots + I_n$ 일 때.

$\phi : R \to \oplus R/I_i = R/I_1 \oplus R/I_2 \oplus \ldots \oplus R/I_n$

은 모든 $a \in R$ 에 대하여

$\phi(a) = (\phi_1(a), \phi_2(a), \ldots, \phi_n(a))$ 로 정의하자.

단, $\phi_i : R \to R/I_i$ 는 모든 $a \in R$ 에 대하여

$\phi_i(a) = a + I_i = \bar{a}$ 로 정의한다.

이제 다음이 성립한다.

i) ϕ는 준동형사상이다.

ii) ϕ 가 surjection 일 필요충분조건은 $I_1, I_2, \ldots, I_n$ 이 서로소이다.

iii) ϕ 가 injection 일 필요충분조건은 $\bigcap_{i=1}^{n} I_i = 0$ 이다.

iv) (i) 과 (ii) 가 성립하면 ϕ 는 isomorphism 이다.

$(proof)$ i) $\phi : R \to R/I$ 는 준동형사상이고

$im\,\phi = R/I, \quad \ker\phi = I$ 이다.

임의의 $a, b \in R$에 대하여

$\phi(a+b) = (a+b) + I = (a+I) + (b+I) = \phi(a) + \phi(b)$

$\phi(ab) = ab + I = (a+I)(b+I) = \phi(a)\phi(b)$

이므로 ϕ는 환 준동형사상이다. 그리고 다음이 성립한다.

$im\,\phi = \{\phi(a) \mid a \in R\} = \{a+I \mid a \in R\} = R/I$

$\ker\phi = \{a \in R \mid \phi(a) = 0 + I\}$

$= \{a \in R \mid a + I = 0 + I\} = I$

ii) ϕ 가 surjection 이라 하자

모든 $a \in R$ 에 대하여 $\phi_{ij}(a) = (a+I_i,\ a+I_j)$ 로 정의되는

$\phi_{ij} : R \rightarrow R/I_i \oplus R/I_j$ 을 생각하자.

ϕ_i 는 surjection 이므로, ϕ_{ij} 는 surjection 이다.

이때, ϕ_{ij} 가 surjection 이므로

즉 $\phi_{ij}(a_i) = (\overline{0},\ \overline{1})$, 즉 $(a_i+I_i,\ a_i+I_j) = (I_i,\ a_i+I_j)$

$\phi_{ij}(a_j) = (\overline{1},\ \overline{0})$, 즉 $(a_j+I_i,\ a_j+I_j) = (a_j+I_i,\ I_j)$

인 $a_i \in I_i$, $a_j \in I_j$ 가 존재한다.

이때 $\phi_{ij}(1-(a_i+a_j)) = (1-(a_i+a_j)+I_i,\ 1-(a_i+a_j)+I_j)$

$$= ((1-a_j)+I_i,\ (1-a_i)+I_j)$$

$$= (\overline{1-a_j},\ \overline{1-a_i})$$

$$= (\overline{1}-\overline{a_j},\ \overline{1}-\overline{a_i})$$

$$= (a_j+I_i-\overline{a_j},\ a_i+I_j-\overline{a_i})$$

$$= ((a_j+I_i-\overline{a_j})+I_i,\ (a_i+I_j-\overline{a_i})+I_j)$$

$$= (I_i,\ I_j)$$

$$= (\overline{0},\ \overline{0})$$

그러므로 $1-(a_i+a_j) \in \ker\phi_{ij} \subseteq I_i \cap I_j \subseteq I_i+I_j$ 이다.

한편 $a_i+a_j \in I_i+I_j$ 이므로 $1 \in I_i+I_j$ 이다.

즉 $I_i+I_j = R$

따라서 $i \neq j$ 일 때 I_i 와 I_j 는 여극대 이다.

역으로 $\forall\, i \neq j$, I_i 와 I_j 는 여극대이라 하자.

즉 $\forall i \neq j$, $I_i + I_j = R$ 이라 한다.

ϕ 가 surjection 임을 보이기 위해서는

$(\overline{a_1}, \overline{a_2}, \ldots, \overline{a_n}) \in \oplus R/I_i$ 에 대하여

$$\begin{aligned}\phi(a) &= (\phi_1(a),\ \phi_2(a),\ \ldots,\ \phi_n(a)) \\ &= (\overline{a_1}, \overline{a_2}, \ldots, \overline{a_n})\end{aligned}$$

인 $a \in R$ 가 존재함을 보이면 충분하다.

n에 관한 induction 을 쓴다.

$n = 1$ 일 때 $\phi : R \to R/I_1$ 를 $\phi(a) = \phi_1(a) = \overline{a_1}$

으로 정의하며 항상 성립한다.

$n = 2$ 일 때 I_1, I_2 가 가정에 의해서 여극대 이므로,

즉 $I_i + I_j = R$ 이므로, $e_1 + e_2 = 1$ 인 $e_1 \in I_1$, $e_2 \in I_2$ 가 존재한다.

이제 $\phi(x) = (\phi_1(x),\ \phi_2(x)) = (\overline{a_1},\ \overline{a_2})$ 인 x를 구하자.

$x = a_1 e_2 + e_1 a_2$ 라 둔다. 이 x에 대하여

$\phi(x) = (\phi_1(x),\ \phi_2(x)) = (\overline{a_1},\ \overline{a_2}) \in R/I_1 \oplus R/I_2$

임을 증명한다.

$$\begin{aligned}\phi_1(x) &= \overline{a_1 e_2 + a_2 e_1} \\ &= \overline{a_1 e_2} + \overline{a_2 e_1} \\ &= \overline{a_1}\,\overline{e_2} + \overline{a_2}\,\overline{e_1} \\ &= \overline{a_1}\,\overline{e_2} = \overline{a_1}(\overline{1 - e_1}) = \overline{a_1} - \overline{a_1}\,\overline{e_1} = \overline{a_1}\end{aligned}$$

$$\begin{aligned}\phi_2(x) &= \overline{a_1 e_2 + a_2 e_1} \\ &= \overline{a_1 e_2} + \overline{a_2 e_1} \\ &= \overline{a_1}\,\overline{e_2} + \overline{a_2}\,\overline{e_1} \\ &= \overline{a_2}(\overline{1 - e_2}) = \overline{a_2} - \overline{a_2}\,\overline{e_2} = \overline{a_2}\end{aligned}$$

그러므로 위의 x가 원하던 원소임을 안다.

$n = 1, 2, \ldots, k-1$ 에 대해서는 성립한다고 가정한다.

Lemma 2-1 에 의해서 $I_1, I_2, \ldots, I_{k-1}, I_k$ 이 여극대이면

$I_k + \bigcap_{i=1}^{k-1} I_i = R$ 이므로

이때 $y + z = 1$ 인 $y \in \bigcap_{i=1}^{k-1} I_i$, $z \in I_k$ 가 존재한다.

수학적 귀납법에 의해서 $\phi_i(\alpha) = \overline{a_i}$ (단, $i = 1, 2, \ldots, k-1$) 인

$\alpha \in R$ 가 존재한다.

이제 $\phi(x) = (\phi_1(x), \phi_2(x), \ldots, \phi_k(x)) = (\overline{a_1}, \ldots, \overline{a_k})$인

x 를 찾자

$x = z\alpha + a_k y$ 라고 두면

$$\begin{aligned}
\phi_k(x) &= \phi_k(z\alpha + a_k y) \in a/I_k \\
&= \overline{z\alpha + a_k y} = \bar{z}\,\bar{\alpha} + \overline{a_k}\,\bar{y} \\
&= \bar{0} \cdot \bar{a} + \overline{a_k}(\overline{1-z}) = \overline{a_k} - \overline{a_k} \cdot \bar{z} = \overline{a_k},
\end{aligned}$$

모든 $i = 1, 2, \ldots, k-1$ 에 대해서

$$\begin{aligned}
\phi_i(x) &= \phi_i(z\alpha + a_k y) = \phi_i((1-y)\alpha + a_k y) \\
&= \phi_i(\alpha + (a_k - \alpha)y) = \phi_i(\alpha) = \overline{a_i}
\end{aligned}$$

이다. 왜냐하면

$(a_k - \alpha)y \in \bigcap_{i=1}^{k-1} I_i \subseteq I_i \quad (i = 1, 2, \ldots, k-1)$ 에 대하여

$\phi_i : R \to R/I_i$ 는 $\phi_i((a_k - \alpha)y) = \bar{0}$ 이다.

따라서, $x = z\alpha + a_k y \in R$ 에 대하여

$\phi(x) = (\phi_1(x), \phi_2(x), \ldots, \phi_n(x))$

$= (\overline{a_1}, \ldots, \overline{a_{k-1}}, \overline{a_k})$ 이므로

ϕ 는 surjection 이다.

그러므로 모든 n에 대하여 성립한다. ∎

iii) ϕ : injection $\Leftrightarrow$ $\bigcap_{i=1}^{n} I_i = 0$ 은 (Theorem 2-10) 제 1동형정리에 의한다.

≪ Corollary ≫

단위원 1을 가진 환 R에서 R의 두 이데알 I, J에 대하여 $R = I + J$일 때

사상 $f : R \rightarrow R/I \oplus R/J$, $\quad f(a) = (a+I,\ a+J)$ 는

위로의($onto$) 환 준동형사상이고 $\ker f = I \cap J$ 이다.

그리고 사상 $\phi : R/I \cap J \rightarrow R/I \oplus R/J$

$\phi(a + I \cap J) = (a+I,\ a+J)$는 환 동형사상이고

$R/I \cap J \cong R/I \oplus R/J$ 이다.

($proof$) 사상 f 는 분명히 환 준동형 사상이다.

그리고 $R = I + J$ 이므로 적당한 원소 $i \in I$, $j \in J$ 에 대하여

$i + j = 1$ 이다.

임의의 $(c+I,\ d+J) \in R/I \oplus R/J$ 에 대하여

$a = jc + id$ 라고 하면

$a - c = jc + id - c = id + (j-1)c = i(d-c) \in I$

$a - d = jc + id - d = jc + (i-1)d = j(c-d) \in J$ 이므로

$c + I = a + I$, $\ d + J = a + J$ 이고

따라서 $f(a) = (a+I,\ a+J) = (c+I,\ d+J)$ 이므로

f 는 위로의 환 준동형사상이다. 그리고

$x \in \ker f \Leftrightarrow (x+I,\ x+J) = (0+I,\ 0+J) \Leftrightarrow x \in I \cap J$

이므로 $\ker f = I \cap J$ 이다.

≪ Theorem 3-2 ≫ (다항식 환에서 중국인의 나머지 정리)

체 F 위의 다항식 $f_1(x), \ldots, f_n(x)$ 가 쌍마다 서로소 일 때

$f(x) = f_1(x) f_2(x) \ldots f_n(x)$ 라고 하면.

사상 $\phi : F[x] \to F[x]/(f_1(x)) \oplus \ldots \oplus F[x]/(f_n(x))$,

$= \phi(g(x)) = (g(x) + (f_1(x)), \ldots, g(x) + (f_n(x)))$,

는 위로의 환 준동형사상이고 또 다음이 성립한다.

$F[x]/(f(x)) \cong F[x]/(f_1(x)) \oplus \ldots \oplus F[x]/(f_n(x))$

$(proof)$ 사상 ϕ 가 환준동형사상 임은 분명하다.

이제 $h_i(x) = \dfrac{f(x)}{f_i(x)}$ $(i = 1, 2, \ldots, n)$ 라고 하면

$f_i(x)$와 $h_i(x)$는 서로 소 이므로

$f_i(x)\, s_i(x) + h_i(x)\, t_i(x) = 1$ 인 다항식

$s_i(x), t_i(x) \in F[x]$ 가 존재한다.

임의의 다항식 $g_1(x), \ldots, g_n(x) \in F[x]$ 에 대하여

$$g(x) = \sum_{i=1}^{n} g_k(x) h_k(x) t_k(x)$$

$= g_1(x) h_1(x) t_1(x) + \ldots + g_n(x) h_n(x) t_n(x)$ 라고 놓으면

각 $i = 1, 2, \ldots, n$ 에 대하여

$f_i(x) \mid (h_i(x) t_i(x) - 1)$, $f_i(x) \mid h_k(x) t_k(x)$ $(k \neq i)$ 이므로

$f_i(x) \mid (g(x) - g_i(x))$ 이다.

즉, 각 $i = 1, 2, \ldots, n$ 에 대하여

$g(x) + (f_i(x)) = g_i(x) + (f_i(x))$ 이다.

(이 식은 환 $F[x] / (f_i(x))$ 에서 성립한다.)

따라서 $\phi(g(x)) = (g(x) + (f_1(x)), \ldots, g(x) + (f_n(x)))$

$$= (g_1(x) + (f_1(x)), \ldots, g_n(x) + (f_n(x)))$$

이므로 ϕ는 위로의 사상이다. 한편

$$\ker\phi = \{ g(x) \in F[x] \mid \phi(g(x)) = (0 + (f_1(x)), \ldots, (0 + (f_n(x))) \}$$

$$= \{ g(x) \in F[x] \mid g(x) \in (f_1(x)), \ldots, g(x) \in (f_n(x)) \}$$

$$= (f_1(x)) \cap \ldots \cap (f_n(x))$$

이고, $f_1(x), \ldots, f_n(x)$가 쌍마다 서로소 이므로

$$\ker\phi = (f_1(x)) \cap \ldots \cap (f_n(x))$$

$$= (f_1(x) f_2(x) \ldots f_n(x)) = (f(x))$$

따라서 제1동형정리 (Theorem 2-10)에 의하여

$F[x] / (f(x)) \cong F[x] / (f_1(x)) \oplus \ldots \oplus F[x] / (f_n(x))$ 이다. ∎

Ⅳ CRT의 응용

≪RSA 암호방식 응용≫

시이저 암호 같은 재래식 암호 체계에서는 송신자와 수신자는 비밀 키를 공유해야 한다. 송신자는 송신하려는 평문을 암호화하기 위하여 키를 사용하고 수신자는 획득된 암호문을 복호화하기 위하여 같은 키를 사용한다. 공개키 암호법은 두 개의 키, 즉 암호화 키와 복호화 키를 사용한다는 점에서 재래식 암호법과 구별된다. 두 개의 키는 서로 역작용을 초래하고 따라서 연관되어 있지만, 암호화 키로부터 복호화 키를 유도할 수 있는 쉬운 계산 방법은 없다. 따라서 복호화 키를 손상시키지 않고 암호화 키가 공개될 수 있다. 각 사용자는 메시지를 암호화할 수 있지만 의도된 (그의 복호화 키가 비밀로 보관된) 수신자만이 복호화할 수 있다. 공개키 암호체계의 주된 이점은 송신자들과 수신자들이 서로 통신하기로 결정하기에 앞서 키를 교환할 필요가 없다는 것이다.

1997년에 리베스트(R. Rivest), 샤밀(A. Shamir) 및 애들먼(A. Adleman)은 수론의 기초적인 지식만을 이용하는 공개키 암호체계를 제안했다. 그들의 암호체계는 알고리즘 발명자들의 머리글자를 따라서 RSA라고 불리운다. 그것의 보안성은, 컴퓨터 기술의 현재 상태에서 큰 소인수를 갖는 합성수의 분해는 불가능할 정도로 시작이 오래 걸린다는 가정에 의존한다.

RSA 암호는 다음과 같은 세 단계를 거쳐 만들어진다.

첫 번째 단계는 공개키를 만드는 단계이다. A라는 사람이 자연수의 순서쌍 (e, m)을 공개하는 것이다. 여기서 e와 m은 다음과 같이 만든다. 50자리에서 100자리 사이의 아주 큰 소수 p와 $q(p \neq q)$를 정하여 첫 번째 비밀키로 한다. 그리고

$$m = pq$$

라 놓은 후 $1, 2, \ldots, m$에서 m과 서로소인 자연수의 개수

$\phi(m) = (p-1)(q-1)$ 을 구한다.

마지막으로 $\phi(m)$ 과 서로소인 3자리 혹은 4자리 자연수 e 를 하나 선택한다.
이렇게 하는 이유는 주어진 200자리 자연수가 소수인지 알아내는 것은 아직까지 매우 어렵지만 200자리 소수를 찾는 것은 어렵지 않기 때문이다.
두 번째 단계는 암호화 단계이다. B라는 사람이 A가 공개한 키 (e, m)을 가지고 A에게 메시지를 보내는 것이다.

$$\text{평문 정수 } x \rightarrow y = x^e \bmod m$$

세 번째 단계는 복호화 단계이다. 즉 비밀키에 관련된 단계이다. A가 B로부터 받은 암호화된 메시지 y 를 해독하기 위해서는 두 번째 비밀키 (d, m)이 필요하다.
즉 $ed = 1 \mod \phi(m)$ 이 되는 d 를 확장된 유클리드 알고리즘으로 계산하여 비밀키로 한다.

$$\text{암호문 } y \Rightarrow \text{평문 정수 } x = y^d \bmod m$$

위와 같은 과정을 거쳐 공개키 암호를 만들 수 있는 것은 다음과 같은 이유 때문이다.

$$ed \equiv 1 \pmod{\phi(m)}$$

즉, $ed = 1 + k\phi(m)$ 이고 $1 \le x < m$ 이라 가정하자.
그러면 m과 서로소인 x에 대하여 오일러 정리를 사용하면

$$\begin{aligned}
(x^e)^d \pmod m &= x^{ed} \pmod m \\
&= x^{1+k\phi(m)} \pmod m \\
&= x^1 (x^{\phi(m)})^k \pmod m \\
&= x(1)^k \pmod m \\
&= x
\end{aligned}$$

다른 한편, x 가 $m = pq$ 과 서로소가 아니라면 $(x, m) = p$ (또는 q)라 놓자.

$$\phi(m) = \phi(p)\phi(q) = (p-1)(q-1)$$

이므로

$$
\begin{aligned}
x^{ed} \pmod q &= x^{1+(p-1)(q-1)k} \pmod q \\
&= x(x^{q-1})^{k(p-1)} \pmod q \\
&= x(1)^{k(p-1)} \pmod q \\
&= x \pmod q
\end{aligned}
$$

그리고 $x \equiv 0$

$\equiv x^{ed} \pmod p$

따라서 중국인의 나머지 정리에 의해

$$x \equiv (x^e)^d \pmod m$$

이 성립한다.

다음은 이해를 돕기 위하여 만든 RSA 암호의 간단한 예이다.

$m = 11413 = pq = 101 \times 113$

$\phi(m) = 11200, \quad d = 6597, \quad e = 3533$

메시지 $x = 9726$

암호화 : $9726^{3533} = 5761 \pmod{11413}$

복호화 : $5761^{6597} = 9726 \pmod{11413}$

계 산 : $5761^{6597} \equiv (9726^{3533})^{6597} \equiv 9726^{23307201}$

$\equiv 9726^{20810 \times 11413 + 1} \equiv 9726 \pmod{11413}$

이러한 RSA 암호체계에서 암호화 과정과 복호화 과정을 거쳐 공개키를 만들기까지는 중국인의 나머지 정리가 중요하게 이용되는 것을 확인할 수가 있다.
중국인의 나머지 정리의 유일한 해에 의해 공개키가 유일하게 정해짐으로서 RSA 암호체계가 확립된다고 할 수 있다.

V 결 론

정수론과 대수학에 있어서의 중국인의 나머지 정리의 관련 내용을 정리하고 몇 가지 정리는 다른 방법의 증명을 정리함으로서 중국인의 나머지 정리를 잘 이해 할 수 있도록 서술하여 놓았다.

또 실용학문인 암호학의 일부분인 RSA 암호체계에 활용되는 중국인의 나머지 정리는 중요한 의미를 갖는다고 할 수 있다.

단순한 하나의 공통해를 구하는데 그치지 않고 다른 분야에도 활용됨을 보여주는 좋은 예라고 할 수 있을 것이다.

본 논문을 통하여 많은 사람들이 중국인의 나머지 정리에 관한 내용의 많은 사실을 알고 활용하며 전달 할 수 있기를 바란다.

참 고 문 헌

1. 김응태 · 박승안, 『현대대수학 제6판』, 경문사, 2008

2. 김응태 · 박승안, 『정 수 론 제6판』, 경문사, 2006

3. 천장호, 『정 수 론』, 경문사, 2009

4. 남호영 · 박제남, 『영재교육을 위한 창의력수학 I』, 경문사, 2006

5. Haward Eves, An Introduction To the history of mathematics.

   이우영 · 신항균 옮김, 『수학사』, 경문사, 2001

6. J. Barshay, Topics in Ring theory, W. A. Benjamin. Inc., 1969

7. L. childs, A Concrete introduction to higher Algebra springer-verlay,

   Newyork, 1998

8. John B, Fraleigh, A First course in abstract algebra,

   Addison-wesley Publishing company, Inc., 1991

9. 송현숙, "중국인의 나머지 정리에 관한 연구", 석사학위 논문, 조선대학교, 1992

10. 김순태, "중국인의 나머지 정리에 관한 연구", 석사학위 논문, 경북대학교, 1993

저작물 이용 허락서

학 과	수학교육	학 번	20078077	과 정	석사
성 명	한글: 신 현 철 한문: 申 炫 哲 영문: Shin Hyun Cheol				
주 소	광주광역시 남구 월산 4동 552-9				
연락처	E-MAIL : shinhyunchol@hanmail.net				
논문제목	한글 : 중국인의 나머지 정리에 관한 연구 영어 : A study on the Chinese Remainder Theorem.				

본인이 저작한 위의 저작물에 대하여 다음과 같은 조건아래 조선대학교가 저작물을 이용할 수 있도록 허락하고 동의합니다.

- 다 음 -

1. 저작물의 DB구축 및 인터넷을 포함한 정보통신망에의 공개를 위한 저작물의 복제, 기억장치에의 저장, 전송 등을 허락함
2. 위의 목적을 위하여 필요한 범위 내에서의 편집·형식상의 변경을 허락함. 다만, 저작물의 내용변경은 금지함.
3. 배포·전송된 저작물의 영리적 목적을 위한 복제, 저장, 전송 등은 금지함.
4. 저작물에 대한 이용기간은 5년으로 하고, 기간종료 3개월 이내에 별도의 의사 표시가 없을 경우에는 저작물의 이용기간을 계속 연장함.
5. 해당 저작물의 저작권을 타인에게 양도하거나 또는 출판을 허락을 하였을 경우에는 1개월 이내에 대학에 이를 통보함.
6. 조선대학교는 저작물의 이용허락 이후 해당 저작물로 인하여 발생하는 타인에 의한 권리 침해에 대하여 일체의 법적 책임을 지지 않음
7. 소속대학의 협정기관에 저작물의 제공 및 인터넷 등 정보통신망을 이용한 저작물의 전송·출력을 허락함.

동의여부 : 동의( ) 반대( )

년 월 일

저작자: 신 현 철 (서명 또는 인)

조선대학교 총장 귀하