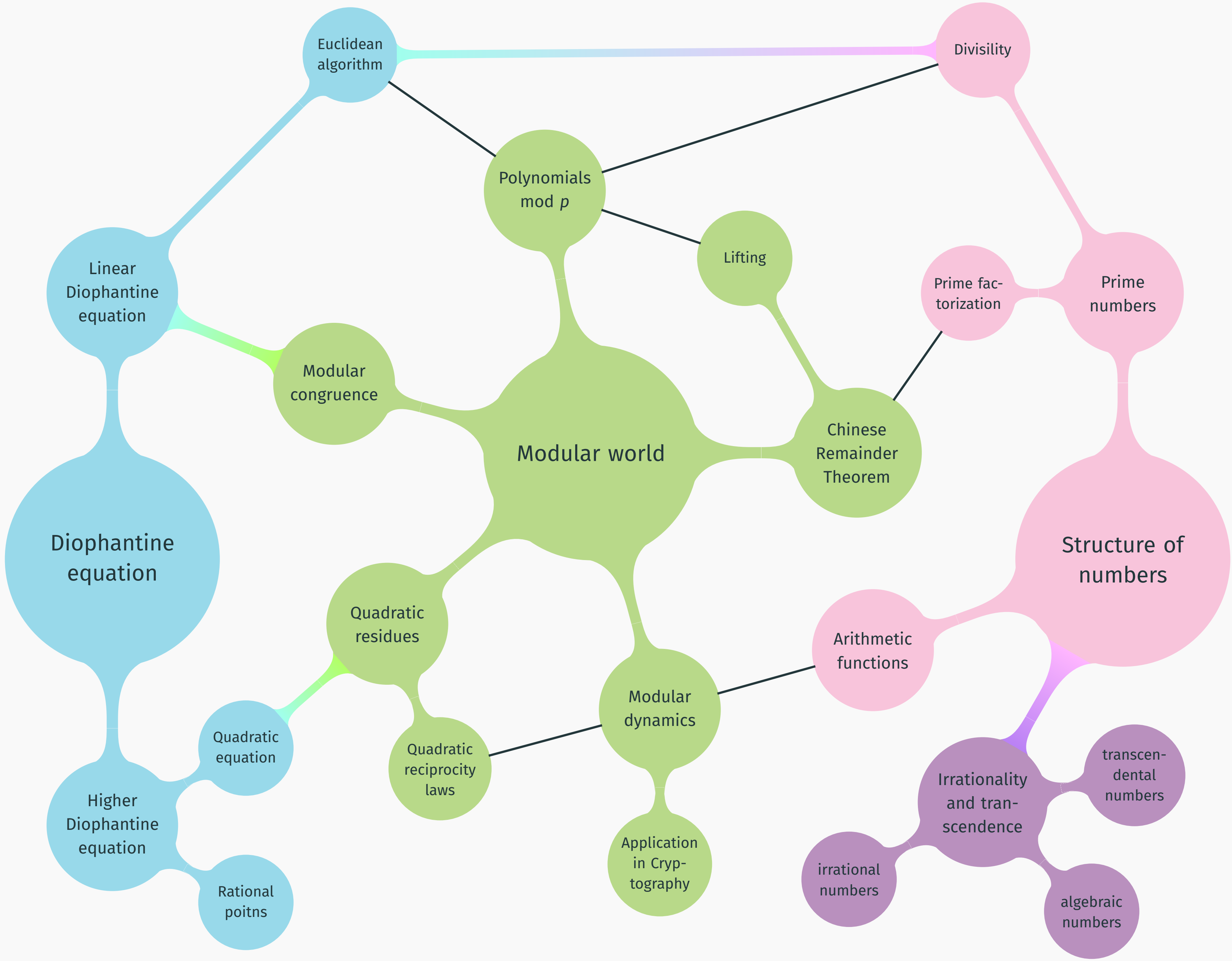
Introduction to Number Theory

Math 110 | Winter 2023

Xu Gao

March 13, 2023


Euclidean algorithm
Divisility
Polynomials mod p
Lifting
Linear Diophantine equation
Prime factorization
Prime numbers
Modular congruence
Modular world
Chinese Remainder Theorem
Diophantine equation
Structure of numbers
Quadratic residues
Arithmetic functions
Modular dynamics
Quadratic equation
Quadratic reciprocity laws
Irrationality and transcendence
transcendental numbers
Higher Diophantine equation
Application in Cryptography
irrational numbers
Rational poitns
algebraic numbers

Further Readings

Congratulations on finishing your introductory course in number theory!

If you’re interested in exploring this fascinating subject further, here are some possible readings suggestions.

Textbooks on Number Theory

First, I would suggest you to finish our **textbook** before moving to the next one. We have covered a lot of its content but not all.

Next, you need knowledge from **abstract algebra** and **complex analysis**. These subjects should be mastered before reading further textbooks.

After that, I would suggest:

- ***A Course in Arithmetic*** by Jean-Pierre Serre. This is a concise introduction to some important topics in number theory. A highly readable masterpiece. (*Second Textbook*)

Textbooks on Number Theory

- ***Introduction to Modern Number Theory: Fundamental Problems, Ideas and Theories*** by Yuri I. Manin and Alexei A. Panchishkin. This is a comprehensive survey of modern number theory, motivated by elementary problems, exposing central ideas of various theories very well. (*Reference Book*)
- ***An Introduction to the Theory of Numbers*** by G.H. Hardy and E.M. Wright. It is a classic, suitable for who want more training on number theory traditionally. (*Complementary advanced textbook*)

We have covered Quadratic Reciprocity Laws in the course and now know how to detect quadratic residues. However, it remains to have a system treatment of ***solving*** modular quadratic equations. This leads to the theory of ***Quadratic Forms***.

Definition 25.1

A ***quadratic form*** is a homogeneous polynomial of degree two in several variables.

The theory of quadratic forms studies their properties, including their representations by other quadratic forms and their values over different rings.

Quadratic Forms

Chapter 9–11 of the textbook is an interesting elementary approach to this topic. For further study, a possible roadmap is:

- Learn the basic definitions and examples of quadratic forms.
- Learn how to **classify** quadratic forms.
- Learn how to **diagonalize** a quadratic form or translate between different forms (**standard** form, **factored** form, and **vertex** form).
- Explore advanced topics such as the **Siegel mass formula** and the connections between quadratic forms and other objects (**lattices**, **modular forms**, **theta functions**, **elliptic curves** etc.).

Geometry of Numbers

You have seen a lot of examples about how a geometric interpretation can help us to solve arithmetic problems. There are two main subjects arising from such an idea.

One is called the ***geometry of numbers***. It studies the geometry of lattices in Euclidean space and its applications to number theory. Our proof of Dirichlet's approximation theorem can also be viewed as a one-dimensional version of such methods. You can take a look at pp. 200–201 on the textbook to see one 2-dimensional example.

A possible roadmap for further study is:

- Learn what a **lattice** is and how to define its **basis**, **rank**, **determinant** and **volume**.
- Learn how to measure the **density** and **distribution** of lattice points, the concept of a **fundamental domain**, and study the **Minkowski embedding theorem**.
- Explore topics such as the **lattice point counting problem**, the **geometry of continued fractions**, and the connection between the geometry of numbers and **Diophantine approximation**.

Algebraic Numbers

There are other number systems sharing similar properties with $\mathbb{Z}$. ***Gaussian integers*** and ***Eisenstein integers***, which are covered in Chapter 4 of the textbook, are two such examples. We can use similar methods to study them. Generally, these systems arise as ***integral rings*** of ***algebraic numbers***.

Recall that algebraic numbers are numbers that satisfy a polynomial equation with integer coefficients. These integral rings arise from our original ring of integers through ***integral extensions*** and the ***Galois theory***.

Algebraic Numbers

A main branch of modern number theory is ***Algebraic Number Theory***. It used to mean the study of algebraic numbers and nowadays means to study arithmetic problems using methods from abstract algebra.

A possible roadmap to approach this subject is:

- Build some **intuitions** through the examples of rational integers, Gaussian integers, Eisenstein integers, and more crucially, some bad behaved examples such as $\mathbb{Z}[\sqrt{-5}]$.
- Learn basic concepts of **abstract algebra** such as **groups**, **rings**, **fields**, **homomorphisms** and **ideals**.

Algebraic Numbers

- Specialize your knowledge from abstract algebra to **number fields**. Learn about their properties such as **degree**, **discriminant**, **norm** and **trace**. Learn about the **ring of integers** in a number field, the **factorization of ideals**, the behavior of **primes**, and the **ideal class group**.
- Learn about some special classes of number fields such as **quadratic fields**, **cyclotomic fields** and **Galois extensions**.
- Explore some applications of algebraic number theory such as **Fermat's last theorem** and **class field theory**.

Books on Algebraic Number Theory

Here are some textbook on algebraic number theory (should be read after your Second Textbook on number theory):

- ***Basic Number Theory*** by A Weil. It is classic but maybe difficult.
- ***Algebraic Number Theory*** by Cassels and Froehlich. It is not a textbook but rather a collection of short courses written by various great mathematicians.
- ***Algebraic Number Theory*** by S. Lang. Well-written, accessible, and comprehensive.
- ***Algebraic Number Theory*** by J. Neukirch. A very extensive and geometric approach.

Analytic Number Theory

Another main branch of modern number theory is ***Analytic Number Theory***. It means to use methods from analysis to study arithmetic problems. It can be mainly divides into two major parts:

- ***Multiplicative number theory***, which deals with the distribution of the prime, including **prime number theorem, primes in specific progressions**. A remarkably important problem is the ***Riemann Hypothesis***.
- ***Additive number theory***, which is concerned with the additive structure of integers. Two classical problems are ***Goldbach's conjecture***, that every even number greater than 2 is the sum of two primes, and ***Waring's problem***, which asks whether every natural number is the sum of certain number of powers.

A possible roadmap to this subject is:

- Learn ***Complex Analysis***, including topics such as **conformal mappings**, **Cauchy's theorem and formula**, **poles and residues**, and **analytic continuation**.
- Learn basic properties of ***Dirichlet Series***, such as their **convergence** and the **Euler product formula**.
- Learn basics of ***zeta functions***, such as the **functional equation** and **special values**.
- Learn how to prove **prime number theorem** and **Dirichlet's theorem on primes in arithmetic progressions**.

Books on Analytic Number Theory

Here are some textbook on analytic number theory:

- ***Introduction to Analytic Number Theory*** by Apostol. A classic textbook for undergraduates. (textbook)
- ***Problems in Analytic Number Theory*** by Murty. Well-organized theory and problems guiding students through the most important areas of analytic number theory.
- ***Multiplicative Number Theory*** by Davenport.
- ***Additive Number Theory*** by Nathanson.

After Analytic Number Theory

After analytic number theory, you can explore topics such as:

- ***Transcendental Number Theory***, which investigates the **transcendental numbers**. **Diophantine approximation** and **transcendence measure** are major topics in this field. One big open problem is ***Schanuel's conjecture***.
- ***Modular Forms***, which are analytic functions with remarkable properties. It is related to many important topics such as **congruence subgroups**, **elliptic curves**, **Hecke operators**, and **L-functions**.
- Then ***Automorphic Forms*** and ***Langlands Program***.

Books on Those Topics

- ***Transcendental Numbers*** by Murty and Rath.
- ***A First Course in Modular Forms*** by Diamond and Shurman.
- ***Automorphic Forms and Representations*** by Bump.
- ***An Introduction to the Langlands Program*** by J. Bernstein and S. Gelbart.
- And also found in textbooks of algebraic number theory.

Arithemtic Geometry

Another subject arising from interpreting arithmetic into geometry is ***Arithmetic Geometry***. It studies the geometric properties of Diophantine equations.

A possible roadmap to approach this topic is:

- Learn about **number fields**, **class field theory**, and **Galois representations** from a book like
  - ***Algebraic Number Theory*** by S. Lang.
  - ***Algebraic Number Theory*** by J. Neukirch.
- Learn about **schemes** and their **cohomology** from a book like
  - ***Algebraic Geometry and Arithmetic Curves*** by Liu,
  - ***Algebraic Geometry*** by Hartshorne,
  - ***The Rising Sea: Foundations of Algebraic Geometry*** by Ravi Vakil.

readable!

- Learn about **elliptic curves**, **modular forms**, and *L*-**functions** from a book like
  - ***The Arithmetic of Elliptic Curves*** by Silverman,
  - ***A First Course in Modular Forms*** by Diamond and Shurman,
  - ***Advanced Topics in the Arithmetic of Elliptic Curves*** by Silverman.
- Learn about *p*-**adic analysis** from a book like
  - *p*-***adic Numbers,*** *p*-***adic Analysis, and Zeta-Functions*** by Neal Koblitz. textbook
  - ***Non-Archimedean Analysis: A Systematic Approach to Rigid Analytic Geometry*** by S. Bosch, U. Güntzer, R. Remmert. Big Book
  - ***Local Fields*** by Jean-Pierre Serre.

    a short book !

Arithemtic Geometry

- Learn about **Arakelov Geometry**:
  - ***Lectures on Arakelov Geometry*** by Mumford et al.
  - ***Arakelov Geometry and Diophantine Applications*** by E. Peyre, and G. Rémond.
- Learn about **Etale cohomology**:
  - ***Etale Cohomology*** by James Milne.
  - ***Etale Cohomology*** by Lei Fu. detailed
- After above, you should have enough knowledge to delve into a specific area. **Enjoy your journey!**