[UCI]I804:24011-200000240331

2010년 7월
교육학석사(수학교육)학위논문

합동식과 그 응용에 관한 연구

조선대학교 교육대학원

수학교육전공

윤 수 지

합동식과 그 응용에 관한 연구

A Study on Congruence and its Application

2010 년 7 월

조선대학교 교육대학원

수학교육전공

윤 수 지

합동식과 그 응용에 관한 연구

지도교수 김 남 길

이 논문을 교육학석사(수학교육)학위 청구논문으로 제출함.

2010 년 7 월

조선대학교 교육대학원

수학교육전공

윤 수 지

윤수지의 교육학 석사학위 논문을 인준함.

심사위원장 조선대학교 교수 박 순 철 인

심사위원 조선대학교 교수 김 남 권 인

심사위원 조선대학교 교수 김 남 길 인

2010 년 7 월

조선대학교 교육대학원

목 차

ABSTRACT

A Study on Congruence and its Application

Su-ji Yun

Advisor : Prof. Nam-gil Kim

Major in Mathematics Education

Graduate School of Education, Chosun University

Congruent expression in number theory have been studied and used since ancient times. Such as Euler's theorem, Fermats theorem, and Wilson's.

But a systematic theory of congruence was firstly introduced in 1801 when Gauss wrote 'Disquisitiones Arithmeticae'. This book was first published as a book on number theory. Gauss showed that the Congruence relations and equal relations similar properties and used the symbol ' ≡ ' which is similar to ' = '.

Gauss raised a question finding solutions of the general polynomial congruence.

Generally, there is no simple method for solving the general polynomial congruence

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots\cdots + a_0 \equiv 0 \pmod{m}.$$

However, given special moduli like prime modulus, solutions for the polynomial equations exist.

This paper aims at introducing the historical and theoretically basic concept of congruences in number theory, studying on the solutions of polynomial congruence using Fermat's theorem, more generalized Euler's theorem, Wilson's theorem, chinese Remainder theorem, Primitive Roots, and Euler's Criterion, ranging from linear polynomial congruence to higher degree polynomial congruence.

And as a primary content, examples of congruence theory applied in a real-life will be discussed.

Ⅰ. 서 론

정수론(number theory)에서 합동식에 대한 여러 가지 사실들이 옛날부터 활발히 연구되었으며 사용되었다.
그중에는 오일러정리(Euler theorem)와 페르마정리(Fermat theorem), 윌슨정리(Wilson theorem) 등이 있다. 그러나 가장 뛰어나고 체계적인 이론으로서의 합동식을 보여주는 것은 가우스(Karl Friedrich Gauss, 1777~1855)라 할 수 있다.

가우스는 1801년에 24세 때 '산술 논고(Disquisitiones Arithmeticae)' 라는 책을 출간하였는데 이 책은 최초로 정수론을 체계적으로 다룬 책이라 할 수 있다. 이 책에서 합동에 대한 개념과 표기법 그리고 이차잉여의 상호법칙을 다루고 있다. 그리고 그는 최소 제곱법과 비유클리드 기하학을 발견하였다. 그가 발표한 '산술 논고'는 가우스를 일류 수학자의 선두주자로서의 위치에 올려놓았다. 19세기 중엽까지 수학은 방대하고 다루기 힘든 구조를 가지면서 발전하였고 이에 따라 수학은 대단히 많은 분야로 세분되어 각 분야는 극히 제한된 전문 수학자만이 이해할 수 있을 정도로 발전하였다. 가우스는 거의 모든 분야를 이해하고 연구할 수 있는 능력을 지닌 완전한 수학자였다. 가우스는 수학의 거의 모든 분야와 천문학, 물리학에 상당한 업적을 남겼지만 항상 정수론을 중요시하고 이에 깊은 관심을 두고 연구하였다. 그는 ' 수학은 과학의 여왕이고, 정수론은 수학의 여왕이다. ' 라고 주장할 정도로 정수론을 중요시하였다.

가우스가 보여준 합동 관계(Congruence relation)는 등호 관계(Equality relation)와 유사한 성질을 가지고 있고 기호도 ' = '와' ≡ '로 비슷하다.
가우스의 합동관계를 쉽게 시간계산의 예를 들어 보자면, 4시에서 3시간 후는 7시라는 것을 알 수 있다. 그런데 9시에서 5시간 후는 2시가 되며 10시에서 7시간 후는 5시가 된다. 이것을 식으로 표현하면 각각 4+3=7, 9+5=2, 10+7=5 이다. 우리가

아는 보통의 덧셈과는 다르지만 이러한 시간 계산 방법은 다른 계산방법과 마찬가지로 산술적으로 많은 성질을 만족시키고 있다.
이 계산방법은 12를 '법(modulus)' 으로 하는 계산법이고 ' = '을 ' ≡ (mod 12)' 로 쓴다. 12를 ' 법 ' 으로 하는 계산법에서 12의 배수는 모두 0 과 같다.

가우스는 일반적인 합동방정식
$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots\cdots + a_0 \equiv 0 \pmod{m}$. $a_n \not\equiv 0 \pmod{m}$의
해를 구하는 문제를 고안해냈다. 이러한 합동방정식은 경우에 따라 해가 존재 하지 않기도 한다. 그러나 주어진 법을 소수로 한정시키면 합동식의 해를 구할 수 있다.

이 논문에서는 합동식의 기본 개념을 소개하고 페르마의 정리, 오일러의 정리, 윌슨의 정리, 중국인의 나머지 정리 등을 이용하여 일차 합동식부터 고차 합동식까지의 해를 구하는 방법을 요약한다.
그리고 가장 중점적으로 다루게 되는 내용으로서 합동이론이 어떻게 이용되고 있는지 알아 볼 것이다.

Ⅱ. 정의 및 기본정리

제1장 합 동

「산술 논고」의 첫째 장에서 가우스는 합동의 개념과 그것을 강력한 기술로 만들어 주는 용어를 사용하였다.

[정의 1] 고정된 양의 정수 m에 대하여, 두 정수 a, b 의 차가 m의 배수일 때, 즉, $m \mid (a-b)$ 일 때, a와 b는 법 (modulus) m에 관하여 **합동 (congruent)** 이라 하고, 이 사실을 $a \equiv b \pmod{m}$ 으로 나타낸다.

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

또, $a \equiv b \pmod{m}$이 아닐 때, 이 사실을 $a \not\equiv b \pmod{m}$로 나타낸다.

그리고 합동기호 '≡'가 들어 있는 식을 **합동식(congruence)**이라고 한다. **[3]**

[예제 1] $7 \equiv 2 \pmod{5}$ $\quad 15 \equiv 0 \pmod{5}$ $\quad 6 \equiv -4 \pmod{5}$

$3 \equiv 6 \pmod{3}$ $\quad 1 \not\equiv -1 \pmod{3}$ $\quad 25 \not\equiv 12 \pmod{7}$

[정리 1] 양의 정수 m과 정수 a, b, c 에 대하여 다음이 성립한다.

(1) $a \equiv a \pmod{m}$ ……반사율(reflexive)

(2) $a \equiv b \pmod{m}$ 이면, $b \equiv a \pmod{m}$ 이다. ……대칭율(symmetric)

(3) $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$ 이면,

$a \equiv c \pmod{m}$이다. ……추이율(transitive) **[5]**

(증명) (1) 분명히 $m \mid (a-a)$ 이므로 $a \equiv a \pmod{m}$ 이다.

(2) $a \equiv b \pmod{m}$ 이면, $m \mid (a-b)$ 이므로 $m \mid (b-a)$ 이고

따라서 $b \equiv a \pmod{m}$ 이다.

(3) $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$ 이면,

$m \mid (a-b)$, $m \mid (b-c)$, $a-c=(a-b)+(b-c)$ 이므로

$m \mid (a-c)$ 이고 따라서 $a \equiv c \pmod{m}$이다.

[정리 2] 양의 정수 m과 임의의 정수 a에 대하여 a를 m으로 나누었을 때 나머지를 r이라고 하면 다음이 성립한다.

$a \equiv r \pmod{m}$ $\quad (0 \le r < m)$

그리고, 법 m에 관하여 0, 1, ……, $m-1$은 어느 둘도 합동이 아니다. **[3]**

(증명) $a=mq+r$, $0 \le r < m$ 인 정수 q가 존재하고 이 때,

$a \equiv r \pmod{m}$ $\quad (0 \le r < m)$ 이다.

또, $0 \le r < m$, $0 \le s < m$ 인 두 정수 r , s 에 대하여 $r \equiv s \pmod{m}$이면

$m \mid (r-s)$ 이고 $-m < r-s < m$ 이므로 $r-s=0$

즉, $r=s$ 이다.

따라서 법 m에 관하여 0, 1, ……, $m-1$은 어느 둘도 합동이 아니다.

[정리 3] 법 m 에 대하여 $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$일 때 다음이 성립한다.

(1) $a \pm c \equiv b \pm d \pmod{m}$, $\quad ac \equiv bd \pmod{m}$

(2) $a \pm c \equiv b \pm c \pmod{m}$, $\quad ac \equiv bc \pmod{m}$ **[3]**

(증명) 정의에 의하여 $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$ 이면,

$m \mid (a-b)$, $m \mid (c-d)$ 이고

또, $(a \pm c)-(b \pm d)=(a-b) \pm (c-d)$

$ac-bd=(a-b)c+b(c-d)$, 이므로 $m \mid \{(a \pm c)-(b \pm d)\}$, $m \mid (ac-bd)$ 이고

따라서 $a \pm c \equiv b \pm d \pmod{m}$, $\quad ac \equiv bd \pmod{m}$

그리고 $c \equiv c \pmod{m}$ 이므로 (1) 에 의하여 (2) 가 성립한다.

[따름 정리 1] $a_1 \equiv b_1 \pmod{m}, \cdots\cdots, a_n \equiv b_n \pmod{m}$ 일 때, 다음이 성립한다.

$$a_1 + \cdots\cdots + a_n \equiv b_1 + \cdots\cdots + b_n \pmod{m},$$

$$a_1 \cdots\cdots a_n \equiv b_1 \cdots\cdots b_n \pmod{m}$$

또, $a \equiv b \pmod{m}$ 이면 양의 정수 n 에 대하여 $a^n \equiv b^n \pmod{m}$ **[3]**

[예제 2] $a = 1! + 2! + 3! + \cdots\cdots + 199! + 200!$ 이라 하자.

n 을 $n \geq 5$인 정수라 하면 $5! = 120 \equiv 0 \pmod{15}$ 이므로

$n! = 5! \cdot 6 \cdot 7 \cdot \cdots\cdots \cdot n \equiv 0 \cdot 6 \cdot 7 \cdot \cdots\cdots \cdot n = 0 \pmod{15}$

$a \equiv 1! + 2! + 3! + 4! + 0 + 0 + \cdots\cdots + 0 = 33 \pmod{15}$

또한 $33 \equiv 3 \pmod{15}$

$a \equiv 3 \pmod{15}$

따라서 $15 \mid (a-3)$, 즉 a 를 15로 나눌 때의 나머지는 3이다. **[11]**

[예제 3] $3^{42} \cdot 5^{24} - 4$ 가 43으로 나누어떨어짐을 보이자.

$3^{20} \equiv 14 \pmod{43}$ 이므로

$3^{21} \equiv 3^{20} \cdot 3 \equiv 14 \cdot 3 = 42 \equiv -1 \pmod{43}$

$3^{42} = (3^{21})^2 \equiv (-1)^2 = 1 \pmod{43}$

위와 같은 방법으로,

$5^3 = 125 \equiv -4 \pmod{43}$, $5^6 = (5^3)^2 \equiv (-4)^2 = 16 \pmod{43}$

$5^{12} = (5^6)^2 \equiv (16)^2 = 256 \equiv -2 \pmod{43}$ 이므로

$5^{24} = (5^{12})^2 \equiv (-2)^2 = 4 \pmod{43}$

따라서 $3^{42} \cdot 5^{24} \equiv 1 \cdot 4 = 4 \pmod{43}$

그러므로 $43 \mid (3^{42} \cdot 5^{24} - 4)$, 즉 $3^{42} \cdot 5^{24} - 4$ 는 43으로 나누어 떨어진다. **[11]**

[정리 4] $ka \equiv kb \pmod{m}$ 이고 $(k, m) = 1$ 이면 $a \equiv b \pmod{m}$ 이다.

특히, $ka \equiv 0 \pmod{m}$ 이고 $(k, m) = 1$ 이면 $a \equiv 0 \pmod{m}$ 이다.

(증명) 가정 $ka \equiv kb \pmod{m}$ 으로 부터 $k(a-b) = lm$ 인 정수 l 이 존재한다.
가정에서 $(k, m) = 1$ 이므로 $k \mid l$ 이다. 즉, $l = ek$ 인 e 가 존재한다.
따라서 $a - b = em$ 이므로 $a \equiv b \pmod{m}$ 이다.
특히, $ka \equiv 0 \pmod{m}$ 이고 $(k, m) = 1$ 이면 $a \equiv 0 \pmod{m}$ 이다.

제2장 잉여류와 완전잉여계

합동식의 기본정리에서 알아본 [정리 1]의 세 조건을 만족하므로 **합동관계 (Congruence relation)** $a \equiv b \pmod{m}$는 Z 위에서의 **동치관계 (Equivalence relation)**이다. 그 관계가 있는 모든 원소들의 집합을 **동치류 (Equivalence class)** 라 한다. 즉, $\bar{r} = \{a \in Z \mid a \equiv r \pmod{m}\} = \{mk + r \mid k \in Z\}$ **[3]**

[정의 2] 양의 정수 m 에 대하여 $Z_m = \{0, 1, \cdots, m-1\}$ 이라고 할 때, 각 정수 $r \in Z_m$ 에 대하여 $a \equiv r \pmod{m}$인 정수 a 전체로 이루어진 집합 $\bar{r} = \{r, r \pm m, r \pm 2m, r \pm 3m, \cdots\}$을 r 에 의하여 결정된 법 m 에 관한 **잉여류** (residue class) 라고 한다. 즉, $a \in \bar{r} \Leftrightarrow a \equiv r \pmod{m}$

[예제 4] 법 3에 관한 잉여류 $\bar{0}, \bar{1}, \bar{2}$ 는 각각 다음과 같다. **[11]**

$$\bar{0} = \{\cdots, -6, -3, 0, 3, 6, 9, \cdots\},$$

$$\bar{1} = \{\cdots, -5, -2, 1, 4, 7, 10, \cdots\},$$

$$\bar{2} = \{\cdots, -4, -1, 2, 5, 8, 11, \cdots\}$$

[정의 3] 법 m 에 관한 m 개의 잉여류 $\bar{0}, \bar{1}, \cdots, \overline{m-1}$ 에서 각각 단 한 개의 정수를 택하여 만든 집합 $S = \{s_0, s_1, \cdots, s_{m-1}\}$를 법 m 에 관한 **완전 잉여계 (complete residue system modulo m)** 라고 한다.

즉, 집합 $S=\{s_0, s_1, \cdots, s_{m-1}\}$의 각 원소가 $Z_m=\{0, 1, \cdots, m-1\}$에 속하는 단 한 정수와 법 m 에 관하여 합동일 때,
S 는 법 m 에 관한 완전잉여계이다. [11]

정수로 이루어진 집합 $S=\{s_0, s_1, \cdots, s_{m-1}\}$에 대하여 다음이 성립할 때,
S는 법 m 에 관한 완전잉여계이다.

(1) $|S|=m$

(2) $s_0, s_1, \cdots, s_{m-1}$은 어느 둘도 법 m에 관하여 합동이 아니다.

즉, $s_i \neq s_j \Rightarrow s_i \not\equiv s_j \pmod{m}$

또, 집합 S 가 법 m 에 관한 완전잉여계이면,
임의의 정수 a 는 법 m 에 관하여 S 에 속하는 단 한 원소와 합동이다.

[정의 4] 각 잉여류에서 음수가 아닌 가장 작은 잉여를 하나씩 선택하여 만든 완전잉여계를 **최소 완전잉여계 (complete system of the least non-negative residues)** 라 한다. 각 잉여류에서 절댓값이 가장 작은 잉여를 하나씩 선택하여 만든 완전잉여계를 **절대 최소 완전잉여계 (complete system of the absolutely least residues)**라 한다.

[예제 5] 법 $m=6$ 에 관하여

$\overline{0}=\{\cdots, -12, -6, 0, 6, 12, \cdots\}=\overline{-6}=\overline{6}=\cdots$

$\overline{1}=\{\cdots, -11, -5, 1, 7, 13, \cdots\}=\overline{-5}=\overline{7}=\cdots$

$\overline{2}=\{\cdots, -10, -4, 2, 8, 14, \cdots\}=\overline{-4}=\overline{8}=\cdots$

$\overline{3}=\{\cdots, -9, -3, 3, 9, 15, \cdots\}=\overline{-3}=\overline{9}=\cdots$

$\overline{4}=\{\cdots, -8, -2, 4, 10, 16, \cdots\}=\overline{-2}=\overline{10}=\cdots$

$\overline{5}=\{\cdots,-7,-1,5,11,17,\cdots\}=\overline{-1}=\overline{11}=\cdots$ 이고,

$Z_6=\{\overline{0},\overline{1},\overline{2},\overline{3},\overline{4},\overline{5}\}=\{\overline{-6},\overline{-5},\overline{-4},\overline{9},\overline{10},\overline{11}\}=\cdots$ 이다.

또한 $S=\{0,1,2,3,4,5\}$,

$T=\{-12,-5,-4,3,10,17\}$

$Q=\{-2,-1,0,1,2,3\}$

$L=\{-3,-2,-1,0,1,2\}\cdots$ 등은 완전잉여계이다.

특히, S 는 최소 완전잉여계이고, Q 와 L 은 절대 최소 완전잉여계이다. [11]

제3장 페르마 정리

페르마(Pierre de Fermat, 1601~1665)의 수학에 대한 관심은 정수론에 있었던 것 같다. 연구 활동 중 가장 두드러진 것은 정수론(整數論) 분야이다. 디오판토스의 수론서(數論書)에 자극되어 관여하게 된 이 분야에서는 소수수열(素數數列:페르마형 소수)의 추측에서 시작하여, 페르마의 소정리, 4n+1형 소수에 관한 제곱수[平方數]의 합의 정리, n=2의 디오판토스방정식의 해답의 정리 등에서 뛰어난 통찰력이 발휘되어 정수론 연구사상 커다란 전기가 되었다.

페르마가 발견하고 스스로 증명하였다고 하는 정리를 증명하는 데 상금까지 붙고 후년의 수학자들이 많은 노력을 기울이면서 정수이론은 많이 발전하게 되었다. 영국의 수학자이자 미국 프린스턴대학교 교수인 앤드루 와일스(Andrew Wiles)는 1993년 6월 23일 영국 뉴턴연구소에서 행한 강연중 이 정리의 증명을 제시하였으며, 그 뒤 발견된 결함은 자신의 제자이자 켐브리지대학교 교수인 리처드 테일러(Richard Taylor)와의 공동연구로 1994년 10월 보완하였다. 그 내용이 1995년 《수학연보 Annals of Mathematics》에 발표되어, 페르마의 '최후의 정리'는 공식적으로 증명되었다.

[정리 5] (페르마의 정리) 정수 p 가 소수일 때, 다음이 성립한다.

(1) 모든 정수 a 에 대하여 $a^p \equiv a \pmod{p}$ 이다.

(2) $(a, p) = 1$인 정수 a 에 대하여 $a^{p-1} \equiv 1 \pmod{p}$ 이다. **[3]**

(증명) (1) 이항정리에 의하면, 임의의 두 정수 a, b 에 대하여 다음이 성립한다.

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1} b + \cdots + \binom{p}{r} a^{p-r} b^r + \cdots + b^p$$

여기서 $\binom{p}{r} = \dfrac{p!}{r!(p-r)!}$ 은 정수이고 $p! = \binom{p}{r} r!(p-r)!$ 이다.

그런데, $1 \le r \le p-1$ 일 때, $p \nmid 1 \cdot 2 \cdot \cdots \cdot r$,

$p \nmid 1 \cdot 2 \cdot \cdots \cdot (p-r)$ 이지만

$p \mid p!$ 이므로 $p \mid \binom{p}{r}$

즉 $\binom{p}{r} \equiv 0 \pmod{p}$ 이다.

따라서 $(a+b)^p \equiv a^p + b^p \pmod{p}$ 이다.

먼저 $n = 1$ 일 때, $n \equiv 1^p \equiv 1 \equiv n \pmod{p}$ 이다.

이제 양의 정수 n 에 대하여 $n^p \equiv n \pmod{p}$ 이라고 가정하면,

위의 결과에 의하여 다음이 성립한다.

$$(n+1)^p \equiv n^p + 1^p \equiv n + 1 \pmod{p}$$

따라서 모든 양의 정수 n 에 대하여 $n^p \equiv n \pmod{p}$ 이다.

다음에, $0^p \equiv 0 \pmod{p}$ 이다. 그리고 , 임의의 양의 정수 n 에 대하여 $p = 2$ 이면 $(-n)^p \equiv n^p \equiv n \equiv -n \pmod{p}$ 이고, 소수 p 가 홀수이면 $(-n)^p \equiv -n^p \equiv -n \pmod{p}$ 이다.

그러므로 모든 정수 a 에 대하여 $a^p \equiv a \pmod{p}$ 이다.

(2) 위의 (1) 에 의하면 모든 정수 a 에 대하여 $a^p \equiv a \pmod{p}$ 이므로,

특히, $(a, p) = 1$인 정수 a 에 대하여 $a^{p-1} \equiv 1 \pmod{p}$ 이다.

위의 페르마의 정리를 페르마의 소정리(little theorem) 라고도 한다.

[예제 6] 정수 117은 소수가 아니다.

실제로, 117이 소수이면, 페르마의 정리에 의하여 $2^{116} \equiv 1 \pmod{117}$ 이어야 한다.

그러나

$2^6 \equiv 64 \pmod{117}$, $\quad 2^7 \equiv 128 \equiv 11 \pmod{117}$,

$2^8 \equiv 22 \pmod{117}$, $\quad 2^{14} \equiv 11^2 = 121 \equiv 4 \pmod{117}$ 이므로 다음이 성립한다.

$2^{116} \equiv 2^{14 \cdot 8+4} = (2^{14})^8 \cdot 2^4 \equiv 4^8 \cdot 2^4 \equiv 2^{20}$

$\equiv 2^{14} \cdot 2^6 \equiv 2^2 \cdot 2^6 \equiv 2^8 \equiv 22 \not\equiv 1 \pmod{117}$ **[3]**

[정리 6] 정수 p 가 홀수인 소수일 때, Mersenne 수 $M_p = 2^p - 1$ 의 소인수는 모두 $q = 2pk+1$ ($k \geq 1$) 과 같은 꼴이다. **[3]**

(증명) 이제 q 를 M_p 의 소인수라고 하자. 이 때, M_p는 홀수이므로 q 는 홀수이고, 따라서 $(2, q) = 1$ 이므로 페르마의 정리에 의하여

$2^{q-1} \equiv 1 \pmod{q}$ 즉 $q \mid (2^{q-1} - 1)$ 이고 또 $q \mid M_p$ 이므로

$q \mid (M_p, 2^{q-1} - 1)$ 이다.

한편, $(M_p, 2^{q-1} - 1) = (2^p - 1, 2^{q-1} - 1) = 2^{(p, q-1)} - 1$ 이므로, $(p, q-1) \neq 1$이고

따라서 $(p, q-1) = p$ 이므로 $p \mid (q-1)$ 이다.

그런데, p 는 홀수이고 $q-1$ 은 짝수이므로 적당한 양의 정수 k 에 대하여

$q - 1 = 2kp$ 이고 이 때 $q = 2pk+1$ 이다.

[예제 7] Mersenne 수 $M_{13} = 2^{13} - 1 = 8191$ 은 소수이다. **[6]**

실제로, M_{13} 이 합성수이면, M_{13}의 소인수 중에는 $\left[\sqrt{M_{13}}\right] = 90$ 이하인 소인수가 존재한다. 또, M_{13}의 소인수는 $26k+1$ 꼴이므로 이러한 소인수는 53, 79 뿐이다.

한편,

$8191 = 53 \cdot 154 + 29 \qquad 8191 = 79 \cdot 103 + 54$

이므로 이들은 M_{13} 의 약수가 아니다. 따라서 M_{13} 는 소수이다.

제4장 오일러 정리

오일러(Leonhard Euler, 1707~1783)는 페르마의 업적을 깊이 이해하고 높이 평가하여 페르마가 증명 없이 발표한 여러 정리를 증명하였고 페르마의 정리를 일반화 하였으며 Euler ϕ 함수를 도입하였고 이차잉여의 상호 법칙을 발견하였다.

[정의 5] (Euler ϕ 함수) 집합 Z_m^*, $m \geq 2$의 위수를 $\phi(m)$로 나타낸다.
즉, $\phi(m) = |Z_m^*|$이다. 임의의 자연수 m을 $\phi(m)$으로 대응시키는 함수 $\phi: N \to Z$를 $\phi-$함수라고 한다. 이때, $\phi(1) = 1$이라고 정의한다. **[5]**

[정리 7](오일러의 정리) 정수 m (≥ 2) 과 (a, m) $= 1$ 인 정수 a 에 대하여

$$a^{\phi(m)} \equiv 1 \pmod{m} \text{ 이다.}$$

특히, 소수 p 와 (a, p) $= 1$ 인 정수 a 에 대하여 $a^{p-1} \equiv 1 \pmod{p}$ 이다. **[3]**

(증명) 먼저 법 m 에 관한 기약잉여계 $R = \{ r_1, r_2, \cdots, r_{\phi(m)} \}$ 를 택하고 (a, m) $= 1$인 정수 a 에 대하여 $T = \{ ar_1, ar_2, \cdots, ar_{\phi(m)} \}$ 가 법 m 에 관한 기약잉여계임을 증명한다.

실제로, $m \geq 2$ 이므로 $a \neq 0$ 이고 따라서 $|T| = |R| = \phi(m)$ 이다.

또, $r_i \in R$ 에 대하여 (r_i, m) $= 1$ 이고 (a, m) $= 1$ 이므로 (ar_i, m) $= 1$이다.

그리고

$$ar_i \equiv ar_j \pmod{m} \Rightarrow r_i \equiv r_j \pmod{m} \Rightarrow r_i = r_j \text{ 이므로}$$

T 는 법 m 에 관한 기약잉여계이다.

따라서 T 의 각 원소 ar_i 는 법 m 에 관하여 R 의 단 한 개의 원소와 합동이므로 다음이 성립한다.

$$ar_1 \cdot ar_2 \cdot \cdots \cdot ar_{\phi(m)} \equiv r_1 r_2 \cdots r_{\phi(m)} \pmod{m}$$

$$a^{\phi(m)} r_1 r_2 \cdots r_{\phi(m)} \equiv r_1 r_2 \cdots r_{\phi(m)} \pmod{m}$$

그런데, 각 $r_i \in R$ 에 대하여 $(r_i, m) = 1$ 이므로 위의 합동식으로부터 $a^{\phi(m)} \equiv 1 \pmod{m}$ 임을 알 수 있다.

[예제 9] 정수 9^{999} 의 일의 자리수를 구하자. **[8]**

오일러 정리에 의해 $9^{\phi(10)} \equiv 9^4 \equiv 1 \pmod{10}$ 이므로

$$9^{999} \equiv (9^4)^{249} \cdot 9^3 \equiv 1^{249} \cdot 9^3 \equiv 729 \equiv 9 \pmod{10}$$ 이다.

따라서 9^{999} 의 일의 자리 수는 9 이다.

Ⅲ. 합동방정식의 해법

제1장 일차 합동식 [10]

[정리 8] 임의의 정수 a, x, y 에 대하여 $\gcd(a, n) = 1$ 이고 $ax \equiv ay \pmod{n}$ 이면 $x \equiv y \pmod{n}$ 이다.

(증명) $ax \equiv ay \pmod{n}$이므로 $n \mid (ax - ay)$이다. 즉 $n \mid a(x-y)$이다.

그런데 $\gcd(a, n) = 1$ 이므로 a는 n의 인수를 갖지 않는다.

그러므로 $n \mid x - y$ 가 되고

따라서 $x \equiv y \pmod{n}$ 이다.

[정리 9] 정수a, x, y에 대하여 $\gcd(a, n) = d$ 이고 $ax \equiv ay \pmod{n}$ 이면

$x \equiv y \pmod{\frac{n}{d}}$ 이다.

(증명) $ax \equiv ay \pmod{n}$ 이라고 하면 적당한 정수 t 에 대하여

$ax - ay = nt$ 이므로 $(\frac{a}{d})(x-y) = (\frac{n}{d})t$,

따라서 $\frac{n}{d} \mid (\frac{a}{d})(x-y)$ 이다.

그런데 $\gcd(\frac{a}{d}, \frac{n}{d}) = 1$ 이므로 $\frac{n}{d} \mid (x-y)$ 이다.

그러므로 $x \equiv y \pmod{\frac{n}{d}}$ 이다.

[정리 10] 일차 합동식 $ax \equiv b \pmod{n}$, $gcd(a, n) = 1$ 은 단 하나의 해를 가진다. 특히, p 가 소수일 때 일차 합동식 $ax \equiv b \pmod{p}$, $a \not\equiv 0 \pmod{p}$ 는 단 한 개의 해를 가진다.

(증명) $\gcd(a, n) = 1$ 이므로 $as + nt = 1$ 인 정수 s, t 가 존재 한다.

이때 $a(sb) + n(tb) = b$ 이므로 $a(sb) \equiv b \pmod{n}$ 이고

$x \equiv sb \pmod{n}$는 주어진 합동식의 해가 된다.

$x \equiv x_1 \pmod{n}$, $x \equiv x_2 \pmod{n}$ 을 주어진 합동식의 해라고 가정하면

$ax_1 \equiv b \equiv ax_2 \pmod{n}$, $\gcd(a, n) = 1$ 이다.

그러므로 위의 [정리 8] 에 의하여 $x_1 \equiv x_2 \pmod{n}$ 이다.

따라서 주어진 합동식은 단 한 개의 해를 갖는다.

[예제 9] 일차 합동식 $7x \equiv 5 \pmod{31}$ 의 해를 구해보자. **[3]**

먼저 $(31, 7) = 1$ 이고 또,

$31 \cdot (-2) + 7 \cdot 9 = 1$,

$31 \cdot (-10) + 7 \cdot 45 = 5$ 이므로 다음이 성립한다.

$7 \cdot 45 \equiv 5 \pmod{31}$

$7 \cdot 14 \equiv 5 \pmod{31}$

따라서 일차 합동식 $7x \equiv 5 \pmod{31}$의 해는 $x \equiv 14 \pmod{31}$이다.

[정리 11] 일차 합동식 $ax \equiv b \pmod{n}$, $a \not\equiv 0 \pmod{n}$ 의 해가 존재하기 위한 필요충분조건은 $\gcd(a, n) \mid b$이다.

또, $d = \gcd(a, n)$, $d \mid b$ 일 때

$x \equiv x_0 \pmod{n}$을 이 합동식의 한 해라 하면 이 합동식은 꼭 d 개의 해

$x \equiv x_0 + (\frac{n}{d})t \pmod{n}$, $t = 0, 1, 2, \cdots, d-1$을 가진다.

(증명) 위의 합동식의 해 $x \equiv u \pmod{n}$ 가 존재 한다면 $au \equiv b \pmod{n}$ 이므로

$au + nv = b$ 인 정수 v 가 존재하고 따라서 $(a, n) \mid b$ 이다.

역으로 $d = \gcd(a, n)$, $d \mid b$ 라고하자 .

그러면 $ax \equiv b \pmod{b} \Leftrightarrow (\frac{a}{d})x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$

그런데 $\gcd(\frac{a}{d}, \frac{n}{d}) = 1$ 이므로 합동식$\Leftrightarrow (\frac{a}{d})x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$는

단 한 개의 해$x \equiv x_0 \pmod{\frac{n}{d}}$을 가진다.

[정리 10] 의 합동식을 만족시키는 x 는 $x \equiv x_0 + (\frac{n}{d})t \quad (t \in Z)$의 꼴이다.

한편, 이 식에서 t 에 $0, 1, 2, \cdots, d-1$을 대입한 값

$x_0, x_0 + \frac{n}{d}, \cdots, x_0 + \frac{n}{d}(d-1)$ 은 법 n 에 대하여 합동이 아니며 t 에 그 밖의 값은 위의 어느 하나와 법 n 에 관하여 합동이다.

따라서 주어진 합동식은 꼭 d 개의해

$x \equiv x_0 + (\frac{n}{d})t \pmod{n}$, $t = 0, 1, 2, \cdots, d-1$을 가진다.

[예제 10] 일차 합동식 $9x \equiv 6 \pmod{15}$ 의 해를 구해보자. **[3]**

먼저 $(15, 9) = 1$ 이므로 이 합동식은 해를 가지며 다음 합동식과 동치이다.

$3x \equiv 2 \pmod{5}$

한편 , $15 \cdot (-1) + 9 \cdot 2 = 3$ 이므로

$5 \cdot (-1) + 3 \cdot 2 = 1$

$5 \cdot (-2) + 3 \cdot 4 = 2$ 이므로

$3 \cdot 4 \equiv 2 \pmod{5}$ 이다.

따라서 일차 합동식 $3x \equiv 2 \pmod{5}$의 해는 $x \equiv 4 \pmod{5}$이다.

그러므로 일차 합동식 $9x \equiv 6 \pmod{15}$의 해는 $x \equiv 4 \pmod{5}$이고,

이 해는 법 15에 관하여 다음과 같이 3개의 해로 나타낼 수 있다.

$x \equiv 4 \pmod{15}$ $\quad x \equiv 9 \pmod{15}$ $\quad x \equiv 14 \pmod{15}$

[정리 12] $\gcd(a, n) = 1$ 이라면 일차 합동식 $ax \equiv b \pmod{n} \Leftrightarrow x \equiv a^* b \pmod{n}$ 인 해를 갖는다. (a^* : 법 n 에 대한 a 의 역수)

(증명) 만약 $ax \equiv b \pmod{n}$ 이면 $aa^{*}x \equiv a^{*}b \pmod{n}$

그러므로 $x \equiv a^{*}b \pmod{n}$

여기서 $aa^{*} \equiv 1 \pmod{n}$

만약 $x \equiv a^{*}b \pmod{n}$ 그러면 $ax \equiv aa^{*}b \equiv 1 \cdot b \equiv b \pmod{n}$

윌슨의 정리는 페르마의 정리와 더불어 정수론에 있어서 대단히 중요한 정리에 속하며 윌슨의 정리는 그 역도 성립하는데 다음과 같다.

[정리 13] p가 1보다 큰 정수일 때 $(p-1)! \equiv -1 \pmod{p}$ 이면 p는 소수이다.

(증명) p를 합성수라 가정하고 d를 $1 < d < p$ 인 p의 약수라 하자

이때 $d \mid (p-1)!$ 이므로 $d \nmid (p-1)!+1$

따라서 $p \nmid (p-1)!+1$ 이므로 $(p-1)! \not\equiv -1 \pmod{p}$

그러므로 $(p-1)! \equiv -1 \pmod{p}$이면 p는 소수이다. **[6]**

위 정리의 역도 성립한다.

제2장 연립 합동식 [10]

[정리 14] 중국인의나머지정리(Chinese Remainder Theorem)

양의 정수 $m_1, m_2, \cdots, m_n$ 가 쌍마다 서로 소 일 때 $c_1, c_2, \cdots, c_n$ 를 임의의 정수라고 하면 연립 일차 합동식

$$x \equiv c_1 \pmod{m_1}$$

$$x \equiv c_2 \pmod{m_2}$$

$$\vdots$$

$$x \equiv c_n \pmod{m_n}$$

은 법 $m_1 m_2 \cdots m_n$ 에 관하여 단 하나의 해를 가진다. **[5]**

(증명) $m = m_1 m_2 \cdots m_n$ 라 놓으면

각 $i\,(i = 1, \cdots, n)$에 대하여 $\dfrac{m}{m_i}$ 은 정수이다.

이제 $M_i = \dfrac{m}{m_i}$ 이라 놓으면 $\gcd(M_i, m_i) = 1$ 이고 $i \neq j$ 이면 $M_j \equiv 0 \pmod{m_i}$이고 각 $i\,(i = 1, \cdots, n)$에 대하여 $M_i N_i \equiv 1 \pmod{m_i}$ 인 정수 N_i 가 존재한다.

만약 $x_0 = c_1 M_1 N_1 + c_2 M_2 N_2 + \cdots + c_n M_n N_n$ 라고 하면

$x_0 = c_1 M_1 N_1 + c_2 M_2 N_2 + \cdots + c_n M_n N_n \equiv a_i M_i N_i \equiv a_i \pmod{m_i}$이므로

$x \equiv x_0 \pmod{m}$은 주어진 연립 합동식의 해이다.

또 $x \equiv x_0 \pmod{m}$, $x \equiv x_1 \pmod{m}$ 을 주어진 합동식의 해라고 하면,

$x_0 \equiv a_i \equiv x_1 \pmod{m_1}\,(i = 1, \cdots, n)$ 이므로 $x_0 \equiv x_1 \pmod{m}$ 이다.

따라서 주어진 연립 합동식은 단 한 개의 해를 갖는다.

[예제 11] 다음 연립 일차 합동식의 해를 구하여라.

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

$$M = 3 \cdot 5 \cdot 7 = 105$$

$$M_1 = \frac{M}{3} = 5 \cdot 7 = 35$$

$$M_2 = \frac{M}{5} = 3 \cdot 7 = 21$$

$$M_3 = \frac{M}{7} = 5 \cdot 3 = 15 \text{ 라 하면}$$

$35N_1 \equiv 1 \pmod 3$ $\quad 21N_2 \equiv 1 \pmod 5$ $\quad 15N_3 \equiv 1 \pmod 7$ 을 만족하는 정수 N_1, N_2, N_3 는 $N_1 = 2, N_2 = 1, N_3 = 1$ 이고,

$u = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233$ 이다.

따라서 구하는 해는 $x \equiv 233 \equiv 23 \pmod{105}$ 이다. **[8]**

[정리 15] $m = p_1^{e_1} \cdot p_2^{e_2} \cdot \cdots \cdot p_r^{e_r}$을 양의 정수 m의 표준분해라 할 때

(1) $x \equiv c(\bmod m)$이 합동식 $f(x) \equiv 0 \ (\bmod m)$ 의 해이면

각 i 에 대하여 $x \equiv c(\bmod p_i^{e_i})$ 은 합동식 $f(x) \equiv 0 \ (\bmod p_i^{e_i})$의 해이다.

(2) 각 i 에 대하여 $x \equiv c_i(\bmod p_i^{e_i})$ 가 합동식 $f(x) \equiv 0 \ (\bmod p_i^{e_i})$의 해이면,

연립합동식 $x \equiv c_1(\bmod p_1^{e_1})$

$\vdots$

$x \equiv c_r(\bmod p_r^{e_r})$

의 유일한 해 $x \equiv c(\bmod m)$ 는 합동식 $f(x) \equiv 0 \ (\bmod m)$의 해이다,

위의 정리에 의하며, 각 $i = 1, 2, \cdots, r$ 에 대하여 합동식 $f(x) \equiv 0 \ (\bmod m)$ 가 꼭 S_i개의 해를 갖는다면

합동식 $f(x) \equiv 0 \ (\bmod m)$ 은 꼭 $S_1, \cdots, S_r$개의 해를 갖게 된다.

특히, $S_1, \cdots, S_r$ 중 적어도 하나가 0 이면 주어진 합동식 $f(x) \equiv 0 \ (\bmod m)$의 해는 존재하지 않는다.

[정리 14]에 의하면 합동식을 푸는 문제는 $f(x) \equiv 0 \ (\bmod p^k)$ (p 는 소수, $k > 0$) 와 같은 꼴의 합동식을 푸는 문제로 귀착된다.

그런데 $f(a) \equiv 0 \ (\bmod p^k)$ 이면 반드시 $f(a) \equiv 0 \ (\bmod p)$ 이어야 하므로

합동식 $f(x) \equiv 0 \ (\bmod p^k)$ 를 만족하는 정수는 모두 합동식 $f(x) \equiv 0 (\bmod p)$를 만족하는 정수 중에서 구할 수 있다.

[정의 6] $f(x) = a_n x^n + \cdots + a_1 x + a_0$ 라 할 때

$f'(x) = n a_n x^{n-1} + \cdots + a_1$ 을 $f(x)$의 **형식적 미분(formal derivative)** 이라 한다.

이제 합동식 $f(x) \equiv 0 \ (\bmod p^{a+1})$ 을 풀어 보자.

x가 합동식 $f(x) \equiv 0 \ (\bmod p^{a+1})$ 의 해이면 x 는 또한 합동식 $f(x) \equiv 0 \ (\bmod p)$

의 해이다.

그러므로 b 가 $b_1, \cdots, b_r$ 중의 하나일 때, $f(x) \equiv 0 \pmod{p^a}$ 라고 하면 임의의 k 에 대하여 $x = b + kp^a$ 로 쓸 수 있고 Taylor 전개식에 의해

$$f(x) = f(b+kp^a) = f(b) + (\frac{f'(b)}{1}(kp^a) + (\frac{f''(b)}{1 \cdot 2})(kp^a)^2 + \cdots + (\frac{f^m(b)}{m!})(kp^a)^m$$

이며 $\frac{f'(b)}{1}, \frac{f''(b)}{1 \cdot 2}, \cdots, \frac{f^m(b)}{m!}$는 모두 정수이다.

또한 $a \geq 1$ 이기 때문에 $a+1 \leq 2a$ 이 되어서 $p^{2a}, p^{3a}, \cdots, p^{ma} \equiv 0 \pmod{p^{a+1}}$ 이므로 $f(x) = f(b) + (\frac{f'(b)}{1})kp^a \pmod{p^{a+1}}$이 된다.

$f(b) \equiv 0 \pmod{p^a}$ 이므로 임의의 t 에 대해 $f(b) = tp^a$ 라 할 수 있고

$f(x) \equiv p^a(t + f'(b)k) \equiv 0 \pmod{p^{a+1}}$이 된다.

$x = b + kp^a$ 에 대해 $f(x) \equiv 0 \pmod{p^{a+1}}$이면 또 그때에 한해

$p^a(t + f'(b)k) \equiv 0 \pmod{p^{a+1}}$이 되며 $t + f'(b)k \equiv 0 \pmod{p}$가 된다.

k 가 합동식 $f(x) \equiv 0 \pmod{p^{a+1}}$의 해 $x = b + kp^a$ 를 만족시키기 위한 조건은

$f'(b)k \equiv -\frac{f(b)}{p^a} \pmod{p}$ 이므로 $f(x) \equiv 0 \pmod{p^{a+1}}$의 해를 결정하기 위해서는 합동식 $f(x) \equiv 0 \pmod{p}$의 해를 알아야 하며 이는 법이 소수인 것에 대한 일차 합동식을 풀어야만 된다.

Case 1 $f'(b) \equiv 0 \pmod{p}$일 때는 합동식은 $\frac{f(b)}{p^a} \equiv 0 \pmod{p}$

즉 $f(b) \equiv 0 \pmod{p^{a+1}}$이어서 두 가지의 경우가 있을 수 있다. 하나는 $x = b + kp^a$ 가 합동식 $f(x) \equiv 0 \pmod{p^{a+1}}$의 해가 될 때 $f(b) \equiv 0 \pmod{p^{a+1}}$이고 다른 또 하나는 $x = b + kp^a$ 가 합동식 $f(x) \equiv 0 \pmod{p^{a+1}}$의 해가 되지 않을 때의 $f(b) \equiv 0 \pmod{p^{a+1}}$ 이다.

Case 2 $f'(b) \equiv 0 \pmod{p}$일 때는 합동식 $f'(b)k \equiv -\dfrac{f(b)}{p^a} \pmod{p}$가 하나의 해

즉 $k = -f'(b)^* \dfrac{f(b)}{p^a} \pmod{p}$인 ($f'(b)^*$는 $f'(b)$의 mod p에 대한 역수이다.)

하나의 해를 갖는다.

그러므로 이러한 경우에 합동식 $f(x) \equiv 0 \pmod{p^{a+1}}$은

$x \equiv b - f'(b)^* \dfrac{f(b)}{p^a} p^a \pmod{p^{a+1}}$ 형태의 해를 갖는다.

제3장 고차 합동식 [10]

이 장에서는 2차 이상의 고차 합동식의 해법과 고차 합동식의 해법에 관련된 문제에 대하여 연구하기로 한다. 고차 합동식의 간단한 일반적 해법은 없으나 주어진 합동식을 법이 소수인 경우로 귀착시켜 문제를 간단히 해결할 수 있다.

앞장에서 전술한 바와 같이 고차 합동식$f(x) \equiv 0 \pmod{m}$에서

$m = p_1^{e_1} \cdot p_2^{e_2} \cdot \cdots \cdot p_r^{e_r}$을 m의 표준분해라 할 때 위의 합동식은 다음 연립합동식과 동치이다.

$$f(x) \equiv 0 \pmod{p_1^{e_1}}$$

$$\vdots$$

$$f(x) \equiv 0 \pmod{p_r^{e_r}}$$

이때 $x \equiv c \pmod{m}$가 $f(x) \equiv 0 \pmod{m}$ 의 해이면

각 $i = 1, 2, \cdots, r$ 에 대하여 $x \equiv c \pmod{p_i^{e_i}}$ 은 $f(x) \equiv 0 \pmod{p_i^{e_i}}$의 해이다.

결국 합동식을 푸는 문제는 $f(x) \equiv 0 \pmod{p^k}$와 같은 꼴의 합동식을 푸는 문제로 귀착된다.

[정의 7] 정수 계수를 갖는 두 다항식 $f(x)=a_0+a_1x+\cdots$와 $g(x)=b_0+b_1x+\cdots$가 있다. 모든 i 에 대하여 개수가 $a_i \equiv b_i \pmod{n}$일 경우에 "$f(x)$가 법 n 에 대하여 $g(x)$와 합동이다" 라고 하고 $f(x) \equiv xg(x) \pmod{n}$ 이라 표시한다.

[정리 16] 다항식 $f(x)=a_mx^m+\cdots+a_1x+a_0$ 의 모든 계수가 정수라 할 때
모든 a_i 는 법n에 대해 0 은 아니라고 하면
그때의 $a_i \not\equiv 0 \pmod{n}$을 만족하는 가장 큰 정수 i 를 법 n 에 관한 f의 차수라 하고 이를 $\deg_n f(x)$ 로 표기한다.

[정리 17] 다항식$f(x)=a_mx^m+\cdots+a_1x+a_0$ 이 정수 계수를 갖고 a를 정수라 하면$f(x)=(x-a)g(x)+f(a)$를 만족하는 정수계수를 갖는 다항식$g(x)$가 존재한다. **[2]**
(증명) $f(x)$가 상수 다항식 즉 $f(x)=a_0$이면 $g(x)=0$ 이다.
차수가 $m-1$ 이하의 모든 다항식에 대해 이 정리가 성립한다고 가정하고
$f_1(x)=f(x)-a_mx^{m-1}(x-a)=(a_{m-1}+a \cdot a_m)x^{m-1}+a_{m-2}x^{m-2}+\cdots+a_0$라 놓으면
$f_1(x)$의 차수는 $m-1$ 이하이므로 다항식 $g_1(x)$가 존재해서
$f_1(x)=(x-a)g_1(x)+f_1(a)$ 를 만족한다.
그러므로 $f(x)=f_1(x)+a_mx^{m-1}(x-a)=(x-a)(g_1(x)+a_mx^{m-1})+f_1(a)$이 되고
$g(x)=g_1(x)+a_mx^{m-1}$이라 하면 $g(x)$는 정수 계수를 갖게 되고
$f(x)=(x-a)g(x)+f_1(a)$가 된다.
위 식에서 $x=a$로 놓으면 $f(a)=f_1(a)$이므로 $f(x)=(x-a)g(x)+f(a)$가 성립된다.

[정리 18] 다항식 $f(x)$가 정수 계수를 가지며 $b_1, b_2, \cdots, b_t$ 가 합동식 $f(x) \equiv 0 \pmod{p}$ 의 비합동인 해라고 하면 $f(x) \equiv x(x-b_1)(x-b_2)\cdots(x-b_t)q(x) \pmod{p}$ 를 만족하는 정수 계수를 갖는 다항식 $q(x)$가 존재한다.
또한 $\deg_p q(x) \le \deg_p f(x)-t$ 이다. **[2]**

(증명) $f(x)=a_m x^m+\cdots+a_1 x+a_0$, $a_m \not\equiv 0$ (mod p), 즉 $\deg_p f(x)=m$ 이라 하면

$f(x)\equiv x(x-b_1)q_1(x)\ (\bmod p)$ ----- (*) 를 만족하여

$\deg_p q(x)\le m-1=\deg_p f(x)-1$ 인 다항식 $q_1(x)$ 가 존재한다.

(*)에 $x=b_2$ 를 대입하면

$f(b_2)\equiv(b_2-b_1)q_1(b_2)\ (\bmod p)$ 이고 $f(x)\equiv 0\ (\bmod p)$ 이므로

$p\,|\,(b_2-b_1)q_1(b_2)$, 즉 $p\,|\,(b_2-b_1)$ 또는 $p\,|\,q_1(b_2)$ 가 된다.

가정에 의해 $b_2\not\equiv b_1\ (\bmod p)$ 이므로 $p\,|\,q_1(b_2)$ 즉 $q_1(b_2)\equiv 0\ (\bmod p)$ 이다.

b_2 는 $q_1(x)$ 의 해이므로 $q_1(x)\equiv x(x-b_2)q_2(x)\ (\bmod p)$를 만족하며

$\deg_p q_2(x)\le \deg_p q_1(x)-1$ 인 다항식 $q_2(x)$가 존재하므로

$f(x)\equiv x(x-b_1)(x-b_2)(x-b_3)q_3(x)\ (\bmod p)$ ----- (**)를 만족하며

$\deg_p q_2(x)\le \deg_p q_1(x)-1\le \deg_p f(x)-1-1=\deg_p f(x)-2$ 가 된다.

(**)에 $x=b_3$을 대입하면 위와 같은 방법으로

$f(x)\equiv x(x-b_1)(x-b_2)(x-b_3)q_3(x)\ (\bmod p)$, $\deg_p q_2(x)\le \deg_p q_1(x)-3$을 구할 수 있다. 위와 같은 과정을 반복하면 [정리17] 이 성립한다.

[정리 19] (Lagrange) p가 소수일 때 n차 합동식

$f(x)=a_n x^n+\cdots+a_1 x+a_0$, $a_n \not\equiv 0$ (mod p)는 많아야 n 개의 해를 가진다.

(증명) 법 p 에 관한 합동식의 차수 n 에 대해 귀납법을 이용하면

$n=1$ 일 때 합동식은 $a_1 x+a_0\equiv 0\ (\bmod p)$, $\gcd(a_1,p)=1$이므로 꼭 한 개의 해를 가진다. $(n-1)$ 차의 합동식에 대해 이 정리가 성립한다고 가정하자.

이때 $x\equiv a\ (\bmod p)$가 합동식 $f(x)\equiv 0\ (\bmod p)$의 해이면 $f(a)\equiv 0\ (\bmod p)$

또한 정수를 계수로 가지는 $(n-1)$차의 다항식 $q(x)$ 가 존재하여

$f(x)\equiv(x-a)q(x)+f(a)\ (\bmod p)$ -- (*) 로 나타내어진다.

그런데 $f(a)\equiv 0\ (\bmod p)$ 이므로 (*)는 $f(x)\equiv(x-a)q(x)\ (\bmod p)$가 된다.

따라서 $b\equiv a$ (mod p)인 정수b에 대하여 $f(b)\equiv 0\ (\bmod p)$가 성립한다면

$q(b)(b-a) \equiv f(b) \equiv 0 \pmod{p}$, $q(b) \equiv 0 \pmod{p}$

즉 $f(x) \equiv 0 \pmod{p}$의 두 해 $x \equiv a \pmod{p}$와 $x \equiv b \pmod{p}$가 서로 다르면

$x \equiv b \pmod{p}$는 합동식 $q(x) \equiv 0 \pmod{p}$의 해이다.

또 (*) 에 의하여 다항식 $q(x)$의 최고차항은 a_n 이고

$a_n \not\equiv 0$ (mod p) 이므로 합동식 $q(x) \equiv 0 \pmod{p}$는 $(n-1)$차의 합동식이다.

그런데 귀납적 가정에 의하여 $(n-1)$ 차의 합동식 $q(x) \equiv 0 \pmod{p}$는 많아야 $(n-1)$ 개의 해를 가진다.

그러므로 합동식 $f(x) \equiv 0 \pmod{p}$는 많아야 n 개의 해를 가진다.

[정리 20] p가 소수일 때 $k \mid p-1$이라 하면 합동식 $x^k \equiv 0 \pmod{p}$는 꼭 k 개의 해를 갖는다.

(증명) $p-1 = kt$ 라 하고 항등식 $x^{p-1} - 1 = (x^k - 1)(x^{k(t-1)} + x^{k(t-2)} + \cdots + 1)$을 이용하자. x 를 정수 $1, 2, \cdots, p-1$ 중의 하나라 하면 $x^{p-1} - 1 \equiv 0 \pmod{p}$

즉 $(x^k - 1)(x^{k(t-1)} + x^{k(t-2)} + \cdots + 1) \equiv 0 \pmod{p}$ 이므로

$p \mid (x^k - 1)(x^{k(t-1)} + x^{k(t-2)} + \cdots + 1)$ 즉 $p \mid x^k - 1$ 또는 $p \mid (x^{k(t-1)} + x^{k(t-2)} + \cdots + 1)$ 이 된다. 다시 말하자면 $1, 2, \cdots, p-1$ 중의 모든 x 는 합동식

$x^{k-1} - 1 \equiv 0 \pmod{p}$ --- (*)

또는 $x^{k(t-1)} + x^{k(t-2)} + \cdots + 1 \equiv 0 \pmod{p}$ --- (**)의 해이다.

$x = 0$ 은 합동식 (*)와 (**)의 해가 아니므로 (*)와 (**)의 해는 모두 $p-1$ 개가 된다. 한편, 합동식 (*)는 많아야 k 개의 해를 가지며 합동식 (**)은 많아야 $k^{(t-1)}$ 개의 해를 가진다.

그러므로 두 합동식의 각자의 해의 수를 합한 수는 많아야 $k + k(t-1) = kt = p-1$ 이다. 따라서 합동식 (*)와 (**)의 해의 수를 합한 것이 $p-1$ 이면 합동식 $x^k - 1 \equiv 0 \pmod{p}$는 꼭 k 개의 해를 가진다.

Ⅳ. 합동식의 응용

오늘날 합동의 개념이 응용되는 부분으로서 가장 두각을 보이는 면은 당연히 암호 이론과 부호이론일 것이다. 실제로 암호이론 중 가장 중심 되는 공개키 RSA 암호 이론에서 정소의 소인수 분해와 합동이론은 가장 필수적인 배경이론이 된다. 또한 부호이론에서 Hamming code를 만들고 에러 검출을 하는데도 합동에 관한 개념 없이는 설명할 수 없다.

이번 장에서는 합동의 개념을 응용한 여러 사례를 통해 수학의 이론이 직접적으로 활용되는 면을 살펴보고자 한다. 합동에 관한 개념은 우리가 일상적으로 경험하는 생활에서 많이 볼 수 있다.

다양한 응용 중에서, 본 논문에서 다루어보는 것은, 기본적인 나눗셈판정법과 residue design, modular계산, round-robin tournament 등이다. 기본적인 나눗셈판정법은 중・고등학교 과정에서도 찾아볼 수 있다.

제1장 나눗셈판정법 [9]

합동이론은 주어진 하나의 정수가 다른 정수에 의해 나누어지는지를 확인하는 간단한 방법을 제시할 수 있다. 중 ・고등학교 교과과정에서 다루어지는 특정한 배수 판정법은 다음과 같다.

2의 배수: 일의 자리의 수가 0 또는 2의 배수인수

3의 배수: 각 자리의 숫자의 합이 3의 배수인 수

4의 배수: 끝의 두 자리 수가 00 또는 4의 배수인 수

5의 배수: 일의 자리의 수가 0 또는 5인 수

9의 배수: 각 자리의 숫자의 합이 9의 배수인 수

11의 배수: 그 수의 홀수자리 숫자 합과 짝수자리 숫자 합이 0이거나 11의 배수

위의 내용을 접하게 되는 많은 학생들은, 이러한 결과를 단순히 암기하려고 한다. 우리는 간단한 증명을 통해. 학생들에게 설명하여 이해시키는 것이 바람직하다고 보인다.

(1) 간단한 배수 판정법

10진법으로 표현된 임의의 자연수 N 은 다음과 같은 전개식으로 나타내진다.

$$N = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0 \ (0 \le a_i \le 9)$$

가령, 자연수 22,222는 $22222 = 2 \cdot 10^4 + 2 \cdot 10^3 + 2 \cdot 10^2 + 2 \cdot 10 + 2$로 전개된다. 주어진 자연수 N 이 어떤 특별한 수로 나누어지는지를 합동식을 사용하여 판정 하는 쉬운 방법을 알아보자.

[정리 21] (2, 5의 배수 판정법) 주어진 자연수 N 을 다음과 같이 표현하자.

$$N = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0 \ (0 \le a_i \le 9)$$

그러면 각 j ($1 \le j \le k$) 에 대해 다음이 성립한다.

$$N = a_{j-1} a_{j-2} \cdots a_1 a_0 \pmod{2^j}$$

$$N = a_{j-1} a_{j-2} \cdots a_1 a_0 \pmod{5^j}$$

(증명) $10 \equiv 0 \pmod 2$이므로, 모든 j 에 대하여 항상, $10^j \equiv 0 \pmod{2^j}$이다.

따라서 N의 전개식을 modulo 2^j 로 계산하면,

$$N = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0$$

$$= a_{j-1} 10^{j-1} + a_{j-2} 10^{j-2} + \cdots + a_1 10 + a_0 \pmod{2^j} \text{ 이므로}$$

$$N = a_{j-1} a_{j-2} \cdots a_1 a_0 \pmod{2^j} \text{ 이다.}$$

마찬가지로 $10 \equiv 0 \pmod 5$이므로 $10^j \equiv 0 \pmod{5^j}$가 되어서,

$$N = a_{j-1} a_{j-2} \cdots a_1 a_0 \pmod{5^j} \text{이 된다.}$$

위 정리에 따르면 N 의 끝자리 수 a_0 가 2 로 나누어지면, N 은 2 로 나누어지

고 N의 끝 두 자리 수 a_1a_0가 2^2 으로 나누어지면 N은 2^2으로 나누어진다. 뿐만 아니라, N의 끝 세 자리 수 $a_2a_1a_0$가 2^3 으로 나누어지면 N은 2^3으로 나누어진다. 그러므로, 자연수 N이 2^j(임의의 j) 로 나누어지는지의 판정은 다음과 같다.

N의 끝자리 수 $a_{j-1}a_{j-2}\cdots a_1a_0$ 가 2^j로 나누어지면 N은 2^j로 나누어진다.

[예제 12] $N=343506076$일 때, N 값이 2의 배수, 2^2의 배수 또는 2^3의 배수가 되는지 알아보자.

끝자리 수 6이 2의 배수이므로 $2\mid 6 \rightarrow 2\mid N$. 따라서, N은 2의 배수이다.

끝 두 자리 수 76이 2^2의 배수이므로 $2^2\mid 76 \rightarrow 2^2\mid N$. 따라서, N은 2^2의 배수이다.

한편, 끝 세 자리 수 076은 2^3의 배수가 아니므로 $2^3 \nmid 076 \rightarrow 2^3 \nmid N$

그러므로, N은 2^3의 배수가 아니다.

[정리 22] $N=a_k10^k+a_{k-1}10^{k-1}+\cdots+a_110+a_0$ 이면 다음이 성립한다.

(1) $N\equiv(-1)^ka_k+(-1)^{k-1}a_{k-1}+\cdots+a_0 \pmod{11}$

(2) $N\equiv a_k+a_{k-1}+\cdots+a_0 \pmod 9$

(3) $N\equiv a_k+a_{k-1}+\cdots+a_0 \pmod 3$ **[1]**

(증명)(1) $10=11-1$을 $N=a_k10^k+a_{k-1}10^{k-1}+\cdots+a_110+a_0$ 에 대입하면

$$N=a_k(11-1)^k+a_{k-1}(11-1)^{k-1}+\cdots+a_0$$

$$N\equiv(-1)^ka_k+(-1)^{k-1}a_{k-1}+\cdots+a_0 \pmod{11}$$ 이다.

(2) $10=9+1$을 $N=a_k10^k+a_{k-1}10^{k-1}+\cdots+a_110+a_0$ 에 대입하면

$$N=a_k(9+1)^k+a_{k-1}(9+1)^{k-1}+\cdots+a_0$$

$$N\equiv a_k+a_{k-1}+\cdots+a_0 \pmod 9$$ 이다.

(3) $10\equiv 1 \pmod 3$이므로 $N\equiv a_k+a_{k-1}+\cdots+a_0 \pmod 3$ 이다.

[예제 13] $N=534206706$일 때, N 이 3의 배수, 9의 배수, 11의 배수가 되는지 알아보자.

정리 내용에서와 같이, 새로운 값 T 를 다음과 같이 계산한다.

$$T=5+3+4+2+0+6+7+0+6=33$$

그러면, 각 자리수의 합이 33으로 3의 배수이므로, $3 \mid T \Leftrightarrow 3 \mid N$.

따라서, N 은 3의 배수이다. 그러나, 33이 9의 배수는 아니므로, $9 \nmid T \rightarrow 9 \nmid N$.

그러므로, N 은 9의 배수는 아니다.

또한 새로운 값 $S=6-0+7-6+0-2+4-3+5=11$

그러면 $11 \mid S \Leftrightarrow 11 \mid N$ 이므로 N 이 11의 배수임을 확인할 수 있다. [1]

(2) Palindromes 판정법

(설명 : Palindromes 라는 것은 역순으로 읽어도 같은 말이 되는 단어를 의미한다. 예를 들어, eye, madam, 오디오 또는 1551 등이 있다.)

가령 1551이나 70855807와 같은 palindromes 수는, 위에서 본 11의 배수 판정법을 사용하여 11에 의해 나눠짐을 볼 수 있다.

[예제 14] 70855807이 11의 배수임을 보이자.

$N=70855807$ 이라 하자. 그러면, $P(x)=7x^7+8x^5+5x^4+5x^3+8x^2+7$ 이고, $P(10) \equiv P(-1) \pmod{11}$이 된다. 그런데, $P(10) \equiv N \pmod{11}$이고,

$$P(-1)=-7-8+5-5+8+7=0 \text{ 이므로, } N \equiv 0 \pmod{11}\text{이다.}$$

따라서, N 은 11에 의해 나누어진다,

이제, 위의 예제를 통하여 다음의 정리를 만들 수 있다.

[정리 23] 짝수개의 숫자로 구성된 palindromes 수는 11에 의해 나누어진다.

(증명) 가령 $N=abba$ 처럼 4개의 숫자로 구성된 정수를 생각해보자.

그러면, $P(x)=ax^3+bx^2+bx+a$ 이고, $P(10)=N$이고, $10 \equiv -1 \pmod{11}$이 된다.

그런데 $P(10) \equiv P(-1) \pmod{11}$

$\llcorner\!\rightarrow -a+b-b+a=0$

이므로, $P(10) \equiv 0 \pmod{11}$이다. 따라서, N은 11에 의해 나누어진다.

위의 정리에서 palindromes 수가 짝수개의 숫자로 구성되어야 한다는 가정은 반드시 필요하다. 즉, 홀수개의 숫자로 이루어진 palindromes에 대해서는 정리의 결과가 적용될 수 없음을 쉽게 확인할 수 있다.
가령, palindromes 수 151은 홀수개의 숫자로 이루어져 있는데, 이것은 11에 의해 나누어 지지 않는다.

[예제 15] 2473742이 11에 의해 나누어지는 알아보자.
$N=2473742$ 이라 하자. 그러면, $P(x)=2x^6+4x^5+7x^4+3x^3+7x^2+4x+2$이다.

그런데 $P(10) \equiv P(-1) \pmod{11}$

$\llcorner\!\rightarrow N$ $\llcorner\!\rightarrow 2-4+7-3+7-4+2=7$ 이므로, $N \equiv 7 \pmod{11}$이다.
따라서, N 은 11에 의해 나누어 지지 않는다.

(3) Casting out nines방법

이제는 일반적으로 Casting out nines (다른 말로하면, canceling number that add to 9)이라고 불리어지는 하나의 기술을 소개한다. 이 기술은 계산상의 에러를 발견하는데 이용된다.
Casting out nines이란 모든 정수는 각 자리수의 합과 $\pmod 9$에 의해 $\pmod 9$로서 합동이라는 사실에 기초하고 있다. 우선 다음의 간단한 예제부터 보자.

[예제 16] Casting out nines방법을 사용하여 $1976 \times 3458 = 6833008$ 인지를 확인하시오.

주어진 정수들의 각 자리를 합하여 $(\bmod 9)$로 계산하면 다음과 같다.

$$1976 \Rightarrow 1+9+7+6=23 \equiv 5 \ (\bmod 9)$$

$$3458 \Rightarrow 3+4+5+8=20 \equiv 2 \ (\bmod 9)$$

따라서, 위의 두 수를 곱하면

$$5 \times 2 = 10 \equiv 1 \ (\bmod 9)$$

한편, $6833008 \Rightarrow 6+8+3+3+0+0+8=28 \equiv 1 \ (\bmod 9)$ 이므로,$1 \equiv 1 \ (\bmod 9)$이다. 실제로, 간단한 계산으로 확인하면, $1976 \times 3458 = 6833008$임을 알 수 있다.

위의 예제에서 보듯이, Casting out nines방법을 사용하여 우리가 할 수 있는 대답은, 어떤 계산이 완전히 틀린 것이거나 혹은 비교적 옳은 것이라는 것을 판정할 수 있다는 것이다.

(4) Digital Root 방법

Casting out nines 와 상당히 밀접한 관계인 개념으로서 digital root 라는 개념이 있다. 일반적으로 반복적인 계산을 필요로 하는 것으로서, 다음과 같은 과정을 취한다.

- 단계 1: 주어진 양의 정수 N 이 있다.
- 단계 2: N 의 각 자리수의 합 S 를 구한다.
- 단계 3: S 의 각 자리수의 합 S_1 을 구한다
- 단계 4: S_1 의 각 자리수의 합 S_2 를 구한다.

이런 방법을 계속하여 한 자리수의 값 d 가 나올 때 까지 반복한다. 이때, d 를 digital root 라고 한다.

[예제 17] 7619 의 digital root를 구해보자. 또한 $(\bmod 9)$에 의한 7619의 값을 구해보자. 위에서 제시한 각 단계를 통해, 다음의 값들을 계산한다.

$N = 7619$

$S = 7 + 6 + 1 + 9 = 23$

$S_1 = 2 + 3 = 5$

S_1이 한자리 수의 값이므로, 여기서 계산을 끝내면, digital root는 5이다.

이번에는 (mod 9)에 의한 7619의 값을 구해보자. Casting out nines의 방법에 의해, (mod 9)에 의한 7619의 값은, 각 자리 수의 합을 (mod 9)로 계산한 것과 일치하므로,

$7619 \Rightarrow 7 + 6 + 1 + 9 = 23 \equiv 5 \pmod 9$ 이 된다.

위의 예제로부터 다음의 사실을 볼 수 있다.

[정리 24] 주어진 정수 N 에서 $N \neq 9$ 라고 하자. 그러면 N 의 digital root는 N 을 9로 나눈 나머지와 같다.

(증명) $N = abcde$라 하자. 그러면, $P(x) = ax^4 + bx^3 + cx^2 + dx + e$ 이다.

그런데, $a + b + c + d + e$는 9 의 배수가 아니다.

그러므로 $a + b + c + d + e$를 (mod 9)로 하면 나머지가 digital root가 된다.

Digital root의 개념이 아주 특별해 보이기는 하나, digital root는 완전 제곱수와 쌍둥이소수를 판정하는데 효율적으로 이용된다. 그러므로, 암호론등에서 필요한 소수 판정과 완전제곱수 판정에 손쉽게 활용될 수 있다.

[정리 25] 완전 제곱수의 digital root는 1 , 4 , 7 , 9 이다

위는 주어진 정수가 완전제곱수인지를 알 수 있는 판정법의 역할을 할 수 있다.

[예제 18] 정수 $N = 16{,}569{,}187{,}453$ 가 완전제곱수인지 아닌지를 판정하시오.

우선 digital root 를 찾기 위해서 다음을 계산한다.

$S = 1+6+5+6+9+1+8+7+4+5+3 = 55$

$S_1 = 5+5 = 10$

$S_2 = 1+0 = 1$

따라서, digital root는 1이므로, N 은 완전제곱수이다.

그러나 위 정리의 역은 일반적으로 옳지 않음도 알 수 있다. 예를 들어 34의 digital root는 7이지만, 34은 완전제곱수가 아니다.

이제 digital root가 쌍둥이 소수 판정에 어떻게 이용되는지 알아보자. 여기서 말하는 쌍둥이 소수란, 가령 3과 5 처럼, 5와 7 처럼, 인접한 두 홀수가 소수인 것을 말한다.

[정리 26] 쌍둥이소수 중 작은 수는 $6n-1$, 큰 수는 $6n+1$(n은 자연수)의 꼴이다 (단, 3 과 5는 제외)

(증명) 기본적으로 필요한 정리는 다음과 같다.

2를 제외한 모든 소수는 2의 배수가 아니다. ……①

3을 제외한 모든 소수는 3의 배수가 아니다. ……②

두 개의 쌍둥이 소수를 각각 $a-1, a+1$이라 한다. (a 는 4 보다 큰 자연수)

이제, 연속한 세 자연수 $a-1, a, a+1$에 대해 생각해보자.

$a-1, a+1$은 3 보다 큰 소수이므로 ①에 의해 2 의 배수가 아니다 (즉, 홀수이다.)

그러면 연속한 세 자연수 $a-1, a, a+1$ 중 $a-1, a+1$의 두 수가 홀수이므로 a 는 짝수이다. ……③

또, $a-1, a+1$ 은 3 보다 큰 소수이므로 ②에 의해 3 의 배수가 아니다. 연속한 세 자연수 $a-1, a, a+1$ 중에서 한 개의 3 의 배수가 존재하고, $a-1, a+1$이 3 의 배수가 아니므로 a 는 3 의 배수이다. ……④

그러면 ③,④에 의해 a 는 2 와 3 의 공배수, 즉 6 의 배수이다. 따라서, $a = 6n$

(n 은 자연수) 꼴의 수이며

$$a-1=6n-1$$

$$a+1=6n+1 \quad \text{꼴의 수이다. (} a>4 \text{ 일 때)}$$

그리고 위에 $a>4$ 일 때라고 쓴 것은 $a=4$ 일 때 유일한 예외인 3 , 5 의 쌍둥이 소수가 발견되기 때문이다.

[정리 27] 3과 5를 제외한 두 쌍둥이 소수의 곱에 관한 digital root는 8 이다.

(증명)[정리 26]에 의해, 두 쌍둥이 소수의 꼴은 $6n-1$, $6n+1$ 이다.

이제, 두 수를 곱하면

$$(6n-1)(6n+1)=35n^2-1 \pmod 9$$

$$\equiv -1 \pmod 9$$

$$\equiv 8 \pmod 9$$ 이 되어 digital root가 8임을 알 수 있다.

[예제 19] 두 쌍둥이 소수 269 와 271 의 곱의 digital root를 구하시오.

Digital root를 구하는 단계를 차례로 적용하여, 다음의 계산을 한다.

$$N=269 \Rightarrow S=2+6+9=17 \Rightarrow S_1=1+7=8$$

$$N=271 \Rightarrow S'=2+7+1=10 \Rightarrow S_1'=1+0=1$$

따라서, digital root 는 8 이다.

제2장 Check Digits [8]

다음에서 알아보려는 합동식의 응용은 Check digits이다. 실제로 합동식은 숫자열의 오류를 검색하는데 사용된다. 예를 들어 비트열에 대한 오류 검색 방법이나 여권번호, 운전면허번호, 주민등록증, 바코드, ISBN등을 확인하는데 사용된 숫자 열에 대한 오류 검사 방법이 있다.

0 이나 1 로만 이루어진 숫자 열 $x_1x_2x_3\cdots x_n$ 을 비트열 (bit strings)라 한다. $x_1+x_2+x_3+\cdots+x_n+x_{n+1}\equiv 0\ (\mathrm{mod}\ 2)$가 되도록 parity check bit라고 하는 x_{n+1}을 비트열의 마지막에 붙인다.

$$x_1x_2x_3\cdots x_n \text{ 중에 } \begin{cases} 1\text{의 개수가 짝수개이면} & x_{n+1}=0 \\ 1\text{의 개수가 홀수개이면} & x_{n+1}=1 \end{cases}$$

이렇게 하면 홀수개의 오류를 검색할 수 있다.

[예제 20] $11010111011\equiv 0\ (\mathrm{mod}\ 2)$ 이므로 수신된 데이터는 송신자에 의해 전송된 원래의 데이터와 일치하거나 짝수개의 오류를 가지고 있다. 한편, $11010110011\equiv 1\ (\mathrm{mod}\ 2)$ 이므로 수신된 데이터는 전송과정 중에서 원래의 전송 데이터 상에 오류가 발생되었다는 사실을 알 수 있다.

(1) 여권번호

여권이란 간단히 말해 한국인의 신분증이다. 즉 해외여행을 위해 국외로 떠나는 사람에게 정부가 여행을 허가해주는 증명서인 동시에 여행 중 한국인임을 증명할 수 있는 신분증명서이다. 어떤 사람이 해외여행을 가기위해 여권을 발급받았을 경우 체크 숫자로 오류를 확인 할 경우, 그 사람은 해외로 나갈 수 없게 된다.
어떻게 하여 여권번호에 오류가 생기는 것을 알게 되었는지 알아본다.

이제 여권번호를 확인하는 방법으로 유럽 몇 국가에서 사용하는 방법을 예로 들어보자. 만약 여권번호의 처음 여섯 자리 숫자열이 $x_1x_2x_3x_4x_5x_6$일 때 check digit x_7 을 다음과 같이 정한다.

$$x_7=7x_1+3x_2+x_3+7x_4+3x_5+x_6\ (\mathrm{mod}\ 10)\quad (0\le x_7\le 9)$$ **[8]**

[예제 21] 여권번호가 2119523 이라면,
$7\cdot 2+3\cdot 1+1\cdot 1+7\cdot 9+3\cdot 5+1\cdot 2=98\equiv 3\ (\mathrm{mod}\ 10)$ 이다.

따라서, 이 여권번호는 정확한 것이 아니다.

(2) ISBN (국제표준서적번호) [8]

요즘 출판되는 모든 서적들은 ISBN(International Standard Book Number)가 정해져 있다. IBSN은 책에 대한 국제적인 주민등록제도라고 할 수 있다. 책과 각종 음반물 각각에 고유번호 ISBN을 부여함으로서, 언어나 문자의 서로 다름에 관계없이 지정하는 자료를 명백하게 식별할 수 있다.
모든 것이 바코드로 입력되는 요즘에 ISBN을 일일이 확인하는 사람이 있을지는 의문이지만 원리를 이해하면 의외의 것들을 알 수 있다. ISBN은 10자리의 숫자로 구성되어 ISBN이라는 문자를 앞세워 표기된다. 10자리 숫자는 4개의 군으로 나누어지는데 각 군은 하이픈(-)이나 공란으로 표시하여 이를 구분한다.
4개의 군은 다음과 같이 나누어진다.

- 제 1군 : 국별번호부분으로 우리나라의 국별번호는 89이다.
- 제 2군 : 발행자번호부분으로서, 특정 발행자(출판사)를 나타낸다.
- 제 3군 : 서명식별번호부분으로서,
  발행자가 제작한 특정서명(또는 표제 서명)이나 판을 나타낸다.
- 제 4군 : 체크기호부분으로,
  ISBN의 정확성 여부를 자동으로 점검할 수 있는 기호

그럼 이제 이러한 체크숫자를 찾는 법에 대해 알아보도록 하자.

10개의 숫자에 10부터 1까지의 자연수를 차례로 곱해서 더한 합이 11의 배수가 되도록 체크 숫자를 찾는다. 11의 배수가 되기 위해서는 체크 숫자로 10을 이용할 경우가 생긴다. 이런 경우에는 X 로 10을 대신한다.
예를 들어 $IBSN\ 89-7282-108-X$ 의 경우가 그렇다.

ISBN의 번호가 89－7282－343－0 에서 끝으로 0은 다음에 설명할 방법에 의해 정해진 체크 숫자이다.

$1 \cdot 8+2 \cdot 9+3 \cdot 7+4 \cdot 2+5 \cdot 8+6 \cdot 2+7 \cdot 3+8 \cdot 4+9 \cdot 3=187 \equiv 0 \pmod{11}$

처음 9개의 숫자는 0~9 중의 하나이고

$$10\text{번째 숫자 } x_{10} \equiv \sum_{i=1}^{9} i x_i \pmod{11} \quad (0 \le x_0 \le 10)$$

이렇게 체크숫자를 정하면, 한 개의 숫자를 잘못 읽은 경우와 인접한 두 숫자를 바꾸어 입력한 경우를 모두 찾아 낼 수 있다. 가중치를 주는 방법을 바꾸고 10 대신에 11이라는 소수를 이용한 효과이다.

[예제 22] 주어진 ISBN 07－1670－438－2 가 정확한지 확인하시오.

$1 \cdot 0+2 \cdot 7+3 \cdot 1+4 \cdot 6+5 \cdot 7+6 \cdot 0+7 \cdot 4+8 \cdot 3+9 \cdot 8=200 \equiv 2 \pmod{11}$

이다. 그러므로 이 ISBN 은 정확한 것이다.

(3) 운전면허번호(Driver's Licence Numbers)

최초의 운전면허 시험에서는 합격, 출발, 정지, 커브만 돌 수 있으면 카드를 발급했는데 가지고 다닐 수 없는 액자크기의 합격증이었다고 한다. 차가 늘어나자 사고가 심심찮게 발생하자 단속하기 위해 6년 후인 1899년 3월 파리경찰이 조그만 카드 식으로 발급하여 휴대를 의무화 했다고 한다. 이러한 운전면허증을 보면 운전면허번호라는 것이 있다. 이 운전면허번호는 9개의 숫자 부호로 매겨져 있다. 여기 8개의 숫자를 $d_1 d_2 d_3 \cdots d_8$이라 하면 9번째 숫자

$$d_9 = \sum_{i=1}^{8} (10-i) d_i \pmod{10}$$

[예제 23] 운전면허번호가 24923056 일 때 체크숫자는 무엇인가?

$d_9 = 9 \cdot 2 + 8 \cdot 4 + 7 \cdot 9 + 6 \cdot 2 + 5 \cdot 3 + 4 \cdot 0 + 3 \cdot 5 + 2 \cdot 6 \equiv 7 \pmod{10}$

따라서, Licence Number $= 249230567$

(4) 주민등록번호

주민등록번호를 보면 고향을 알 수 있다고들 하지만 정확한 얘기는 아니다.
주민등록번호 앞자리가 1이면 남자, 2이면 여자라는 것은 대개가 알고 있는 상식이다. 하지만 이 역시 완전한 지식인 것은 아니다. 우리나라는 지난 75년부터 생년월일 6자리, 개인 정보 7자리로 구성된 지금의 주민등록번호를 쓰기 시작했다. 그럼 뒷부분 7자리에는 구체적으로 어떤 정보가 들어있는지 알아보자.
맨 앞 숫자는 성별을 나타낸다. 1은 남자, 2는 여자다. 그러나 이 구분은 100년 단위로 달라진다. 2000년 출생자부터는 남자는 3, 여자는 4를 부여 받는다. 앞서 1800년대에 출생한 노인들의 성별 코드는 남자 9, 여자0이었다. 그런데, 5와 6을 사용하는 사람도 있다. 5를 사용하는 사람은 외국인 한국인으로 귀화한 경우이다.
성별 코드 다음 네 개의 숫자는 지역 코드이고, 그 다음 한자리는 출생신고 당일, 그 출생 신고가 해당 읍-면-동 사무소에 몇 번째로 접수된 것인가를 나타낸다.
마지막 숫자는 '검증번호'다. 이는 앞의 번호들이 정상적으로 조합되었는지를 확인하는 일종의 암호이다. 생년월일을 포함한 앞 12개 숫자 모두를 특정한 공식에 대입해서 산출한다. 따라서 앞의 12자리 숫자가 차례로 정해지면, 마지막에 올 수 있는 번호는 딱 하나로 결정된다. 컴퓨터 통신 ID를 만들면서 엉터리 주민 등록 번호를 입력할 경우 컴퓨터가 금방 '그런 번호는 없다'고 거부하는 것은, 이 마지막 번호가 공식에 안 맞는 숫자이기 때문이다.
우선 국가가 관리하고 있는 개인정보의 문제를 알아보기 전에 개인 정보의 핵심 중의 핵심이라 할 수 있는 주민등록번호에 대한 재미있는 사실 몇 가지를 알아 보도록 하겠다.

[정리 28] (주민번호검증방법) 주민등록번호가 $a_1a_2a_3a_4a_5a_6 - b_1b_2b_3b_4b_5b_6b_7$ 라 할

때, b_7 을 구하는 법은 다음과 같다.

$(2a+3a_2+4a_3+5a_4+6a_5+7a_6+8b_1+9b_2+2b_3+3b_4+4b_5+5b_6) \div 11 \pmod{11}$

이 때 나오는 값을 r 이라 하자.

그러면, $11-r=b_7$이 된다.

[예제 24] 주민등록번호 160312－2067514 은 맞은 주민등록번호인지 알아보자.

각 번호에 2 , 3 , 4 , 5 , 6 , 7 , 8 , 9 , 2 , 3 , 4 , 5 를 곱해주면 다음과 같다.

$2\times1+3\times6+5\times3+6\times1+7\times2+8\times2+2\times6+3\times7+4\times5+5\times1=129$

이 11로 나눈 나머지가 8이고 $x_{13} \equiv 11-8 \equiv 3 \pmod{10}$이므로

주민등록번호가 아니다. **[6]**

그러므로, 이 주민등록번호 가지고는 인터넷상에서 회원가입뿐만 아니라,

모든 서류상에서 오류가 발생할 것이다.

(5) 바코드(상품번호)

출생신고를 하면서 부여되는 주민등록번호를 시작으로 학교와 직장에서의 번호, 전화번호, 아파트동수와 호수, 버스번호, 전철과 도로 등 우리는 숫자와 생활하고 있다고 해도 과언이 아니다.

슈퍼마켓과 서점에서 구입하는 대부분의 상품과 서적에도 숫자가 붙어있다.

이 숫자들은 여러 개의 검은 막대와 흰 막대를 달고 다닌다. 이것이 해당하는 숫자를 나타내는 바코드이다. 그런데 바코드가 잘 읽히지 않아 스캐너를 여러 번 접촉시키다가 결국에는 키보드로 숫자를 입력하는 경우를 종종 볼 수 있다. 뿐만 아니라 바코드가 불명확하거나 유통 과정에서 손상되면, 스캐너는 다른 숫자로 읽을 수도 있다. 이런 문제에 대비해 바코드에는 체크숫자라는 안전장치가 돼 있다. 이것은 상품의 정보를 간직한 고유번호가 잘못 읽혀지는 것을 찾아내기 위한 숫자다.

바코드를 보면 흰색 바탕에 굵고 가는 검은색 막대로 구성되어 있는데, 이 막대들은 2진수 0과 1을 나타내며 막대들의 배열은 0에서 9까지 의 10진수를 나타낸다. 결국 바코드 밑에 써있는 숫자들을 굵고 가는 막대로 표시한 것인데 컴퓨터는 우리가 쓰는 숫자를 인식하기에는 어려움이 있기 때문에 바코드를 써서 2진수로 인식할 수 있게 만든 것이다.
바코드는 일반적으로 식별코드 3자리, 제조업체코드 4자리, 상품코드 5자리, 검사숫자 1자리 등 13자리로 구성된다. 13개의 숫자 중 가장 오른쪽의 체크 숫자의 판단 방법은 다음과 같다.

[정리 29] 체크숫자를 제외한 12개의 숫자에 대하여
10-[{홀수 번째 숫자의 합)+(짝수 번째 숫자의 합 × 3}의 일의 자리 수]=검사숫자가 성립하면 옳게 된 바코드이다.

슈퍼나, 비디오가게 등 일상생활에서 바코드는 많이 이용되고 있다. 그런데 바코드를 잘못 인식하여 요금을 많이 내는 경우가 발생하지 않을까하는 의문이 들곤 하지만 위의 정리에 의해 체크숫자가 있어 기계가 잘못 읽는 것을 막을 수 있다.
만일 기계가 바코드를 잘못 읽으면 바코드의 숫자로 검증 셈을 했을 때 10의 배수가 되지 않아 기계는 경고음을 내게 된다. 즉, 체크 숫자는 일종의 안전장치이다.

[예제 25] 아래의 바코드를 위의 정리에 의해 계산하면,
$10-[8+0+2+4+6+8)+(8+1+3+5+7+9)\times 3$의 일의 자리 수$]=3$ 이다. 따라서,

번호는 8801234567893 이다.

이렇게 체크 숫자를 정하면, 한 개의 숫자를 잘못 읽은 경우를 모두 (100%)

찾아내고, 인접한 두 숫자를 바꾸어 입력한 경우도 '대부분'(정확하게는 88.9%) 찾아낼 수 있다. 이것은 짝수 번째 자리의 숫자에 3을 곱하는 가중치를 둔 효과다. 바코드의 약점 중 하나는 인접한 두 숫자의 차가 일 때, 이 두 숫자를 바꾸어 입력한 경우에는 오류를 찾아낼 수 없다는 점이다.

예를 들어 8801037002782바코드에서 27 을 72 로 바꾸어 8801037007282 로 입력했다고 하자. 그래도 결과는 10의 배수가 되므로 컴퓨터는 오류를 인식할 수 없다. 따라서 제조업자는 상품 번호를 정할 때 이런 경우를 미리 피해야 한다.

담배 같은 경우는 상품 번호가 8개의 숫자로 (8800－9605) 이뤄졌다.
이런 경우에는 홀수 번째 자리에 있는 숫자들을 3 배해서 더하고 짝수 번째에 있는 숫자들은 그대로 더한 전체의 합이 10 의 배수가 되도록 체크숫자를 정한다. 왜냐하면 체크 숫자에는 가중치가 곱해지지 않도록 하기 위해서다.

제3장 Modular 계산 [9]

Modular 계산은 아름다운 디자인을 만드는데 사용될 수 있다. 이 절에서는 m개의 점으로 이루어진 별모양과 (m,n) residue design, 그리고 퀼트 디자인 등의 세 가지 디자인을 연구한다. 수학의 합동 개념을 사용하여 예술적인 아름다운 디자인을 할 수 있다는 것을 보일 수 있다.

(1) m개의 점으로 이루어진 별모양

m개의 점으로 이루어진 별모양을 만들이 위해 다음의 작업을 순서대로 수행한다.

- 단계 1: 우선 커다란 원 위에 m개의 점을 균등하게 찍는다.
- 단계 2: 각 점 위에 법 m으로 계산한 값 0 부터 $m-1$ 까지를 표시한다.
- 단계 3: $\gcd(m,i)=1$이 되는 최소의 값 i 를 선택한다.
- 단계 4: 각 점 x를 $x+i \pmod m$ 인 점과 연결한다.

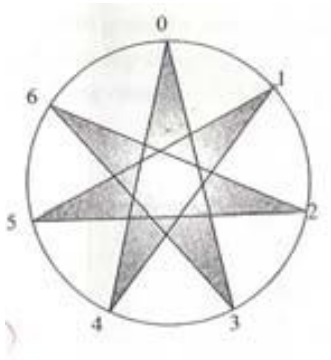
• 단계 5: 그러면 m개의 점으로 이루어진 별 모양의 디자인을 만들 수 있다.

[예제 26] 7개의 점으로 이루어진 별 모양에 대해 알아보자.

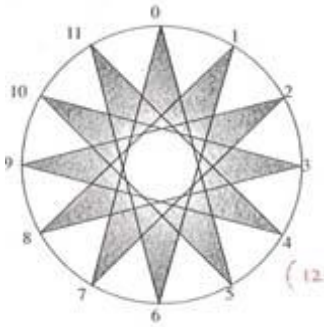
커다란 원 위에 균등하게 7개의 점을 찍는다. 각 점에 0~6까지 표시한다.

$\gcd(7, i) = 1$이 되게 잡는다. (여기서 i =3으로 택한다.)

각 점 x를 $x + i \pmod 7$인 점과 연결하면 다음과 같은 <그림1>이 나타난다.



A seven-pointed star.



A twelve-pointed star.

<그림 1> <그림 2>

원 위에 동일한 개수의 점을 가지고 있는 경우에도, 서로 다른 i 를 택하면,

다른 디자인을 만들게 된다.

즉, 위의 예에서와 같이 원 위에 7개의 점을 택하는데, 단지 i 의 값을 3이 아니라 2로 택해보면 새로운 디자인이 생긴다.

원 위에 점의 개수를 바꾸면, 물론 새로운 디자인을 얻는다.

위의 <그림 2>는 12개의 점으로 이루어진 별 모양이다. (점의 개수 12, i=5)

(2) (m, n) residue design

$1 \le n < m$이며 $\gcd(m, n) = 1$ 인 두 정수 m, n 을 생각해보자. 이제 다음의 작업을 순서대로 수행한다.

• 단계 1: 커다란 원 위에 m 개의 점을 균등하게 찍는다.

• 단계 2: 각각의 점을 1부터 $m-1$까지 표시한다.

• 단계 3: 각 점 x를 $nx \pmod m$인 점과 연결한다.

[예제 27] $(19,9)$ residue design을 만들어보자.

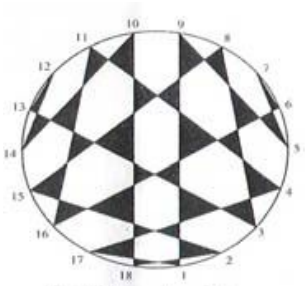
커다란 원의 둘레에 18 개의 점을 균등하게 찍은 후, 1부터 18 까지 번호를 부친다. 각 점의 번호에 9 를 곱하여 mod 19 로 계산하면 다음 표와 같다.

원래점x	1	2	3	4	5	6	7	8	9
$9x \pmod{19}$	9	18	8	17	7	16	6	15	5

원래점x	10	11	12	13	14	15	16	17	18
$9x \pmod{19}$	14	4	13	3	12	2	11	1	10

<표 1>

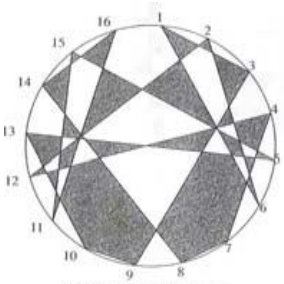
이제 점 1 을 9 와 연결하고, 2 를 18 과, 3 을 8 과, ... 그리고 18 을 10 과 연결한다. 그 후 만들어진 디자인에 색칠을 하면 다음과 같은 디자인을 얻게 된다.



The (19, 9) residue design.

<그림 3>

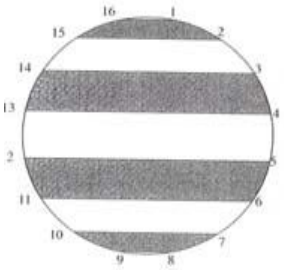
(m, n) residue design에서, m, n값을 바꾸면 새로운 디자인이 생긴다.



The (17, 6) residue design.

<그림 4>

(17,6) residue : 각 점 x를 6x (mod 17)와 연결.



The (17, 16) residue design.

<그림 5>

(17, 16) residue: 각 점 x를 16x (mod 17)와 연결.

(3) 퀼트 디자인

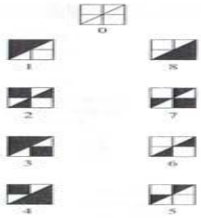
이제는 법 m에 관한 덧셈과 곱셈표를 이용하여 아주 예술적이고 흥미로운 디자인을 만들어보기 위해 다음의 예제로부터 시작해보자.

[예제 28] $m=9$라 하자. 잉여군 Z_9 의 덧셈표를 만들어보자.

+	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8	0
2	2	3	4	5	6	7	8	0	1
3	3	4	5	6	7	8	0	1	2
4	4	5	6	7	8	0	1	2	3
5	5	6	7	8	0	1	2	3	4
6	6	7	8	0	1	2	3	4	5
7	7	8	0	1	2	3	4	5	6
8	8	0	1	2	3	4	5	6	7

<표 2> 덧셈에 관한 연산표

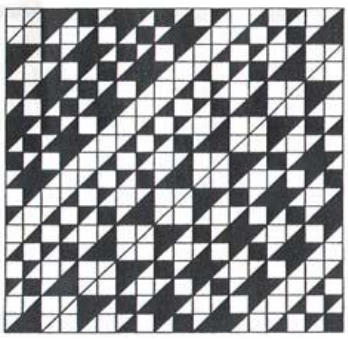
기본 디자인 9개를 만들어서 각각의 수 0 부터 8 까지 대응시킨다. 가령

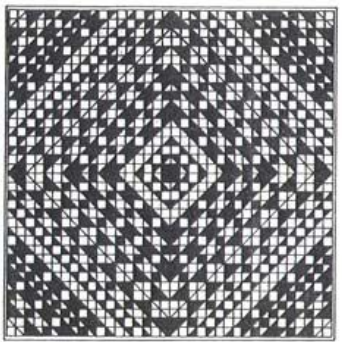


<그림 6>

기본 디자인 9개를 덧셈표 내의 수 0 부터 8 까지 대응시키면 다음과 같은 퀼트 디자인을 만들 수 있다.

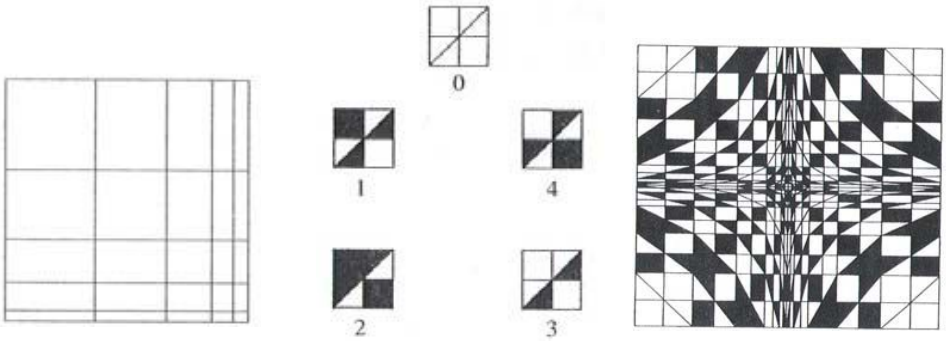
위의 디자인을 몇 개 붙이면 다음과 같은 디자인도 만들 수 있다.


<그림 7>


<그림 8>

앞의 퀼트를 만드는 과정에서, 각 숫자 0 부터 8까지에 대응시킨 '기본 디자인은 임의로 택한 것'이다.

그러므로 각각의 기본 디자인의 모습을 바꿀 때 마다 우리는 새로운 퀼트를 얻게 된다. 즉, 각 디자인의 모양을 정사각형 격자창으로 만드는 대신에, 직사각형 격자창을 만들어보면 더욱 흥미 있는 디자인을 만들 수도 있다.



<그림 9>

위의 예제에서는 덧셈표를 통하여 디자인을 만들었지만, 곱셈표를 이용하면 더욱 아름다운 디자인을 만들 수 있다. 또한 격자창의 모양을 서로 다른 형태로 하면 다양한 디자인을 만들어 낼 수 있다.

제4장 Round-robin tournament [1]

N팀이 겨루는 경기에서 한 팀이 나머지 모든 상대팀과 꼭 한 번씩 경기를 치루는 방식을 Round-robim tournament 라 부른다. 흔히 우리가 말하는 리그전이다. 이제 N팀이 겨루는 Round-robim tournament 의 대진표를 작성하는 방법을 생각해 본다. 각 팀에 1, 2 $\cdots$, N의 숫자를 부여해준다. N이 홀수인 경우는 여분의 한 팀을 만들고 그 팀에 $N+1$팀으로 이름 붙여 둔다. 만약 어떤 팀이 어느 회전에서 $N+1$팀과 시합을 하도록 편성되면 그 팀은 쉬는 것으로 약속한다. 그러므로 우리는 팀 수 N이 짝수라고 가정한다. 팀이 N개 있으므로 각 팀은 $N-1$번의 경기를 치러야 한다. 지금부터 $k(1 \le k \le N-1)$회전에 $i(1 \le i \le N-1)$팀이 경기를 할 팀을 결정하자.

주어진 $k(1 \le k \le N-1)$와 $i(1 \le i \le N-1)$에 대하여

$$i+j \equiv k(\mathrm{mod}\ N-1) \qquad (*)$$

을 만족하는 $j(1 \le j \le N-1)$가 단 하나 존재한다. 만약 $i \ne j$이면 k회전에서 i팀과 j팀이 경기를 한다. 그러나 $i=j$이면 i팀은 k회전 대진표에서 빠지게 된다.

위의 $(*)$합동 방정식에서 $i=j$인 경우는

$$2i \equiv k(\mathrm{mod}\ N-1)$$

을 만족하고 여기서 $(2, N-1)=1$이므로 위의 합동 방정식은 단 하나의 해를 가진다. 따라서 위의 $(*)$합동방정식에서 $i=j$인 경우는 단 한 팀이다. N팀 역시 대진표에서 빠진 것은 당연하다. 이때 i팀은 N팀과 경기를 치른다.

[예제 29] $N=4$일 때 Round-robim tournament 대진표를 작성하라.

위의 방식을 이용하여 1회전의 대진표를 작성해보자. $i(1 \le i \le 3)$에 대하여 합동방정식

$$i+j \equiv 1 (\text{mod } 3)$$

을 푼다. $i=1,2,3$인 각 경우를 풀자.

$$1+j \equiv 1 \ (\text{mod } 3),\ 2+j \equiv 1 \ (\text{mod } 3),\ 3+j \equiv 1 \ (\text{mod } 3)$$

을 풀면 각각 $j=3, j=2, j=1$을 얻는다. 그러므로 1회전에서 1번과 3번 팀, 2번과 4번 팀이 경기를 갖는다. 같은 방법으로 2, 3회전을 계산하면 다음 표를 얻는다.

팀 / 회전	1	2	3	4
1	3	4	1	2
2	4	3	2	1
3	2	1	4	3

<표 3>

제5장 암호 기법에의 응용 [1]

예로부터 군사적, 외교적 또는 경제적 목적으로 메시지를 특정한 사람에게 비밀리에 전달한 필요가 있다. 따라서 받는 사람 외에 다른 사람은 그 메시지의 내용을 이해하지 못하게 해야 한다. 이렇게 하기 위해 보내는 사람과 받는 사람 사이에 특별한 암호가 필요하다. 고대 로마시대부터 이러한 암호는 사용되어 왔으며 오늘날은 컴퓨터의 계산 능력의 향상과 더불어 더 안전한 암호기법(Crytography)더불필요해 졌다. 이것이 계기가 되어 오늘날 암호학(Cryptology)더불학문으로 발전하게 되었다. 암호기법은 우선 주어진 원문(plaintext뜩한 적당한 열쇠(key)를 이용하여 암호문(ciphertext뜩으로 변화시키는 작업과 이 암호문한 호기법열쇠 또는 다른 열쇠를 이용하여 해독하는 작업한 포함한다. 암호학기법더 안전한 암호기법한 연구하는 학문이다. 암호체계는 열쇠의 공개여부에 따라 두 가지 분류된다. 하나는 보내는 사람과 받는 사람만이 암호의 열쇠를 알고 있는 경우(p 변화키는al key cryptosystem뜩와 또 다른 하나는 암호의 열쇠가 일반에게 공개된 경우(public key cryptosystem뜩이다. 전자가 안전할 것으로 생각되나 통신기술 및 컴퓨터 계산 능력의 향상에 따라 전자의 경우 열쇠의 보안문제나 단순한 열쇠 해독기법 때문에 20세기 후반부터 후자가 더 유용하게 이용된다. 이 몇 가지 암호기법한 소개한다. 불행히도 이러한 암호기법이 서구오늘날발달하였기 때문에 영어로 작성된 문장에 대한 암호기법을 소개한다.

(1) 개인 대 개인 열쇠 암호체계(personal key cryptosystem)

① 시저 암호(Caesar cipher)

B.C. 50세기경에 로마황제 시저(Caesar)는 알파벳을 세 문자씩 앞쪽으로 옮기고 마지막 세 문자는 처음 세 문자로 대체하는 이동암호를 사용하여 시서로(Cicero)에

게 편지를 보냈다. 따라서 시저의 암호문은 원문의 알파벳을 다음 알파벳으로 대체하여 작성되었다.

원문 : A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

암호문 : D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

예를 들어 원문

CAESAR WAS GREAT

는 위의 규칙에 의해 암호문으로 바꾸면

FDHVDU ZDV JUHDW

이다. 만약 다음과 같이 알파벳에 숫자를 대응시키면 시저의 암호는 합동식으로 표현된다.

A	B	C	D	E	F	G	H	I	J	K	L	M
01	02	03	04	05	06	07	08	09	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

만약 P 를 원문에 대응되는 숫자라 하고 C 를 암호문에 대응되는 숫자라 하면

$$C \equiv P + 3 \pmod{26}$$

를 얻는다. 예를 들어 위에 주어진 원문 CAESAR WAS GREAT을 숫자로 변환하면

03 01 05 19 01 18 23 01 19 17 18 05 01 20

이다. 합동식 $C \equiv P + 3 \pmod{26}$을 이용하여 암호문

06 04 08 22 04 21 26 04 22 20 21 08 04 23

를 얻는다. 따라서 이 암호문으로부터 원문을 얻기 위해 합동식

$$P \equiv C - 3 \equiv C + 23 \pmod{26}$$

을 이용하면 된다. 시저의 암호는 간단하고 안전이 보장되지 않기 때문에 시저 자신도 사용을 포기하였다. 시저 암호의 약간 일반화된 변환은 3 대신 정수 b를 이용하여 b만큼 이동시키는 이동암호(shift cipher)를 생각할 수 있다. 이 경우에

$$C \equiv P + b \pmod{26},\ 1 \le C \le 26$$

로 나타난다.

② 아파인 변환(Affine Transformation) [4]

시저의 이동암호를 좀 더 일반화하여 다음과 같은 변환을 생각해 보자. $(a, 26) = 1$을 만족하는 두 정수 a, b에 대하여 변환

$$C \equiv aP + b \pmod{26},\ 1 \le C \le 26$$

을 아파인 변환이라 부른다. 이때 $a = 1, b = 3$이면 시저의 이동암호를 얻는다. $(a, 26) = 1$이므로 a는 법 26에 관한 역원 x를 갖는다.

즉 Z_{26}^{*}에서

$$\overline{a}\,\overline{x} = \overline{1} \text{이고 } ax \equiv 1 \pmod{26}$$

이다. 오일러의 정리에 의해 $x \equiv a^{\phi(26)-1} = a^{11} \pmod{26}$이다. 그러므로 이렇게 변환된 암호문을 원문으로 바꾸는 것은 합동식

$$P \equiv x(C - b) \pmod{26},\ 1 \le P \le 26$$

을 이용하면 된다.

[예제 30] $a = 7, b = 10$일 때 아파인 암호 $C \equiv aP + b \pmod{26},\ 1 \le C \le 26$을 이용하여 다음 물음에 답하라.

(1) 암호문의 알파벳에 숫자를 부여하라.

(2) 원문 “PLEASE SEND MONEY”을 암호화하라.

(3) 암호문 “NW HWT PCXCUD TVC ECYPCT”원문을 구하라.

(풀이) (1) 아파인 암호 $C \equiv 7P + 10 \pmod{26}$에 의해 알파벳에 부여된 숫자는 다음과 같다.

원문에 부여된 숫자 :	A	B	C	D	E	F	G	H	I	J	K	L	M
	01	02	03	04	05	06	07	08	09	10	11	12	13

	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	14	15	16	17	18	19	20	21	22	23	24	25	26
암호문에 부여된 숫자 :	A	B	C	D	E	F	G	H	I	J	K	L	M
	17	24	05	12	19	01	07	14	21	02	09	16	23
	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	04	11	18	25	06	13	20	01	08	15	22	03	10

(2) 예를 들어 원문의 P는 숫자 16이 부여되고 암호문의 숫자 16은 L에 대응된다. 마찬가지 방법으로 원문 "PLEASE SEND MONEY"을 암호화하면

"LDCUEC ECHN SWHCQ"

를 얻는다.

(3) (2)의 방법을 역으로 적용하면 암호문의 N은 원문의 D 에 해당한다. 마찬가지로 계산하면 암호문 "NW HWT PCXCUD TVC ECYPCT"의 원문은

"DO NOT REVEAL THE SECRET"

이다.

위에서 주어진 시저 암호나 아파인 암호도 결정적인 약점을 갖고 있다. 실제로 영어 단어에서 각 알파벳이 등장하는 확률을 이용하면 대체로 누구나 암호를 해독할 수 있다.

③ 블록 암호(Block Ciphers) [7]

아파인 암호에서 나타나는 약점을 보완하기 위해 블록 암호가 등장하였다. 여기서는 비즈네르(Vigenere) 암호와 힐(Hill) 암호를 간략하게 소개한다. 비즈네르 암호는 프랑스의 외교관이자 암호학자인 블레즈 드 비즈네르(Blaise de Vigenere)에 의해 알려진 암호로써 원문의 각 문자에 같은 방법으로 암호를 부여하는 대신 암호를 부여하는 방법을 다양화하였다. 비즈네르 암호의 핵심은 열쇠 단어(key

word) $l_1 l_2 \cdots l_n$의 각 문자 l_i에 숫자 k_i를 대응시키고 원문을 블록으로 나누어 각 블록에 k_i만큼 시저의 이동암호를 적용한다. 즉, 원문에 숫자 p_i가 부여된 블록의 암호문에 부여하는 숫자는

$$c_i \equiv p_i + k_i \pmod{26},\ 1 \le c_i \le 26$$

이다.

[예제 31] 열쇠 단어 YTWOK를 사용하여 원문 CRYPTOLOGY의 비즈네르 암호를 구하라.

(풀이) 원문에 부여된 숫자는

$$p_1 p_2 p_3 p_4 p_5 p_6 p_7 p_8 p_9 = 03\ 18\ 25\ 16\ 20\ 15\ 12\ 15\ 07\ 25$$

이며 열쇠 단어 YTWOK에 부여된 숫자는

$$k_1 k_2 k_3 k_4 k_5 = 25\ 20\ 23\ 15\ 11$$

이다. 비즈네르 암호기법에 의해 부여된 숫자는

$$c_1 = p_1 + k_1 = 3 + 25 \equiv 2 \pmod{26}$$

$$c_2 = p_2 + k_2 = 18 + 20 \equiv 12 \pmod{26}$$

$$c_3 = p_3 + k_3 = 25 + 23 \equiv 22 \pmod{26}$$

$$c_4 = p_4 + k_4 = 16 + 15 \equiv 5 \pmod{26}$$

$$c_5 = p_5 + k_5 = 20 + 11 \equiv 5 \pmod{26}$$

$$c_6 = p_6 + k_1 = 15 + 25 \equiv 14 \pmod{26}$$

$$c_7 = p_7 + k_2 = 12 + 20 \equiv 6 \pmod{26}$$

$$c_8 = p_8 + k_3 = 15 + 23 \equiv 12 \pmod{26}$$

$$c_9 = p_9 + k_4 = 7 + 15 \equiv 22 \pmod{26}$$

$$c_{10} = p_{10} + k_5 = 25 + 11 \equiv 10 \pmod{26}$$

이다. 그러므로 암호문은 “BLVEE NFLVJ”이다.

다음은 1929년에 레스터 힐(Lester Hill)에 의해 개발된 힐 암호에 대해 소개한

다. 힐 암호체계는 원문을 n 문자들의 블록들로 나누고 하나의 블록에 속하는 알파벳에 대응되는 숫자를 $P_1, P_2, \cdots, P_n$으로 둔다. 마지막 블록에 속하는 알파벳의 숫자가 n보다 적으면 임의로 여분의 문자를 채워 n개가 되도록 한다. 여기서 $(\det A,\ 26)=1$을 만족하는 $n \times n$ 행렬 A를 선택하고 주어진 블록에 규칙

$$C \equiv AP \pmod{26},\ C=\begin{pmatrix} C_1 \\ C_2 \\ \cdot \\ \cdot \\ \cdot \\ C_n \end{pmatrix}, P=\begin{pmatrix} P_1 \\ P_2 \\ \cdot \\ \cdot \\ \cdot \\ P_n \end{pmatrix}$$

에 의해 n개의 숫자 $C_1, C_2, \cdots, C_n$을 구한다. 이 숫자에 대응되는 알파벳을 이 블록의 암호문으로 선택한다. 각 블록에 같은 작업을 수행하여 힐 암호가 완성된다. 역으로 힐 암호를 해독하는 과정은 암호문의 각 블록에 암호를 부여하는 역 과정을 수행하여 해독한다. 행렬 A가 $(\det A, 26)=1$을 만족하므로 A는 법 26에 관한 역행렬 X를 갖는다. 즉 $XA \equiv I_n \pmod{26}$이므로

$$XC \equiv (XA)P \equiv P \pmod{26}$$

이다. 따라서 암호문을 각 블록을 해독하여 원문을 얻을 수 있다.

[예제 32] 행렬 $A=\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$을 이용하여 CRYPTOLOGY의 힐 암호를 구하라.

(풀이) 03 18 25 16 20 15 12 15 07 25가 원문 CRYPTOLOGY에 숫자를 부여한 것이다. 두 숫자씩 블록을 만들어

$$P_1=\begin{pmatrix} 3 \\ 18 \end{pmatrix}, P_2=\begin{pmatrix} 25 \\ 16 \end{pmatrix}, P_3=\begin{pmatrix} 20 \\ 15 \end{pmatrix}, P_4=\begin{pmatrix} 12 \\ 15 \end{pmatrix}, P_5=\begin{pmatrix} 7 \\ 25 \end{pmatrix}$$

라 둔다. 그러면

$$C_1=AP_1=\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 3 \\ 18 \end{pmatrix}=\begin{pmatrix} 24 \\ 21 \end{pmatrix} \equiv \begin{pmatrix} 24 \\ 21 \end{pmatrix} \pmod{26}$$

이다. 마찬가지로

$$C_2=\begin{pmatrix} 66 \\ 41 \end{pmatrix} \equiv \begin{pmatrix} 14 \\ 15 \end{pmatrix} \pmod{26},\ C_3=\begin{pmatrix} 55 \\ 35 \end{pmatrix} \equiv \begin{pmatrix} 3 \\ 9 \end{pmatrix} \pmod{26}$$

$$C_4 = \begin{pmatrix} 39 \\ 27 \end{pmatrix} \equiv \begin{pmatrix} 13 \\ 1 \end{pmatrix} \pmod{26}, \ C_5 = \begin{pmatrix} 39 \\ 32 \end{pmatrix} \equiv \begin{pmatrix} 13 \\ 6 \end{pmatrix} \pmod{26}$$

을 얻는다. 그러므로 CRYPTOLOGY의 힐 암호는 XU NO CI MA MF 이다.

(2) 공개 열쇠 암호체계

개인 대 개인 열쇠 암호체계는 암호문을 작성할 때 사용하는 열쇠와 해독할 때 사용하는 열쇠가 같거나 단순한 역 과정이기 때문에 열쇠가 노출되면 비밀을 보장하기 힘들다. 요즘은 인터넷 및 컴퓨터 사용의 활성화로 열쇠의 노출 위험성이 점차 증가하고 있다. 이러한 단점을 보완하기 위해 암호문을 작성할 때 사용하는 열쇠와 해독할 때 사용하는 열쇠를 다르게 할 필요가 있다. 이 경우에 암호문을 작성할 때 사용하는 열쇠는 공개하고 해독할 때 사용하는 열쇠는 수신자가 만들어 사용한다. 이러한 공개 열쇠 암호체계의 대표적인 것이 RSA암호체계이다. 이외에 배낭 암호(knapsack cipher)등이 있으나 여기서는 RSA암호체계만 소개한다.

① RSA 암호체계

RSA 암호체계는 1977년 리베스트(R. Rivest), 셰미르(A. Shamir) 그리고 아델만(L. Adleman)에 의해 제시되었으며 개발자들의 이름의 첫 알파벳을 이용하여 RSA 암호라 이름 붙여졌다. 이 암호체계는 상당히 큰 합성수의 표준분해를 구하는 것이 어렵다는 수론의 기본적인 성질을 사용한다. 먼저 암호문을 작성하는 과정을 소개한다. 암호문을 작성하기 위해 매우 큰 두 소수의 곱으로 표현되는 양의 정수 $n = pq, (p, q$는 소수$)$를 선택하고 $\phi(n)$과 서로 소인 양의 정수 $k(k < n)$를 선택한다. 원문을 n보다 작은 문자가 포함되도록 블록으로 나누고 각 블록을 다음과 같이 암호화한다. 먼저 원문에 포함되어 있는 알파벳이나 숫자에 다음 규칙으로 숫자화한다.

A	B	C	D	E	F	G	H	I	J	K	L	M	
01	02	03	04	05	06	07	08	09	10	11	12	13	
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
14	15	16	17	18	19	20	21	22	23	24	25	26	
,	.	?	0	1	2	3	4	5	6	7	8	9	!
27	28	29	30	31	32	33	34	35	36	37	38	39	40

그리고 00은 두 문자 사이의 공란으로 지정한다. 숫자 P가 부여된 블록에

$$P^k \equiv C \pmod{n},\ 0 \le C \le n-1$$

을 만족하는 C를 구한다. 여기서 구한 C가 이 블록의 암호문이다.

이러한 암호문 작성 과정에서 등장하는 n, k는 공개된다. 그러나 n의 소수들의 곱으로의 표현은 공개하지 않는다. 이제 이렇게 작성된 암호문의 해독과정을 알아본다. $(k, \phi(n)) = 1$이므로

$$kj \equiv 1 \pmod{\phi(n)}$$

을 만족하는 정수 j가 존재한다. 따라서

$$kj = 1 + \phi(n)t$$

을 만족하는 t가 존재한다. 만약 $(P, n) = 1$이면 오일러의 정리에 의해 $P^{\phi(n)} \equiv 1 \pmod{n}$이고, 따라서

$$\begin{aligned} C^j = (P^k)^j &\equiv P^{1+\phi(n)t} \\ &\equiv P(P^{\phi(n)})^t \equiv P \pmod{n} \end{aligned}$$

을 얻는다. 만약 $(P, n) \ne 1$이면 $n = pq$이고 $P < n$이므로 $(P, n) = p$ 또는 $(P, n) = q$이다. 어느 경우에도

$$C^j \equiv P \pmod{p}\text{이고 } C^j \equiv P \pmod{q}$$

이다. 그러므로

$$C^j \equiv P \pmod{n}$$

이다. P를 알파벳이나 숫자로 변환한 것이 이 블록의 원문이다. 여기서 주어진 k를 암호지수(enciphering exponent) 그리고 j 를 복구지수(recovery exponent)라

부른다. RSA 암호체계에서 n, k는 공개되지만 n의 소수로의 표준분해 pq와 j가 공개되지 않는다. j를 구하기 위해 먼저 $\phi(n)$을 구해야 한다. $\phi(n) = (p-1)(q-1)$을 구하기 위해 n의 인수분해가 반드시 필요하나 매우 큰 수 n의 인수분해는 매우 긴 시간을 요구하거나 또는 불가능하다. 따라서 RSA 암호체계에서 합법적인 수신자는 n의 인수분해를 이미 알고 있어야 한다. 그러므로 합법적인 수신자 이외의 사람은 암호문을 해독하는 것이 불가능하다.

[예제 33] $n = 1537, k = 47$에 대하여 다음 물음에 답하라.

(1) 복구지수 j를 구하라.

(2) 원문 "NO WAY"의 RSA 암호문을 구하라.

(3) (2)에서 구한 암호문을 해독하여 원문이 나오는지를 확인하라.

(풀이) (1) $n = 1537 = 29 \cdot 53$이므로

$$\phi(n) = (p-1)(q-1) = 28 \cdot 52 = 1456$$

이다. $(47, 1456) = 1$이므로 $47j \equiv 1 \pmod{1456}$을 만족하는 j는 법 1456에 관하여 단하나 존재한다. 이 합동방정식을 풀면 $j = 31$을 얻는다.

(2) 원문을 숫자화하면

$$P = 141500230125$$

를 얻는다. 이것을 세 숫자씩 네 개의 블록을 만든다. 따라서 첫 블록은 141이고 이것을 RSA 암호화하면

$$141^{47} \equiv 658 \pmod{1537}$$

을 얻는다. 각 블록들을 다 계산하면

$$500^{47} \equiv 1408 \pmod{1537}$$

$$230^{47} \equiv 1250 \pmod{1537}$$

$$125^{47} \equiv 1252 \pmod{1537}$$

를 얻는다. 그러므로 RSA 암호문은

$$C = 0658\ 1408\ 1250\ 1252$$

이다.

(3) 먼저 암호문의 각 블록에서 주어진 숫자에 대하여 원문에 부여한 숫자를 구한다. 이들의 관계는

$$P^k \equiv C \pmod{n} \Leftrightarrow C^j \equiv P \pmod{n}$$

이다. 그러므로 이 관계를 이용하여 암호문

$C = 0658\ 1408\ 1250\ 1252$의 각 블록에 대응되는 원문에 부여한 숫자

$$658^{31} \equiv 141 \pmod{1537},\ 1408^{31} \equiv 500 \pmod{1537},$$

$$1250^{31} \equiv 230 \pmod{1537},\ 1252^{31} \equiv 125 \pmod{1537}$$

를 얻는다. 따라서

$$P = 141500230125$$

이며 이것을 알파벳이나 숫자로 바꾸면 NO WAY을 얻는다.

V. 결　　론

현재 대학에서 다루어지는 합동식의 정수론적인 개념과 정리들은 대부분의 수업이 순수 수학적인 내용을 그대로 도입하여 설명하는 방식으로 이루어지고 있다.

이에 본 논문은 학생들이 공부를 하며 합동식에 대한 학습이 보다 의미 있고 중요하다는 것을 인지할 수 있도록 하기 위하여 그 대안적 방안으로 합동식과 실생활과의 관련성을 설명하였다.

합동식을 처음 접하는 학생들에게 그 기본적인 내용에 이해를 돕기 위해 각각의 정리에 예를 들면서 자세하게 설명하였다. 그리고 합동식을 이해하는데 그리스 시대부터 다루어져온 수론의 고전적인 정리들이 얼마나 가치 있게 적용되는지를 드러내어 수학의 의미와 실용성까지 인식할 수 있도록 하였다. 이를 위하여 수론적 개념과 정리를 실생활과 관련하여 서술을 할 때에 되도록 자세하게 기술하였다.

이러한 관점에서 합동식을 학습한 학생들의 이해를 돕고 합동식에 대해서 어느 정도 이해하고 있는 학생들의 심화연구에 도움을 주고자 한다. 그리고 이를 가르치고자하는 교사에게 도움을 줄 수 있을 것이라 생각한다. 또한 합동식이 일상생활에 직접적으로 응용되는 것을 실감하게 될 것이다.

본 논문에서 합동식에 관심 있는 학생과 교사들에게 도움이 되고자 합동식에 관하여 개념 설명과 자세한 실용적인 내용을 열거한 것이 도움이 되길 기대한다.

참 고 문 헌

[1] 천장호. 『정수론』, 경문사 , 2009

[2] 한재영. 『정수론』, 경문사 , 2008

[3] 김응태・박승안. 『정수론 제 7판』, 경문사 , 2007

[4] 원동호. 『현대 암호학』, 도서출판 그린 , 2004

[5] 신현용.『교사를 위한 정수론』, 교우사 , 2008

[6] 이민섭. 『정수론과 암호학』, 교우사 , 2007

[7] 이민섭. 『현대 암호학』, 교우사 , 2007

[8] 조승렬. “합동식에 관한 연구 ”(군산대학교 교육대학원, 2007)

[9] 김유리. “합동식과 그 응용 ”(한남대학교 교육대학원, 2005)

[10] 김병기. “合同方程式의 解法에 관한 硏究 ”(연세대학교 교육대학원, 2003)

[11] 임근빈.전송기.임동만. 『알기쉬운 정수론』, 경문사 , 2007

저작물 이용 허락서

학 과	수학교육	학 번	20078208	과 정	석사
성 명	한글: 윤 수 지	한문: 尹 수 지	영문: yun.su-ji		
주 소	광주광역시 서구 금호동 코아루 아파트 105동 2003호				
연락처	010-4562-1557	E-MAIL: yunsusie@naver.com			
논문제목	한글 : 합동식과 그 응용에 관한 연구 영문 : A Study on Congruence and its Application				

본인이 저작한 위의 저작물에 대하여 다음과 같은 조건 아래 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 의사표시가 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.

2010년 7월 9일

저작자: 윤 수 지 (서명 또는 인)

조선대학교 총장 귀하