# Introduction to Number Theory

## Math 110 | Summer 2023

Xu Gao (xgao26@ucsc.edu)

June 25, 2023

UC Santa Cruz

Part

# Introduction

# General course Information

# Outcomes of this course

By the end of this course, you will be able to:

1. Familiarize yourself with fundamental concepts, ideas, and problems in number theory that play essential roles in modern mathematics.
2. Develop a deep understanding of the role of theorems, proofs, and counterexamples, and recognize their significance in mathematical reasoning.
3. Enhance your problem-solving skills through the exploration and application of various number theory techniques and strategies.
4. Cultivate the ability to communicate mathematical ideas clearly, concisely, and precisely through discussions, written assignments, and math writing practices related to number theory.
5. Acquire proficiency in using basic LaTeX formatting for mathematical notation, equations, and proofs, as it is an integral part of the course.

# What to expect in a lecture?

1. *Lectures (recorded videos)*
    - Recorded videos of the lectures will be uploaded to Canvas for students to access at their convenience. Please keep an eye on the announcement and assignments for updates.

# What to expect in a lecture?

1. *Lectures (recorded videos)*
    - Recorded videos of the lectures will be uploaded to Canvas for students to access at their convenience. Please keep an eye on the announcement and assignments for updates.
2. *Quiz*
    - Mandatory quizzes will be integrated into the lectures to assess understanding and encourage active learning.
    - Quizzes will be graded either by completion or with unlimited attempts.

# What to expect in a lecture?

1. *Lectures (recorded videos)*
   - Recorded videos of the lectures will be uploaded to Canvas for students to access at their convenience. Please keep an eye on the announcement and assignments for updates.
2. *Quiz*
   - Mandatory quizzes will be integrated into the lectures to assess understanding and encourage active learning.
   - Quizzes will be graded either by completion or with unlimited attempts.
3. *Supplementary Materials*
   - Historical notes, terminology explanations, online resources, and additional content that may not be fully covered in the lecture.
   - You are encouraged to explore these materials and use them as references in your assignments, exams, and essays.

## After-class Studies?

1. *Glossary*
    - Throughout the course, you will maintain a glossary of terms and results that you find difficult to digest or wish to remember.
    - Add your thoughts on them, and whenever possible, include examples as well.
    - Submit your glossary as a PDF file to Gradescope before the Final week.
    - The glossary can be used as an index to resources for solving exam problems.

# After-class Studies?

1. *Glossary*
2. *Exercises*
    - Attached to each lecture and some supplementary notes, there will be short questions named exercises for practice and self-assessment.
    - Exercises are not mandatory: they will not be collected or graded.
    - However, they are highly recommended as they help reinforce understanding of lecture topics and practice important methods.
    - The difficulty of exercises is between quizzes and homework problems.

# After-class Studies?

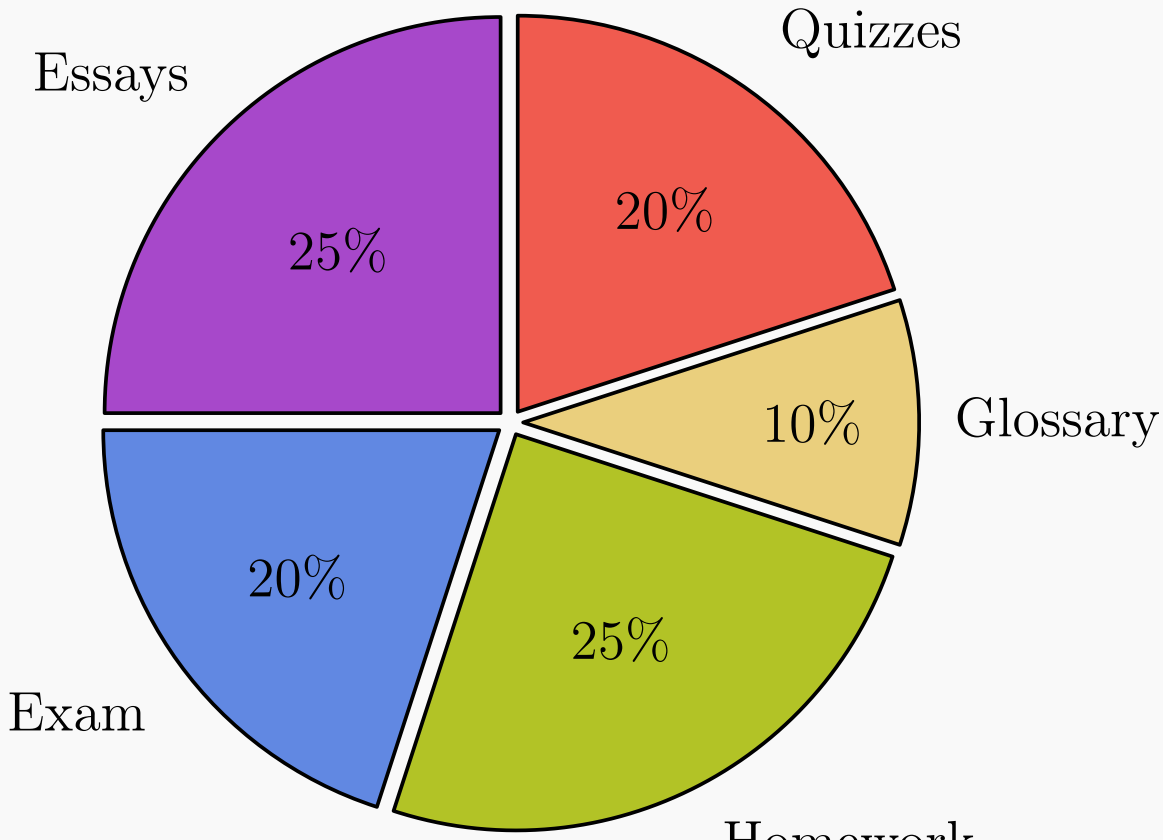
1. *Glossary*
2. *Exercises*
3. *Homework*
    - There will be a total of four weekly homework assignments.
    - Collaborative discussions with peers are encouraged. However, you must write the solutions in your own words and acknowledge collaborators.
    - Homework is expected to be typed using LaTeX.
    - Pay close attention to clear and well-reasoned writing.
    - References used in homework answers should be listed (either manually or using BibTeX). Immediate problem-solving resources should be avoided.
    - Submissions should be compiled into a PDF file and uploaded to Gradescope.

# Exam and Essay

- There will be one take-home `Final Exam`.
    - The final exam will consist of approximately 6–8 problems and is estimated to take around 3–4 hours to complete.
    - It will be released at the beginning of the last week and due at the end of the session.
    - Only results (theorems/lemmas/propositions/examples) provided during the lectures or in the homework are allowed for reference.
    - Solutions should be handwritten on the exam paper. You can upload either a scanned copy or an annotated PDF file.
    - Before submitting the final exam, ensure that your solutions are well-reasoned, and your writing is clear and legible.
    - If you have any questions, please reach out to me or the TA for assistance.

- There will be one take-home `Final Exam`.
- `Essay`
  - In the middle of the course, you will be provided with a sample essay. Your task is to complete it by filling in the missing steps or details.
  - Afterward, you need to choose a topic related to number theory and write your own essay, following the format of the provided sample.
  - Essays are expected to be typed using LaTeX.
  - The purpose of the essay is to practice mathematical writing. While originality is not a requirement, it is essential to adhere to academic integrity, write clearly, and acknowledge collaboration and references.

The grade will be based on five parts:



# What is this course about?

# What is this course about?

Number theory studies “Numbers”.

Number theory studies "Numbers".

- Natural numbers $\mathbb{N} = \{0, 1, 2, \cdots\}$ "Natural"
  Used for counting and ordering on finite sets.
  - Hence, you should expect properties of natural numbers are closely related to those of finite sets. $\rightsquigarrow$*Combinatorics*

  Our natural numbers will include $0$.
  - Therefore, it will have a *neutral element* for both addition and multiplication.

Number theory studies "Numbers".

- Natural numbers $\mathbb{N} = \{0, 1, 2, \cdots\}$ "Natural"
- Integers $\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$ "Zahlen"
  This is the set of numbers we will mostly focus on.
  - The subset of positive integers will often be used. We will denote it by $\mathbb{Z}_+$. Be aware that it is different from $\mathbb{N}$.
  - The tuple $(\mathbb{Z}, +, \cdot, 0, 1)$ forms a *ring*.

# What is this course about?

Number theory studies "Numbers".

- Natural numbers $\mathbb{N} = \{0, 1, 2, \cdots\}$ "Natural"
- Integers $\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$ "Zahlen"
- Rational numbers $\mathbb{Q} = \left\{ \frac{a}{b} \,\middle|\, a, b \in \mathbb{Z}, b \neq 0 \right\}$ "Quotient"
  These numbers arise from the *quotient* operation on integers.
  - The terminology *rational* refers to the fact that a rational number represents a ratio of two integers.
  - There are important quantities that are not rational. For example, $\sqrt{2}$, the diagonal length of a unit square; or $\pi$, the ratio of a circle's circumference to its diameter.

Number theory studies "Numbers".

- Natural numbers $\mathbb{N} = \{0, 1, 2, \cdots\}$ "Natural"
- Integers $\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$ "Zahlen"
- Rational numbers $\mathbb{Q} = \left\{\frac{a}{b} \,\middle|\, a, b \in \mathbb{Z}, b \neq 0\right\}$ "Quotient"
- Real numbers $\mathbb{R}$ "Real"
  They are numbers with a decimal representation.
  - Technically, $\mathbb{R}$ is built from $\mathbb{Q}$ through a *completion* process.
  - They are the numbers used for measurement.

Number theory studies "Numbers".

- Natural numbers $\mathbb{N} = \{0, 1, 2, \cdots\}$ "Natural"
- Integers $\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$ "Zahlen"
- Rational numbers $\mathbb{Q} = \left\{\frac{a}{b} \,\middle|\, a, b \in \mathbb{Z}, b \neq 0\right\}$ "Quotient"
- Real numbers $\mathbb{R}$ "Real"
- Complex numbers $\mathbb{C} = \left\{a + b\sqrt{-1} \,\middle|\, a, b \in \mathbb{R}\right\}$ "Complex"
  - This is an *algebraic closed field*: every polynomial with complex coefficients has a complex root.
  - Among complex numbers, there are *algebraic ones*, which serves as a root of an integer polynomial; and there are *transcendental ones*, which is never a root of an integer polynomial.

Number theory studies "Numbers".

- Natural numbers $\mathbb{N} = \{0, 1, 2, \cdots\}$ "Natural"
- Integers $\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$ "Zahlen"
- Rational numbers $\mathbb{Q} = \left\{\frac{a}{b} \,\middle|\, a, b \in \mathbb{Z}, b \neq 0\right\}$ "Quotient"
- Real numbers $\mathbb{R}$ "Real"
- Complex numbers $\mathbb{C} = \left\{a + b\sqrt{-1} \,\middle|\, a, b \in \mathbb{R}\right\}$ "Complex"
- *$p$-adic numbers* $\mathbb{Q}_p$
  They are made with rational numbers through a different *completion* process from that of $\mathbb{R}$.

Number theory studies "Numbers".

- Natural numbers $\mathbb{N} = \{0, 1, 2, \cdots\}$ "Natural"
- Integers $\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$ "Zahlen"
- Rational numbers $\mathbb{Q} = \left\{\frac{a}{b} \,\middle|\, a, b \in \mathbb{Z}, b \neq 0\right\}$ "Quotient"
- Real numbers $\mathbb{R}$ "Real"
- Complex numbers $\mathbb{C} = \left\{a + b\sqrt{-1} \,\middle|\, a, b \in \mathbb{R}\right\}$ "Complex"
- *$p$-adic numbers* $\mathbb{Q}_p$
- *etc.*

Topics in Number Theory:

- Diophantine equations

  They are equations in multiple unknowns and the interesting solutions are in a given set of numbers.

Topics in Number Theory:

- Diophantine equations

  They are equations in multiple unknowns and the interesting solutions are in a given set of numbers.

  - The equation $x + y = 1$ has infinitely many integer solutions, while $2x + 2y = 1$ has no integer solutions.
    $\rightsquigarrow$ *Linear Diophantine equation*.

## What is this course about?

Topics in Number Theory:

- Diophantine equations

  They are equations in multiple unknowns and the interesting solutions are in a given set of numbers.

  - The equation $x + y = 1$ has infinitely many integer solutions, while $2x + 2y = 1$ has no integer solutions.
    $\rightsquigarrow$ *Linear Diophantine equation*.
  - The equation $x^2 + y^2 = 1$ has infinitely many rational solutions. They form *rational points* on the unit circle and are given by *Pythagorean triples*.
    $\rightsquigarrow$ *Rational points in arithmetic geometric objects*.

Topics in Number Theory:

- Diophantine equations

  They are equations in multiple unknowns and the interesting solutions are in a given set of numbers.

  - The equation $x + y = 1$ has infinitely many integer solutions, while $2x + 2y = 1$ has no integer solutions.
    $\rightsquigarrow$ *Linear Diophantine equation*.
  - The equation $x^2 + y^2 = 1$ has infinitely many rational solutions. They form *rational points* on the unit circle and are given by *Pythagorean triples*.
    $\rightsquigarrow$ *Rational points in arithmetic geometric objects*.
  - Solutions of $y^2 = x^3 + ax + b$. $\rightsquigarrow$ *Elliptic curves*.

# What is this course about?

Topics in Number Theory:

- Diophantine equations

  They are equations in multiple unknowns and the interesting solutions are in a given set of numbers.
- Prime numbers

  They are basic building blocks of integers. The study of prime numbers is therefore crucial.

Topics in Number Theory:

- Diophantine equations

  They are equations in multiple unknowns and the interesting solutions are in a given set of numbers.
- Prime numbers

  They are basic building blocks of integers. The study of prime numbers is therefore crucial.
  - Distribution of prime numbers.

    An important result is the *Prime Number Theorem*.

    *Gaps between primes*, *infinitude of a certain type of primes* are also important topics.

# What is this course about?

Topics in Number Theory:

- Diophantine equations
  They are equations in multiple unknowns and the interesting solutions are in a given set of numbers.
- Prime numbers
  They are basic building blocks of integers. The study of prime numbers is therefore crucial.
  - Distribution of prime numbers.
    An important result is the *Prime Number Theorem*.
    *Gaps between primes, infinitude of a certain type of primes* are also important topics.
  - Applications such as the *RSA crypto system*.

# What is this course about?

Topics in Number Theory:

- Diophantine equations

  They are equations in multiple unknowns and the interesting solutions are in a given set of numbers.
- Prime numbers

  They are basic building blocks of integers. The study of prime numbers is therefore crucial.
- Transcendence/constructability

  Related to questions asking whether a certain construction is possible.

Topics in Number Theory:

- Diophantine equations

  They are equations in multiple unknowns and the interesting solutions are in a given set of numbers.
- Prime numbers

  They are basic building blocks of integers. The study of prime numbers is therefore crucial.
- Transcendence/constructability

  Related to questions asking whether a certain construction is possible.
  - *Square a circle*: can there be a square with area $\pi$?

# What is this course about?

Topics in Number Theory:

- Diophantine equations

  They are equations in multiple unknowns and the interesting solutions are in a given set of numbers.

  $\rightsquigarrow$ Solve Diophantine equations.
- Prime numbers

  They are basic building blocks of integers. The study of prime numbers is therefore crucial.

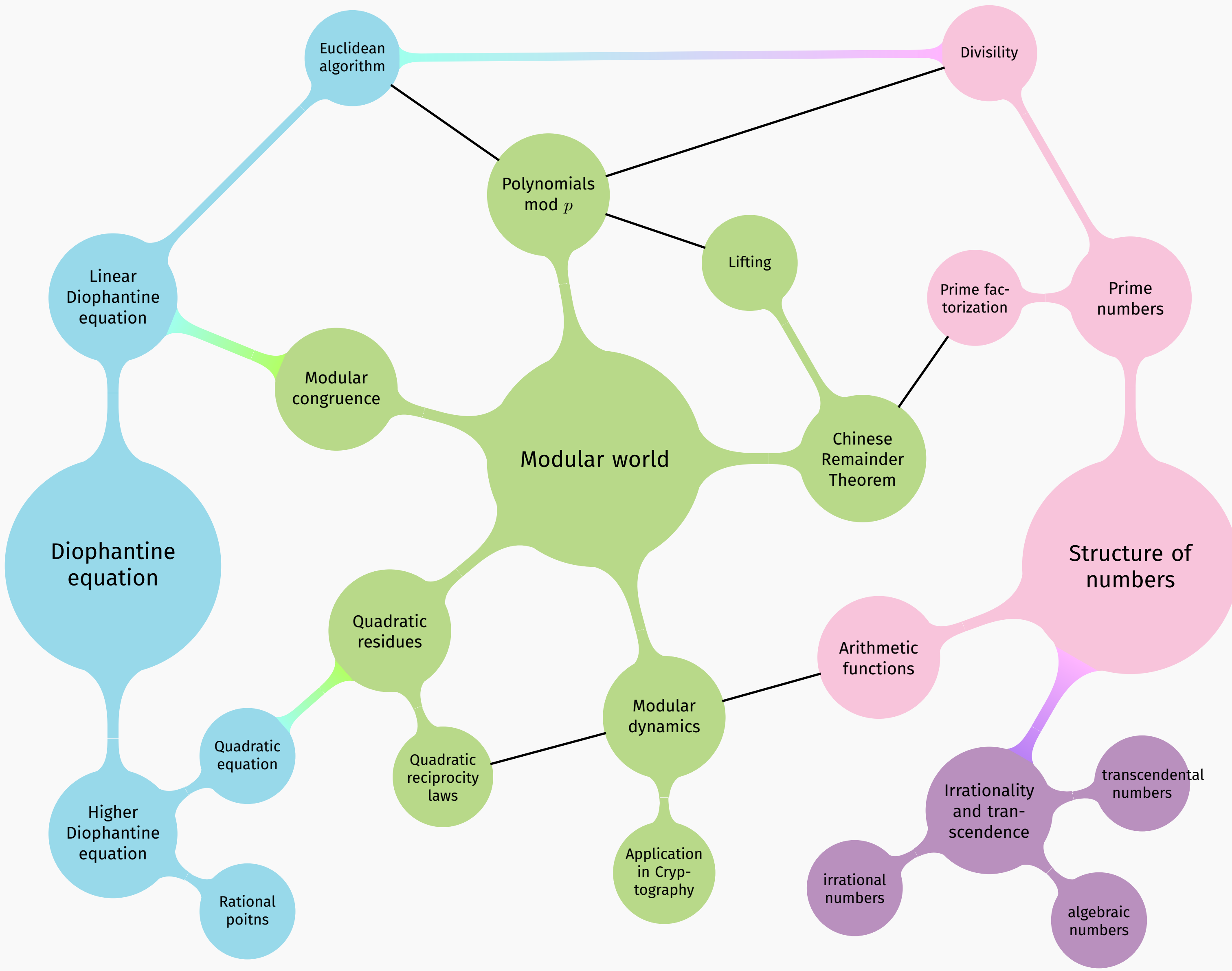
  $\rightsquigarrow$ Understand the structure of numbers.
- Transcendence/constructability

  Related to questions asking whether a certain construction is possible.

  $\rightsquigarrow$ Prove impossibility.

# Structure of this course

# Structure of this course

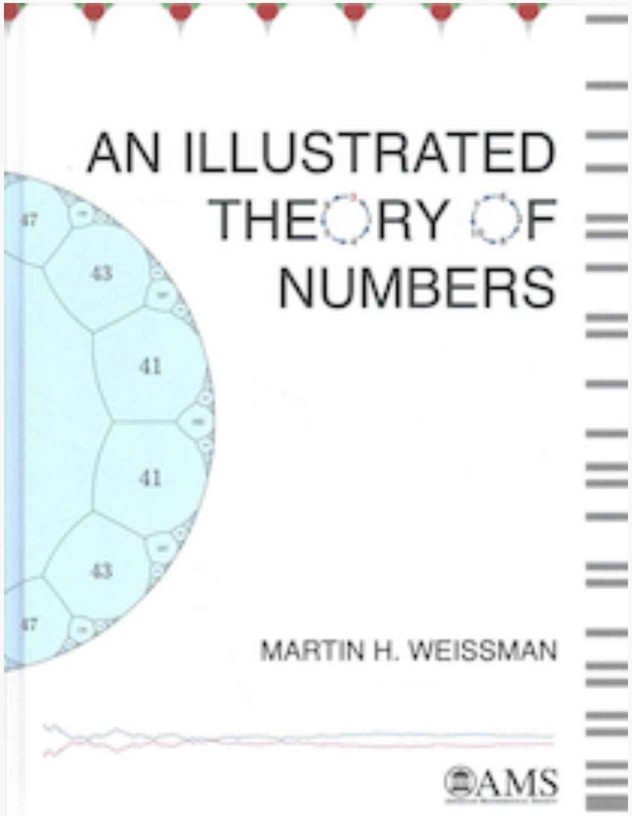


# Textbook and useful resources

We will follow
*An Illustrated Theory of Numbers*
by Martin H. Weissman,
focusing on Chapters 1 - 8.

Online recourses:

- Overleaf: an online LaTeXeditor with a wealth of documentations.
- Proofwiki: a wiki of proofs.
- Math.stackexchange: a question and answer site for people studying math.



<table>
<tr><th>Week</th><th>Topic</th><th>Textbook</th></tr>
<tr><td rowspan="2">Week 1</td><td>Linear Diophantine Equations</td><td>Chapter 0 – 1</td></tr>
<tr><td rowspan="2">Prime Numbers</td><td rowspan="2">Chapter 2</td></tr>
<tr><td rowspan="2">Week 2</td></tr>
<tr><td>Rational and Algebraic Numbers</td><td>Chapter 3</td></tr>
<tr><td>Week 3</td><td rowspan="2">The Modular Worlds and Modular Dynamics</td><td rowspan="2">Chapter 5 – 6</td></tr>
<tr><td rowspan="2">Week 4</td></tr>
<tr><td>Assembling Modular Worlds</td><td>Chapter 7</td></tr>
<tr><td>Week 5</td><td>Quadratic residues</td><td>Chapter 8</td></tr>
</table>