현빈 : 13 수의 합동

March 31, 2015

Contents

1 유클리드 호제법 (Euclid Algorithm)

정의 1) 최대공약수와 최소공배수

자연수 a, b에 대해 a, b의 최대공약수를 (a, b), 최소공배수를 $[a, b]$로 표시한다. 셋 이상의 자연수 a_1, a_2, a_3, $\cdots$, a_n의 최대공약수는 $(a_1, a_2, a_3, \cdots, a_n)$로, 최소공배수는 $[a_1, a_2, a_3, \cdots, a_n]$로 표시한다.

예시 2)

252와 198의 최대공약수를 구해보자.

먼저

$$252 = 1 \times 198 + 54$$

이므로 $(252, 198) = (198, 54)$이다. 또

$$198 = 3 \times 54 + 36$$

이므로 $(198, 54) = (54, 36)$이다. 또

$$54 = 1 \times 36 + 18$$

이므로 $(54, 36) = (36, 18)$이다. 마지막으로

$$36 = 2 \times 18$$

이므로 $(36, 18) = 18$이다.

따라서 $(252, 198) = 18$이다.

예시 2에서 사용한 최소공배수를 구하는 방법을 유클리드 호제법이라고 한다. 이 일련의 과정들이 정당화되기 위해서는 일단 다음 정리를 증명해야 한다.

정리 3)

자연수 a, b에 대해 $(a \geq b)$ a를 b로 나눈 몫이 q이고 나머지가 r일때, 즉

$$a = bq + r \quad (0 \leq r < b)$$

일 때,

$$(a, b) = (a, r)$$

이다.

(힌트 : a와 b의 공약수가 a와 r이 공약수이고, a와 r의 공약수가 a와 b이 공약수라는 것을 증명하고 이를 활용하면 된다.)

증명)

이 정리를 토대로 다음 정리를 증명할 수 있다.

정리 4) 유클리드 호제법 (Euclid Algorithm)

자연수 a, b에 대해서 $(a \geq b)$ $r_0 = a, r_1 = b$라고 하자. 주어진 $r_j, r_{j+1} (j \geq 0)$에 대해서, r_j를 r_{j+1}로 나눈 나머지를 r_{j+2}로 정하자. 즉

$$r_0 = r_1 q_1 + r_2 (0 \leq r_2 < r_1)$$
$$r_1 = r_2 q_2 + r_3 (0 \leq r_3 < r_2)$$
$$r_2 = r_3 q_3 + r_4 (0 \leq r_4 < r_3)$$
$$\vdots$$

이다. 이때 다음이 성립한다.

(1) $r_n = 0$인 n이 존재한다.

(2) $r_{n-1} = (a, b)$이다.

증명)

연습문제 5)

유클리드 호제법을 사용하여 다음을 구하여라.

(1) $(45, 75)$

(2) $(102, 222)$

(3) $(666, 1414)$

(4) $(20785, 44350)$

풀이)

2 Bezout의 정리(Bezout's Identity)

유클리드 호제법을 사용하면 두 자연수의 최대공약수를 그 두 자연수를 이용하여 간단히 표현해낼 수 있다는 것도 밝힐 수 있다. 예시 1)에서의 숫자들을 다시 살펴보면 다음과 같다.

예시 6)

세 번째 식에서

$$18 = 54 - 1 \times 36$$

이다. 두 번째 식을 변형해 대입하면

$$18 = 54 - 1 \times (198 - 3 \times 54)$$

이다. 첫 번째 식을 변형해 대입하면

$$18 = (252 - 1 \times 198) - 1 \times [198 - 3 \times (252 - 1 \times 198)]$$

이다. 이를 정리하면

$$18 = 4 \times 252 - 5 \times 198$$

이다. 즉

$$18 = 252x + 198y$$

를 만족시키는 정수 x와 y가 존재한다.

이와 같은 결과를 일반화하면 다음과 같은 정리를 얻을 수 있다.

정리 7) Bezout의 정리(Bezout's Identity)

자연수 a, b에 대해 $(a \geq b)$

$$ax + by = (a, b)$$

를 만족시키는 정수 x, y가 존재한다.

(힌트 : 유클리드 호제법을 이용해 증명할 수 있다.)

증명)

연습문제 8)

예시 6에서 사용한 방법을 이용해 다음과 같이 주어진 a, b에 대해서 (a, b)를 $(a, b) = ax + by$꼴로 표현하여라.

(1) $a = 45$, $b = 75$

(2) $a = 102$, $b = 222$

(3) $a = 666$, $b = 414$

(4) $a = 20785$, $b = 44350$

풀이)

3 수의 합동

a, b는 정수, m은 자연수라고 가정하자.

정의 9) 합동관계(Congruence Relation)

$$m \mid a-b$$

이면

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

이라고 쓴다.

정리 10)

합동관계는 다음을 만족한다.

(1) 임의의 정수 a에 대해 $a \equiv a \pmod{m}$이다.

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

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

증명)

합동관계는 세 가지 좋은 성질을 만족하므로 다루기가 매우 편하다. 위의 세 가지 성질을 만족하는 관계를 '동치관계 (Equivalence Relation)' 라고 한다. 따라서 합동관계는 동치관계의 일종이다.

다음 정리는 거의 당연하다.

정리 11)

$a \equiv b \pmod{m}$ 이면 $a = b + km$ 을 만족시키는 정수 k 가 존재한다. 또 $a = b + km$ 을 만족시키는 정수 k 가 존재하면 $a \equiv b \pmod{m}$ 이다.

증명)

정리 12)

c 가 정수이고, $a \equiv b \pmod{m}$ 이면

(1) $a + c \equiv b + c \pmod{m}$

(2) $a - c \equiv b - c \pmod{m}$

(3) $ac \equiv bc \pmod{m}$

이다.

증명)

정리 13)

c가 정수이고, $(c, m) = 1$이고 $ac \equiv bc \pmod{m}$이면 $a \equiv b \pmod{m}$이다.
이다.

(힌트 : $ab \mid c$이고, $(a, c) = 1$이면 $b \mid c$이다.)

증명)

연습문제 14)

$(c, m) \neq 1$ 일 때 정리 13이 성립하지 않는 반례를 들여라.

풀이)

정리 12는 합동식의 양변에 같은 수를 더하거나 빼거나 곱해도 여전히 성립한다는 것을 보여준다. 정리 13과 정리 14는 합동식의 양변에 같은 수를 나눌 때에는 특별한 경우에만 성립한다는 것을 나타낸다.

다음 정리는 정리 12를 조금 더 일반화한 것이다.

정리 15)

$a \equiv b \pmod{m}$ 이고 $c \equiv d \pmod{m}$ 이면

(1) $a + c \equiv b + d \pmod{m}$

(2) $a - c \equiv b - d \pmod{m}$

(3) $ac \equiv bd \pmod{m}$

이다.

증명)

정리 16)

자연수 k에 대해서 $a \equiv b \pmod{m}$이면 $a^k \equiv b^k \pmod{m}$이다.

증명)

정리 17)

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

$$a \equiv b \pmod{[m_1, m_2, \cdots, m_k]}$$

이다.

증명)

4 일차합동식 (Linear Congruence)

다음은 일차방정식과 대응되는 개념이다.

정의 18) 일차합동식 (Linear Congruence)

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

꼴의 합동식을 '일차합동식'이라고 한다. 이 일차합동식을 만족시키는 정수 x를 '일차합동식의 근'이라고 한다. 그리고 일차합동식의 근을 구하는 과정을 '일차합동식을 푼다'고 말한다.

예시 19)

일차합동식

$$3x \equiv 4 \pmod{5}$$

을 풀어보자. 숫자를 하나씩 대입해보면, x가 1, 2일 때는 성립하지 않고, 3일 때에는 성립함을 알 수 있다. 또 4, 5, 6, 7일 때에는 성립하지 않고 8일 때는 성립함을 알 수 있다. 즉 x가 $5k+3$꼴의 정수일 때에만 성립한다는 것을 알 수 있다. 따라서 이 일차합동식의 해를 $x \equiv 3 \pmod{5}$로 표현할 수 있을 것이다.

이 일차합동식의 해는 무한히 많다. 하지만 mod 5의 관점에서 보면 해는 유일하다고 말할 수 있다.

예시 20)

일차합동식

$$6x \equiv 1 \pmod{9}$$

을 풀어보자. 숫자를 하나씩 대입해보면, 어떤 숫자도 주어진 일차합동식을 만족하지 못한다. 즉 이 합동식의 근은 없다.

예시 21)

일차합동식

$$6x \equiv 3 \pmod{9}$$

을 풀어보자. 숫자를 하나씩 대입해보면, x가 1일 때는 성립하지 않고, 2일 때에는 성립함을 알 수 있다. 또 3, 4일 때에는 성립하지 않고 5일 때는 성립함을 알 수 있다. 또 6, 7일 때에는 성립하지 않고 8일 때는 성립함을 알 수 있다. 또 9, 10일 때에는 성립하지 않고 11일 때는 성립함을 알 수 있다. 즉 x가 $3k+2$꼴의 정수일 때에만 성립한다는 것을 알 수 있다. 따라서 이 일차합동식의 해를 $x \equiv 2 \pmod{3}$로 표현할 수 있을 것이다. 혹은 $x \equiv 2, 5, 8 \pmod{9}$로 표현할 수도 있다.

이 일차합동식의 해는 무한히 많다. 하지만 mod 9의 관점에서 보면 해는 세 개가 있다고 말할 수 있다.

위의 세 예시들에서 알 수 있는 사실 중 하나는, 어떤 숫자가 일차합동식의 근일 때 $\mod m$의 관점에서 그 숫자와 같은 모든 숫자는 그 일차방정식의 근이라는 것이다. 즉 다음 정리가 성립한다.

정리 22)

x_1이 일차합동식

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

의 근이고 $x_1 \equiv x_2 \pmod{m}$이면 x_2도 이 일차합동식의 근이다.

증명)

일차방정식

$$2x = 4$$

를 풀기 위해서 통상적으로 쓰는 방법은, 양변을 2로 나누는 것이다. 이는 양변에 2의 역수인 $\frac{1}{2}$를 곱하는 것이라고도 말할 수 있다. 일차합동식을 푸는 데에도 이와 같은 방법이 쓰일 수 있다. 이를 위해 '역수'에 해당하는 개념을 다음과 같이 정의한다.

정의 23) 역원 (Modular Inverse)

정수 a 와 자연수 m 에 대해 $ax \equiv 1 \pmod{m}$ 을 만족시키는 x 를 a 의 역원 (inverse) 라고 하고 $\bar{a}$ 라고 쓴다.

예시 24)

예를 들어, $2x \equiv 1 \pmod{3}$ 을 만족하는 x 는 $x = 2$, $x = 5$ 등이 있다. 즉 2, 5 등은 mod 3 에서 2 의 역원이다. 또 $7x \equiv 1 \pmod{31}$ 을 만족하는 x 는 $x = 9$, $x = 40$ 등이 있다. 즉 9, 40 등은 mod 31 에서 7 의 역원이다.

반면 $2x \equiv 1 \pmod{4}$ 을 만족하는 x 는 존재하지 않는다. 따라서 mod 4 에서 2 의 역원은 존재하지 않는다.

연습문제 25)

mod 13 에서 다음 수들의 역원을 구하시오.

(1) 2

(2) 3

(3) 5

(4) 11

정리 26)

$(a, m) = 1$ 이면 a 의 역원 $\bar{a}$ 은 존재하며, mod m 에 대해 유일하다.

증명)

예시 27)

$$7x \equiv 22 \pmod{31}$$

의 근을 구하기 위해 양변에 7의 역원인 9를 곱하면

$$63x \equiv 198 \pmod{31}$$

이고

$$x \equiv 12 \pmod{31}$$

이다.

연습문제 28)

다음 일차합동식들의 해를 구하시오.

(1) $2x \equiv 5 \pmod{7}$

(2) $19x \equiv 30 \pmod{40}$

(3) $103x \equiv 444 \pmod{999}$

(4) $3x \equiv 6 \pmod{9}$

(5) $9x \equiv 5 \pmod{25}$

(6) $980x \equiv 1500 \pmod{1600}$

풀이)

정리 29)

$(a, m) = 1$ 이면 일차합동식 $ax \equiv b \pmod{m}$ 의 근은 존재하며, mod m 에 대해 유일하다.

증명)