합동식 굴절어 문법

레장

이론 기초

이산수학 기초 – 1

- **이항관계**: 한 원소를 다른 한 원소에 대해 짝 지은 것.
- **그래프**: 관계의 집합.
- 주의: 그래프 $\subseteq$ 카르테시안 곱.

- 이항관계의 예시:

$$(a, b), (1,2), (1, q), \dots$$

- 주의: $(a, b) \neq (b, a)$

이산수학 기초 – 2

- **반사성**: 자기 자신에 대한 관계가 존재하는 성질;

$$\forall x \in A[(x, x) \in R]$$

- **대칭성**: 두 원소 사이에 양방향으로 관계가 존재하는 성질.

$$\forall x, y \in A[(x, y), (y, x) \in R]$$

- **추이성**: 한 원소를 건너는 간접적인 관계가 직접적으로도 이어지는 성질.

$$\forall x, y, z \in A[(x, y), (y, z) \in R \rightarrow (x, z) \in R]$$

- 위 세 성질을 모두 만족하면 그 관계는 **동치 관계**이며, 한 원소에 대해 동치인 원소들을 모은 집합을 그 원소의 **동치류**라고 함.
- 단순히 일부에 대해 성립하는 것이 아니라 모든 원소에 대해 성립해야 인정!

시계 산술

- 어떤 수로 나눈 나머지가 같으면 서로 같다고 간주하는 산술.

$$10 \equiv 7 \equiv 4 \equiv 1 \pmod 3$$

- 이를 테면, 2시 38분의 분침과 11시 38분의 분침은 가리키는 방향이 같음.
- 오늘의 14시는 내일의 14시와 어제의 14시와 같은 시각임.
- 이와 같이, 어떤 수로 나눈 나머지가 같으면 서로 같다고 간주. 더불어, 같다고 간주되는 수들은 그 주기가 제수와 같음.

합동식

- 시계 산술 체계를 따르는 방정식. 예) $3x \equiv 8 \pmod{25}$
- 도형의 합동에 빗대어 합동식이라고 함.
- 종종 해가 없는 경우도 있음.
- 경우에 따라서는 역수를 정의할 수도 있음. (중요!!)
  예) $3 \cdot 11 \equiv 8 (\mathrm{mod}\ 25) \Leftrightarrow 11 \equiv 3^{-1} \cdot 8 (\mathrm{mod}\ 25)$

베주 항등식

- 두 수 a와 b가 있고 그 최대공약수가 d라 하자.
- $d = ax + by$를 만족하는 x, y가 반드시 존재한다.
- 최대공약수는 각 수의 정수 배수로 나타낼 수 있는 가장 작은 양수이다.
- 그 이외의 정수 배수로 나타낸 수는 모두 d의 배수이다.

유클리드 알고리즘

- $a \bmod b = c, b \bmod c = d, \ldots$와 같은 과정을 재귀적으로 반복하여 최대공약수를 구하는 알고리즘; 나머지가 0이 나왔을 때의 除數가 최대공약수.

- 예)
  132 mod 84 = 48
  84 mod 48 = 36
  48 mod 36 = 12
  36 mod 12 = 0
  ∴ gcd(132, 84) = 12

오일러 정리

- $a^{\phi(n)} \equiv 1 \pmod{n}$
- $\phi(n)$: n보다 작은 자연수 중 n과 서로 소인 수의 개수.

위수와 원시근

- $a^x \equiv 1 \pmod{n}$을 만족하는 최소의 양의 정수 x를 “법 n에 대한 a의 **위수**”라고 한다.
- 위수가 $\phi(n)$과 같으면 a를 n의 **원시근**이라 한다.
- 원시근이 존재한다는 것은 2, 4, p^n, $2p^n$ 꼴 중 하나에 해당한다는 것과 동치. (필요충분조건)

중국인의 나머지 정리

- 서로 소인 모든 除數들의 곱보다 작은, 음이 아닌 정수 중에서, 연립 합동식의 해가 유일하게 존재한다는 것.
- $$\begin{cases} x \equiv r_1 \pmod{b_1} \\ x \equiv r_2 \pmod{b_2} \\ \quad \cdots \end{cases} \Leftrightarrow x \equiv r_1 \frac{b}{b_1}\left(\frac{b}{b_1}\right)^{-1} + r_2 \frac{b}{b_2}\left(\frac{b}{b_2}\right)^{-1} + \cdots \pmod{b_1 b_2 \ldots}$$

  (단, $\frac{b}{b_n}\left(\frac{b}{b_n}\right)^{-1} \equiv 1 (\mathrm{mod}\ b_n)$) (합동식에서의 역수에 대해서는 6페이지 참고.)

문법