

# 기초정수론 (Elementary Number Theory)

2023년 5월 24일

시니어 수학교실 (Math for Seniors)

웹사이트:

저자: JB

이메일: mathforseniors@gmail.com

# Contents

<b>1</b>	<b>강의소개와 사전지식</b>	<b>2</b>
1.1	이상적인 수강생 모델 . . . . .	2
1.2	주의사항 . . . . .	3
1.3	강의토픽과 일정 . . . . .	3
1.4	사전지식 . . . . .	4
1.4.1	논리(Logic)와 명제(Proposition) . . . . .	4
1.4.2	집합(Sets) . . . . .	4

## Chapter 1

# 강의소개와 사전지식

본 강좌는 정수론의 기초와 그를 이용한 작은 개인/그룹과제 해결을 통해 수학에 대한 관심과 소양을 얻기위해 만들어졌습니다. 더 중요한 목적은 실생활에서의 응용외에 하나의 철학으로 삶의 의지와 의미를 찾기위함에 있습니다.

### 1.1 이상적인 수강생 모델

강좌는 아래와 같은 조건에 해당하시는 수강생들이 공부하기에 최적화되어있습니다.

- 은퇴를 하셨거나 여유시간이 많으나 의미있는 활동을 찾기힘드신 분 중 지적 성취감을 느끼고 싶으신 분.
- 평소 수학/과학/공학에 관심이 많으신 분.
- 자극적이고 단편적인 뉴스, 유튜브등의 미디어에 중독되어 이를 극복하고자 하시는 분.
- 논리적인 사고력을 키워 토론에서 자신의 의견을 합리적으로 표현하고자 하시는 분.
- 수학을 통해 세상과 신을 이해하고 싶으신 분.

## 1.2 주의사항

본 강좌에 관한 주의사항을 아해와 같습니다.

- 정수론의 소양과 관련이 적은 주제에 대해 지나치게 엄밀한 논리가 필요한 부분은 효과적인 강의를 위해 가급적 피하겠습니다.
- 수학용어들은 영어번역을 같이 표기하겠습니다. 우리가 쓰는 한글 수학용어는 가끔 혼동을 일으키곤 합니다. 일례로 ‘소수(小數)’와 ‘소수(素數)’는 동음이의어로 한글로만 썼을때 상당한 혼란을 가져올 수 있습니다. 그리고, 차후 논문이나 원서를 읽으실때 미리 용어를 영어로 알아두시는것도 좋을꺼라 생각합니다.
- 마지막으로 가장 중요한 주의사항은 **최대한 본인들이 직접 문제를 해결 하려고 노력해야합니다.** 이것은 절대적인 요소입니다. 수학은 미디어에서 보여지는 것과 달리 실제로는 수많은 시행착오와 오랜 시간의 고민을 통해서 답을 찾을 수 있습니다. 만약 참을 수 없을 정도로 오래 노력해도 답을 얻을 수 없을때 본 강사나 동료들과의 대화에서 힌트를 얻기를 바랍니다.

## 1.3 강의토픽과 일정

본 강좌에서 공부할 토픽들을 다음과 같습니다.

- 수체계: 정수(Integers), 유리수(Rational numbers), 실수(Real Numbers), 복소수(Complex Numbers), 대수적 수(Algebraic Numbers), 초원수(Transcendental Numbers) 등.
- 연산(Operations), 모듈러 연산(Modular Arithmetic)
- 방정식(Equations), 함수(Functions)

첫 10강의는 차후 공개될 개인/그룹 프로젝트 문제들을 해결하기위해 필요한 정수론의 기본 정의(Definition)/용어(Terminology)/정리(Lemma, Proposition, Theorem)들을 공부하겠습니다.

수강생에게 부여될 프로젝트 문제들의 답은 정해진 날짜전에 강사의 이메일이나 저장소에 제출하시면 되겠습니다. 제출된 모든 답은 강사의 리뷰와 함께 모든 수강생들이 열람가능하도록 하겠습니다. 수강생 각자 수학자라고 생각하고 자신의 답에 자부심을 가지게 되었으면 합니다.

## 1.4 사전지식

### 1.4.1 논리(Logic)와 명제(Proposition)

정의를 위한 기호  $:=$  같다라는 기호  $=$

### 1.4.2 집합(Sets)

**정의 1.4.1.** 집합(Set)은 **정의할 수 있는 서로 다른 객체들의 모임**이다. 주어진 집합  $S$ 안의 각 객체  $a$ 를  $S$ 의 원소(Element)라고 부르고  $a \in S$ 라고 쓰고, 만약 어떤 객체  $b$ 가 집합  $S$ 에 속해 있지 않다면  $b \notin S$ 라고 씁니다.

어떤 객체도 없는 집합도 정의할 수 있습니다. 마치 정수에서 0처럼 말이죠. 이 특별한 집합을 공집합(Empty set)이라고 부르고 기호로는  $\{\}$  또는  $\emptyset$ 을 씁니다.

집합을 수학적으로 표기할 때의 규정은 다음과 같습니다. 만약 집합  $A$ 는 원소  $a, b, c$ 를 갖는다고 하면  $A = \{a, b, c\}$ 라고 씁니다. 자연수(Natural numbers)는 0부터 1씩 더해지는 원소들의 집합이라고 정의되고 간단히  $\mathbb{N}$ 이라고 쓰는데 이것을 위와같이 모든 원소들을 다 나열해서 쓰기는 불가능하죠? 이렇듯 원소들이 자명할때는 그냥  $\{0, 1, 2, \dots\}$ 라고 쓰기도 합니다.

자연수 중 모든 짝수들의 집합을 어떻게 표현하면 좋을까요? 물론  $\{0, 2, 4, 8, 10 \dots\}$ 이라고 쓸수있지만  $\{2a \mid a \in \mathbb{N}\}$ 라고 쓸수도 있습니다. 다시말해, 자연수 집합  $\mathbb{N}$ 의 각 원소  $a$ 에 2를 곱해서 만들어지는 수들의 집합으로 표현할 수 있습니다. 그럼, 자연수 중 모든 홀수들의 집합은 어떻게 표현할 수 있을까요? 각자 생각해봅시다.

위에서 봤듯이, 모든 집합은 원소의 갯수를 셀수있는 집합과 그렇지 않은 집합으로 분류됩니다. 전자를 유한집합(Finite set), 후자를 무한집합(Infinite set)이라고 부릅니다. 일례로  $\emptyset$ 은 원소의 갯수가 0인 유한집합, 자연수 집합  $\mathbb{N}$ 은 무한집합입니다.

**정의 1.4.2.** 집합  $A$ 의 모든 원소가 집합  $B$ 의 원소일때  $A$ 는  $B$ 의 부분집합(*Subset*)이라고 하고,  $A \subset B$  라고 씁니다.

두 집합  $A$ 와  $B$ 가 같다라는 것을 수학적으로 어떻게 정의할 수 있을까요? 한 방법은  $A$ 에서 어떤 원소  $a$ 를 꺼내서  $B$ 에서  $a$ 를 찾아서 제거하는 과정을  $A$ 안의 모든 원소에 대해 거치면 결국  $B$ 는 공집합이 된다고 할수있겠죠. 괜찮은 방법인데 좀더 생각해 보면 같은 집합에 대한 정의를 간단히 부분집합으로도 할 수 있습니다. 즉  $A \subset B$  그리고  $B \subset A$ 일때  $A = B$ 라고 정의할 수도 있겠죠?

집합들 사이에는 연산도 존재합니다. 두 집합  $A$ 와  $B$ 를 이용해 어떻게 다른 집합을 만들어낼수 있을까요? 우리가 자주 쓰는 연산들은 다음과 같습니다.

- 곱집합(Intersection):  $A \cap B := \{x \mid x \in A \text{ 그리고 } x \in B\}$
- 합집합(Union):  $A \cup B := \{x \mid x \in A \text{ 또는 } x \in B\}$
- 여집합(Difference set):  $B - A := \{x \mid x \in B \text{ 그리고 } x \notin A\}$

예를들어,  $B = \{0, 1, 2\}$ 이고  $A = \{1, 3\}$ 이라면  $A \cap B = \{1\}$ ,  $A \cup B = \{0, 1, 2, 3\}$ ,  $B - A = \{0, 2\}$  그리고  $A - B = \{3\}$ 입니다. 여기서 한가지 재밌는 점은  $A \cap B = B \cap A$ 이고  $A \cup B = B \cup A$ 이지만  $A - B$ 와  $B - A$ 는 항상 같지는 않다는 점이지요. 마치 정수들의 덧셈은 서로 항들을 교환가능하지만 뺄셈은 안되는것과 마찬가지로요.

# Bibliography

- [AF] AMS Author FAQ, <http://www.ams.org/authors/author-faq>
- [MDF] The `mdframed` package, Marco Daniel and Elke Schubert, 2013/07/01, v1.9b, <http://mirror.ctan.org/macros/latex/contrib/mdframed>
- [NDS] The `needspace` package, Peter Wilson, 2010/09/12, v1.3d, <http://mirror.ctan.org/macros/latex/contrib/needspace>
- [THT] `Thmtools` Users' Guide, Ulrich M. Schwarz, 2014/04/21 v66, <http://mirror.ctan.org/macros/latex/exptl/thmtools>