Introduction to Number Theory

Math 110 | Winter 2023

Xu Gao

January 9, 2023

General course Information

Who teach this course?

Instructor:	Xu Gao (xgao26@ucsc.edu)
Lecture time:	MWF 4:00 PM - 5:05 PM
Location:	Engineer 2 194
Office Hours:	MW 2:30 – 3:30 PM or by appointment
Location:	McHenry Library 1292 or remote
Teaching Assistant:	Changhan Zou (czou3@ucsc.edu)
Discussion Section A:	Friday 9:20 AM - 10:25 AM
Discussion Section B:	Tuesday 1:20 PM - 2:25 PM
Location:	McHenry Clrm 1279

Check Canvas and the course website[1] for detailed syllabus.

[1] https://gausyu.github.io/Teaching/Winter-2023

Outcomes of this course

- Familiarize Ideas and problems in number theory that play essential roles in modern mathematics.
- Understand the roles of theorems, proofs, and counterexamples.
- Develop problem-solving skills.
- Practice clear, concise, and precise mathematical writing.

+ You will need basic LaTeX for this course.

What to expect in a lecture?

1. `Attendance form`
    - The lectures are mandatory, so there will be an attendance record. According to the course schedule, there will be 26 lectures besides this one. Please attend all of them.
    - At the beginning of a lecture, you will see a QR code. Scan it to complete the attendance form. This is also the place to submit your quiz answer (if there is a quiz). You can also use this form to give your feedback to this lecture. The QR code will appear again at the end of the lecture.
    - If you cannot attend, please contact me before the lecture to avoid lack of attendance record.

What to expect in a lecture?

1. `Attendance form`
2. `Lecture`
    - The lecture will be recorded and automatically uploaded to Canvas. You can find it at the YuJa page.
    - The lecture note will be uploaded with an announcement of your after-class learning material and suggestions.

What to expect in a lecture?

1. `Attendance form`
2. `Lecture`
3. `Quiz`
    - There may be quizzes during the lecture.
    - You may or may not be asked to submit your answer with the attendance form.
    - Quizzes will not be graded.

What to expect in a lecture?

1. `Attendance form`
2. `Lecture`
3. `Quiz`
4. `Off-topic remarks`
    - They are either historical notes or terminology explanation.

What to expect in a lecture?

1. `Attendance form`
2. `Lecture`
3. `Quiz`
4. `Off-topic remarks`
5. `Responds to questions.`
    - I will give you several times to ask questions during a lecture.

After-class Studies?

1. `After-class reading`
    - Material relevant to the lecture, content in textbook not fully covered in the lecture, and some online resources.
    - Will appear in the announcement of lecture notes.

After-class Studies?

1. `After-class reading`
2. `Homework`
    - Due ***every week***. Request of extensions must before the due date.
    - You are encouraged to ***discuss*** the problems with your peers. However, you must write the homework ***by yourself*** using your words and ***acknowledge your collaborators***.
    - Pay close attention to the presentation and the clarity of your reasoning. This course is writing-intensive.
    - List the ***references*** you have used in your answer. You should avoid using resources that solve the problem immediately.
    - The homework is expected to be typed using ***LaTeX***.
    - To submit the homework, navigate to the Homework page and upload the ***compiled PDF*** file (not the .tex file) to Gradescope.

After-class Studies?

1. After-class reading
2. Homework
3. Exercises
    - Short questions related to the lecture, easier than homework and exam but may be harder than quizzes.
    - Exercises are not mandatory. So you do not need to submit them.
    - But they are highly recommended because:
    - They can help you better understand the topics in lecture, familiarize the concepts, and practice important methods.

After-class Studies?

1. `After-class reading`
2. `Homework`
3. `Exercises`
4. `Glossary`
    - 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.
    - The glossary can be typed or handwritten, long or short, but it ***cannot be empty***.
    - Share your glossary every month. To do this, navigate to the Glossary page and upload a ***PDF*** file to Gradescope.
    - You can use the glossary as an index to resources you need to solve problems in exams.

Grade

- The grade will be based on two parts:
  - Classwork and Homework (50 %)
  - Exams (50 %)
- We will use a grading scheme considering both the overall course statistics and individual responsibility.
- To pass the course, your grade should be at least C.

Midterm and Final

- General rules:
  - Exams will be in person.
  - You can use your notes, homework, glossary, and textbook during the exams. But you **cannot discuss** the problems with others.
  - The only results (theorems/lemmas/propositions) you're allowed to use are either provided during the lectures or in the homework.
- Midterms:
  - Monday, January 30, 4:00-5:00 p.m.
  - T~~BD~~, 4:00-5:00 p.m. Mon Feb 27.

  lower one will be dropped.
- Final:
  - Thursday, March 23, 12:00-3:00 p.m.

What is this course about?

What is this course about?

Number theory studies “Numbers”.

What is this course about?

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.

$\forall a \in \mathbb{N} : a + 0 = 0 + a = a$ $\quad \underline{0}$ for $+$

$\forall a \in \mathbb{N} : a \cdot 1 = 1 \cdot a = a$ $\quad \underline{1}$ for $\cdot$

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"
  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***.

add mult

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 π, the ratio of a circle's circumference to its diameter.

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"
- 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.

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”
- 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.

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"
- 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 $\mathbb{R}$.

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"
- 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.***

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.

  e.g. $\mathbb{Z}$ or $\mathbb{Q}$

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.

  $(n, 1-n)$

  - The equation $x + y = 1$ has infinitely many integer solutions, while $2x + 2y = 1$ has no integer solutions.

    ⇝ ***Linear Diophantine equation***.

    4

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***.

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***.
  - 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.

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.

$\#\{\text{prime} \leq x\} \sim \frac{x}{\log x}$

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.

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.
  - ***Square a circle***: can there be a square with area π? No!

    $\sim \pi$ is trans...

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.

  ⇝ Solve Diophantine equations.
- Prime numbers

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

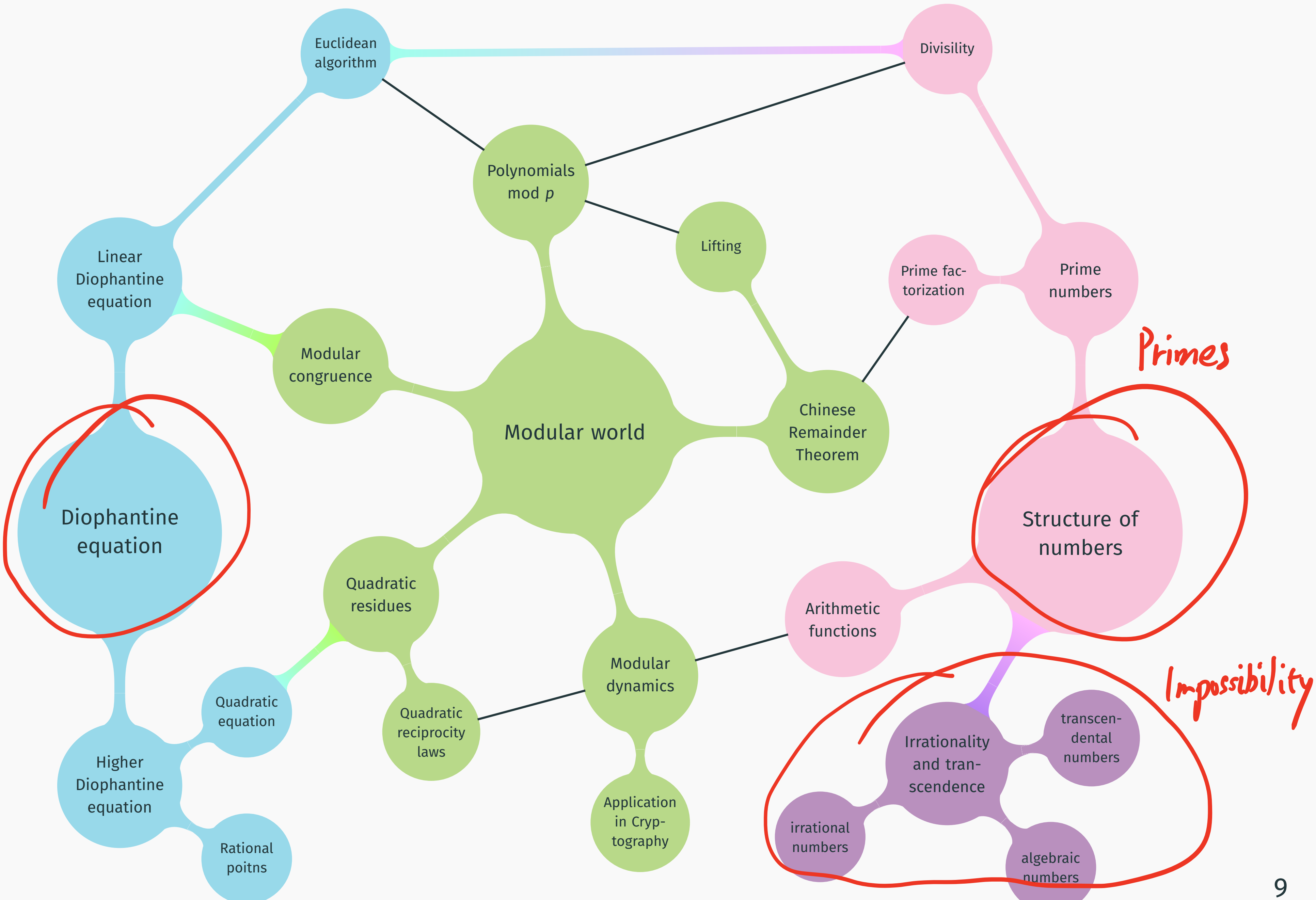
  ⇝ Understand the structure of numbers.
- Transcendence/constructability

  Related to questions asking whether a certain construction is possible.

  ⇝ Prove impossibility.

Structure of this course

Structure of this course

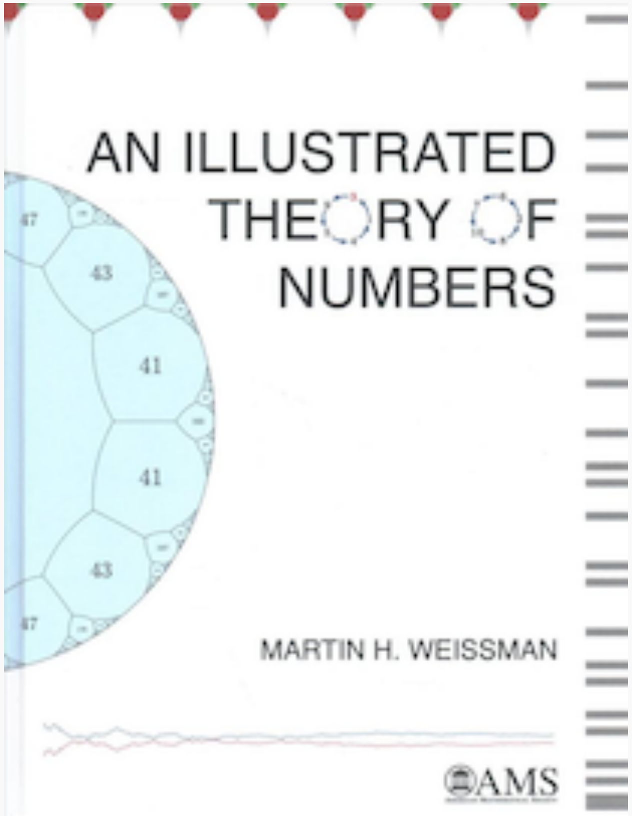


Textbook and useful resources

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

Online recourses:

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



Tentative plan of lectures

Week	Topic	Textbook
Week 1	Linear Diophantine Equations	Chapter 0–1
Week 2 Week 3	Prime Numbers	Chapter 2
Week 4	Rational and Algebraic Numbers	Chapter 3
Week 5 Week 6 Week 7	Modular Worlds and Modular Dynamics	Chapter 5–6
Week 8	Assembling Modular Worlds	Chapter 7
Week 9 Week 10	Quadratic Residues	Chapter 8

Part I

Linear Diophantine Equations

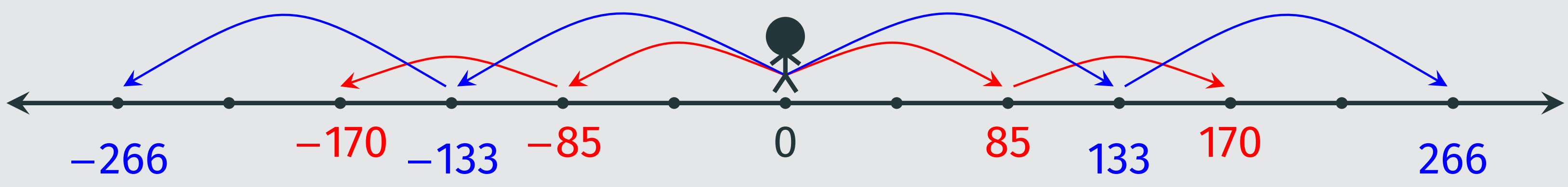
A motivating example

A motivating example

Question

Suppose you are standing at 0 on the number axis and you're allowed to

- **hop** *133 steps left (-133) or right (+133)*
- **skip** *85 steps left (-85) or right (+85)*



Can you hop x-many times and skip y-many times to get to 1?

A motivating example

- For example, hopping twice to the right and skipping thrice to the left gets you

$$2 \cdot \overset{\text{hop}}{133} + (-3) \cdot \overset{\text{skip}}{85} = 266 - 255 = 11$$

A motivating example

- For example, hopping twice to the right and skipping thrice to the left gets you

$$(+2) \cdot 133 + (-3) \cdot 85 = 266 - 255 = 11$$

- If you can hop x-many times and skip y-many times to get to 1, then you can hop xz-many times and skip yz-many times to get to z for any integer $z \in \mathbb{Z}$.

$$x \cdot 133 + y \cdot 85 = 1$$

multi by z

$$xz\,133 + yz\,85 = z$$

A motivating example

- For example, hopping twice to the right and skipping thrice to the left gets you

$$(+2) \cdot 133 + (-3) \cdot 85 = 266 - 255 = 11$$

- If you can hop x-many times and skip y-many times to get to 1, then you can hop xz-many times and skip yz-many times to get to z for any integer $z \in \mathbb{Z}$.
- The answer is ***Yes***. We can solve this problem using ***(Euclidean) Division Algorithm***.

"$x \cdot 133 + y \cdot 85 = 1$"

(Euclidean) division algorithm

(Euclidean) division algorithm

1. Start with two positive integers a, b, assume $a \geq b$.
2. Divide a by b

   quotient remainder

$$a = q \cdot b + r, \quad 0 \leqslant r < b, \quad q \in \mathbb{Z}.$$

3. If $r = 0$, ***halt***. Otherwise, repeat the previous steps with the pair (a, b) replaced by (b, r).
4. Continue until your remainder is 0, this process will terminate in finite steps. Output the last nonzero remainder.

(Euclidean) division algorithm

Now, we apply the (Euclidean) Division Algorithm to our example.

$$
\begin{aligned}
133 &= (1) \cdot 85 + 48 \\
85 &= (1) \cdot 48 + 37 \\
48 &= (1) \cdot 37 + 11 \\
37 &= (3) \cdot 11 + 4 \\
11 &= (2) \cdot 4 + 3 \\
4 &= (1) \cdot 3 + 1 \longrightarrow \text{outputs} \\
3 &= (3) \cdot 1 + \underline{\underline{0}}
\end{aligned}
$$

(Euclidean) division algorithm

Now, we apply the (Euclidean) Division Algorithm to our example.

$$
\begin{aligned}
133 &= (1)\cdot 85 + 48 \\
85 &= (1)\cdot 48 + 37 \\
48 &= (1)\cdot 37 + 11 \\
37 &= (3)\cdot 11 + 4 \\
11 &= (2)\cdot 4 + 3 \\
4 &= (1)\cdot 3 + 1 \\
3 &= (3)\cdot 1 + 0
\end{aligned}
$$

$$
\begin{aligned}
1 &= 4 + (-1)\cdot 3 \\
&= 4 + (-1)\cdot (11 - 2\cdot 4) \\
&= (-1)\cdot 11 + (3)\cdot 4 \\
&= (-1)\cdot 11 + (3)\cdot (37 - 3\cdot 11) \\
&= (3)\cdot 37 + (-10)\cdot 11 \\
&= (3)\cdot 37 + (-10)\cdot (48 - 1\cdot 37) \\
&= (-10)\cdot 48 + (13)\cdot 37 \\
&= (-10)\cdot 48 + (13)\cdot (85 - 1\cdot 48) \\
&= (13)\cdot 85 + (-23)\cdot 48 \\
&= (13)\cdot 85 + (-23)\cdot (133 - 1\cdot 85) \\
&= \underbrace{(-23)}_{x}\cdot 133 + \underbrace{(36)}_{y}\cdot 85
\end{aligned}
$$

After Class Work

Prerequisites

In order to successfully complete this course, it is important to meet the following prerequisites:

1. familiar with the style of proof-based mathematics;
2. have a good understanding of proof formats and methods;
3. have basic knowledge of set theory and combinatorics, which are covered in Math 100;
4. solid grasp of lower division math courses, such as calculus and linear algebra.

In addition, you will meet some concepts which will be explored in greater depth in later courses. They will be used as terminology, and you should have ability to unpackage the abstract definitions.

After Class Work

1. Please read Chapter 0 of the textbook by yourself.
2. Unpackage the definitions of ***division with remainder*** and ***divisibility*** and try to use them to solve the following exercises.

Exercise 1.1

Let a, b, c be integers, then show that

1. $a \mid b$ if and only if $|a| \mid |b|$.
2. If $a \mid b$ and $b \neq 0$, then $|a| \leqslant |b|$.
3. If $c \neq 0$, then $a \mid b$ if and only if $ac \mid bc$.

Terminology

We say a ***relation*** $\preccurlyeq$ on a set S is a ***partial order*** if it satisfies:

- (***reflexivity***) for all $a \in S$, $a \preccurlyeq a$;
- (***antisymmetry***) for all $a, b \in S$, if $a \preccurlyeq b$ and $b \preccurlyeq a$, then $a = b$;
- (***transitivity***) for all $a, b, c \in S$, if $a \preccurlyeq b$ and $b \preccurlyeq c$, then $a \preccurlyeq c$.

A set equipped with a partial order is called an ***ordered set***.

Exercise 1.2

Show that the divisibility $(\cdot \mid \cdot)$ on $\mathbb{Z}_+$ and on $\mathbb{N}$ are partial orders. However, it is not a partial order on $\mathbb{Z}$.

After Class Work

Terminology

A ***monoid*** is a set M together with a binary operation $*$ and a specific element e (called its ***neutral elements***) satisfying the following axioms:

- (***associativity***) $(a * b) * c = a * (b * c)$ for all $a, b, c \in M$;
- (***neutrality***) $a * e = e * a = a$ for all $a \in M$.

Exercise 1.3

Determine whether the following triples are monoids: (endomaps of a set S, composition, id), $(\mathbb{N}$, multiplication, $1)$, $(\mathbb{Z}_+$, multiplication, $1)$, $(\mathbb{Z}$, multiplication, $1)$, $(\mathbb{Z}_+$, division, $1)$, $(\mathbb{N}$, addition, $0)$, $(\mathbb{Z}_+$, addition, $0)$, $(\mathbb{Z}$, addition, $0)$.

Terminology

We say a ***property*** P defined for elements of a monoid $(M, *, e)$ satisfies the ***2-out-of-3 principle*** if for any $a, b, c \in M$ satisfying the equation $a * b = c$, we have: if any two of $\{a, b, c\}$ satisfy P, then so does the third element.

Exercise 1.4

Determine whether the following properties satisfy the 2-out-of-3 principle.

1. The monoid is $(\text{endomaps of a set } S, \text{composition}, \mathrm{id})$ and the property is "being bijective".
2. The monoid is $(\mathbb{Z}, \text{addition}, 0)$ and the property is "being divided by d", where d is a positive integer.