MTH 311

Introduction to Higher Mathematics

Dr. Adam S. Sikora, Dr. Joseph A. Hundley, and Dr. Michael J. Cowen

Version January 22, 2024

Preface

The first objective of this course is to teach students the skills of precision in thinking, master the art of theorem proving, and of communicating mathematics using precise language and proper notation.

The second objective is to introduce students into higher mathematics. After discussing logic, sets, and functions, these notes follow the traditional development of numbers, starting with Peano's Axioms for the naturals and then successive definitions of integers, rationals, reals, and complex numbers. Students learn a variety of topics along the way: recursive sequences including Fibonacci numbers, equivalence relations, elements of number theory, including Fermat's Little Theorem, and Russell's Paradox.

Additionally, the course introduces foundational elements of abstract algebra, particularly focusing on the concepts of rings and fields.

Finally, countability of a set is discussed, including uncountability of the reals, the notion of cardinal numbers, Cantor's Hypothesis, and its independence from Peano's axioms.

These notes are enriched with a substantial number of proofs and examples to aid in understanding and application

How this course differs from others

This course differs from previous courses you have taken in three ways:

1. In calculus and other elementary math courses you encountered a variety of routine mathematical problems and established methods for solving each of them. After each class, you practiced these problems following the examples explained in detail in class.

There will only a LIMITED amount of this approach in this course. You will tackle less conventional problems without ready-made solutions. Proof writing, a skill central to this course, doesn't follow a universal formula and may be challenging for some. The aim is to develop your ability to think independently and creatively in mathematical problem-solving.

2. The course covers the most abstract mathematics you have ever encountered. Sometimes, it may be hard to "draw a picture" or give a simple example to illustrate a new concept.

3. In lower level math courses, your focus was on finding the correct answer to a problem, typically a number or a function, which appears at the bottom of your solution, most of which might have looked like a scratch work.

That kind of solution work will NOT be satisfactory here, as proper, clear mathematical communication will be important in this course. Here, the entire solution process is as important as the final answer. Solutions must be clear, logical, and well-structured, enabling others to understand your thought process. NO scratch style work will be accepted. Answers need to be well-reasoned, with every assumption or conclusion clearly justified.

Proper English and clear presentation are essential.

As future mathematicians or professionals you will need to explain complex concepts to others. Such challenging subject as math cannot be explained with messy notation, undefined symbols and stream-of-consciousness style of writing. Leave that to post-modern poets. We will discuss further details on solution writing and proof writing in Section 3.

How to do well.

- Come to class and recitation.
- Study these notes beforehand.
- Mathematics requires PRECISION. A implies B does not mean that B implies A. Make sure you have a precise understanding of the definitions and theorems. "Sort-of" understanding is not enough in this course. If you are asked to compute the range of a certain function, then you have to know precisely what the range of a function means.
- Ask questions on the material you do not understand. The best place to ask questions is in class and in recitation. That way others can also learn.
- Learn the definitions and statements of propositions (lemmas, theorems,..) thoroughly.
- Memorize each definition and proposition. You may find that flashcards of definitions and propositions are a useful tool.
- Go over each definition, giving examples and non-examples, until you understand the idea behind the definition and can recite all this information in your sleep.
- Go over each proposition until you understand the central idea behind it. Sometimes it will have some specific assumptions. Why are they needed?
- Memorize the central ideas behind the proofs and the flow of the proof. Do not memorize proofs. Work through a proof of each proposition while referring to your lecture notes. Then work through a proof of each proposition *without* referring to your lecture notes.

- The problems in this course vary from easy ones (following directly from a definition or proposition) to sophisticated (requiring an idea you have to come up with on your own). Do not expect to look at a problem and solve it immediately, as you may have done with most calculus problems. If you struggle with a problem, try working it out on a specific example first. That example should be simple, so you can work out all the details, but not so trivial that you can't gain any insight from it.
- If you still can't solve a problem, come back to it later and work on the next problems in the meanwhile. Often they will not be linked together. Note this means that you need to start doing the homework assignments early, to give yourself enough time to think. Only when you make a genuine effort and are still lost, should you consider asking your TA, or others for help. That's one of the best ways to learn math.
- You should plan on spending a minimum of 10 hours a week in preparation/homework. Try not to fall behind. Help is available from the TA and from your instructor.

None of these tasks is easy. Practice and repetition will make the tasks easier.

As these notes may be too compact at times for many of you, I recommend that you purchase

"Mathematical Proofs, A Transition to Advanced Mathematics" by Chartrand, Polimeni, and Zhang (4th ed or any earlier one).

which covers many of the topics of this course in more details.

Additionally, you may consider

"How to prove it, a structured approach," 2nd ed., Daniel J. Velleman, Cambridge U. Press, 2006. (inexpensive)

I recommend that you buy both of these books. The first one covers more topics then the second. However, the second has more insights about proofs.

Contents

1. Basic Logic

See also “Mathematical Proofs”, Ch. 2 or “How to Prove it” Ch. 1.1-2,1.5.

Definition 1.1 (Statement)**.** *A statement P is a sentence that is either true or false (but not both).*

For example, “Chickens are birds” is a statement.
However, “Most cows have four legs” is not a statement, since the word “most” does not have a precise meaning.

Definition 1.2 (Negation)**.** *If P is a statement, then the negation of P is $\neg P$, read “not P.” The negation of P is defined to be true if P is false and false if P is true.*

P	$\neg P$
T	F
F	T

Definition 1.3 (Conjunction)**.** *If P and Q are statements, then their conjunction $P \wedge Q$, read “P and Q,” is true if P and Q are both true; otherwise their conjunction is false.*

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

Note the similarity between the symbol “$\wedge$” and the letter “A” for “and”.

Definition 1.4 (Disjunction)**.** *If P and Q are statements, then their disjunction $P \vee Q$, read “P or Q,” is true if either P or Q or both are true; otherwise their disjunction is false.*

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

Note that $\vee$ is the inclusive “or”, e.g. “$1 + 1 = 2$” $\vee$ “$2 \times 2 = 4$” is true. In common (non-mathematical) use, one also encounters the exclusive “or”: “do you want Coke or Pepsi?”

The next operation is that of an implication, $P \Rightarrow Q$. In life and in science, an implication usually means a logical implication which refers to a situation in which a statement Q logically follows from P, eg.

(1) “If $x = y$ then $x^2 = y^2$”,

or
"If consumers have more disposable income, their spending increases."
P is called the premise, Q is called the conclusion and $P \Rightarrow Q$ is read "if P then Q", or alternatively, as "P implies Q", "P only if Q", "Q if P", "P is sufficient for Q", "Q is necessary for P".

Note that by applying a correct logic a true statement always leads to a true statement. On the other hand, a false statement can imply both a false or true statement. For example, applying $x = 1, y = -1$ to (1), we see that a falsity may correctly imply a true statement. Hence, we have the following possibilities:

(2) Truth $\Rightarrow$ Truth, Falsity $\Rightarrow$ Truth, Falsity $\Rightarrow$ Falsity.

Since the notion of logical implication is difficult to define precisely, one considers "formal implications" in mathematical logic, in which one is concerned with the truth or falsity of P and Q only, not with the meaning of P and Q or with a reasoning leading from P to Q. (2) implies the following truth table for formal implications:

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

Consequently,

"Cows are mammals $\Rightarrow$ 7 is a prime number"

is a true formal implication.

Some people use $\rightarrow$ instead of $\Rightarrow$ to denote all implications or the formal ones (including the authors of "How to Prove it"! Sigh...). We believe $\Rightarrow$ is the most common notation and therefore, we insist that you always use this one in this class.

Definition 1.5 (Converse)**.** *The converse of an implication $P \Rightarrow Q$ is the implication $Q \Rightarrow P$.*

Note that the converse of a true implication could be false and the converse of a false implication could be true.

Definition 1.6 (Equivalence)**.** *If P and Q are statements, then P and Q are equivalent, written $P \Leftrightarrow Q$ and read "P if and only if Q" or "P is equivalent to Q", if $P \Rightarrow Q$ and $Q \Rightarrow P$. The words "if and only if" are often abbreviated to "iff". Hence, P iff Q is another way to state equivalence of P and Q.*

Note that "iff" is the logic version of the equality sign, "=."

Compound Statements. An expression "$P \vee Q \wedge \neg P \Rightarrow Q$" is called a compound statement. P and Q are its components.

Note that the meaning of $P \vee Q \wedge R$ depends on the way we perform the operations, since $(P \vee Q) \wedge R$ is not necessarily $P \vee (Q \wedge R)$.

Recall that in arithmetic we have the following order of operations: powers, multiplication and division, addition and subtraction. For example, $1 + 2 \cdot 3^2 = 1 + (2 \cdot 9)$ and not $(1 + 2 \cdot 3)^2$ or $1 + (2 \cdot 3)^2$.

A commonly used "order of precedence" in logic is: negation, $\wedge$, $\vee$, implications, $\Leftrightarrow$, "=". This is consistent with the order of precedence: negation, $\wedge$, $\vee$, and "=" that is used in the computer language C. (Implications are not implemented in C.) Hence, $P \vee Q \wedge \neg P \Rightarrow Q$ means $(P \vee (Q \wedge (\neg P))) \Rightarrow Q$.

However, to avoid any ambiguity, you should use parentheses.

A statement which is true for all possible values of its components is called a tautology. For example, $P \vee \neg P$ is a tautology.

Theorem 1.7 (De Morgan's Laws)**.** *For all statements P and Q:*

- $\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$
- $\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$

By order of precedence, the right hand sides above mean $(\neg P) \wedge (\neg Q)$ and $(\neg P) \vee (\neg Q)$, respectively.

Proof of Theorem 1.7(1) is by the "Truth Table":

P	Q	$P \vee Q$	$\boldsymbol{\neg(P \vee Q)}$	$\neg P$	$\neg Q$	$\boldsymbol{\neg P \wedge \neg Q}$
T	T	T	F	F	F	F
T	F	T				
F	T	T				
F	F	F				

The proof of (2) is left to the reader. □

We can illustrate the first de Morgan's Law with the following example: Draw a card from the standard playing deck. Consider statements

"My card is hearts". Let D="My card is diamonds".

Then

$H \vee D$ = "My card is hearts or diamonds" = "My card is red suit".

In the above first de Morgan's Law,

Left side = $\neg(H \vee D)$ = "My card is not red suit".

Right side = $(\neg H) \wedge (\neg D)$= "not hearts and not diamonds".

So,

Left Side = "I have a black card" = Right Side.

What can be said about $(\neg H) \vee (\neg D)$?

Definition 1.8 (Contrapositive)**.** *For all statements P and Q: The contrapositive of the implication $P \Rightarrow Q$ is the implication $\neg\, Q \Rightarrow \neg P$.*

Theorem 1.9 (An implication and its contrapositive are equivalent)**.**

$$(P \Rightarrow Q) \Leftrightarrow (\neg\, Q \Rightarrow \neg P)\,.$$

Proof. by constructing a truth table. □

The above theorem implies that for the purpose of proving $P \Rightarrow Q$, it is enough to show its contrapositive, $\neg\, Q \Rightarrow \neg P$.

PROBLEMS 1.

Problem 1.1. *For each of the following statements, find P and Q so that the statement is equivalent to the implication $P \Rightarrow Q$:*

(1) I am happy if I am listening to music.
(2) I am happy only if I am listening to music.
(3) Being at least 30 years old is necessary for serving in the U.S. Senate.
(4) Being born in the U.S. is a sufficient condition for being a U.S. citizen.

Problem 1.2. *Prove that $(P \Rightarrow Q) \Leftrightarrow (\neg P \vee Q)$ is a tautology.*

Problem 1.3. *Simplify the expression $\neg(P \Rightarrow Q)$.*

Problem 1.4. *Show that $(P \vee Q) \wedge R$ and $P \vee (Q \wedge R)$ are not equivalent for some statements $P, Q,$ and R.*

Problem 1.5. *Roll a die. Let P denote the outcome 1 and Q denote the outcome 2. For what outcomes (out of $1, 2, 3, 4, 5, 6$) are the following true?*
(a) $\neg P \vee \neg Q$ (b) $\neg(P \wedge Q)$ (c) $\neg P \wedge \neg Q$

Problem 1.6. *Consider the implication: If x and y are even, then $x \cdot y$ is even.*
1a. State the implication using "only if".
1b. Is this implication true or false? Give a reason for your answer.
2a. State the converse of the implication.
2b. Is the converse of the implication true or false? Give a reason for your answer.
3a. State the contrapositive of the implication.
3b. Is the contrapositive of the implication true or false? Give a reason for your answer.

2. Sets

The most fundamental notion in mathematics is that of a set and its elements. You are used to seeing sets of numbers. However sets may contain any sort of elements. Even other sets. According to Wikipedia, "A set is a collection of distinct objects, considered as an object in its own right."

"Math Proofs", Ch. 1 and Ch. 4.4-6, "How to Prove It", Ch. 1.2-4.

Examples:

- $\emptyset$ — the "empty set" (set with no elements)
- {apple, horse, 2}
- $\{4, \{4\}, \{2, 4\}\}$

We use the Greek letter epsilon, $\in$, to write that a certain object is an element of a set, e.g. 2 $\in$ {apple, horse, 2}, but {2} is not an element of $\{apple, horse, 2\}$, because the expression {2} is not listed between the commas.

Definition 2.1 (Subset)**.** *Let A and B be sets. We say that A is contained in B, or A is a subset of B, written $A \subseteq B$, if whenever $x \in A$, then $x \in B$. As an alternative, we sometimes say that B contains A, written $B \supseteq A$.*

Note that $\emptyset \subseteq A$ for all sets A.

Definition 2.2 (Equality of Sets)**.** *We say that A equals B, written $A = B$, if $A \subseteq B$ and $A \supseteq B$.*

Hence

$$\{\text{apple, horse, 2}\} = \{\text{horse, 2, apple}\} = \{\text{horse, 2, apple, horse}\}.$$

Sets can be elements of other sets, e.g. $A = \{\{3, 5, 7\}, 1\}$ is a set of two elements, one of which is a set itself. If $B = \{1, 3, 5, 7\}$, then $A \neq B$, since B has 4 elements. Also, $A \neq \{\{1, 3, 5\}, 7\}$, since 7 is not an element of A.

We say that A is a proper subset of B if $A \subseteq B$ but $A \neq B$. We denote this by $A \subsetneq B$.

Warning: For some mathematicians $\subset$ means the same as $\subseteq$ and for others it means $\subsetneq$. For us and for most people, $\subset$ is the same as $\subseteq$, even though your textbook adopted the other convention! Hence, in this course $\subset$ means any subset. For example, the statement $A \subset A$ is True for all sets A, according to our convention. Note that $7 \leq 7$ but not $7 < 7$, hence there is some inconsistency between the arithmetic and set theory notation. Similar inconsistencies happen in every language, not just the language of mathematics.

It is important to distinguish between the symbols $\in$ and $\subset$. The following are true: $\emptyset \subseteq \{1,2\}$, $1 \in \{1,2\}, \emptyset \in \{\emptyset, 5\}$. The following are FALSE: $\emptyset \in \{1,2\}$, $1 \subseteq \{1,2\}$.

If you are still confused about $\in$ and $\subset$, you may want to think of sets as boxes. Then $a \in A$ means that box A contains a and $A \subset B$ means that B contains everything in A (and possibly more). Sometimes a set may A may contain set C as its element, the same way a box may contain another box, but is somewhat unusual one may say. For example, all sets considered in Calculus I contain numbers only.

If A is a set then we often define its subsets by writing

$$\{x \in A : x \text{ satisfies some condition}\},$$

e.g. $\{x \in \mathbb{R} : x^2 < 4\}$ is the set of all real numbers x such that $x^2 < 4$. This is called a set-builder notation.

The number of elements of a set A is called its *cardinality* and it is denoted by $|A|$. For example, $|\{3, \{3\}\}| = 2$, $|\mathbb{R}| = \infty$. (∞ is not a number, but a useful symbol.)

Russell's Paradox. Note that according to the Wikipedia definition at the beginning of this section, the collection of all sets is a set in itself. This set contains itself as its own element! One might be willing to accept that, if not for the fact that the following argument of British philosopher Bertrand Russell leads to a contradiction:

Let us say that a set A is *wild* if A contains A as its own element. Otherwise A is *tame*. Hence the set of all sets is wild. On the other hand, the set of real numbers or any other sets you encountered in calculus class are tame.

Let Ω be the set of all tame sets. (Ω being the last letter of the Greek alphabet is often used to denote "large" sets.) Is Ω tame? If it is, then it belongs to Ω and hence, Ω is wild. On the other hand, if Ω is wild then Ω is its element. Since by definition, all elements of Ω are tame, Ω is tame as well. Therefore, we proved that wildness of Ω implies its tameness and tameness of Ω implies its wildness.

This is the famous Russell's Paradox which led the early 20th century mathematicians to rewrite the foundations of mathematics. Their efforts were not completely satisfactory, since they were unable to formulate a rigorous definition of a set. (Since every definition describes a notion in terms of simpler ones, one cannot define a "set" since it is the most basic notion of mathematics.)

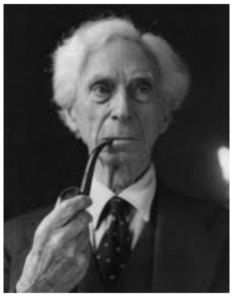

FIGURE 1. Bertrand Russell

Unable to define sets, mathematicians settled on the next best thing and described sets by axioms — fundamental properties upon which all mathematicians agree. The most common set of axioms was formulated by Zermelo and Fraenkel. We will not discuss their axioms here, since they are more complicated than you might expect, c.f.
`http://en.wikipedia.org/wiki/Zermelo-Fraenkel_set_theory`

Remark 2.3.
(1) These axioms require that a set cannot be its own element. Hence, wild sets are "illegal." In particular, one cannot call the collection of all sets "a set"! (As you can see, we used an informal word "collection" to refer to all sets).
(2) All mathematical knowledge of human civilization can be derived from these axioms.
(3) In particular all mathematical notions (except sets) can be rigorously defined on the basis of set theory.
(4) We do not know if these axioms are consistent (i.e. do not lead to a contradiction, analogous to Russell's paradox). However, most mathematicians believe that they are consistent, since no contradiction has been found in the last 100 years.
(5) There are limits to what can be proved from any consistent set of axioms. In particular, we will see that the validity of some statements cannot be either proved or disproved– c.f. Section 16.

Operations on sets.

Definition 2.4 (Union and intersection)**.** *The union $A \cup B$ of two sets A and B is defined by $A \cup B = \{x : \ x \in A \text{ or } x \in B\}$. Recall that 'or' in mathematics means 'and/or.' The intersection $A \cap B$ is defined by $A \cap B = \{x : \ x \in A \text{ and } x \in B\}$. (Sometimes $A \cap B$ is abbreviated to AB, but we will not use that notation.)*

Similarly, we define unions of multiple sets

$$\bigcup_{i=1}^{n} A_i = A_1 \cup ... \cup A_n = \{x : x \in A_i \text{ for some } i \in \{1, ..., n\}\}$$

and their intersections, $\bigcap_{i=1}^{n} A_i$.

Sometimes infinite unions are useful. For example,

$$\{x \in \mathbb{R} : \sin(x) > 0\}.$$

(in set builder notation) can be also written more explicitly, as

$$\bigcup_{k \in \mathbb{Z}} (2\pi k, 2\pi k + \pi),$$

meaning a union of intervals $(2\pi k, 2\pi k + \pi)$ for all possible integral values of k.

Here and throughout the notes, the symbols $\mathbb{R}$ and $\mathbb{Z}$ denote the set of all real numbers and the set of all integers (whole numbers). Note that the symbols R and Z may be used to denote various other things at various times.

Definition 2.5 (Disjoint). *Sets A and B are disjoint if $A \cap B = \varnothing$.*

Definition 2.6 (Power set). *The power set of a set A, denoted 2^A or $P(A)$, is the set of all subsets of A. That is, $2^A = \{X : X \subseteq A\}$.*

Example 2.7. *Every subset B of $A = \{1, 2, 3\}$ is determined by a sequence of Yes's and/or No's answering the following three questions:*
- *Does 1 belong to B?*
- *Does 2 belong to B?*
- *Does 3 belong to B?*

For example, Y, N, Y corresponds to $B = \{1, 3\} \subseteq A$ and N, N, N corresponds to $\emptyset \subseteq A$. Since there are $2 \times 2 \times 2 = 8$ possible sequences like that, $|2^A| = 8$.

More generally, one can prove that $|2^A| = 2^{|A|}$. That fact motivates the term "power set" and the notation for it.

Proposition 2.8 (Basic properties of sets). *If A, B, C are sets, then*

(1) $\varnothing \cap A = \varnothing$; $\varnothing \cup A = A$

(2) $A \cap B \subseteq A$

(3) $A \subseteq A \cup B$

(4) $A \cup B = B \cup A$; $A \cap B = B \cap A$ *("commutative" property of $\cup, \cap$)*

(5) $A \cup (B \cup C) = (A \cup B) \cup C$. *(associative property of $\cup$). The same for $\cap$.*

(6) $A \cup A = A \cap A = A$
(7) If $A \subseteq B$*, then* $A \cup C \subseteq B \cup C$ *and* $A \cap C \subseteq B \cap C$

("Propositions" are "little" theorems. We will comment more about them later.)

Proof. The proofs are very easy. Let us prove (2) for example: Let $x \in A \cap B$. Then $x \in A$ and $x \in B$. Hence, in particular, $x \in A$. In other words, every element of $A \cap B$ belongs to A. □

Proposition 2.9 (Distributive Rules)**.** *If* A, B, C *are sets, then*
(1) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
(2) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

To prove that two sets, X and Y coincide (i.e. are equal), one usually needs to show separately that $X \subseteq Y$ and $Y \subseteq X$.

Proof of (1): Proof of $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$:
Let $x \in A \cap (B \cup C)$. Then $x \in A$ and, furthermore, $x \in B$ or $x \in C$. Hence, $x \in A \cap B$ in the first case and $x \in A \cap C$ in the other. Therefore, $x \in A \cap B \cup A \cap C$ for all such x.
Proof of $A \cap (B \cup C) \supset (A \cap B) \cup (A \cap C)$: in class or HW.

Proof of (2): in class or HW. □

Remark 2.10. *You cannot prove Propositions 2.8 and 2.9 "by example", because the claim is that the statements hold for* <u>*all*</u> *sets* A, B, C*. For example, verifying*

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

for

$$A = \{a, b, c\}, \ B = \{d, e\}, \ C = \{a, d\}$$

does not constitute a proof of Proposition 2.9(1).

However, "there exists" statements can be proved by example. For example, consider the problem:
Prove that there exist sets A, B *such that* $A \cup B \neq A \cap B$*.*
Proof: Take $A = \{a, b\}$*,* $B = \emptyset$*. Then* $A \cup B = \{a, b\}$ *and* $A \cap B = \emptyset$ *are different.* □

Definition 2.11 (Complement)**.** *If* X *and* A *are sets, the* <u>*complement,*</u> *of* A *in* X*, denoted by* $X - A$*, is defined by* $X - A = \{x \in X : \ x \notin A\}$

$X - A$ is alternatively written as $X \setminus A$. $X - A$ is also called the <u>set difference</u> but that can be ambiguous as the difference of sets may refer to $X - A$ or to $A - X$.

Proposition 2.12 (de Morgan's laws)**.** *If* A, B *and* X *are sets then*

(1) $X - (A \cup B) = (X - A) \cap (X - B)$
(2) $X - (A \cap B) = (X - A) \cup (X - B)$

The proofs of these properties can be visualized by use of Venn diagrams.

There is no well established comprehensive order of precedence in set theory. However, $\cap$, $\cup$ and $=$ correspond to $\wedge$, $\vee$, and $\Leftrightarrow$. Hence, these set theory operations should be interpreted in the order written above. For example, the first distributive rule above can be written as $A \cap (B \cup C) = A \cap B \cup A \cap C$.

According to this analogy between set theory and logic, the set subtraction should precede $\cap$, but that rule is not universally followed. To avoid ambiguities, use parentheses instead.

Pairs and Cartesian products. As mentioned in Remark 2.3, all mathematical notions can be defined in terms of set theory. Let us take the first challenge then of defining a pair (a, b), like the one used to denote the coordinates of a point on a plane. Note that $(a, b) \neq \{a, b\}$ since $(a, b) \neq (b, a)$ for $a \neq b$.

See "Math Proofs" 1.6 and "How to Prove it" 4.1. They fail however to define "ordered pairs" and just take them intuitively for granted.

Definition 2.13 (Formal definition of ordered pair)**.** *Let A and B be sets, let $a \in A$, $b \in B$. Then we define the ordered pair (a, b) by $(a, b) = \{\{a\}, \{a, b\}\}$.*

The following proposition shows that (a, b) behaves as "a pair". Note that $(1, 2)$ may also mean an open interval from 1 to 2. As some words in various languages have double or multiple meanings (such words are called "homonyms"), so do some mathematical notations. The meaning of (a, b) will depend on the context or will be specified by words if needed.

Proposition 2.14 (Fundamental property of ordered pairs)**.** *Let a and c be in A; and b and d be in B. Then $(a, b) = (c, d)$ if and only if $a = c$ and $b = d$.*

Proof. Since the $\Leftarrow$ implication is obvious, we only need to prove $\Rightarrow$.

Let $a, c \in A$ and $b, d \in B$ be such that $(a, b) = (c, d)$. Observe that (a, b) is a set of 1 or 2 elements depending on whether a equals b or not. Indeed, if $a = b$ then

$$(a, b) = \{\{a\}, \{a, b\}\} = \{\{a\}, \{a\}\} = \{\{a\}\} \tag{3}$$

and if $a \neq b$ then (a, b) contains two different elements. (Why?)

For the proof, assume first that $a = b$. Then $(a, b) = (c, d)$ is a 1 element set and, hence, $c = d$. Furthermore, by (3), $\{a\} = \{c\}$. Hence $a = c$ and the implication follows.

If $a \neq b$ then (a, b) contains 2 elements: a 1 element set, $\{a\}$, and a 2 element set, $\{a, b\}$. By assumption $(a, b) = (c, d)$. Therefore (c, d) is also a 2 element set, i.e. $\{c, d\} \neq \{c\}$. Since a one element set cannot equal a two element set (recall that two sets are equal if they have the same elements), our assumptions imply that $\{a\} = \{c\}$ and $\{a, b\} = \{c, d\}$. Hence $a = c$ and $b = d$. □

Definition 2.15 (Cartesian Product)**.** *The Cartesian product $A \times B$ of sets A and B is defined by $A \times B = \{(a, b) : \ a \in A \text{ and } b \in B\}$*

Note: writing $(a, b) \in A \times B$ implies that $a \in A$ and $b \in B$.

We define $A^1 = A$, and $A^2, A^3, \ldots$ recursively by $A^{n+1} = A^n \times A$. For simplicity, we denote $((a, b), c)$ in $A^3 = A^2 \times A$ by (a, b, c). Hence A^3 is the set of all triples of elements of A. Similarly we define n-tuples as elements of A^n.

Since every point in space can be uniquely identified (in a given system of coordinates) by its x, y, and $z-$coordinates, which are real numbers, the infinite 3-dimensional space is often denoted by $\mathbb{R}^3$.

PROBLEMS 2.

Problem 2.1. *What is the cardinality of $A = \{\emptyset\}$, $B = \{\emptyset, \emptyset\}$, $C = \{\emptyset, \{\emptyset\}\}$. Are any of these two sets equal? Justify your answer.*

Problem 2.2. *Write the elements of $(\{a, b, c\} - \{a, b, d\}) \cup \{c, d\}$, where $a, b, c,$ and d are distinct.*

Problem 2.3. *Write down all elements of the set $\{x \in \mathbb{R} : x^3 - x = 0\}$.*

Problem 2.4. *Write the set $\{x \in \mathbb{R} : \cos(x) \geq 1/2\}$ as an infinite union of intervals.*

Problem 2.5. *Determine the sets*
(1) $X = \bigcap_{n=1}^{\infty} (n, \infty)$,
(2) $Y = \bigcap_{s \in [1,\infty)} (-s, s)$,
(3) $Z = \bigcap_{s \in (1,\infty)} (-s, s)$,
where as usual, (,) denotes an open interval of real numbers and [,) denotes a half-closed one.

Problem 2.6. *For $A = \{a, b\}$, determine $A \times 2^A$.*

Problem 2.7. *Which of the following are correct beginnings of a proof of $A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C)$? Justify each answer.*
(1) Since $a \in A$,...
(2) Since $a \in A, b \in B,$ and $c \in C$,...
(3) Let $a \in A$.
(4) Let $a \in A, b \in B$ and $c \in C$.

(5) Let $x \in (A \cap B) \cup (A \cap C)$.
(6) Let $a \in (A \cap B) \cup (A \cap C)$.
(7) By drawing a Venn diagram, we see that .....

Problem 2.8. *Could a pair (a, b) be alternatively defined as $\{a, b\}$ instead of by the definition in these notes? Justify your answer.*

3. Statements and Proofs in Mathematics

Important mathematical statements are called "theorems". Sometimes they have been given names, such as the Fundamental Theorem of Calculus, which states that the derivative of $F(x) = \int_a^x f(t)\,dt$ is $f(x)$. Smaller statements are called "propositions". Yet smaller ones are "lemmas" — these are auxiliary statements needed for the purpose of proving theorems and propositions. A small statement which follows as an immediate consequence of another statement is usually called a "corollary."

Mathematical statements usually have the form "If A, then B", or " Let us assume A. Then B," or something similar. In such a statement, "A" is called an assumption, hypothesis, or premise, while "B" is called the consequence or conclusion.

"How to Prove it" Ch. 3, "Math Proofs" Ch. 0 and 3.

One of the primary objectives of this course is teaching theorem proving. A proof is a deductive argument (or reasoning) for a statement, based on logic, axioms, and other previously proved statements. A proof must demonstrate that a statement is definitely true– it can not leave any possibility of the statement being false. An argument which only shows that the falsity of a statement is very unlikely or counter-intuitive is not a proof. Also, a proof can not rely on any unproven statements other than axioms, no matter how reasonable they seem.

Many theorems have the form of a quantified open statement. "For every positive integer n, $\sum_{j=1}^{n} j^2 = \frac{n(n+1)(2n+1)}{6}$", for example. When dealing with such a statement, a proof must demonstrate that the statement is *always* true. Enumeration of many confirmatory cases is insufficient. Therefore, a statement referring to all sets or all numbers (explicitly or implicitly) cannot be proved "by example". On the other hand, an existential statement– one which calls for the existence of an object with certain properties, can be proved by exhibiting one example. For example,

"Prove that there is a set A such that $A \cap 2^A \neq \emptyset$"

is an existential statement. To prove it, it suffices to find one such A. What is perhaps more interesting is that it is sometimes possible to prove an existential statement *without* exhibiting an example.

Unlike other scientists, mathematicians rely on proven statements only. Mathematics is called "Queen of the Sciences" because of that and because all other sciences rely on it.

An unproven statement that is believed to be true is known as a conjecture.

The simplest proof is a direct proof. We used it to prove Proposition 2.9(1). In a direct proof of an implication $P \Rightarrow Q$ one begins from P and proceeds to Q by a series of steps, each of them either logic, an axiom, a previously proved statement, or the simple "plugging in" of some definition.

An indirect proof is any proof which is not direct. In an indirect proof of $P \Rightarrow Q$, one typically starts not from P, but from $\neg Q$. We will use this technique in the next example.

Problem 3.1. *Suppose $A \cap C \subseteq B$ and $a \in C$. Prove that $a \notin A - B$.*

Proof by contradiction: Suppose that $a \in A - B$. Then $a \in A$ and $a \notin B$. By assumption, $a \in C$ and, hence, $a \in A \cap C$. Finally, by assumption, $a \in B$. Contradiction. □

This type of proof of $P \Rightarrow Q$ starts by assuming that Q is false (assuming $\neg Q$) and then shows that such an assumption leads to a contradiction (with P and with logic in general). The Latin term for it is "Reductio ad absurdum" or "Reduction ad impossiblem". In this case, our statement is $P \Rightarrow Q$ where

$$P = \text{“}(A \cap C \subseteq B) \wedge (a \in C),\text{”}$$

and

$$Q = \text{“}a \notin A - B.\text{”}$$

Starting from $P \wedge (\neg Q)$ we were able to derive $R \wedge (\neg R)$ where $R =$"$a \in B$." But $R \wedge (\neg R)$ is a contradiction– a compound statement formed by conjoining a statement with its own negation. Such a statement is automatically false: $X \wedge (\neg X)$ is false for both truth values of X. Hence, in the case at hand, we know that $R \wedge (\neg R)$ is False by logic — without needing to know the truth value of R! But if something false follows from $P \wedge (\neg Q)$, then it must be the case that $P \wedge (\neg Q)$ itself is false. That is $\neg(P \wedge (\neg Q))$ is true. But we have seen that $\neg(P \wedge (\neg Q))$ is equivalent to $P \Rightarrow Q$.

The method of contradiction should be declared at the beginning of the proof (as above). The reason is that in the direct proof one cannot introduce new assumptions (which are not part of the statement). The "Suppose that $a \in A - B$" above would be such new assumption.

A common special case of proof by contradiction is proof by contrapositive. In this type of proof, one provides an indirect proof of the statement $P \Rightarrow Q$ by giving a direct proof of the contrapositive $\neg Q \Rightarrow \neg P$, which is logically equivalent to $P \Rightarrow Q$. (This can be also thought of as a proof that $P \wedge (\neg Q)$ implies the contradiction $P \wedge (\neg P)$.)

Proofs by contradiction are often useful to prove that a certain set is empty. For example:

Proposition 3.2. *For any sets A and B, we have $(A-B)-A=\emptyset$.*

Proof by contradiction: Suppose that $(A-B)-A\neq\emptyset$. Then there is some element x in $(A-B)-A$. It belongs to $A-B$ and, hence, to A, but it does not belong to A — a contradiction. □

Later we will encounter other types of proofs.

Each proof starts with "Proof" and ends with Q.E.D. (abbreviation for Latin "Quod Erat Demonstrandum" —"that which was to be demonstrated") or, simply, with □.

In lower level math courses, your focus was on finding the correct answer to a problem, usually a number or a function, which appeared at the bottom of your solution. The rest of your solution, leading to the desired answer, might have looked like a scratch work.

That kind of solution work will NOT be satisfactory here. Our goal is to learn a proper, clear mathematics communication, style, which you can use in the future, to explain math to others who don't have the same background as you. NO scratch style work will be accepted.

There are some very short proofs which do not require many words. For example, for any sets A,B,C one has

$$A\cap(B-C)=(A\cap B)-C. \tag{4}$$

Proof. $x\in A\cap(B-C)$ iff $(x\in A)\wedge(x\in B-C)$ iff $(x\in A)\wedge(x\in B)\wedge(x\notin C)$ iff $x\in(A\cap B)-C$. □

However, as a general rule, proofs have to be written in full sentences. In the majority of proofs, words are as important as numbers and symbols. If you removed all words from our proof of

$$A\cap(B\cup C)\subseteq(A\cap B)\cup(A\cap C)$$

(Proposition 2.9(1)) you would get something completely incomprehensible: $x\in A\cap(B\cup C)$ $x\in A$ $x\in B$ $x\in C$ $x\in A\cap B$ $x\in A\cap C$ $x\in A\cap B\cup A\cap C$.

Use proper English in proofs. End each sentence with a period! Exclamation marks are acceptable too! It is difficult to understand your logic not knowing where the sentences end. Math is a challenging subject and it can't be explained in stream-of-consciousness style writing.

Use commas where needed. For example, after "for example", "therefore", "hence".

Generally speaking, each sentence should begin with a word (not a symbol or equation) and each symbol has to be defined.

When proving that $A\subseteq B$ one usually starts the proof with "Let $x\in A$", "Let x be in A","Take any $x\in A$", or "Consider any $x\in A$". One then uses the given assumptions and logic to prove that $x\in B$. Generally speaking, if a symbol, say x, is not defined yet, do not start a sentence with "$x = 2$" or "$x \in B$". Even if x is defined already, you need to explain why $x = 2$ or why $x \in B$. For example: "Because of ... and of ..., $x \in B$". You will use these constructions often: "Because of P, (we have) Q", "Since P, then Q", "Q, since P", "P. Therefore, Q."

Never write "Then $x \in A$, $x \in B$". You need "and" or "or" in between "$x \in A$" and "$x \in B$".

After writing "Let $x \in A$" do not write "If $x \in A$", since that was assumed already! (Writing $x \notin A$ makes even less sense.)

Besides attention to English, you should use math notation carefully. Don't confuse $\{, [,$ and (. Implications are denoted by $\Rightarrow$. The arrow $\rightarrow$ is used for function notation, $f : X \rightarrow Y$. However, there are some differences in the use of math symbols between different communities of mathematicians around the world. For example, "How to Prove It" uses $\rightarrow$ for implications. Your calculus textbook ends a proof with a little triangle. For consistency and clarity we will only use symbols in the way introduced here. Our implications will be denoted by $\Rightarrow$ only.

Some people abbreviate "Therefore" by $\therefore$. "Contradiction" is sometimes abbreviated by #, or $\Rightarrow\Leftarrow$, or $\perp$. You can use any notation you like, as long as it does not contradict itself, but if you want to use a notation which is not introduced in these notes, you must define it.

Further rules for proving theorems:

1. To prove "iff" statements one usually needs to to prove the "$\Rightarrow$" and "$\Leftarrow$" implications separately. Please clearly mark these two parts of the proof "Proof of $\Rightarrow$: ..." and "Proof of $\Leftarrow$: ..." Exceptions to this rule are simple statements like "$x^3 = -8$ iff $x^5 = -32$."

2. Proving that two sets are equal, $A = B$, usually requires showing that $A \subseteq B$ and $B \subseteq A$. Some easy statements can be sometimes proved by a sequences of "iff"s, as in our proof of equality (4).

3. While proving a statement in these notes you can rely on a statement preceding it but not following it. Hence, you can not prove a statement in Sec. 3 by referring to a statement in Sec 4. Similarly, in order to prove Proposition 2.12 part (2) you may rely on part (1) but not the other way around, since that would lead to a circular reasoning.

Please read further discussion on writing mathematics in "Mathematical Proofs", Chapters 0 and 3 and in "How to Prove it" Ch. 3.

If you ignore these rules, you will have to redo your HW!

Proofs are like jigsaw puzzles or like finding your way through a labyrinth. In general, there are no step-by-step procedures for writing proofs (unlike for all Calculus problems). Most statements can be proved in various ways. There is no single proof for them or a flow-chart matching a proof with a statement. That makes proving statements much harder than solving calculus problems. Mathematics programs like Mathematica, Maple, or Sage can compute integrals, derivatives, areas, and can solve equations. But they cannot prove theorems! You will often need to devise your own proofs in this course (based on examples in class). You will often need to make several attempts, each improving on the previous one, to achieve a correct and complete proof. That is what makes this course harder than other math courses. As with every skill, proofs will become easier with practice. And for some types of statements, e.g. proving that two sets are equal, the method of proof is more or less standard (as discussed above).

Any logically correct and complete proof is satisfactory, although simpler and shorter proofs are preferred over longer and complicated ones.

PROBLEMS 3.

Problem 3.1. *Prove that if $A \subseteq B$ and $C \subseteq D$ then*
a) $A \cup C \subseteq B \cup D$.
b) $A \cap C \subseteq B \cap D$.
(Use proofs in this and previous sections as examples, e.g. the proof of Proposition 2.9.)

Problem 3.2. *Prove that $A \cup B = A$ if and only if $B \subseteq A$.*
Hint: You need to show the two implications, ⇒, ⇐ separately.

Problem 3.3. *Prove that if A is a subset of X, then*
a) $A \cap (X - A) = \varnothing$.
b) $A \cup (X - A) = X$.
c) $X - (X - A) = A$. *Hint: use a) and b).*

Problem 3.4. *Prove that if A and B are subsets of X, then*
a) $A - B = A \cap (X - B)$.
b) $X - (A \cap B) = (X - A) \cup (X - B)$.
c) $A \subseteq B$ *if and only if* $X - B \subseteq X - A$.

Problem 3.5. *Prove that for any sets A, B, C,*
$A \cap (B - C) = (A \cap B) - (A \cap C)$.

Problem 3.6. *For any sets A, B, prove that $(A - B) \cap (B - A) = \emptyset$.*
Hint: *You can use a proof by contradiction.*

Problem 3.7. *Prove or disprove the following statement: For all sets $A, B,$ and C, we have $A \cap (B \cup C) = A \cap B \cap C$. ("Disproving" means proving that it is not true.)*

Problem 3.8. *Prove or disprove the following statement: if* $A \cap B \cap C = \emptyset$*, then one of the sets* $A \cap B$*,* $B \cap C$ *or* $C \cap A$ *is empty too.*

Problem 3.9. *Let* A *and* B *be sets. Prove that* $A \times \emptyset = \emptyset \times B = \emptyset$*. (See Definition 2.15)*

Problem 3.10. *Let* A, B, C *be non-empty sets, with* $B \subseteq C$*. Prove that* $A \times B \subseteq A \times C$*.*

Problem 3.11. *Let* A, B, C *be non-empty sets. Prove that*
(i) $A \times (B \cup C) = (A \times B) \cup (A \times C)$
(ii) $A \times (B \cap C) = (A \times B) \cap (A \times C)$*.*

Problem 3.12. *Let* A *and* B *be non-empty sets. Prove that* $A \times B = B \times A$ *if and only if* $A = B$*. Where do you use that* A *and* B *are non-empty?*

Problem 3.13. *Is the following true? Prove it or find a counterexample. For any sets* A, B*, we have* $2^A \cap 2^B \subseteq 2^{A \cap B}$*.*

4. Quantifiers

“How to prove it” Ch. 2 and “Mathematical Proofs”, Sec. 2.10.

Definition 4.1. *An open sentence is a sentence which contains one or more variables, which takes a truth value (i.e., becomes a statement) when each variable is specialized to a specific element of a given set (the domain of the variable).*

We write $P(x), P(x,y)$, etc. for open sentences depending on the variables x or x and y, etc.

One way to make an open sentence into a statement is to precede it with a “quantifier.”

Definition 4.2 (Existential Quantifier)**.** *The existential quantifier is denoted by the symbol $\exists$. It reads “there exists.”*

Definition 4.3 (Universal quantifier)**.** *The universal quantifier is denoted by the symbol $\forall$. It reads “for all” or “for every.”*

Example 4.4. *If $X = \{a, b\}$ then $\forall_{x\in X} P(x) = P(a) \wedge P(b)$ and $\exists_{x\in X} P(x) = P(a) \vee P(b)$.*

For example, the existence of $\sqrt{2}$ can be stated as

$$\exists x \in \mathbb{R} \text{ such that } x^2 = 2 \text{ and } x \geq 0,$$

or, more compactly, as

$$\exists_{x\in[0,\infty)}\, x^2 = 2.$$

Note that you put the part of the sentence before words “such that” in the subscript after $\exists$.

Additionally, a quantifier $\exists!$ is used to state the existence of a *unique* element with a certain property. For example,

$$\exists!_{x\in(0,\infty)}\, x^2 = 2$$

holds, but

$$\exists!_{x\in\mathbb{R}}\, x^2 = 2$$

does not (since $x^2 = 2$ for two real x’s: $\sqrt{2}$ and $-\sqrt{2}$).

The fact that $\sqrt{2}$ is irrational can be written as

$$\forall_{x\in\mathbb{Q}}\, x^2 \neq 2$$

or

$$\forall_{x\in\mathbb{R}}\, x \in \mathbb{Q} \Rightarrow x^2 \neq 2$$

(The set of rational numbers is traditionally denoted by $\mathbb{Q}$, coming from the word “quotient”.)

Note that the sentence above means $\forall_{x\in\mathbb{R}}\, (x \in \mathbb{Q} \Rightarrow x^2 \neq 2)$. What can be said about the sentence $(\forall_{x\in\mathbb{R}}\, x \in \mathbb{Q}) \Rightarrow x^2 \neq 2$?

Theorem 4.5. *Let $P(x)$ be an open sentence. Then*

(1) $\neg(\forall_{x\in X} P(x)) \Leftrightarrow (\exists_{x\in X} \neg P(x))$
(2) $\neg(\exists_{x\in X} P(x)) \Leftrightarrow (\forall_{x\in X} \neg P(x))$

Example 4.6. *Let $X = \{a, b\}$. Then the left hand side of Thm 4.5(1) is $\neg(\forall_{x\in X} P(x)) = \neg(P(a) \wedge P(b)) = \neg P(a) \vee \neg P(b)$ (by De Morgan's Laws) which is $\exists_{x\in X}\neg P(x)$. Hence the law above, generalizes De Morgan's Law.*

Thm 4.5(2) is a generalization of De Morgan's second law.

Note that $\forall$ is usually stronger than $\exists$. For example, "there exists a black cat" is true and "every cat is black" is false. However, that is not always the case as we will see now.

Note that $\exists_{x\in\emptyset} P(x)$ is false, independently of what $P(x)$ is. Hence, $\neg\,(\exists_{x\in\emptyset} P(x))$ is true and, by Theorem 4.5(2), $\forall_{x\in\emptyset}\,\neg P(x)$ is true for every $P(x)$. If we take $Q(x)$ to be any statement and $P(x) = \neg Q(x)$, then we conclude with:

Corollary 4.7. $\forall_{x\in\emptyset}\, Q(x)$ *holds (i.e. is true), for every open sentence $Q(x)$.*

Example 4.8. *Let X be the set of all unicorns. Let $Q(x)$ be the open sentence "unicorn x is white". Then $S = \forall_{x\in X}\, Q(x)$ is the statement that all unicorns are white.*

If we assume that no unicorns exist then $X = \emptyset$ and the above statement S holds — that is, assuming no unicorns, all unicorns are white!

By the same token, the statement

$$\text{P="}x = 5 \text{ for all real } x \text{ such that } x^2 + 1 < 0\text{"}$$

is true. Indeed, note that the set of x's such that $x^2 + 1 < 0$ is empty. Therefore P says "$x = 5$ for all $x \in \emptyset$" and, consequently, $\neg P$ says

$$\text{"}x \neq 5 \text{ for some element } x \in \emptyset\text{"}$$

Since there are no elements in $\emptyset$, the above statement is false. Hence P is true.

As stated in Remark 2.10, "there exists" statements can be proved by example.

Example 4.9. *Prove that there is*
1. a positive integer which is smaller than the sum of its proper divisors.
2. a non-zero integer N such that $2N, 3N, 4N, 5N$ and $6N$ have the same digits as N (but in different orders).

Which of the following are true?

(1) $\forall_{x\in\mathbb{R}}\ \exists_{y\in\mathbb{R}}\ y > x$
(2) $\exists x \in \mathbb{R}\ \forall_{y\in\mathbb{R}}\ y > x$
(3) $\forall_{x\in\mathbb{R}}\ \forall_{y\in\mathbb{R}}\ y > x$

You have seen statements combining universal and existential quantifiers in Calculus. Do you recall the meaning of $\lim_{n\to\infty} a_n = L$ for an infinite sequence $a_1, a_2, ...$?

Remark 4.10. *Although "there exists" statements can be in principle proved by example, that is not always feasible in practice. In fact, many powerful existence theorems, such as the Intermediate Value Theorem, are proved by other methods.*

PROBLEMS 4.

Problem 4.1. *(a) Write the negation of the statement "There exists a cat with 9 lives" in standard English. (You cannot start it with "It is not true that...")*
(b) Write the negation of the statement "All cats have 9 lives." (You cannot start it with "It is not true that..." nor "Not all cats...").

Problem 4.2.

1. *Let P be the statement "$x^2+2=11$ for all real numbers x such that $x^3+32=5$." Is P true? Why or why not?*
2. *Let Q be the statement "$x^3+32=5$ for all real numbers x such that $x^2+2=11$." Is Q true? Why or why not?*
3. *Let R be the statement "$x^3+32=5$ for all real numbers x such that $x^2+32=0$." Is R true? Why or why not?*

Problem 4.3. *Find all values of $a \in \mathbb{R}$ for which*

$$P(a) = \text{“}x^3 = x^2 \text{ for every } x \text{ such that } x^2 = a\text{”}$$

holds.

Problem 4.4. *As you should remember from Calculus, every cubic polynomial with real coefficients has a real root. Express that statement using $\forall$, $\exists$ quantifiers and other math symbols but without using any words. (By the way, note that not every quadratic polynomial has a real root.)*

Problem 4.5. *Are the following statements true for every set X and all open sentences $P(x)$ and $Q(x)$?*
(a) $(\forall_{x\in X} P(x) \Rightarrow Q(x)) \Rightarrow (\exists_{x\in X} P(x) \Rightarrow Q(x))$.
(b) $((\exists_{x\in X} P(x)) \wedge (\forall_{x\in X} P(x) \Rightarrow Q(x))) \Rightarrow \exists_{x\in X} Q(x)$.
Justify your answer.

Problem 4.6. *Consider the following open sentences:*

- *$P(x) =$ "x is a duck"*
- *$Q(x) =$"x is one of my poultry"*
- *$R(x) =$ "x is an officer"*
- *$S(x) =$ "x is willing to waltz"*

Let the universe of discourse consist of all living creatures. Match appropriate letters with numbers:

1. $\forall_x P(x) \Rightarrow \neg S(x)$ *2.* $\forall_x R(x) \Rightarrow S(x)$ *3.* $\forall_x Q(x) \Rightarrow \neg R(x)$

4. $\forall_x Q(x) \Rightarrow P(x)$ *5.* $\exists_x P(x) \Rightarrow \neg S(x)$

a) Some ducks are not willing to waltz.
b) No ducks are willing to waltz.

c) No officers ever decline to waltz.
d) All my poultry are ducks.
e) My poultry are not officers.

Problem 4.7. *Which of the following are true for* $A = \{(1,1),(1,2),(2,1),(3,2)\}$*? Justify your answers.*

(1) $\forall_{x\in\{1,2,3\}}\ \exists_{y\in\{1,2,3\}}\ (x,y)\in A$
(2) $\exists x\in\{1,2,3\}\ \forall_{y\in\{1,2,3\}}\ (x,y)\in A$
(3) $\exists_{x\in\{1,2,3\}}\ \exists_{y\in\{1,2,3\}}\ ((x,y)\in A\wedge(y,x)\in A).$

5. Functions

Informally speaking a function f from a set X to a set Y is an assignment such that every element of X is assigned an element of Y. We write $f : X \to Y$. If f sends x to y then we write, $f(x) = y$.

“Math Proofs”, Ch. 9, “How to Prove It” Ch. 5.1-2,5.4

We mentioned before that all mathematical notions can be defined rigorously on the basis of set theory. Can we define functions as sets then? Yes! For that, we use the fact that each function is determined by its graph, which is a subset of $X \times Y$.

Definition 5.1 (Formal Definition of Function)**.** *A function is a triple (X, Y, f), where X, Y are sets and f is a subset of $X \times Y$ with the following properties:*
(1) If $x \in X$, then there exists $y \in Y$ such that $(x, y) \in f$.
(2) If $(x, y) \in f$ and $(x, z) \in f$, then $y = z$.

Note that using the quantifier $\exists!$ introduced in Sec 2, we can combine these conditions into one: $\forall_{x \in X} \exists!_{y \in Y} (x, y) \in f$.

We call X the domain of the function and Y its codomain. The more traditional notation for a function (X, Y, f) is $f : X \to Y$. (From now on we will use this notation.) We write $f(x) = y$ if $(x, y) \in f$. Note that (1) means that for each $x \in X$, $f(x)$ exists. Conditions (1) – (2) mean that $f(x)$ has a unique value. (“unique” = “only one”). In other words, these conditions are the vertical line test.
Functions are also often referred to as maps.

Any function f on a finite set can be easily visualized like this:

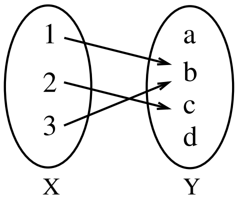

Figure 2. Example of function $f : \{1, 2, 3\} \to \{a, b, c, d\}$.

The formal definition of this function is ....

Functions whose arguments and values are real numbers can be visualized by their graphs. For example, see Figure 3 below.

More generally functions f from $X \subseteq \mathbb{R}^n$ into $Y \subseteq \mathbb{R}^m$ can be visualized by their graphs, cf. Problem 5.7.

Definition 5.2 (Identity function)**.** *The identity function $id_X : X \to X$ is defined by $id_X(x) = x$ for all $x \in X$.*

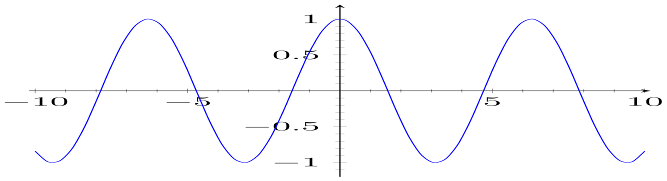

FIGURE 3. Graph of $y = cos(x)$

Definition 5.3 (Composition)**.** *If $f\colon X \to Y$ and $g\colon Y \to Z$ then the composition of f with g is the function $g \circ f$ from X to Z defined by $(g \circ f)(x) = g(f(x))$.*

Example 5.4. *If $f, g : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$ and $g(x) = x + 1$ then $g \circ f =$... and $f \circ g =$....*

If you are asked to show that a function with certain properties exists, usually you accomplish it by defining such function. For example, show that there is a function $g : \{a, b, c, d\} \to \{1, 2, 3\}$ such that f of Figure 2 composed with g satisfies: $(g \circ f)(1) = 1$ and $(g \circ f)(2) = 2$.

Definition 5.5 (Image)**.** *Let $f\colon X \to Y$ be a function and let A be a subset of X. Then the image of A under f, denoted $f(A)$, is defined by $f(A) = \{f(a) : a \in A\}$. Alternatively,*

$$f(A) = \{y \in Y : y = f(a) \textit{ for some } a \in A\}.$$

Example 5.6. *For the function in Fig. 2, $f(\{2, 3\}) = f(\{1, 2, 3\}) = \{b, c\}$.*

The image of f is $f(X)$, i.e. it is the image of X under f, often called the range of f. That is, the image of f, a.k.a the range of f is $\{f(x) : x \in X\}$.

Definition 5.7 (Inverse image)**.** *Let $f\colon X \to Y$ be a function and let B be a subset of Y. Then the inverse image of B under f, or preimage of B under f, denoted $f^{-1}(B)$, is defined by*

$$f^{-1}(B) = \{x \in X : f(x) \in B\}.$$

Note that f^{-1} can also denote the inverse function, which is related but different notion and will be discussed in the next section.

Example 5.8. *If $f(x) = x^3 - x$, $f : \mathbb{R} \to \mathbb{R}$, then $f^{-1}(\{0\}) = \{-1, 0, 1\}$.*

To recap:

$y \in f(A)$ means that $y = f(a)$ for some $a \in A$.

$x \in f^{-1}(B)$ means that $f(x) \in B$.

Proposition 5.9 (Image of inverse image is a subset)**.** *$f(f^{-1}(B)) \subseteq B$ for all $B \subseteq Y$.*

Proof. Let $y \in f(f^{-1}(B))$. We need to prove that $y \in B$. By the definition of the image, $y = f(x)$ for some $x \in f^{-1}(B)$. By the definition of the inverse image, $f(x) \in B$. Therefore, $y \in B$. □

PROBLEMS 5.

Problem 5.1. *Let $X = \{1, 2, 3, 4\}$ and $Y = \mathbb{Z}$. Using the formal definition of function, check whether the following subsets of $X \times Y$ correspond to functions of X to Y. Give your reasons why these are or are not functions:*

(1) $f = \{(1, 4), (2, 3), (1, -2), (3, 1), (4, 1)\}$
(2) $f = \{(1, 0), (2, -1), (3, 1)\}$.

Problem 5.2. *Using the formal definition of function, check whether the following subsets of $X \times Y$ correspond to functions of X to Y. Give your reasons why these are or are not functions:*

(1) $f = \{(x, y) \in X \times Y : \ x = y^4\}$, *where* $X = \{x \in \mathbb{R} : \ x \geq 0\}$ *and* $Y = \mathbb{R}$.
(2) $f = \{(x, y) \in X \times Y : \ x^2 + y^2 = 1$ *and* $y \geq 0\}$, *where* $X = \mathbb{R}$ *and* $Y = \{y \in \mathbb{R} : \ y \geq 0\}$.

Problem 5.3. *Let $X = \{1, 2\}$ and $Y = \{1, 2, 3\}$. Write down all functions from X to Y.*

Problem 5.4. *Let $f : X \to Y$ be a function. Let $x \in X$ and $y \in Y$. Is it true that $f(x) = y$? If not true, then give a counterexample.*

Problem 5.5. *Let X be a finite set with m elements, and Y be a finite set with n elements. Find a formula expressing the number of different functions from X to Y. Prove your result. What notation does this suggest for "the set of all functions from X to Y"?*

Problem 5.6. *If X is a finite set, then the set of all functions from X to $\{0, 1\}$ has the same number of elements as the power set of X, by Problem 5.5 above and by the discussion of power sets in Section 2. So let X be a set (finite or not). Show that each function of X to $\{0, 1\}$ determines a subset of X and vice-versa.*

Problem 5.7. *What kind of a geometric figure is the graph of a continuous function*
(a) $f : \mathbb{R}^2 \to \mathbb{R}$*?*
(b) $f : \mathbb{R} \to \mathbb{R}^2$

Problem 5.8. *Let* $X = \{1, 2, 3, 4\}$ *and* $Y = \{1, 2, 3, 4, 5\}$*. Define a function* $f : X \to Y$ *by* $f(1) = 2, f(2) = 2, f(3) = 5, f(4) = 4$*.*

i. *Find the image of* f*.*

ii. *Find* $f^{-1}(\{3, 4\})$*.*

iii. *Find* $f(\{1, 2, 4\})$*.*

iv. *Find* $f^{-1}(\{3\})$*.*

v. *Find* $f(f^{-1}(\{2, 3\}))$*.*

Problem 5.9. *Describe the set* $sin^{-1}(\{1\})$ *explicitly using math symbols only (no words).*

Problem 5.10. *Let* $X = \{1, \ldots, 5\}, Y = \{1, \ldots, 6\}, Z = \{1, \ldots, 4\}$*. Define* $f : X \to Y$ *by* $1, 2, 3, 4, 5 \to 2, 4, 3, 6, 1$ *and* $g : Y \to Z$ *by* $1, 2, 3, 4, 5, 6 \to 4, 4, 1, 3, 2, 2$*. Find* $g \circ f$*.*

Problem 5.11. *Let* $f, g : \mathbb{R} \to \mathbb{R}$ *be defined by* $f(x) = x^3 + 1$ *for all* $x \in \mathbb{R}$ *and* $g(t) = 1 - t$ *for all* $t \in \mathbb{R}$*. Find* $(f \circ g)(3)$ *and* $(g \circ f)(3)$*.*

Problem 5.12. *Let* $f : X \to Y$ *be a function.*
(i) Let $B \subseteq Y$ *be a subset. Prove that* $f(f^{-1}(B)) = B$ *if and only if* $B \subset \text{image}\, f$*.*
(ii) Prove that $A \subseteq f^{-1}(f(A))$ *for all* $A \subseteq X$*.*

Problem 5.13. *Let* $f : X \to Y$ *be a function. Let* X_1 *and* X_2 *be subsets of* X *and* Y_1 *and* Y_2 *be subsets of* Y*. Prove the following:*

i) $f(X_1 \cup X_2) = f(X_1) \cup f(X_2)$

ii) $f(X_1 \cap X_2) \subseteq f(X_1) \cap f(X_2)$

iii) $f^{-1}(Y_1 \cup Y_2) = f^{-1}(Y_1) \cup f^{-1}(Y_2)$

iv) $f^{-1}(Y_1 \cap Y_2) = f^{-1}(Y_1) \cap f^{-1}(Y_2)$

v) Give an example where $f(X_1 \cap X_2) \neq f(X_1) \cap f(X_2)$*.*

Problem 5.14. *Let* X *be a set and let* $f : X \to \{1, 2, 3, 4\}$ *be a function. Let* $X_i = f^{-1}(\{i\})$ *for* $i = 1, 2, 3,$ *and* 4*.*

i) Prove that $X_i \cap X_j = \emptyset$ *for* $i \neq j$*.*

ii) Prove that $X = X_1 \cup \ldots \cup X_4$*.*

6. Inverse Functions

Definition 6.1 (One to one)**.** *A function $f \colon X \to Y$ is one to one (or, "1-1" or "injective") if $f(x_1) = f(x_2)$ for some x_1 and x_2 in X always implies that $x_1 = x_2$.*

"Math Proofs" Ch. 9.6, "How To Prove It" Ch. 5.3

Definition 6.2 (Onto)**.** *A function $f \colon X \to Y$ is onto (or, "surjective") if for each $y \in Y$ there is an $x \in X$ such that $f(x) = y$.*

Note that f is onto if and only if $f(X) = Y$.

Example 6.3. *Consider $f(x) = x^2$. (Formally, $f = \{(x, y) \in X \times Y : y = x^2\} = \{(x, x^2) : x \in X\}$. Then*
(a) f considered as function from $\mathbb{R}$ to $\mathbb{R}$, $f : \mathbb{R} \to \mathbb{R}$, is neither 1-1 *nor onto.*
(b) $f : (0, \infty) \to \mathbb{R}$ is 1-1 *but not onto.*
(c) $f : \mathbb{R} \to [0, \infty)$ is onto but not 1-1.
(d) $f : (0, \infty) \to (0, \infty)$ is 1-1 *and onto.*

The example above shows that the specification of the domain and of the codomain is an important and integral part of a function's definition.

Recall that formally speaking a function is a triple (X, Y, f) (where $f \subseteq X \times Y$ has to satisfy some properties). In that formal approach, the inverse function to f is the triple (Y, X, f^{-1}), where

$$f^{-1} = \{(y, x) \in Y \times X : \ (x, y) \in f\},$$

if f^{-1} satisfies the condition of being a function.

We will be content, however, with the calculus definition of the inverse function:

Definition 6.4. *We say that $g : Y \to X$ is an inverse function to $f : X \to Y$ iff $g \circ f$ is the identity on X and $f \circ g$ is the identity on Y, i.e. $g \circ f = id_X$, $f \circ g = id_Y$ (where id stands for the identity function defined in the previous section).*

Theorem 6.5. *A function f has an inverse function if and only if f is one to one and onto. In this case, the inverse function is unique.*

Proof in class.

Definition 6.6 (bijection)**.** *A function which is* 1-1 *and onto is called a bijection.*

Definition 6.7. *If $f : X \to Y$ is a bijection, we denote the inverse function $Y \to X$ by f^{-1}.*

Note: The same symbol "f^{-1}" is used for both the inverse functions and preimages. If X, Y are sets, $f : X \to Y$, $S \subseteq Y$ then we previously defined $f^{-1}(S)$ to be the preimage of S under f, namely $\{x \in X : f(x) \in S\}$. Notice that this is defined for **any** function f, whereas the inverse function is defined **only** if f is a bijection.

Example 6.8. *If $f : \mathbb{R} \to \mathbb{R}$ is given by $f(x) = x^2$ then $f^{-1}(1)$ has not been defined, but $f^{-1}(\{1\})$ has been defined. It is $\{1, -1\}$. Likewise $f^{-1}([0, 1)), f^{-1}(\mathbb{R})$ and $f^{-1}(\{0\})$ have been defined.*

Note that if $g : Y \to X$ is the inverse function to $f : X \to Y$ then for every $x \in X$ and $y \in Y$, $f(x) = y$ iff $g(y) = x$.

Remark 6.9. *Let $f : X \to Y$ and $g : Y \to X$ be functions. Then neither of the conditions, $g \circ f = id_X$, $f \circ g = id_Y$ alone guarantees that g is the inverse of f. In other words, any one of these conditions does not imply the other.*

Proposition 6.10. *Let $f : X \to Y$ and $g : Y \to Z$ be one to one and onto functions. Then $g \circ f : X \to Z$ is one to one and onto; and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

Theorem 6.11. *If X, Y are sets of equal, finite cardinality then*
(a) every 1-1 *function $f : X \to Y$ is onto.*
(b) every onto function $f : X \to Y$ is 1-1.
These statements are called "the Pigeonhole Principle". The Pigeonhole Principle does not hold for infinite X, Y.

Remark 6.12. *The most basic version of the Pigeonhole Principle states that if there are n pigeonholes and $n+1$ pigeons, then 2 pigeons must share a pigeonhole. See Figure 4.*

Figure 4. Pigeonhole Principle

Question 6.13. *How do you call a bijection $f : X \to X$ from a finite set X (eg. $X = \{1, 2, ..., n\}$) to itself?*

PROBLEMS 6.

Problem 6.1. *Let $X = \{1, 2, 3, 4\}$ and $Y = \{1, 2, 3, 4, 5\}$. Define a function $f : X \to Y$ by $f(1) = 2, f(2) = 2, f(3) = 5, f(4) = 4$.*

a. Is f one to one? Why or why not?

b. Is f onto? Why or why not?

c. Is there $g : Y \to X$ such that $g \circ f = id_X$?

d. Is there $g : Y \to X$ such that $f \circ g = id_Y$?

Problem 6.2. *Express the fact that a function $f : X \to Y$ is* 1-1 *using $\forall$ and $\exists$ quantifiers and other math symbols, without using any words.*

Problem 6.3. *Let $f : X \to Y$ be a one to one function, and let $A \subseteq X$ be a subset. Let x be an element of X. Prove that if $f(x) \in f(A)$ then $x \in A$.*

Problem 6.4. *Let $f : X \to Y$ be a function. Prove that $A = f^{-1}(f(A))$ for all $A \subseteq X$ if and only if f is one to one. Note: part of the problem was done in Problem 5.12(ii).*

Problem 6.5. *Let $X = \{1, 2, 3, 4\}$ and $Y = \{2, 3, 4, 5\}$. Define $f : X \to Y$ by $1, 2, 3, 4 \to 4, 2, 5, 3$. Check that f is one to one and onto and find the inverse function f^{-1}.*

Problem 6.6. *Let $f : X \to Y$ and $g : Y \to X$ be functions.*

i) Prove that $g \circ f = id_X$ implies f is one to one.

ii) Prove that $f \circ g = id_Y$ implies f is onto.

Problem 6.7. *Let $f : X \to Y$ be one to one and onto.*

i) If $g : Y \to X$ satisfies $g \circ f = id_X$, prove that $g = f^{-1}$.

ii) If $g : Y \to X$ satisfies $f \circ g = id_Y$, prove that $g = f^{-1}$.

Problem 6.8. *Let $X = \{1, 2, 3\}$, $Y = \{a, b, c, d, e\}$.*
(a) Let $f : X \to Y$ be a function, given by $f(1) = a$, $f(2) = b$, $f(3) = c$. Prove there exists a function $g : Y \to X$ such that $g \circ f = id_X$. Is g the inverse function to f? Hint: define g on $f(X)$ to make $g \circ f = id_X$. Then define g on $Y - f(X)$. Does it matter how you define g on $Y - f(X)$?
(b) Is it true that such function g exists for $f(1) = a$, $f(2) = f(3) = c$? Justify your answer.

Problem 6.9. *Let $f : X \to Y$ be a function, where X and Y are nonempty sets. If f is one to one, prove there exists a function $g : Y \to X$ such that $g \circ f = id_X$.* Hint: define g on $f(X)$ to make $g \circ f = id_X$. Then define g on $Y - f(X)$. Does it matter how you define g on $Y - f(X)$?

Problem 6.10. *Prove Proposition 6.10.*

Problem 6.11. *Give an example showing that Theorem 6.11(a) does not hold for* $X = Y = \mathbb{N}$ *(set of all natural numbers) and an example showing that Theorem 6.11(b) does not hold for* $X = Y = \mathbb{N}$ *either.*

Problem 6.12. *Let* $f : X \to Y$ *be a function, where* X *and* Y *are non-empty sets. If* f *is onto, prove there exists a function* $g : Y \to X$ *such that* $f \circ g = id_Y$*.*

Problem 6.13. *Using the formal definition of function, which of the following functions is* 1-1*? Which of them is onto?*
(1) f *is the set of all points of the form* (x, x^2) *in* $\mathbb{R} \times \mathbb{R}$
(2) f *is the set of all points of the form* (x, x^2) *in* $[0, \infty) \times \mathbb{R}$
(3) f *is the set of all points of the form* (x, x^2) *in* $\mathbb{R} \times [0, \infty)$

Problem 6.14. *Let* $f = \{(x, y) \in \mathbb{R}^2 : \ y = x^5 + 4x^3 + x + 1\}$*.*
(1) Prove that
  (a) f *is onto.*
  (b) f *is* 1-1*.*
(2) Prove that $g = \{(x, y) \in \mathbb{R}^2 : \ x = y^5 + 4y^3 + y + 1\}$ *is a function.*
(You will need to use calculus to prove part (1).)

Problem 6.15. *Give an example of* $f : X \to Y$ *and* $g : Y \to X$ *such that* $g \circ f = id_X$ *but* g *is not the inverse of* f*.*

7. Natural Numbers

As we mentioned in Section 2, all mathematical notions can be defined in terms of set theory. That applies to numbers, too. Assuming a common sense knowledge of mathematics, we could define the natural numbers $1, 2, ...$ something like this:
$1 = \{\emptyset\}$, a set with 1 element
$2 = \{\emptyset, \{\emptyset\}\}$, a set with two elements
$3 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$, a set with 3 elements
and so on.

More generally, we say that the successor A' of a set A is given by

$$A' = A \cup \{A\}.$$

We could then define the set $\mathbb{N}$ of natural numbers as the smallest set containing 1, and such that for every n in $\mathbb{N}$ also n' is in $\mathbb{N}$. (The existence of such set is guaranteed by one of the Zermelo-Frankel axioms of set theory.) Some mathematicians (but not us) include 0 in the set of natural numbers.

We could then use the Zermelo-Frankel axioms of set theory to develop the arithmetic of natural numbers (addition, multiplication, and their properties), but that would be rather technical. Instead, we will follow an alternative approach to natural numbers, through five axioms formulated by a 19th century Italian mathematician, G. Peano. Later we will define rational numbers and, more generally, real and complex numbers on the basis of the natural numbers.

Peano's axioms for the natural numbers $\mathbb{N}$.

Axiom 1: 1 is a natural number. (That is, the set $\mathbb{N}$ is not empty.)

Axiom 2: For each n there exists exactly one natural number, called the successor of n, which will be denoted by n'. (We cannot call it $n+1$ since $+$ is not defined yet.)

Axiom 3: For every n, we have $n' \neq 1$.

Axiom 4: If $n' = m'$ then $n = m$. (We will often use its contrapositive: If $n \neq m$ then $n' \neq m'$.)

Axiom 5 (Axiom of Induction, also known as Principle of Mathematical Induction) Let $P(n)$ be a statement for each $n \in \mathbb{N}$. If both of the following hold:

"Math Proofs" Ch. 6.1, "How to Prove it" Ch.6

(1) $P(1)$ is true (<u>the base step</u>)
(2) For each $k \in \mathbb{N}$, if $P(k)$ is true then $P(k')$ is true (<u>the inductive step</u>)

then $P(n)$ is true for all $n \in \mathbb{N}$.

This principle is often explained by analogy with falling dominoes:

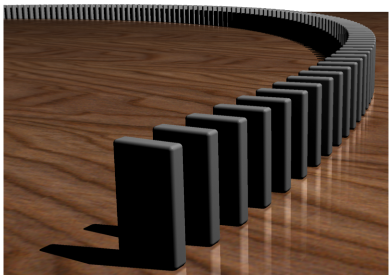

Figure 5. Dominoes

The idea here is that if

- the first domino falls, and
- any falling domino trips the next one

then all dominoes fall.

More on the Principle of Mathematical Induction can be found in "Mathematical Proofs", Ch. 6.

Note that all known properties of the natural numbers can be defined and be derived from Peano's axioms.

Using Axiom 2, we define
$2 = 1'$,
$3 = 2'$,
$4 = 3'$,
$5 = 4'$, $6 = 5'$, $7 = 6'$, $8 = 7'$, $9 = 8'$.

Note that by Axiom 3, we have that $2 \neq 1$. We are going to see later that if m is obtained from n by taking a sequence of its successors, then $m \neq n$. Let us start with a simple instance of this claim:

Proposition 7.1. $3 \neq 1$ *and* $3 \neq 2$.

Proof. $3 \neq 1$ by Axiom 3. We prove $3 \neq 2$ by contradiction.
Suppose that the statement is false, i.e. that $3 = 2$. Then, by Axiom 4, we have $2 = 1$, contradicting Axiom 3 since $2 = 1'$. □

Axiom 5 implies that the only natural numbers are $1, 2, 3, 4, 5, ...$

We denote the set of all natural numbers by $\mathbb{N}$. Hence $\mathbb{N} = \{1, 2, 3, 4, ...\}$.

One uses Axiom 5 to prove various statements about natural numbers, as illustrated below:

Theorem 7.2. $\forall_{n\in\mathbb{N}}\ n' \neq n$.

Proof. (by the Axiom of Induction).
Let $P(n) =$ "$n' \neq n$". Then $P(1) =$ "$2 \neq 1$" holds by Axiom ....
The inductive step says that if $k' \neq k$ then $(k')' \neq k'$. This implication follows from Axiom 4 for $n = k$ and $m = k'$. □

Theorem 7.3. *For every $n \neq 1$, there exists m such that $n = m'$.*

Proof left as HW.

The addition of natural numbers is defined through the following theorem:

Theorem 7.4 (Existence of addition)**.** *To every pair of natural numbers n and m we may assign in exactly one way a natural number, written $n + m$, such that*
(1) $n + 1 = n'$ for every n,
(2) $n + m' = (n + m)'$ for every n and every m.

Proof. (Difficult. Sketch) First one needs to prove that for each n there is a way of defining $n+m$ for all $m \in \mathbb{N}$ such that the conditions above hold. Then one needs to show that this can be done in only one way. Both steps are proved by induction on m. □

From now on we can (and will) denote n' by $n + 1$.

Theorem 7.5 (Associativity of $+$ in $\mathbb{N}$)**.** $\forall_{a,b,c\in\mathbb{N}}\ (a+b)+c = a+(b+c)$

We often denote $(a + b) + c$ and $a + (b + c)$ by $a + b + c$.

Theorem 7.6 (Commutativity of $+$ in $\mathbb{N}$)**.** $\forall_{a,b\in\mathbb{N}}\ a + b = b + a$

The proofs of Theorems 7.4-7.6 are by Axiom of Induction as well, see E. Landau, Foundations of Analysis. We skip these proofs since they are too difficult and lengthy for inclusion here.

We will apply this principle to the proof of the following:

Theorem 7.7. $\forall_{a,b\in\mathbb{N}}\ a + b \neq b$.

Proof. Fix $a \in \mathbb{N}$. Let $P(b)$ be the statement "$a + b \neq b$." We are going to prove $P(b)$ for all $b \in \mathbb{N}$ by the Principle of Mathematical Induction:
By Theorem 7.4(1) and Axiom 3, $a + 1 = a' \neq 1$. Hence, the base step, $P(1)$, holds.
Inductive Step: Assume that $P(k)$ holds. Then $a + k \neq k$. By Axiom 4, $(a + k)' \neq k'$. Therefore, by Theorem 7.4, $a + k' \neq k'$. Since $k' = k + 1$, $P(k + 1)$ holds. Since both, the base step and the inductive step hold, the statement $P(b)$ is true for all $b \in \mathbb{N}$ by the Principle of Induction. □ □

Definition 7.8.
- *$a > b$ if $a = b + c$ for some $c \in \mathbb{N}$. Equivalently, we write $b < a$.*
- *$a \geq b$ iff $a > b$ or $a = b$. Similarly, $a \leq b$ iff $a < b$ or $a = b$.*

Theorem 7.9. $\forall_{n\in\mathbb{N}}\ n \geq 1$.

Proof. By Thm 7.3, either $n = 1$ or $n = m + 1$ for some m. The latter case implies that $n > 1$. □

Theorem 7.10. *For every $a, b \in \mathbb{N}$ exactly one of the following must hold:*
(1) $a = b$
(2) $a > b$
(3) $b > a$.

Proof. (i) It follows from Theorem 7.7 that for every $a, b \in \mathbb{N}$ at most one of the above conditions hold. Details left as HW.
(ii) For every $a, b \in \mathbb{N}$ at least one of the above conditions hold: For any a, let C_a be the set of natural numbers b such that at least one of the conditions (1)-(3) holds. Then one can prove that $1 \in C_a$, and that for any n if $n \in C_a$ then $n + 1 \in C_a$. (Details may be discussed in class or HW). Therefore, by the Principle of Mathematical Induction $C_a = \mathbb{N}$. That means that for every a and b, at least one of the above conditions (1)-(3) hold. □

Theorem 7.11 (including Definition)**.** *If $a > b$ then there is a unique c such that $a = b + c$. We denote such c by $a - b$.*

Theorem 7.12 (Well-ordering Principle)**.** *Every non-empty set $A \subseteq \mathbb{N}$ has its smallest element, that is an $a_0 \in A$ such that $a_0 \leq a$ for all $a \in A$.*

In other words, every non-empty set of natural numbers has the smallest element. Note that many other sets, e.g. the interval $(0, 1)$, do not have the smallest element.

Proof of Thm 7.12 by induction: Let $P(n)$ be the statement that every $A \subseteq \mathbb{N}$ with at least one element $a \leq n$ has the smallest element. Then the base case, $P(1)$, holds since every subset $A \subseteq \mathbb{N}$ with an element $a \leq 1$ has $a = 1$ as its smallest element.

Assume now that the statement P holds for n. We will prove $P(n+1)$ for $n + 1$. Take any $A \subseteq \mathbb{N}$ with at least one element $a \leq n + 1$.

- If A has an element smaller or equal to n then the statement holds by the inductive assumption.

- Otherwise, A has no element smaller or equal to n. Then the $a \in A$ above is $n+1$ and by the above assumptions, it is the smallest element of A.

Hence, the statement of theorem follows by induction. □

Our proof of Well-ordering Principle was based on the Induction Principle.

Multiplication.

Theorem 7.13 (Existence of multiplication)**.** *To every pair of natural numbers n and m we may assign in exactly one way a natural number, written $n \cdot m$, such that*

- $n \cdot 1 = n$ *for every* n,
- $n \cdot m' = n \cdot m + n$ *for every* n *and every* m.

We often abbreviate $n \cdot m$ to $n\,m$.

Theorem 7.14 (Commutativity of Multiplication)**.** *For all m and n in $\mathbb{N}$, $m \cdot n = n \cdot m$.*

Theorem 7.15 (Distributive Law for Multiplication)**.** *For all ℓ, m and n in $\mathbb{N}$, $\ell \cdot (m + n) = \ell \cdot m + \ell \cdot n$.*

Theorem 7.16 (Associativity of Multiplication)**.** *For all ℓ, m and n in $\mathbb{N}$, $(\ell \cdot m) \cdot n = \ell \cdot (m \cdot n)$.*

PROBLEMS 7.

Problem 7.1. *Prove that 4 (defined as $3'$) is not equal to 1, 2, nor 3.*

Problem 7.2. *Using your knowledge (not restricted to these notes) show that the set $[0, \infty)$ (the non-negative real numbers) does not satisfy the Well-ordering principle.*

When solving these problems you can only refer to axioms and statements made in these notes only.

Problem 7.3. *Prove Thm 7.3.*
Hint 1: Prove it by induction. What should $P(n)$ be?
Hint 2: $P(n)$ should be "$n = 1$ or $n = m'$ for some m".

Problem 7.4. *Prove the following piece of Thm 7.10: For every $a, b \in \mathbb{N}$ at most of one of the three alternatives of Thm 7.10* holds. *Hint: Use Thm 7.7.*

Problem 7.5. *Prove that if $a < b$ and $b < c$ then $a < c$.*

Problem 7.6. *State the Principle of Mathematical Induction for* $P(n)$, $n \in \mathbb{N}$, *using math symbols, without any words.*

8. Integers

For each natural number, n, consider a new number (symbol), $-n$. The numbers $1, 2, 3, ..., -1, -2, -3, ...$ and zero, 0, are called integers.

$$\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}.$$

($\mathbb{Z}$ stands for German "Zahlen" — numbers.)

We call $1, 2, ...$ positive integers and the numbers $-1, -2, -3, ...$ negative integers. Hence, negative integers are defined as natural numbers with a minus sign (dash), in front of them. Note that the minus sign is a unary operation here, different than the binary operation of subtraction of natural numbers of Sec. 7. The set of positive integers is just $\mathbb{N}$. We denote the set of negative integers by $-\mathbb{N}$.

Definition 8.1 (The absolute value)**.** *If $n \in \mathbb{N}$ then $|n| = n$ and $|-n| = n$. Additionally, $|0| = 0$.*

Definition 8.2 ($-n$)**.** *We define -0 to be 0. For $n \in -\mathbb{N}$, we define $-n$ to be $|n|$. We refer to $-n$ as "the negative of n" or "negative n".*

Lemma 8.3 ($-(-n) = n$)**.** *For all $n \in \mathbb{Z}$, $-(-n) = n$.*

Proof. There are three cases to consider: $n \in \mathbb{N}, n \in -\mathbb{N}$ and $n = 0$. We'll just do one here. (The others might be given as homework of quiz problems.) Suppose $n \in \mathbb{N}$. Then $-n \in -\mathbb{N}$. So, according to definition 8.2, $-(-n) = |-n|$. But according to definition 8.1, $|-n| = n$. □

Definition 8.4 ($+$ on $\mathbb{Z}$)**.** *We define addition of integers as follows,*

$$a + b = \begin{cases} a + b & \text{if } a, b \text{ are positive} \\ -(|a| + |b|) & \text{if } a, b \text{ are negative} \\ a & \text{if } b = 0 \\ b & \text{if } a = 0. \end{cases}$$

If a is positive and b negative, then

$$a + b = \begin{cases} a - |b| & \text{if } a > |b| \\ -(|b| - a) & \text{if } |b| > a \\ 0 & \text{if } |b| = a. \end{cases} \tag{5}$$

If a is negative and b positive, then we define $a + b$ similarly.

Theorem 8.5 (Associativity Law for Integers)**.** $\forall_{a,b,c\in\mathbb{Z}}\ (a + b) + c = a + (b + c)$.

Theorem 8.6 (Commutativity Law for Integers)**.** $\forall_{a,b\in\mathbb{Z}}\ a + b = b + a$.

Lemma 8.7. *For all $a, b \in \mathbb{N}$, such that $a > b$ $a - b = a + (-b)$.*

Proof. By associativity, $(a+(-b))+b = a+(b+(-b))$. By the definition of $+$, this is equal to $a+0$ and thence to a. Thus, $a+(-b) = a-b$ by the definition of $a-b$. □

Definition 8.8. *We define $a-b$ to be $a+(-b)$ for $a, b \in \mathbb{Z}$ such that $a-b$ is not already defined.*

Another way mathematicians often approach this type of situation is to say, "we define $a-b$ to be $a+(-b)$ for all $a, b \in \mathbb{Z}$; note that this is compatible with our previous definition."

Lemma 8.9. *For all $a \in \mathbb{Z}$, $a-a=0$.*

Proof. One just checks it from the definitions in the three cases: $a \in \mathbb{N}, a \in -\mathbb{N}$ and $a=0$. □

Proposition 8.10. *If $a=b+c$ then $c=a-b$.*

Proof. If $a=b+c$ then $a+(-b)=c+b+(-b)=c$. □

Corollary 8.11 (Cancellation Property)**.** *If $a+c=b+c$ then $a=b$.*

Proof. $a=(a+c)+(-c)=(b+c)+(-c)=b$. □

Multiplication. We now extend the definition of multiplication in $\mathbb{N}$ to elements of $\mathbb{Z}$ that are not in $\mathbb{N}$.

Definition 8.12 (Multiplication)**.** *Take $a, b \in \mathbb{Z}$. Then $a \cdot b$ is defined to be*

$$\begin{cases} a \cdot b & \text{if } a, b \in \mathbb{N} \text{ (defined in Sec. 7} \\ 0, & \text{if } a=0 \text{ or } b=0, \\ |a||b| & \text{if } a, b \in -\mathbb{N}, \\ -(|a||b|) & \text{if } a \in -\mathbb{N}, b \in \mathbb{N}, \text{ or } a \in \mathbb{N}, b \in -\mathbb{N}. \end{cases}$$

Since this covers all possibilities for $a, b \in \mathbb{Z}$ except $a, b \in \mathbb{N}$, the product $a \cdot b$ is now defin ed for all $a, b \in \mathbb{Z}$.

Theorem 8.13 (Commutative property of multiplication in $\mathbb{Z}$)**.**
For all $a, b \in \mathbb{Z}$, $a \cdot b = b \cdot a$.

Proof. Can be done by considering cases: $a \in \mathbb{N}$, $a=0$, and $a \in -\mathbb{N}$ and, similarly, $b \in \mathbb{N}$, $b=0$, and $b \in -\mathbb{N}$. Altogether, there are $3 \times 3 = 9$ cases. In the first, case, $a, b \in \mathbb{N}$, it is the consequence of Theorem 7.14. The proof of remaining cases is left to the reader. □

Lemma 8.14. *For all $a, b \in \mathbb{Z}$, $-(a+b)=(-a)+(-b)$.*

Proof. Follows from Theorem 8.5 and Lemma 8.9:

$$\begin{aligned}(a+b)+((-a)+(-b)) &= (a+b)+((-b)+(-a))\\ &= ((a+b)+(-b))+(-a))\\ &= (a+(b+(-b))+(-a))\\ &= a+(-a)\\ &= 0\end{aligned}$$

It then follows that $-(a+b)=(-a)+(-b)$. □

Theorem 8.15 (Distributivity of multiplication over addition in $\mathbb{Z}$)**.** *For every $a, b, c \in \mathbb{Z}$ we have*

$$a\cdot(b+c)=a\cdot b+a\cdot c.$$

Theorem 8.16 (Associativity of Multiplication in $\mathbb{Z}$)**.**

$$\forall_{a,b,c\in\mathbb{Z}}\ a\cdot(b\cdot c)=(a\cdot b)\cdot c.$$

Proof. Can be done by exhaustion. Split into cases based on the definition of $\cdot$, and handle each case using the commutativity of multiplication in $\mathbb{N}$. (All or part of this may be used as a homework, quiz, or exam problem.) □

Proposition 8.17. *(1)* $\forall_{a\in\mathbb{Z}}\ a\cdot(-1)=-a$.
(2) $\forall_{a,b\in\mathbb{Z}}\ (-a)\cdot b=a\cdot(-b)=-(ab)$.
(3) $\forall_{a,b\in\mathbb{Z}}\ (-a)(-b)=ab$.

Proof. Left to the reader – may be used as a homework, quiz, or exam problem. □

Note that $a\cdot(-1)=-a$ is a property of multiplication and not the definition of $-a$ (which for $a\in\mathbb{N}$ was defined formally as a with the minus sign in front of it).

Theorem 8.18. *If $a\neq 0$ and $b\neq 0$ then $a\cdot b\neq 0$.*

Corollary 8.19 (Cancellation of multiplication)**.** *If $a\neq 0$, then $a\cdot b=a\cdot c$ implies $b=c$.*

Ordering of integers

Definition 8.20. *For any $a,b\in\mathbb{Z}$ we say that $a>b$ iff $a-b\in\mathbb{N}$.*

Note that this definition agrees with the previous one for $a,b\in\mathbb{N}$.

Theorem 8.21 (Properties of inequalities)**.**

(1) If $a<b$ and $b<c$ then $a<c$.

(2) If $a < b$ then $a + c < b + c$
(3) If $a < b$ and $c > 0$ then $ac < bc$.
(4) If $c < 0$ and $a < b$, then $ac > bc$.
(5) If $c > 0$ and $ac < bc$, then $a < b$.
(6) If $c < 0$ and $ac < bc$, then $a > b$.
(7) If $0 < a < b$ and $0 < c < d$, then $a \cdot c < b \cdot d$.

Theorem 8.22. *For every $a, b \in \mathbb{Z}$ exactly one of the following must be the case: $a > b$ or $a < b$ or $a = b$.*

PROBLEMS 8.

When solving these problems you can only refer to axioms and statements made in these notes only.

Problem 8.1. *Prove Proposition 8.17(1),(2).*
Note that once you prove one of the statements, (1) or (2), you can use it to prove the other one, but you cannot claim that (1) follows from (2) and (2) follows from (1) at the same time. (That would be a circular reasoning.)

Problem 8.2. *Prove Proposition 8.17(3).*
Hint: Prove the statement by induction with respect to b.

Problem 8.3. *Prove Corollary 8.19. Hint: Use Thm 8.18.*

Problem 8.4. *Prove Prop. 8.21(1)-(3).*

Problem 8.5. *The formulas $a - |b|$ and $-(|b| - a)$ in the first two cases on the right hand side of (5) "look" the same. Why do we need to write them in these two ways? (A single sentence answer is sufficient.)*

9. Examples of Inductive Proofs

Definition 9.1. *For any integer x, let x^n be defined as follows: $x^1 = x$ and $x^{n+1} = x^n \cdot x$ for all $n \in \mathbb{N}$.*

"Math Proofs", Ch. 6, "How to Prove it" Ch.

Let us illustrate the method of induction by the following example:

Proposition 9.2.

$$1 + 2 + ... + n = \frac{n(n+1)}{2}$$

for every n.

Proof (by induction): The inductive statement is

$$P(n) = \text{“ } 1 + 2 + ... + n = \frac{n(n+1)}{2} \text{ ''}.$$

The base case, P(1)=" $1 = \frac{1 \cdot 2}{2}$ " holds.

The proof of the inductive step: Assume $P(k)$ for some $k \in \mathbb{N}$, i.e.

$$1 + 2 + ... + k = \frac{k(k+1)}{2}. \tag{6}$$

We need to prove $P(k+1)$, i.e.

$$1 + 2 + ... + (k+1) = \frac{(k+1)(k+2)}{2}. \tag{7}$$

Note that subtracting (6) from this equation reduces it to

$$k + 1 = \frac{(k+1)(k+2)}{2} - \frac{k(k+1)}{2}. \tag{8}$$

Therefore, it is enough to prove this identity. By simplifying the right side, we reduce it to

$$\frac{(k+1)(k+2-k)}{2} = k + 1 \tag{9}$$

and, hence, indeed (8) holds. Consequently, (6) holds. Having verified the base step and the inductive step, the Principle of Induction implies $P(n)$ for all n. □

Note that every equation in this proof is accompanied by words which put it in a proper context. These words are necessary. Without them, these equations would be ambiguous and incomprehensible to anyone (other than those who already know the proof). Let us illustrate it further with the following:

Remark 9.3. *For the sake of example consider an expression "$y = 2x + 1$". It may have multiple meanings:*

- *It defines y in terms of x and, it may or may not be a part of a definition of a function.*
- *It defines x as a solution of this equation for a certain, given y.*
- *It is given by assumption (of the statement being proven), eg. like* (6) *above.*
- *The writer claims that he or she proved $y = 2x + 1$, where x and y were defined already. (An additional explanation, "how", may be needed.)*
- *The writer declares an intention to prove $y = 2x + 1$, where x and y were defined already., eg. like* (7) *(and* (8)*, although there is more context to it).*
- *The equation holds for all possible values of variables appearing in it, eg. like* (9)*.*
- *The equation may have another more nuanced context.*

  It is necessary that you always specify the context of every equation you write, as for example in the proof above.

Remark 9.4. *Note that the inductive step proof starts with "Assume $P(k)$ for* <u>*some*</u> *$k \in \mathbb{N}$." The word "some" necessary because every new symbol in any mathematical reasoning should be introduced with the existential ("for some" or "there exists") or the universal quantifier ("for every" = "for all"). If the quantifier is missing then it is assumed universal; however that may be confusing to some readers.*

For example: "$(x+2)^2 = x^2 + 2x + 4$ for $x \in \mathbb{Z}$" means that is holds for every $x \in \mathbb{Z}$. However, it is better to state that explicitly, to avoid any ambiguity. (Note that replacing"for every" by "for some" modifies the statement. It is still true, but much weaker.)

On the other hand, "$x \cdot 3 = 12$ for $x \in \mathbb{Z}$" is false. You need to write "$x \cdot 3 = 12$ for some $x \in \mathbb{Z}$" or "There exists $x \in \mathbb{Z}$ such that $x \cdot 3 = 12$."

Going back to mathematical induction: In the inductive step, one assumes $P(k)$ for some $k \in \mathbb{N}$ (not "for every $k \in \mathbb{N}$") and proves $P(k+1)$.

Proposition 9.5.

(1) $\forall_{x,y\in\mathbb{Z},\, n\in\mathbb{N}}\ (xy)^n = x^n y^n$.
(2) $\forall_{x\in\mathbb{Z},\, n,m\in\mathbb{N}}\ x^m x^n = x^{m+n}$.
(3) $\forall_{x\in\mathbb{Z},\, n,m\in\mathbb{N}}\ (x^m)^n = x^{mn}$.
(4) $\forall_{x,y\in\mathbb{N},\, n\in\mathbb{N}}$ *if $x < y$ then $x^n < y^n$.*

Proof. (1) in class. Proofs of (2), (3), (4) are HW. All these proofs are by induction. □

Although so far we have defined natural numbers and integers only, in the rest of this section we assume the existence of real numbers and we take their basic arithmetic properties for granted.

A famous mathematical problem of 17th century asked about the value of

$$\sum_{i=1}^{\infty} \frac{1}{i^2} = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + ... =?$$

Leonard Euler proved in 1735 that it is precisely $\pi^2/6 \simeq 1.644...$ (This is the same mathematician who realized the importance of the base of the natural logarithm $e \simeq 2.718$.)

Figure 6. Leonard Euler

We will prove a weaker result:

Proposition 9.6.

$$\sum_{i=1}^{\infty} \frac{1}{i^2} \leq 2.$$

Proof. $\sum_{i=1}^{\infty} a_i$ is defined as the limit of partial sums, $lim_{n\to\infty} \sum_{i=1}^{n} a_i$. Therefore, it is enough to prove that

$$\sum_{i=1}^{n} \frac{1}{i^2} \leq 2$$

for every n.

Although this statement depends on n, it would not be possible to prove it by induction on n, because every succeeding inequality is harder than the previous one. However, quite unexpectedly, this inequality will be easier to prove if we make it stronger! Specifically, we will show

$$P(n) = \text{“ } \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \ldots + \frac{1}{n^2} \leq 2 - \frac{2}{n+1} \text{ ”},$$

for all $n \geq 1$ by induction on n.

Base step: $P(1)$ reads "$\frac{1}{1^2} \leq 2 - \frac{2}{1+1}$." Hence $P(1)$ is true. (Check this!)

Inductive Step: Assume that $P(k)$ holds, i.e.

$$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \ldots + \frac{1}{k^2} \leq 2 - \frac{2}{k+1}. \tag{10}$$

We need to prove $P(k+1)$, i.e.

$$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \ldots + \frac{1}{(k+1)^2} \leq 2 - \frac{2}{k+2}. \tag{11}$$

To get the left hand side of (11), we add $\frac{1}{(k+1)^2}$ to both sides of (10):

$$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \ldots + \frac{1}{(k+1)^2} \leq 2 - \frac{2}{k+1} + \frac{1}{(k+1)^2}. \tag{12}$$

Given (12), is enough to prove[1] that

$$2 - \frac{2}{k+1} + \frac{1}{(k+1)^2} \leq 2 - \frac{2}{k+2}.$$

(This approach is called "a forward-backward proof.") This is equivalent to

$$-\frac{2}{k+1} + \frac{1}{(k+1)^2} \leq -\frac{2}{k+2}.$$

By multiplying both sides by -1 we get (remember to change the inequality sign!)

$$\frac{2}{k+1} - \frac{1}{(k+1)^2} \geq \frac{2}{k+2},$$

i.e.,

$$\frac{2k+1}{(k+1)^2} \geq \frac{2}{k+2}.$$

By multiplying both sides by $(k+1)^2(k+2)$, we get

$$(2k+1)(k+2) \geq 2(k+1)^2.$$

Expanding, we get

$$2k^2 + 5k + 2 \geq 2k^2 + 4k + 2.$$

This is equivalent to $k \geq 0$. Therefore we proved $P(k+1)$ (assuming $P(k)$). In other words, we proved the inductive step. By the Principle of Induction, $P(n)$ holds for all $n \in \mathbb{N}$. □

[1] Note that I didn't write: "We need to prove" or "we must prove" here. Why?

Remarks:

• The proof above of the inductive step is written in the way a mathematician will usually derive it: by a sequence of successive simplifications of the statement which needs to be proved, until it becomes obvious. This is a special case of a forward-backward proof — it works forward from A and backward from B; the proof concludes when these two sequences of statements converge. Some people don't find such presentation of a proof elegant. We present a different version of that proof below, in which the argument develops forward rather than backwards.

• Note the bold faced words "it is enough to prove". It is important to realize that these words cannot be replaced by "we have to prove". Why?

Here is another version of the above proof of the inductive step, which some people find more elegant:

By the inductive assumption,

$$\frac{1}{1^2}+\frac{1}{2^2}+\frac{1}{3^2}+\ldots+\frac{1}{k^2}\le 2-\frac{2}{k+1}.$$

Hence

$$\frac{1}{1^2}+\frac{1}{2^2}+\frac{1}{3^2}+\ldots+\frac{1}{(k+1)^2}\le 2-\frac{2}{k+1}+\frac{1}{(k+1)^2}. \tag{13}$$

Now, notice that since $k\ge 0$, we have

$$2k^2+5k+2\ge 2k^2+4k+2.$$

By factoring we get,

$$(2k+1)(k+2)\ge 2(k+1)^2.$$

Now, by dividing both sides by $(k+1)^2(k+2)$, we get

$$\frac{2k+1}{(k+1)^2}=\frac{2}{k+1}-\frac{1}{(k+1)^2}\ge\frac{2}{k+2}.$$

Hence

$$-\frac{2}{k+1}+\frac{1}{(k+1)^2}\le-\frac{2}{k+2}$$

and

$$2-\frac{2}{k+1}+\frac{1}{(k+1)^2}\le 2-\frac{2}{k+2}. \tag{14}$$

Since $\le$ is transitive (i.e. $a\le b$ and $b\le c$ implies $a\le c$), and the right side of (13) is the left side of (14), we get

$$\frac{1}{1^2}+\frac{1}{2^2}+\frac{1}{3^2}+\ldots+\frac{1}{(k+1)^2}\le 2-\frac{2}{k+2}.$$

This is $P(k+1)$. This completes the proof of the inductive step. □

Notice that this proof starts from simple statements (e.g. $k > 0$) and concludes more complicated ones from them until it achieves its goal (proof of $P(k+1)$). In writing this proof, we were guided by the previous one. We rewrote the previous one in reverse order. It would be very difficult to guess this proof without having the previous one!

In Principle of Mathematical Induction both conditions, base step and the inductive step, are equally important. Consider for example, the following statement $P(n) =$ "$n = n+1$". If $k = k+1$ for some k then, by adding 1 to both sides, we get $k+1 = (k+1)+1$. Hence $P(k)$ implies $P(k+1)$. However $P(1)$ is false and, therefore, the Principle of Induction does not apply.

Here is another interesting example of faulty logic in an induction proof:

"Theorem" All cats have the same color.

"Proof": Take any group of n cats, where $n = 1, 2, ...$ We need to prove that all cats in this group have the same color. This is an obvious statement for $n = 1$.
Inductive step: Assume that the statement holds for k. We need to prove it for $k+1$. Consider a group of $k+1$ cats. Label them by numbers from 1 to $k+1$. By the inductive assumption, cats $1, ..., k$ have the same color. Similarly, by the inductive assumption cats $2, ..., k+1$ have the same color, since there are k of them. Since these two sets intersect, all $k+1$ cats have the same color. □

Where is the error in this proof? (We answer that in the class).

Below are two useful generalizations of the Principle of Induction.

Theorem 9.7 (Induction with base $\boldsymbol{m}$)**.** *Let $P(n)$ be a statement for each integer $n \geq m$. If both of the following hold:*

(1) $P(m)$ is true (the base case)
(2) For each $k \geq m$, $P(k+1)$ is true under the assumption that $P(k)$ is true (the induction step)

then $P(n)$ is true for all $n \geq m$.

Theorem 9.8 (Complete Induction)**.** *Let $Q(n)$ be a statement for each integer $n \geq 1$. If both of the following hold:*

(1) $Q(1)$ is true (the base case)
(2) For each $k \geq 1$, $Q(k+1)$ is true under the assumption that $Q(1), \ldots, Q(k)$ are all true (the complete induction step)

then $Q(n)$ is true for all $n \geq 1$.

Complete induction is also called "strong induction". Proof of this theorem is assigned as HW.

One can also use a complete induction with base other than 1. For example, consider the following statement:

Proposition 9.9. *Prove that any amount of postage of at least 6 cents can be made from 3- and 4-cent stamps.*

Proof. Let $Q(n)$ be the statement that postage of n cents can be made from 3- and 4-cent stamps.
Then $Q(6)$, $Q(7)$ and $Q(8)$ hold because $6 = 3 + 3$, $7 = 3 + 4$, and $8 = 4 + 4$. You can consider $Q(6)$, $Q(7)$ and $Q(8)$ as the base steps. Now assume that $Q(6), ..., Q(k)$ hold for $k \geq 6$. We need to prove that $Q(k + 1)$. Since $Q(6), Q(7), Q(8)$ hold, we can assume that $k + 1 \geq 9$. Then $k + 1$ postage can be composed of 3-cent stamp and $(k + 1) - 3$ postage. Since $(k + 1) - 3 \geq 6$, that postage can be made from 3- and 4-cent stamps by the inductive assumption. □

Note that the normal induction is insufficient in the above proof, as $Q(k)$ alone does not imply $Q(k + 1)$.

We will see an application of the complete induction below.

PROBLEMS 9.

Problem 9.1. *Guess a formula for* $1+3+5+\ldots+(2n-1)$ *and prove your result by induction for* $n \geq 1$.

Problem 9.2. *Use induction to prove that* $1^3+\ldots+n^3 = (1+\ldots+n)^2$.

Problem 9.3. *Use induction to prove Proposition 9.5 (2) and (3).*

Problem 9.4. *Use induction to prove Proposition 9.5 (4).*

Problem 9.5. *Prove that* $2^n \geq n^2$ *for all integers* $n \geq 4$. *(Hint: use induction with base step* $n = 4$.*)*

Problem 9.6. *Prove Theorem 9.8. Hint: Let* $P(k)$ *be the statement "*$Q(1), Q(2), ..., Q(k)$ *are true." Show that the complete induction step for* $Q(k)$ *implies the induction step for* $P(k)$.

Problem 9.7. *Prove that every* $n \in \mathbb{N}$ *is a sum of distinct powers of 2, i.e., it is of the form* $n = 2^{i_1} + \cdots + 2^{i_h}$ *for some integers* $0 \leq i_1 < i_2 < ... < i_h$. *(Hint: Use complete induction. To ensure distinctness, use the largest power of 2 as the first "building block" in the induction step.)*

10. Linear Recursive sequences

A (linear) recursive sequence is an infinite sequence $(s_n)_{n=1}^{\infty}$ which satisfies a relationship of the form

$$s_{n+1} = c \cdot s_n \tag{15}$$

for all $n \in \mathbb{N}$ and some fixed constant c,
or the form

$$s_{n+2} = c_1 \cdot s_{n+1} + c_2 \cdot s_n \tag{16}$$

for all n and some fixed constants c_1, c_2, or,
more generally, the form

$$s_{n+N} = c_1 s_{n+N-1} + c_2 s_{n+N-2} + ...c_N s_n \tag{17}$$

for all $n \in \mathbb{N}$ and some fixed constants $c_1, \ldots, c_N$, where N is a fixed natural number called the order of the recursive sequence. (These c's can be real or complex numbers.)

Remark 10.1. *Every recursive sequence satisfying (15) has the form $s_2 = c \cdot s_1$, $s_3 = c^2 \cdot s_1$, and so on. Hence, $s_n =$....................*
Consequently, each such sequence is determined by c and its first term, s_1, and it has exponential growth (or decay).

Moving on to sequence (16) we can observe that it is determined by its first two terms, s_1 and s_2, which can be arbitrary. However, a formula for a solution is harder to guess. We can use the following trick:

Consider the characteristic equation

$$x^2 = c_1 x + c_2.$$

Suppose that the solutions to this equation are x_1 and x_2, where $x_1 \neq x_2$. Then ${x_1}^2 = c_1 x_1 + c_2$ and ${x_2}^2 = c_1 x_2 + c_2$ and, by multiplying these by ${x_1}^{n-1}$ and by ${x_2}^{n-1}$ respectively, we obtain

$${x_1}^{n+1} = c_1 {x_1}^n + c_2 {x_1}^{n-1} \text{ and } {x_2}^{n+1} = c_1 {x_2}^n + c_2 {x_2}^{n-1}.$$

This means that $s_n = {x_1}^{n-1}$ and $s_n = {x_2}^{n-1}$ for $n \in \mathbb{N}$, satisfy the recursive relation (16)!

For example, if $c_1 = 5$ and $c_2 = -6$ then $x^2 - c_1 x - c_2 = 0$ has solutions $x_1 = 3$ and $x_2 = 2$. Then the sequences $(3^{n-1})_{n=1}^{\infty}$ and $(2^{n-1})_{n=1}^{\infty}$ satisfy the recursive relation

$$s_{n+2} = 5 s_{n+1} - 6 s_n. \tag{18}$$

for all $n \in \mathbb{N}$. (Check it!) Furthermore, we have

Theorem 10.2.
(1) if $(s_n)_{n=1}^{\infty}$ satisfies a linear recursive equation satisfying (17) for all $n \in \mathbb{N}$ then $(d \cdot s_n)_{n=1}^{\infty}$ satisfies (17) too for any constant d.
(2) if $(s_n)_{n=1}^{\infty}$ and $(s'_n)_{n=1}^{\infty}$ satisfy (17) for all $n \geq 1$ then $(s_n + s'_n)_{n=1}^{\infty}$ satisfies it too.

Proof. (1) If $s_{n+N} = c_1 s_{n+N-1} + c_2 s_{n+N-2} + \dots . c_N s_n$ holds then $ds_{n+N} = c_1 ds_{n+N-1} + c_2 ds_{n+N-2} + \dots . c_N ds_n$ holds too.
(2) If $s_{n+N} = c_1 s_{n+N-1} + c_2 s_{n+N-2} + \dots . c_N s_n$ and $s'_{n+N} = c_1 s'_{n+N-1} + c_2 s'_{n+N-2} + \dots . c_N s'_n$ hold then $s_{n+N} + s'_{n+N} = c_1(s_{n+N-1} + s'_{n+N-1}) + c_2(s_{n+N-2} + s'_{n+N-2}) + \dots . c_N(s_n + s'_n)$ holds too. □

Consequently, if $({x_1}^{n-1})_{n=1}^{\infty}$ and $({x_2}^{n-1})_{n=1}^{\infty}$ satisfy $s_{n+2} = c_1 s_{n+1} + c_2 s_n$ then $d_1 {x_1}^{n-1} + d_2 x_2^{n-1}$ does it too for any constants d_1, d_2. If you took Linear Algebra, then you will notice that the set of infinite sequences $(s_n)_{n \in \mathbb{N}}$ satisfying (16) forms a vector space.

Consequently, in our example with $c_1 = 5$ and $c_2 = -6$, the sequence $(d_1 \cdot 3^{n-1} + d_2 \cdot 2^{n-1})_{n=1}^{\infty}$ satisfies (18) for any d_1, d_2.

As a side note, the theory of recursive relations is analogous to that of linear differential equations. The differential equation $y'' = 5y' + 6y$ has a general solution $y = d_1 e^{3x} + d_2 e^{2x}$. To make the solution unique, one needs to specify the initial conditions $y(0)$ and $y'(0)$.

Problem 10.3. *Find a formula for s_n satisfying (18) with the initial terms $s_1 = 1$, $s_2 = 4$.*

Solution: By the discussion above, $s_n = d_1 \cdot 3^{n-1} + d_2 \cdot 2^{n-1}$ satisfies (18) for any d_1 and d_2. We find the values of d_1 and d_2 by considering the initial terms:

$$\begin{cases} 1 = s_1 = d_1 + d_2, \\ 4 = s_2 = d_1 \cdot 3 + d_2 \cdot 2. \end{cases}$$

That implies that $d_1 = 2$ and $d_2 = -1$. Hence,

$$s_n = 2 \cdot 3^{n-1} - 2^{n-1}.$$

The "closed" formula above for s_n is often more convenient to use than the recursive definition of the sequence. We used some clever tricks to derive it. However, we can also prove it by a complete induction:

Proposition 10.4. *The sequence $s_1 = 1$, $s_2 = 4$, and defined by $s_{n+2} = 5s_{n+1} - 6s_n$ for $n \geq 1$, is given by the formula $s_n = 2 \cdot 3^{n-1} - 2^{n-1}$.*

Proof. (By complete induction, with base $n = 1$ and 2). Let $P(n) =$ "$s_n = 2 \cdot 3^{n-1} - 2^{n-1}$." We show that $P(n)$ is true for all $n \geq 1$. $P(1)$ and $P(2)$ are true since $1 = 1$ and $4 = 2 \cdot 3 - 2$.

Inductive step: Assuming $P(1), ..., P(k)$ hold, we need to prove $P(k+1)$ for $k \geq 2$. By our assumption, $s_{k-1} = 2 \cdot 3^{k-2} - 2^{k-2}$ and $s_k = 2 \cdot 3^{k-1} - 2^{k-1}$. Hence,

$$s_{k+1} = 5s_k - 6s_{k-1} = 5(2 \cdot 3^{k-1} - 2^{k-1}) - 6(2 \cdot 3^{k-2} - 2^{k-2}) =$$
$$10 \cdot 3^{k-1} - 5 \cdot 2^{k-1} - 12 \cdot 3^{k-2} + 6 \cdot 2^{k-2} = 10 \cdot 3^{k-1} - 5 \cdot 2^{k-1} - 4 \cdot 3^{k-1} + 3 \cdot 2^{k-1} =$$
$$6 \cdot 3^{k-1} - 2 \cdot 2^{k-1} = 2 \cdot 3^k - 2^k.$$

Hence, we have proved $P(k+1)$. □

The same method allows finding closed formulas for all other recursively defined sequences, at least when the roots of the characteristic equation are distinct.

The Fibonacci numbers are defined by the following recursive definition:

$$F_1 = 1, \ F_2 = 1, \text{ and } F_{n+2} = F_{n+1} + F_n \text{ for all } n \in \mathbb{N}.$$

Hence $F_3, F_4, ...$ are $2, 3, 5, 8, 13, 21, 34, \ldots$. These numbers appear in various disciplines of science and even in sunflower seed patterns! See e.g. `http://momath.org/home/fibonacci-numbers-of-sunflower-seed-spirals/` and in the solar system, c.f. `https://imgur.com/gallery/zAdw8`.

We can find a closed (i.e. non-recursive) formula for the n-th Fibonacci number, by the method discussed above:

$$F_n = d_1 \cdot {x_1}^{n-1} + d_2 \cdot {x_2}^{n-1},$$

for some d_1, d_2, where x_1, x_2 are the roots of $x^2 - x - 1$, i.e. $x_1 = \frac{1+\sqrt{5}}{2}$, $x_2 = \frac{1-\sqrt{5}}{2}$. Solving $\begin{cases} F_1 = 1 = d_1 + d_2 \\ F_2 = 1 = d_1 \cdot x_1 + d_2 \cdot x_2, \end{cases}$ we obtain $d_1 = \frac{1+\sqrt{5}}{2\sqrt{5}}$, $d_2 = -\frac{1-\sqrt{5}}{2\sqrt{5}}$. Hence,

Corollary 10.5. $F_n = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2} \right)^n$.

Note that $\frac{1+\sqrt{5}}{2} = 1.618...$, $\frac{1-\sqrt{5}}{2} = -0.618...$ The growth of F_n is ...

The ratio b/a of numbers $0 < a < b$ is golden if it is the same as the ratio of $a+b$ to b:

$$\frac{a+b}{b} = \frac{b}{a}.$$

That is, $x = b/a$ is in the golden ratio, if and only if x is the positive root of $\frac{1}{x} + 1 = x$. The golden ration is often denoted by φ, the Greek letter phi. Its value is $\frac{1+\sqrt{5}}{2}$.

That ratio appears in many ways in nature, in architecture, and in the arts. For example, the ratios of various dimensions of the Greek

Parthenon in Athens and of the Egyptian pyramids are golden. (See Figure 7)

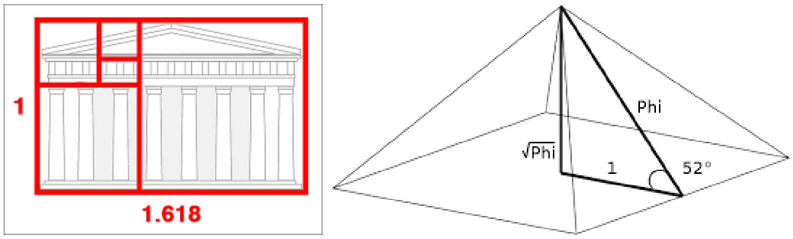

Figure 7. Parthenon, Pyramids, and the Golden Ratio.

The approach above applies to all (linear) recursive equations. For example, to find a closed formula for a sequence $(s_n)_{n=1}^{\infty}$ satisfying

$$s_{n+3} = c_1 \cdot s_{n+2} + c_2 \cdot s_{n+1} + c_3 \cdot s_n \tag{19}$$

one needs to find all (complex) roots x_1, x_2, x_3 of the characteristic equation

$$x^3 = c_1 x^2 + c_2 x + c_3. \tag{20}$$

If the roots are distinct, then the sequences $({x_1}^{n-1})_{n=1}^{\infty}$, $({x_2}^{n-1})_{n=1}^{\infty}$, and $({x_3}^{n-1})_{n=1}^{\infty}$ satisfy the recursive relation (19) and can be used as "building blocks" for the formula for $(s_n)_{n=1}^{\infty}$. Specifically,

$$s_n = d_1 {x_1}^{n-1} + d_2 {x_2}^{n-1} + d_3 {x_3}^{n-1}$$

for every n, where appropriate d_1, d_2, d_3 can be found by solving

$$\begin{cases} s_1 = d_1 + d_2 + d_3 \\ s_2 = d_1 x_1 + d_2 x_2 + d_3 x_3 \\ s_3 = d_1 {x_1}^2 + d_2 {x_2}^2 + d_3 {x_3}^2. \end{cases}$$

Remark 10.6. *We used an intuitive justification for the recursive definitions in this section. There is a Recursion Theorem providing a rigorous justification for these constructions.*

PROBLEMS 10.

Problem 10.1. *Let* $s_1 = 1,\ s_2 = 1,$ *and* $s_{n+2} = 2s_{n+1} + s_n$ *for* $n \geq 1$.
(1) Find a closed formula for s_n.
(2) Prove that your formula is correct using complete induction.

Problem 10.2. *Find a recursive relation satisfied by* $s_n = 2^{n-1}+3^{n-1}+4^{n-1}$, *for* $n = 1, 2, ...$ *(Hint: Reverse engineer the method of finding a formula for the n-th term of a recursive sequence.)*

Problem 10.3. *Find a recursive relation satisfied by* $\sin(1), \sin(2), \sin(3), ...$ *(Hint: Use formulas for* $\sin(a + b)$ *and* $\sin(a - b)$. *Predicting possible questions: by* $\sin(1)$ *we do not mean* $\sin(1 \cdot \pi)$ *or anything other than* $\sin(1)$ *itself.)*

11. Divisibility, Congruences, Integral Quotients

We are again assuming nothing more than Peano's axioms and the results derived from them in the previous Sections.

"Math Proofs" Ch. 4.1-2, 8.5-6, 11

Definition 11.1. • *We say that an integer a divides an integer n if there exists an integer b such that $n = a \cdot b$. We write $a \mid n$.*
• *We write $a \nmid n$ if a does not divide n.*

Remark 11.2. *The following are all equivalent ways of writing the same thing:*

(1) a divides n
(2) a is a factor of n
(3) a is a divisor of n
(4) n is a multiple of a

Remark 11.3. *If $a \mid n$ then $-a \mid n$ and $a \mid -n$.*

An integer n is called "even" iff $2 \mid n$. Otherwise, it is called "odd".

Proposition 11.4. *If a and n are positive integers such that $a \mid n$, then $a \leq n$.*

Proof. left as HW □

Definition 11.5. *A positive integer n is a prime number (or a prime) if $n > 1$ and the only positive factors of n are 1 and n.*

1 is not a prime, because of tradition and also to make the Unique Factorization of Natural Numbers work (see below).

Proposition 11.6. $2, 3, 5, 7$ *are prime numbers.*

Proof. By Proposition 11.4, the only positive divisors of 2 are 1 and 2. Hence 2 has no positive divisors other than 1 and itself. Proof of primality of $3, 5, 7$ is left as HW. □

Theorem 11.7. *Every natural number $n > 1$ is either a prime or a product of prime numbers.*

Proof. in class, by complete induction. □

Such a decomposition is called a prime factorization of a number. For example, $300 = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5$.

Theorem 11.8 (Unique Factorization of Natural Numbers)**.** *If*

$$n = p_1 \cdot \ldots \cdot p_r \quad \text{and} \quad n = q_1 \cdot \ldots \cdot q_s$$

are two prime factorizations of $n \in \mathbb{N}$ then $r = s$ and the primes $p_1, \ldots, p_r$ coincide with $q_1, \ldots, q_s$ up to a permutation (i.e. reordering).

This theorem is also known as the Fundamental Theorem of Arithmetic.
Proof — later in this section.

Theorem 11.9. *There are infinitely many prime numbers.*

Proof by contradiction: Suppose that there are only a finite number of primes. Denote them by $p_1, \dots, p_N$. Consider then $X = (p_1 \cdot \ldots \cdot p_N)+1$. Since X is larger than any p_i, by our assumption X is not a prime. Then by the Unique Factorization Theorem, X is divisible by a prime. Let us say that X is divisible by p_i. Then p_i divides $X - (p_1 \cdot \ldots \cdot p_N) = 1$ as well — a contradiction. □

Congruences, Integral Division.

Definition 11.10. *We say that integers m_1, m_2 are congruent modulo n and we write*

$$m_1 = m_2 \mod n$$

iff $m_1 - m_2$ is divisible by n.

For example, $7 = -8 \mod 5$.

The "mod n" term refers to the equal sign as well as to m_2. In our opinion, $m_1 =_n m_2$ would be a better notation. And, indeed, it is sometimes used, but since it is not standard, we will use "mod n" notation.

Example 11.11. $m_1 = m_2 \mod 2$ *iff ....*

Example 11.12. *There are 365 days in a non-leap year. Denote them by 1, 2, 3, ..., 365. (Hence, day 32 means February 1st.) Then $m_1 = m_2$ mod 7 means....*

Proposition 11.13. *Congruence modulo n is an equivalence relation on $\mathbb{Z}$ (see Section 13):*
(1) For every $a \in \mathbb{Z}$, $a = a \mod n$.
(2) If $a = b \mod n$ then $b = a \mod n$.
(3) If $a = b \mod n$ and $b = c \mod n$, then $a = c \mod n$.

Proof. In class or HW. □

Proposition 11.14. *If $a_1 = b_1 \mod n$ and $a_2 = b_2 \mod n$ then*
(1) $a_1 + a_2 = b_1 + b_2 \mod n$,
(2) $a_1 - a_2 = b_1 - b_2 \mod n$, and
(3) $a_1 a_2 = b_1 b_2 \mod n$.

Proof. In class or HW. □

Corollary 11.15. *If $a = b \mod n$ then $a^k = b^k \mod n$ for every $k \in \mathbb{N}$.*

Proof. follows by induction from Proposition 11.14(2). □

Proposition 11.14 and Corollary 11.15 have many useful applications:

Problem 11.16. *Prove that $3^{300} - 1$ is divisible by* 31.

A computation (in Mathematica, for example) shows that $(3^{300}-1) = 31 \cdot N$, where $N =$ 441585416318027019326858152845446180536979663307540117649936097026996765088706698689678084373190133510485433679348367880043589460534502498600 0, but can we prove it without a computer? Here is a solution based on Proposition 11.14 and Corollary 11.15:

$$3^{300} - 1 = (3^3)^{100} - 1 = 27^{100} - 1 = (-4)^{100} - 1 \mod 31.$$

Now $(-4)^{100} - 1 = ((-4)^5)^{20} - 1 = (-1024)^{20} - 1$. Since $1024 = 33 \cdot 31 + 1$, the reminder of the division of 1024 by 31 is 1. Hence

$$3^{300} - 1 = (-1024)^{20} - 1 = (-1)^{20} - 1 = 0 \mod 31.$$

This means that $3^{300} - 1$ is divisible by 31.

Although the sequence of simplifications above of $3^{300} - 1 \mod 31$ was chosen ad hoc, every sequence of simplifications will yield the same result.

There is an alternative approach to the problem above using Fermat's Little Theorem, see Theorem 12.22, below.

Lower and Upper Bounds.

For some proofs in this section (Theorem 11.20 and Proposition 12.3) and later we need the following:

Definition 11.17. *(1) We say that a set $A \subset \mathbb{Z}$ is bounded from below iff there exists $n \in \mathbb{Z}$ such that $\forall_{a \in A}\, n \leq a$. Such an n is called a lower bound for A.*
(2) Similarly, $A \subset \mathbb{Z}$ is bounded from above iff there exists $n \in \mathbb{Z}$ such that $\forall_{a \in A}\, a \leq n$. Such an n is called an upper bound for A.

(In the definition above, one can consider subsets A of $\mathbb{R}$ as well.)

Theorem 11.18. *(1) Every non-empty subset $A \subset \mathbb{Z}$ that is bounded from below contains a smallest element, i.e. an element $m \in A$ such that $\forall_{a \in A}\, m \leq a$.*
(2) Every non-empty subset $A \subset \mathbb{Z}$ that is bounded from above contains a largest element, i.e. an element $m \in A$ such that $\forall_{a \in A}\, a \leq m$.

Remark 11.19. *(1) Note that Theorem 11.18 is a generalization of the Well-Ordering Principle (Theorem 7.12).*
(2) The theorem above does not hold if $\mathbb{Z}$ is replaced by $\mathbb{R}$. For example, the open interval $(1, \infty)$ is bounded from below (for example by -5, though the largest lower bound for A is 1). However, $(1, \infty)$ does not have a smallest element, since for every $a \in (1, \infty)$ the number $\frac{1+a}{2}$ is in A and it is smaller than a.

Proof of Theorem 11.18(1): Motivation: If $A \subset \mathbb{N}$ then the statement follows from the Well-Ordering Principle, Thm 7.12. Therefore our goal is to define a new set $B \subset \mathbb{N}$ such that the existence of a smallest element in B is equivalent to the existence of a smallest element in A.

Here is a formal proof: Assume that A is bounded from below by n. If $n \in A$, then n is the smallest element of A and the statement holds. Therefore, assume now that $n \notin A$. Let $B \subseteq \mathbb{Z}$ be the set of all numbers of the form $a - n$, where $a \in A$.

Then $\forall_{a \in A}\, n \leq a$ implies (by subtracting n from both sides) that $\forall_{a \in A}\, 0 \leq a - n$. Since $a - n \neq 0$, we have $\forall_{a \in A}\, 0 < a - n$, i.e. $B \subseteq \mathbb{N}$. By the Well-Ordering Principle, Thm 7.12, B has a smallest element. Let us denote it by b_m. (Subscript "m" stands for "minimum".) By definition of B, $b_m = a_m - n$ for some $a_m \in A$. We claim that a_m is the smallest element of A. Indeed, for every $a \in A$, $a - n \in B$ is greater or equal to $b_m = a_m - n$. Hence $\forall_{a \in A}\, a - n \geq a_m - n$. By adding n to both sides of this inequality, we see that a_m is the smallest element of A.

The proof of (2) is analogous — left as HW. □

Integral Quotients.

Theorem 11.20. *Let $n \in \mathbb{N}$. For every $m \in \mathbb{Z}$ there exists $q, r \in \mathbb{Z}$ such that*

$$m = q \cdot n + r \quad \text{and} \quad 0 \leq r < n. \tag{21}$$

Furthermore such q and r are unique.

Proof. Case (1): $m \geq 0$.

We show the existence of q and r. Let $A = \{a \in \mathbb{Z} : a \cdot n \leq m\}$. Since $n \geq 1$,

$$\forall_{a \in A}\, a = a \cdot 1 \leq an \leq m.$$

Hence A is bounded from above and, therefore, it contains a largest element, q, by Theorem 11.18(2). Let $r = m - q \cdot n$. By our construction, $q \cdot n \leq m$. Hence $r \geq 0$. Since q is the largest element of A, $q + 1 \notin A$ and, hence, $(q + 1)n > m$. This implies that $qn + n > qn + r$, i.e. $n > r$.

Case (2): $m < 0$.

Let $k = -m$, so $k > 0$. By case (1), there exist integers p and s such that $k = pn + s$, where $0 \leq s < n$. This implies that $m = -k = (-p)n + (-s)$. If $s = 0$ we are done: let $q = -p$ and $r = 0$.

If $s \neq 0$, we would like to just let $q = -p$ and $r = -s$. Since $0 < s < n$ then r would not satisfy $0 \leq r < n$, but rather we would have $0 > r > -n$.

So if $s \neq 0$, instead of letting $r = -s$, we let $r = n - s$. Then $0 > -s > -n$ implies $n > n - s > 0$, so r now satisfies $0 < r < n$. Now we just have to balance the equation $m = (-p)n + (-s)$. We add n to the second term and subtract n from the first to get $m = -(p+1)n + (n - s)$. Let $q = -(p+1)$ and let $r = n - s$ and we are done: $m = qn + r$.

(3) Uniqueness of q and of r:

We need to prove that if $q, r \in \mathbb{Z}$ and $q', r' \in \mathbb{Z}$ satisfy condition (21) then $q = q'$ and $r = r'$.

We prove first that $r = r'$: Assume that $r \neq r'$. Then either $r' > r$ or $r > r'$, by Theorem 8.22. Without loss of generality, we can assume that $r' > r$. We have

$$q \cdot n + r = m = q' \cdot n + r'.$$

Since $r' - r = (q - q')n$, the number $r' - r$ is divisible by n. Since $r' - r \in \mathbb{N}$, by Proposition 11.4, $n \leq r' - r$. But then $n \leq n + r \leq r' \leq n - 1$. This is a contradiction. Therefore, we have proved that $r = r'$.

Now $q \cdot n + r = m = q' \cdot n + r'$ implies that $(q - q')n = 0$. By Theorem 8.18, $q - q' = 0$ (since $n \in N$ and, hence $n \neq 0$.) Therefore $q = q'$. □

Definition 11.21 (integral quotient, remainder). *If $m \in \mathbb{Z}, n \in \mathbb{N}$, and q and r are the unique integers such that $0 \leq r < n$ and $m = q \cdot n + r$, then q is called the integral quotient of m by n and r is called the remainder of the division of m by n.*

In this situation, we clearly have $m = r \mod n$.

For example, the integral quotient of 20 by 7 is .... and the remainder is .... The integral quotient of the of -20 by 7 is .... and the remainder is ....

By Theorem 11.20 for $n = 2$, every integer m is equal to $2a + r$ for $r = 0$ or 1. Recall that integers not divisible by 2 are called odd. Hence every odd integer is of the form $2a + 1$.

Note that:

Proposition 11.22. *The following hold:*

- *the sum of two even numbers is even,*

- *an even number plus an odd one is odd,*
- *the sum of two odd numbers is even,*
- *the product of an even number with any integer is even,*
- *the product of two odd numbers is odd.*

PROBLEMS 11.

Problem 11.1. *Prove that* $\forall_{a\in\mathbb{Z}}\, a \mid a$.

Problem 11.2. *Prove that if* $a, b, c \in \mathbb{Z}$ *and* $a \mid b$ *and* $b \mid c$ *then* $a \mid c$.

Problem 11.3. *Prove Proposition 11.4.*

Problem 11.4. *Prove that the only natural number that divides* 1 *is* 1.

Problem 11.5. *Let* a *and* b *be natural numbers such that* $a \mid b$ *and* $b \mid a$. *Prove that* $b = a$.

Problem 11.6. *Prove that* 3 *is prime.*

Problem 11.7. *Prove that if* $k^2 + 3$ *is prime for some* $k \in \mathbb{Z}$, *then* k *is even.*

Problem 11.8. *Is it true that if* k *is even then* $k^2 + 3$ *is prime? Why or why not?*

Problem 11.9. *Prove Proposition 11.13(3).*

Problem 11.10. *Prove Proposition 11.14.*

Problem 11.11. *Prove that*
(a) $3^{40} - 4$, *and*
(b) $3^{41} - 5$
are divisible by 7. *(You cannot rely on a calculator in your solution.)*

Problem 11.12. *Find the last digit in the decimal notation for* 2^{2014}. *You cannot rely on a calculator in your solution.*
Hint: This is equivalent to finding $0 \le r \le 9$ *such that* $2^{2014} = r$ *mod* 10.

Problem 11.13. *Prove Theorem 11.18(2).*

Problem 11.14. *Find the integral quotient and the remainder of the division of*
(a) 60 *by* 11. *(b)* -60 *by* 11.

12. Further properties of integers

Decimal and binary notation. Recall that $1, 2 = 1', 3 = 2'$,...,$9 = 8'$ are natural numbers defined by Peano axioms. Together with 0, they are called "digits". We do not have special symbols for $9'$, $9''$ etc. Instead, we denote larger natural numbers by using multiple digits. For example, 9' is denoted by 10. We can then express any natural number as multiple digits in the decimal system with the aid of the following result.

Proposition 12.1. *Let $a \in \mathbb{N}$. Let q_0 be the integral quotient of a by 10 and let b_0 be the remainder of that division. Define $q_1, q_2, ...$ and $b_1, b_2, ...$ recursively as follows: q_{i+1} is the integral quotient of q_i by 10 and b_{i+1} is the remainder of that division. Let q_n be the first zero number in this sequence. Then*
(1) $a = b_n 10^n + b_{n-1}10^{n-1} + \ldots + b_2 10^2 + b_1 10 + b_0$.
(2) $b_0, ..., b_n$ are the only possible digits for which the above equation holds.

A sequence of digits $b_n b_{n-1} ... b_1 b_0$ (as above) is called a decimal notation for a.

Proof. Proof in class. □

Note that "n" in the proposition above is the largest natural number such that $10^n \leq a$.

Definition 12.2. *A sequence of digits $b_n b_{n-1} ... b_1 b_0$ is called a decimal notation for*

$$a = b_n 10^n + b_{n-1}10^{n-1} + \ldots + b_2 10^2 + b_1 10 + b_0.$$

The "base" of this notation is 10.

One can easily generalize the statement of this proposition to bases other than 10. Of particular importance is base 2, leading to binary notation.

Here is an adaptation of Proposition 12.1 to the base 2 (binary notation) for $a = 37$: $q_0 = 18$, $b_0 = 1$, $q_1 = 9$, $b_1 = 0$, $q_2 = 4$, $b_2 = 1$, $q_3 = 2$, $b_3 = 0$, $q_4 = 1$, $b_4 = 0$, $q_5 = 0$, $b_5 = 1$. Therefore, 37 is $b_5 b_4 b_3 b_2 b_1 b_0 = 100101$ in the binary notation. Equivalently, $37 = 1 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2 + 1 \cdot 2^0$.

Let x be given by 31 in the octal (i.e. base 8 notation). How much is it in the decimal notation? Can you make it into a joke about Halloween?

Greatest Common Divisor.

"Math Proofs" Ch. 11

Proposition 12.3. *If at least one of the integers m, n is non-zero then the set*

$$\{d \in \mathbb{Z} : d \mid m \text{ and } d \mid n\}$$

of common divisors of m and n has a largest element.

Proof. Let A be the set of common divisors of n and m. Then A is non-empty (why?). For every $a \in A$, a divides $|n|$ and, hence, by Proposition 11.4, $a \leq |n|$. Therefore A is bounded from above. By Theorem 11.18(2), A contains a largest element. This element satisfies the definition of the greatest common divisor of n and m. □

"Math Proofs" Ch. 11.

Definition 12.4 (Greatest common divisor)**.** *Let $m, n \in \mathbb{Z}$, with m and n not both zero. The greatest common divisor of m and n, denoted by* $\gcd(m, n)$*, is the largest integer that divides both m and n.*

Note that the gcd is always positive.

Definition 12.5. *We say that integers m and n, not both zero, are relatively prime (or coprime) if* $\gcd(m, n) = 1$*.*

Note that m and n are relatively prime iff they have no common divisors other than 1 and -1.

Note that since $gcd(n, m)|n$ and $gcd(n, m)|m$, we have

$$gcd(n, m)|(x \cdot n + y \cdot m)$$

for all $n, m, x, y \in \mathbb{Z}$. The next result says that you can choose x, y such that $x \cdot n + y \cdot m$ is actually equal to $gcd(n, m)$.

Lemma 12.6 (Bézout's Lemma)**.** *For any integers m, n, not both zero, there exist integers x, y such that $mx + ny = gcd(m, n)$.*

Proof. Fix $m, n \in \mathbb{Z}$. Let $M = \{mx + ny : x, y \in \mathbb{Z} \text{ and } mx + ny > 0\}$. Since M is a (non-empty — why?) subset of a well ordered set, $\mathbb{N}$, then M contains its smallest element. Denote the smallest element by d. By definition, $d = mx_0 + ny_0$, for some $x_0, y_0 \in \mathbb{Z}$.

Claim: d divides m and n.

Proof of Claim. $m = kd + r$ for some $k \in \mathbb{Z}$ and some $0 \leq r < d$ by Theorem 11.20. If d does not divide m then $r > 0$. Since

$$r = m - kd = m(1 - kx_0) + n(-ky_0),$$

$r \in M$. This contradicts the assumption that d is the smallest element of M. Hence d divides m. Proof of $d|n$ is analogous. *End proof of Claim*

Continuation of the proof of Bézout's Lemma: It is easy to see that d is the largest common divisor of m and n. Indeed, if d' is any other common divisor of m and n then d' divides $d = mx_0 + ny_0$ as well. If d' is negative, then it is smaller than d. If d' is positive then it is not larger than d by Proposition 11.4. □

Example 12.7. *By Bézout's Lemma, the equation $11x + 13y = 1$ has at least one solution $x, y \in \mathbb{Z}$. (Note that a solution to this equation consists of two numbers, x and y.) This may look surprising, since no such x and y immediately come to mind. Finding such integers is left as HW.*

Proposition 12.8. *If $gcd(n, a) = 1$ and $n|(a \cdot b)$ then $n|b$.*

Proof. Suppose that $gcd(n, a) = 1$ and n divides $a \cdot b$. By Bézout's Lemma, $nx + ay = 1$ for some $x, y \in \mathbb{Z}$. Multiplying both sides by b we get $nxb + aby = b$. Since n divides both terms on the left, it divides b as well. □

The following statement is known as Euclid's lemma (or Euclid's first theorem). It appears as Proposition 30 in Book VII of Euclid's Elements, written c. 300 BC.

Lemma 12.9 (Euclid's lemma)**.** *If p is prime dividing $a \cdot b$ then $p \mid a$ or $p \mid b$.*

Proof. left as HW. □

Question 12.10. *Is the assumption p being prime above necessary?*

Furthermore, we can prove

Lemma 12.11. *If a prime p divides $a_1 \cdot a_2 \cdot ... \cdot a_n$, then $p \mid a_i$ for some $i \in \{1, 2, ..., n\}$.*

Proof. in class or HW. □

Now we are ready for
Proof of Unique Factorization Theorem can be proved by complete induction on n or by a contradiction. Here is a proof by contradiction: Let $n > 1$ be the smallest natural number that can be written as (at least) two different products of prime numbers. Denote these two factorizations of n as $p_1 \cdot ... \cdot p_r$ and $q_1 \cdot ... \cdot q_s$. Hence

$$p_1 \cdot p_2 \cdot ... \cdot p_r = q_1 \cdot q_2 \cdot ... \cdot q_s. \tag{22}$$

Since $p_1|n$, by Lemma 12.11, p_1 divides q_i for some $i = 1, 2..., s$. Since q_i is prime, $p_1 = q_i$. Hence n/p_1 has two different factorizations

$$p_2 \cdot ... \cdot p_r \text{ and } q_1 \cdot ... \cdot q_{i-1} \cdot q_{i+1} \cdot ... \cdot q_s$$

– contradicting the assumption that n was the smallest natural number with two different factorizations. □

Factorials, Binomial Coefficients and Fermat's Little Theorem.

Definition 12.12 (Factorials)**.** $0! = 1! = 1$. *For every* $n \in \mathbb{N}$, $n! = (n-1)! \cdot n$.

A definition of this type is called "recursive".

Definition 12.13 (Binomial coefficients)**.** *Let* k *and* n *be integers,* $0 \leq k \leq n$*. Define the* *binomial coefficient* $\binom{n}{k}$*, by:*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

$\binom{n}{k}$ is often read "n choose k", since it is the number of all k element subsets of an n element set. For example $\binom{4}{2} = 6$ is the number of 2 element subsets of $\{1,2,3,4\}$. (These subsets are $\{1,2\}$, $\{1,3\}$, $\{1,4\}$, $\{2,3\}$, $\{2,4\}$, $\{3,4\}$.)

Remark 12.14. *For every integer* $n \geq 0$*,* $\binom{n}{0} = \binom{n}{n} = 1$.

Proposition 12.15 (Pascal's Triangle)**.** *If* $0 < k < n$*, then* $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.

Proof. in class, by direct computation. □

Proposition 12.16. $\binom{n}{k}$ *is an integer, for all integers* k *and* n *such that* $0 \leq k \leq n$.

Proof. by induction on n, in class. □

Theorem 12.17 (Binomial Theorem)**.** *For every* $x, y \in \mathbb{R}$ *and every* $n \in \mathbb{N}$,

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

Proof. We prove the statement

$$P(n) = \text{“ } (x+y)^n = \textstyle\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} \text{ ”}$$

for all $n \in \mathbb{N}$ by induction. The base case, $P(1)$, is obvious.
Inductive step: Assume $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$ for some n (and all $x, y \in \mathbb{R}$). To prove that $P(n)$ implies $P(n+1)$ we need to show that

$$\left(\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} \right) \cdot (x+y) = \sum_{k=0}^{n+1} \binom{n+1}{k} x^k y^{n+1-k}.$$

Sketch of proof: expand the left hand side and then substitute $k-1$ in the first sum for k. That trick relies on the identity

$$\sum_{k=a}^{b} c_k = \sum_{k=a+1}^{b+1} c_{k-1}.$$

(Indeed, both sides of it are equal to $c_a + c_{a+1} + ... + c_b$.). Finally, combine the two sums you get on the left hand side by using Pascal's triangle, Proposition 12.15. □

Corollary 12.18. $\sum_{k=0}^{n} \binom{n}{k} = 2^n$.

Lemma 12.19. *For every prime p and every integer k,$1 \leq k \leq p-1$, the binomial coefficient $\binom{p}{k}$ is divisible by p.*

Proof. in class. □

For example, $\binom{5}{1} = \binom{5}{4} = 5$, $\binom{5}{2} = \binom{5}{3} = 10$ are divisible by 5.

Proposition 12.20. *For every prime p, $\forall_{a,b\in\mathbb{Z}}\,(a+b)^p = a^p + b^p \mod p$.*

Proof. By Binomial Theorem (Thm 12.17),

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1}b + ... + \binom{p}{p-1} ab^{p-1} + b^p.$$

By Lemma 12.19, all terms on the right are divisible by p except for the first and the last one. Hence $(a+b)^p = a^p + b^p \mod p$. □

Corollary 12.21. *For every prime p and all $a_1, a_2, ..., a_n \in \mathbb{Z}$,*

$$(a_1 + a_2 + ... + a_n)^p = a_1^p + ... + a_n^p \mod p.$$

Proof. by induction, using Proposition 12.20. □

By taking $a_1 = a_2 = ... = a_n = 1$ we obtain the following neat result:

Theorem 12.22 ("Fermat's Little Theorem")**.** *If p is prime then $n^p = n \mod p$ for every $n \in \mathbb{Z}$. In other words, $p \mid n^p - n$.*

The word "little" is used to distinguish that theorem from the Fermat's "great" one, discussed later. See Appendix A for the discussion of applications of Fermat's Little Theorem to internet security.

Take $n = 2$ now. We have $2 \mid 2^2 - 2$, $3 \mid 2^3 - 2$, $4 \nmid 2^4 - 2$, (4 does not divide $2^4 - 2$), $5 \mid 2^5 - 2$, $6 \nmid 2^6 - 2$, $7 \mid 2^7 - 2$, $8 \nmid 2^8 - 2$, $9 \nmid 2^9 - 2$,...

So it seems that $a \mid 2^a - 2$ if and only if a is prime. This is called the "Chinese hypothesis." It was believed to be true because it holds for all $a < 341$. However, $341 \mid 2^{341} - 2$ despite the fact that 341 is not prime. $(341 = 11 \cdot 31.)$ This break of a pattern for $n = 341$ exemplifies the importance of proving statements, rather than just interpolating them from known examples. A statement may hold true for numbers $a < 341$ but fail for higher ones.

Corollary 12.23. *If p is prime and n not divisible by p then $p|n^{p-1}-1$.*

Proof. in class. □

Alternative Solution to Problem 11.16: By Fermat's Little Theorem, $31 \mid 3^{31} - 3 = 3(3^{30} - 1)$. By Proposition 12.8, $31 \mid 3^{30} - 1$. Hence $3^{30} = 1 \mod 31$. By Corollary 11.15,

$$3^{300} = (3^{30})^{10} = 1^{10} = 1 \mod 31.$$

□

For $n \in \mathbb{N}$, let $\phi(n)$ be the number of natural numbers coprime with n and less than n, i.e. $\phi(n) = |\{k \in \mathbb{N} : k < n \wedge gcd(k, n) = 1\}|$.

For example, $\phi(p) = p - 1$ for p prime. But $\phi(4) = \phi(6) = 2$. $\phi : \mathbb{N} \to \mathbb{N}$ is called Euler's totient function.

The following statement is a generalization of the Corollary above.

Theorem 12.24 ("Euler's Little Theorem")**.** *For every $n, a \in \mathbb{N}$ coprime, $a \mid n^{\phi(a)} - 1$.*

For example, for natural numbers n coprime with 4 (which ones are these?) $4 \mid n^2 - 1$.

Rings, non-uniqueness of factorization and Fermat's Last Theorem.

For a given $d \in \mathbb{Z}$, denote by $\mathbb{Z}[\sqrt{d}]$ be the set of all numbers of the form $a+b\sqrt{d}$ for $a, b \in \mathbb{Z}$. These numbers are real if $d \geq 0$ and complex if $d < 0$.

Proposition 12.25. *$\mathbb{Z}[\sqrt{d}]$ is closed under addition, subtraction, and multiplication, i.e. if $x, y \in \mathbb{Z}[\sqrt{d}]$ then $x + y$, $x - y$ and $x \cdot y$ are elements of $\mathbb{Z}[\sqrt{d}]$.*

Proof. — Left as HW. □

A set which is closed under addition, subtraction and multiplication, and such that the addition is distributive with respect to multiplication $(a(b+c) = ab+ac)$ is called a ring. We will discuss this notion in detail in Sec. 17.

For technical reasons let us assume that $d \neq -1, 3$. As before, we can define the prime numbers in $\mathbb{Z}[\sqrt{d}]$ to be those x which are divisible by ±1 and $\pm x$ only. One can prove that each number has a prime factorization. But unlike for integers, such a factorization does not have to be unique!

Example 12.26. *One can show that* $2, 1+\sqrt{5}, -1+\sqrt{5}$ *are all prime in* $\mathbb{Z}[\sqrt{5}]$. *However, we have* $4 = 2 \cdot 2$ *and* $4 = (1+\sqrt{5})(-1+\sqrt{5})$.

Despite much effort by mathematicians, it is unknown to this day for which $d \in \mathbb{Z}$, $\mathbb{Z}[\sqrt{d}]$ has the unique factorization property.

We finish this section with the following famous statement of Fermat:

Theorem 12.27 ("Fermat's Last Theorem"). *For every* $n > 2$ *there are no* $a, b, c \in \mathbb{N}$ *such that* $a^n + b^n = c^n$.

Figure 8. Pierre Fermat, 1607-1665

The assumption of $n > 2$ is essential since the statement does not hold for $n = 2$. For example, $3^2 + 4^2 = 5^2$.

Fermat wrote his theorem on a margin of a book in 1637, together with a comment that he has an easy proof but this margin is too small to include it there. It took mathematicians over 300 years to figure out a proof of this theorem. Its only known proof (completed by A. Wiles in 1995) is an enormously difficult and complicated argument. Therefore, it is very unlikely that Fermat's proof was correct. Most mathematicians believe that Fermat took the unique factorization of numbers in every ring for granted. Using that, one can indeed prove Fermat's Last Theorem.

Further Open Problems in Number Theory.

Conjecture 12.28. *(Goldbach's Conjecture) Every even integer n greater than* 2 *is a sum of two prime numbers.*

For example, $4 = 2+2$, $\quad 6 = 3+3$, $\quad 8 = 3+5$, $\quad 10 = 7+3 = 5+5$, $12 = 5+7$, $\quad 14 = 3+11 = 7+7$. Goldbach's conjecture have been verified for all numbers $n < 10^{18}$ by computers.

Conjecture 12.29. *(Twin Prime Conjecture) There are infinitely many pairs of primes of the form $p, p+2$.*

Here are a few examples of pairs of "twin" primes: $(3,5)$, $(5,7)$, $(11,13)$, $(17,19)$, $(29,31)$. The conjecture is quite surprising since the differences between consecutive primes grow on average, as the numbers grow. For example, $113, 127$ is a pair of consecutive primes, since all 13 numbers between them are composite. The Twin Prime Conjecture states that, nonetheless, there are infinitely many pairs of primes of distance 2 only!

Further open questions:

(1) For which $d \in \mathbb{Z}$, does the ring $\mathbb{Z}[\sqrt{d}]$ have a unique factorization property?
(2) Is there a prime number between any two consecutive squares?
(3) A prime number of the form $2^n + 1$ is called a Fermat prime. Are there infinitely many such primes?
(4) A prime number of the form $2^n - 1$ is called a Mersenne prime. Are there infinitely many such primes?

A polynomial equation with integer coefficients is called "Diophantine". Finding integral solutions to Diophantine equations is a very difficult problem, studied by Diophantus already in the 3rd century in Alexandria.

In 1900, David Hilbert proposed the solvability of all Diophantine equations as the tenth of his 23 fundamental problems for the 20th century. In 1970, Yuri Matiyasevich proved that a general algorithm for solving all Diophantine equations cannot exist.

Figure 9. David Hilbert

PROBLEMS 12.

Problem 12.1. *(a) Write* 13 *in binary notation.*
(b) Write 100 *in tertiary notation (that is with base* 3*).*

For both parts, make sure you got correct answer by verifying the equation of Proposition 12.1.
(Hint: Use the algorithm given in the proof of Proposition 12.1.)

Problem 12.2. *Find $x, y \in \mathbb{Z}$ satisfying the equation of Example 12.7.*

Problem 12.3. *(1) Does $7a + 11b = 1$ have an integral solution, i.e. $a, b \in \mathbb{Z}$ satisfying this equation? If yes, then find at least one such pair a, b. Otherwise, explain why such pair does not exist.*
(2) Do the same problem for $7a + 11b = 2$
(3) Do the same problem for $15a + 12b = 7$
(4) Do the same problem for $15a + 12b = 3$
Hint: Use Bézout's Lemma.

Problem 12.4. *Prove Euclid's Lemma.*

Problem 12.5. *Let $a, b, n \in \mathbb{Z}$. Prove that if $gcd(a, b) = 1$ and a and b divide n then $a \cdot b$ divides n.*

Problem 12.6. *Use induction to prove that $n^3 - n$ is divisible by 6 for all $n \geq 0$.*

Problem 12.7. *Prove that $3^{2n-1} + 1$ is divisible by 4 for all $n \in \mathbb{N}$.*

Problem 12.8. *Use induction to prove that $11^{n+1} + 12^{2n-1}$ is divisible by 133 for all $n \in \mathbb{N}$.*

Problem 12.9. *Prove that for all $a \in \mathbb{Z}$ not divisible by 7, $a^{12} + a^6 + 5$ is divisible by 7. Hint: Corollary 12.23.*

Problem 12.10. *Prove Lemma 12.11.*

Problem 12.11. *Prove Proposition 12.15.*

Problem 12.12. *Prove Proposition 12.25.*

Problem 12.13. *How many 13 card "hands" can be drawn from a deck of 52 cards? (The order of cards doesn't matter.)*

13. Binary Relations

More on binary relations in "Mathematical Proofs", Ch. 8.1-8.3 and "How to Prove It" Ch 4.2-4.

A binary relation on a set A is a certain property of some pairs of elements of A.

Examples 13.1.

(1) A is the set of all people alive. R is the "fatherhood relation". That is, aRb if a is the father of b.

(2) A is as above. S is the relation on A such that aSb iff a and b have the same mother.

(3) A is the set of all Math 311 class students. aTb iff a and b are in the same study group.

(4) A is as above. J is the relation on A such that aJb iff a is strictly younger than b.

(5) $\leq$ is a relation on $A = \mathbb{Z}$. E.g. $2 \leq 4$

(6) $m \in \mathbb{Z}$ is in the "divisibility relation" with $n \in \mathbb{Z}$ iff $n \mid m$. E.g. 4 is in a divisibility relation with 2, but not vice versa.

(7) Fix $n \in \mathbb{N}$. Then $m_1, m_2 \in \mathbb{Z}$ are in "the mod n congruence relation" iff $m_1 = m_2 \mod n$.

A formal definition is as follows:

Definition 13.2. *A relation on a set A is a subset of $A \times A$.*

In Example (1) above, the relation R on A is defined by the set of all pairs (father,son) in $A \times A$, i.e.

$$R = \{(a, b) \in A \times A : a \text{ is the father of } b\}.$$

We identify the relation R with this set. Hence, we write aRb iff $(a, b) \in R$.

A relation R on A is reflexive if $\forall_{a \in A}\ aRa$. R is symmetric if

$$\forall_{a,b \in A}\ aRb \Rightarrow bRa.$$

Finally, R is transitive if $\forall_{a,b,c \in A}\ (aRb \wedge bRc) \Rightarrow aRc$.

For the seven examples above we have:

Example	Refl	Sym	Trans
1	N	N	N
2	Y	Y	Y
3	Y	Y	Y
4	N	N	Y
5	Y	N	Y
6	Y	N	Y
7	Y	Y	Y

A reflexive, symmetric, and transitive relation is called an equivalence relation, as in Examples (2),(3) above. The most important one is the equality relation, "=". (Note that the Preliminary Axioms in Section 7 are to make sure that $=$ is an equivalence relation.) You will see in Section 14 and, more broadly, in many topics of advanced math, that equivalence relations are very important in mathematics, because they allow us to identify different objects. For that reason we often denote equivalence relations by $\sim$ or $\simeq$ (by analogy with "=").

"Mathematical Proofs", Ch. 8.3-4,"How to Prove It" Ch 4.6.

Definition 13.3. *Let $\sim$ be an equivalence relation on A. The equivalence class of an element a of A, denoted by $[a]$ is the set $[a] = \{b \in A : b \sim a\}$.*

For every $a \in A$, $[a]$ is a subset of A.

Example 13.4. *For congruence mod 3 (Example 13.1(7)),*

$$[0] = \{..., -9, -6, -3, 0, 3, 6, 9, ...\}, \quad [1] = \{..., -8, -5, -2, 1, 4, 7, 10, ...\},$$

$$[2] = \{..., -7, -4, -1, 2, 5, 8, 11, 14, ...\}.$$

Observe also that

$$... = [-6] = [-3] = [0] = [3] = [6] = ...,$$

i.e. all numbers divisible by 3 have the same equivalence class. Similarly,

$$\begin{aligned} ... = [-5] = [-2] = [1] = [4] = [7] = ..., \quad &\textit{and} \\ ... = [-4] = [-1] = [2] = [5] = [8] = ... \end{aligned}$$

Example 13.5. *Let T be the equivalence relation of Example 13.1(3). The equivalence class of a student is the set of all students in his/her study group.*

Observe that in Example 13.4 there are only three distinct equivalence classes, $[0], [1]$, and $[2]$. They are disjoint and their union is the set of all integers. Similarly, in Example 13.5 there are 9 distinct equivalence classes, since there are 9 study groups in Math 311. They are disjoint and their union is the set of all Math 311 students. More generally, we have:

Proposition 13.6. *Let $\sim$ be an equivalence relation on A. For every $a, b \in A$,*
(a) if $a \sim b$ then $[a] = [b]$
(b) if $a \not\sim b$ then $[a] \cap [b] = \emptyset$.

Proof of this proposition is assigned as HW.

Definition 13.7. *A collection P of non-empty subsets of a set A is a partition of A iff*
(1) $\forall_{a\in A}\exists_{S\in P}\ a\in S$, and
(2) for every $S,T\in P$, either $S=T$ or $S\cap T=\emptyset$.

For example, $\{\{1,2\},\{3,4,5\},\{6,7\}\}$ is a partition of $\{1,2,3,4,5,6,7\}$ but $\{\{1,2,3\},\{3,4,5\},\{6,7\}\}$ is not.

Proposition 13.6 implies now

Corollary 13.8. *For every equivalence relation $\sim$ on a set A, the set of all equivalence classes of $\sim$ is a partition of A.*

Mod 3 congruence of Example 13.4 partitions $\mathbb{Z}$ into three subsets

$$\{...,-9,-6,-3,0,3,6,9,...\},\quad \{...,-8,-5,-2,1,4,7,10,...\},$$
$$\{...,-7,-4,-1,2,5,11,14,...\}.$$

The equivalence relation of Example 13.5 partitions all Math 311 students into 9 study groups.

The partitioning property of equivalence relations is very useful for "identifying" different elements of a set. For example, 2 is never equal to 5, but $[2]=[5]$ in Example 13.4! This method of identifying (or equating) different elements of a set is very important in advanced algebra and topology, as well as in many other areas of mathematics. We will use it in the next section to define rational numbers.

Definition 13.9. *If $\sim$ is an equivalence relation on A then the quotient set of A by $\sim$, denoted by $A/\sim$, is the set of all equivalence classes of $\sim$.*

For example, let $\sim$ be the mod 3 congruence on $\mathbb{Z}$. Then $\mathbb{Z}/\sim$ has three elements.

PROBLEMS 13.

Problem 13.1. *Find an example of a relation (on a set of your choice) which is symmetric and transitive, but not reflexive. (Try to make this example as simple as you can.)*

Problem 13.2. *Which of the following are relations on $A=\{1,2,3\}$ are symmetric, reflexive, transitive? Justify your answer whenever you claim that one of these properties fails.*
$R_1=\{(1,1),(1,2),(2,1),(2,2),(3,3)\}$
$R_2=\{(1,1),(2,2),(3,3),(1,2),(2,1),(2,3),(3,2)\}$
$R_3=\{(1,1),(2,2),(3,3),(1,2),(2,3),(1,3)\}$.

Problem 13.3. *Prove Proposition 13.6.*

Problem 13.4. *Let R be a relation on $\mathbb{N}$ such that aRb iff $a|b$ or $b|a$. Is R an equivalence relation?*

Problem 13.5. *Consider a "square" $S = \{-2,-1,0,1,2\}\times\{-2,-1,0,1,2\}$,*
(a) Let $(x,y) \sim (x',y')$ iff $|x| + |y| = |x'| + |y'|$. It is an equivalence relation on S. (You don't need to prove it.) Write the elements of $S/\sim$.

(b) Let $(x,y) \sim (x',y')$ iff

- *x and x' have the same sign (both positive, both negative, or both 0), and*
- *y and y' have the same sign (defined as above).*

It is an equivalence relation on S. (You don't need to prove it.) Write the elements of $S/\sim$.

Problem 13.6. *(a) How many different relations are on $X = \{1,2,3\}$.*
(b) How many different equivalence relations are on this set?

Problem 13.7. *For this problem you can assume all your knowledge about the set of real numbers, $\mathbb{R}$. Consider the relation $\sim$ on $\mathbb{R}$, given by $x \sim y$ iff $x - y \in \mathbb{Z}$.*
(a) Is it an equivalence relation?
(b) Compute $[1/2]$
(c) Classify all elements of $\mathbb{R}/\sim$. That is state: "Every element of $\mathbb{R}/\sim$ is of the form ..." — include all the details, so that you don't count any element twice.
(d) What would be a geometric way of thinking about $\mathbb{R}/\sim$?

Problem 13.8. *Let $X = \{1,2,3,4,5,6\}$ and let $\sim$ be given by*
$\{(1,1),(2,2),(3,3),(4,4),(5,5),(6,6),(1,3),(1,5),(2,4),(3,1),(3,5),$
$(4,2),(5,1),(5,3)\}$. *Is $\sim$ an equivalence relation? If yes, write down $X/\sim$.*

14. Rational Numbers

You were taught that a rational number (or "rational") is one of the form n/m, where $n \in \mathbb{Z}$ and $m \in \mathbb{Z} - \{0\}$. That definition requires the notion of division of all integers n/m (for $m \neq 0$) which results in rational numbers. Hence, this approach leads to a chicken and egg problem: one needs rationals to define devision of integers, but one needs division of integers to define rationals.

One could attempt to resolve this problem by declaring that n/m, for $m > 0$, is a number such that the sum of m of such numbers yields n. For example, that the number $1/3$ is characterized by the following property:

$$1/3 + 1/3 + 1/3 = 1.$$

However, this definition still involves division in disguise: How do we know that such number exists and that declaring its existence does not lead to a contradiction in mathematics. Indeed, if we insisted to declare that n/m exist with their "well known" properties then why we require that $m \neq 0$? (This is also reminiscent of the story of the barber who shaves all people in the village who don't shave themselves. The assumptions in this story seem very reasonable and yet they are contradictory.)

For that reason, we, mathematicians, need to define rational numbers in a precise way, without a reference to division of integers. That is not an easy task!

In order to do that, let us ignore for now the fact that the bar in $1/3$ means division. We will treat it as a formal symbol for now. With this approach, one could try to define a rational number as a formal expression: an integer followed by a bar "/", followed by a non-zero integer, e.g. $1/3$. Alternatively, we write this formal expression as $\frac{1}{3}$.

Any such expression is really a pair of numbers and, therefore, can be thought as an element of $\mathbb{Z} \times (\mathbb{Z} - \{0\})$. This preliminary definition has one major fault: $1/3$ and $2/6$ are different formal expressions. We want them to be equal. We are going to "identify" them using the method of the last section. For that we need an equivalence relation $\sim$ on $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ such that

$$(a, b) \sim (c, d) \text{ iff } a/b = c/d$$

Although the right side is not defined properly (since we didn't define rational numbers yet), by multiplying both sides by bd we obtain an equality which makes formal sense in the context of the integers:

Definition 14.1. *Let $\sim$ be a relation on $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ such that*

$$(a, b) \sim (c, d) \text{ iff } ad = bc.$$

Proposition 14.2. *The relation $\sim$ is an equivalence relation on $\mathbb{Z} \times (\mathbb{Z} - \{0\})$.*

Proof of this proposition is assigned as HW.

The equivalence class of $(1, 3)$ with respect to this relation is $[(1, 3)] = \{(1, 3), (2, 6), (3, 9), ..., (-1, -3), (-2, -6), (-3, -9), ...\}$. Equivalently, $[(1, 3)] = \{(a, b) \in \mathbb{Z} \times (\mathbb{Z} - \{0\}) : 1 \cdot b = 3 \cdot a\}$.

Now we are ready for the formal definition of a rational number:

Definition 14.3. *A rational number (or "rational" for short) is an equivalence class of the relation $\sim$ (defined in Def. 14.1) on $\mathbb{Z} \times (\mathbb{Z} - \{0\})$. We denote the equivalence class $[(a, b)]$ by a/b or $\frac{a}{b}$.*

This is the most abstract construction you have seen in this class! It says that $1/3$ is an infinite subset of $\mathbb{Z} \times (\mathbb{Z} - \{0\})$,

$$1/3 = [(1, 3)] = \{(1, 3), (2, 6), (3, 9), ..., (-1, -3), (-2, -6), (-3, -9), ...\}.$$

Notice that

$$2/6 = [(2, 6)] = \{(1, 3), (2, 6), (3, 9), ..., (-1, -3), (-2, -6), (-3, -9), ...\},$$

Hence $1/3 = 2/6$. Therefore, we have achieved our goal of identifying $1/3$ and $2/6$!

We denote the set of all rational numbers by $\mathbb{Q}$. (Q stands for "Quotients".) In other words, $\mathbb{Q}$ is the quotient set

$$\mathbb{Q} = (\mathbb{Z} \times (\mathbb{Z} - \{0\}))/\sim$$

(using here the notion of quotient introduced in the last Section). Now we need to define addition and multiplication of rational numbers.

Definition 14.4. *If $x = [(a, b)]$ and $y = [(c, d)]$ then*

$$x + y = [(ad + bc, bd)] \quad \text{and} \quad xy = [(ac, bd)].$$

For example, $1/3$ is the equivalence class of $(1, 3)$ and $1/2$ is the equivalence class of $(1, 2)$. Hence,

$$1/3 + 1/2 = [(5, 6)] = 5/6 \text{ and } 1/3 \cdot 1/2 = [(1, 6)] = 1/6.$$

Therefore, the definition above works as expected.

Unfortunately, there is a hidden potential problem with this definition. Since the definition of $x + y$ and $x \cdot y$ allows a choice of (a, b) and (c, d) such that $x = [(a, b)]$ and $y = [(c, d)]$, we need to make sure that the definition of $x+y$ and $x \cdot y$ does not depend on the choice of (a, b) and of (c, d). For example, $-1/3 = [(-1, 3)] = [(1, -3)] = [(2, -6)]$ and we need to make sure that the formulas for $-1/3+1/2$ and $(-1/3)\cdot 1/2$ do not depend on whether we represent $-1/3$ by $(-1,3)$ or by $(2,-6)$. In mathematics lingo, we need to check that addition and multiplication are "well defined."

The following result shows that sums and products are well defined:

Proposition 14.5. *The above definition of $x+y$ and $x\cdot y$ does not depend on the choice of a representative (a,b) of x and the choice of a representative (c,d) of y.*

Proof. We need to prove that if $[(a,b)]=[(a',b')]$ and $[(c,d)]=[(c',d')]$ then

$$[(ad+bc,bd)]=[(a'd'+b'c',b'd')] \text{ and } [(ac,bd)]=[(a'c',b'd')].$$

The premise of this implication says that $(a,b)\sim(a',b')$ and $(c,d)\sim(c',d')$. The conclusion says

$$(ad+bc,bd)\sim(a'd'+b'c',b'd') \text{ and } (ac,bd)\sim(a'c',b'd').$$

We leave the details of the proof to the reader. □

From now on we will identify an integer n with the rational number $\frac{n}{1}$. Hence $\mathbb{Z}\subseteq\mathbb{Q}$. Observe that

$$\frac{n}{1}+\frac{m}{1}=\frac{n+m}{1}.$$

In other words, the addition of n and m thought of as rational numbers coincides with the addition of integers defined in Section 8. Similarly,

$$\frac{n}{1}\cdot\frac{m}{1}=\frac{n\cdot m}{1}$$

implies that multiplication of integers thought of as rational numbers coincides with the multiplication of integers defined in Section 8. These observations fully justify identifying integers n with rational numbers $\frac{n}{1}$.

Now we are ready for stating the fundamental arithmetic properties of rational numbers.

Theorem 14.6.

1. *addition of rational numbers is commutative and associative,*
2. *$\forall_{x\in\mathbb{Q}}\ x+0=x$ (i.e. $0=\frac{0}{1}$ is the "additive identity"),*
3. *multiplication of rational numbers is commutative and associative,*
4. *$\forall_{x\in\mathbb{Q}}\ x\cdot 1=x$ (i.e. $1=\frac{1}{1}$ is the "multiplicative identity"),*
5. *$\forall_{x,y,z\in\mathbb{Q}}\ (x+y)z=xz+yz$ (i.e. multiplication is distributive over addition).*

Proof. In class. □

Since $(-m,n) \sim (m,-n)$ for every $m,n \in \mathbb{Z}$, $n \neq 0$, we have $\frac{-m}{n} = \frac{m}{-n}$. We denote it by $-\frac{m}{n}$ and call it the additive inverse of $\frac{m}{n}$, since $\frac{m}{n} + \left(-\frac{m}{n}\right) = 0$. A multiplicative inverse of a number x is a number y such that $x \cdot y = 1$. The multiplicative inverse of $\frac{m}{n}$ is $\frac{n}{m}$, as long as $m \neq 0$. Therefore, every non-zero rational number has a multiplicative inverse.

We denote the multiplicative inverse of x by x^{-1} and, more generally, the multiplicative inverse of x^n by x^{-n}. For any $x,y \in \mathbb{Q}$, we denote $x \cdot y^{-1}$ by x/y or $\frac{x}{y}$. This is the division (or quotient) of x by y. Therefore, $2/3$ means two things: (a) the rational number $[(2,3)]$ and (b) the quotient of 2 by 3. It is not difficult to prove that these two definitions coincide.

Definition 14.7. *We say that $\frac{a}{b} < \frac{c}{d}$ iff either ($bd > 0$ and $ad < bc$) or ($bd < 0$ and $ad > bc$).*

Note that this is not a self-referential definition, since the right side of "iff" above involves inequality relation among integers only, which was defined in Section 8.

As usual, $y > x$ is equivalent to $x < y$ and $x \leq y$ means $x < y$ or $x = y$.

Proposition 14.8. *(1) For every $x,y \in \mathbb{Q}$, exactly one of the following cases holds: $x = y$, $x > y$, or $y > x$.*
(2) $<$ is transitive on $\mathbb{Q}$,
(3) $\forall_{x,y,z \in \mathbb{Q}}\ x < y \Rightarrow x + z < y + z$,
(4) $\forall_{x,y,z \in \mathbb{Q}}$ if $z > 0$ and $x < y$ then $x \cdot z < y \cdot z$.

PROBLEMS 14.

Problem 14.1. *Prove Proposition 14.2.*

Problem 14.2. *Which of the following are true? Justify your answer.*
(1) A rational number is an element of $\mathbb{Z} \times (\mathbb{Z} - \{0\})$.
(2) A rational number is an infinite set.
(3) Every infinite subset of $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ is a rational number.

Problem 14.3. *Write the definition of $2/5$.*

Problem 14.4. *Prove that if rational numbers x and y are not equal to zero, then $x \cdot y \neq 0$. (Hint: Use Theorem 8.18.)*

Problem 14.5. *Complete the proof of Proposition 14.5.*

15. Equivalence of sets

"Math Proofs" Ch. 10, "How to Prove it" Ch. 7.1-2

Definition 15.1 (Correspondence)**.** *A function $f\colon A \to B$ is a bijection or a 1-1 correspondence if f is 1-1 and onto.*

Note the difference between 1-1 function and 1-1 correspondence: the first one does not have to be onto.

Recall that bijections were defined in Definition 6.6. The emphasis there was on the bijection itself, in this section it is on the fact that a bijection exists.

Definition 15.2 (Equivalent sets, Cardinality)**.** *Sets A and B are equivalent, written $A \sim B$, if there exists a 1-1 correspondence $f\colon A \to B$. We also say in this situation that A and B have the same cardinality.*

"Mathematical Proofs" calls equivalent sets "numerically equivalent."

Remark 15.3. *To prove that A is equivalent to B it is enough to find a function $f : A \to B$ and to verify that it is 1-1 and onto. For example, $\mathbb{Z}$ is equivalent with the set of odd integers $Odd = \{..., -3, -1, 1, 3, ...\}$ via a function f given by $f : \mathbb{Z} \to Odd$, $f(n) = 2n + 1$. However, there are many other functions which work here as well, e.g. $f(n) = -2n+3$. In this section we will consider many interesting equivalences of sets where an appropriate f is much harder to find.*

Proposition 15.4. *Equivalence of sets is:*

(1) reflexive ($A \sim A$)
(2) symmetric ($A \sim B$ implies $B \sim A$)
(3) transitive ($A \sim B$ and $B \sim C$ implies $A \sim C$).

Remark 15.5. *$\sim$ is "like" an equivalence relation. Formally speaking though, it is not a relation, since by definition a relation is a property of pairs of elements of a certain set. But by Russell's paradox, discussed earlier in this class, there is no such thing as the set of all sets!*

Definition 15.6. *(1) A set A has cardinality n, where $n \in \mathbb{N}$, (or, equivalently, A has n elements) if A is equivalent to the set $\{1, ..., n\}$. We then write that $|A| = n$.*
(2) A is finite if it has n elements for some $n \in \mathbb{N}$ or if $A = \emptyset$ (in this case it has zero elements).
(3) A set is infinite (or, equivalently, it has infinitely many elements) if it is not finite.

Below we summarize some obvious properties of finite and infinite sets.

Proposition 15.7. *(1) Two finite sets are equivalent if and only if they have equal an number of elements.*
(2) If A and B are finite sets, then $A \cup B$ is finite.
(3) $\mathbb{N}$ is infinite.

We have already observed that two finite sets are equivalent if and only if they have the same numbers of elements. On the other hand, equivalence of infinite sets is a much more interesting subject. We are going to see soon that not all infinite sets are equivalent.

Definition 15.8 (Countable Sets)**.**
(1) A set equivalent to $\mathbb{N}$ is called <u>*countably infinite*</u>*. (It is also called* <u>*denumerable*</u>*, for example in "Mathematical Proofs".)*
(2) A set is <u>*countable*</u> *if either finite or countably infinite.*
(3) A set which is not countable is called <u>*uncountable*</u>*.*

Observe that a set A is countably infinite if every element of A is labeled by a unique natural number, such that different elements of A have different labels and all natural numbers are utilized.

Proposition 15.9. *Every subset of $\mathbb{N}$ is countable.*

Proof. If $A \subseteq \mathbb{N}$ is finite then it is countable by definition. Assume that A is infinite. We define $f : \mathbb{N} \to A$ as follows:
Let $f(1)$ be the smallest element of A. (This element exists by the Well-ordering principle, Theorem 7.12.)
Now we continue defining f recursively: Suppose that $f(1), ..., f(n) \in A$ are defined already. We define $f(n+1)$ to be the smallest element of $A - \{f(1), ..., f(n)\}$. (Since A is infinite, $A - \{f(1), ..., f(n)\}$ is a non-empty subset of $\mathbb{N}$ and, therefore, it contains a smallest element by the Well-ordering principle.)

To complete the proof we need to show that f is an equivalence. It is 1-1 since if $n < m$ then $f(m) \in A - \{f(1), ..., f(m-1)\}$ and, hence, $f(m) \neq f(n)$.

f is also onto. To see that, take any $a \in A$. Denote the number of elements of A smaller than a by n. Then these elements are $f(1), f(2), ..., f(n)$. Hence $a = f(n+1)$. Since $a \in A$ was chosen arbitrarily, that shows that f is onto. □

Proposition 15.10. *For every set A the following are equivalent:*
(1) A is countable
(2) there is a 1-1 function $f : A \to \mathbb{N}$
(3) A is equivalent to a subset of $\mathbb{N}$.

Remark 15.11. *(1) The words "the following are equivalent" are often denoted by the acronym TFAE.*

(2) The statement claims that (i) $\Rightarrow$ (j) for all $i, j \in \{1, 2, 3\}$. To prove it, it is enough to show the implications:

$$(1) \Rightarrow (2), \quad (2) \Rightarrow (3), \quad (3) \Rightarrow (1).$$

All other implications will then follow. For example, (3) $\Rightarrow$ (1) and (1) $\Rightarrow$ (2) imply
(3) $\Rightarrow$ (2).

Proof of Prop. 15.10:
(1) $\Rightarrow$ (2): If A is finite then there is a 1-1 correspondence $f : A \to \{1, 2, ..., n\}$. In particular, f is a 1-1 function into $\mathbb{N}$.
If A is infinite countable then, by definition, there is a 1-1 function $f : A \to \mathbb{N}$.
(2) $\Rightarrow$ (3): If f is 1-1 then f is a 1-1 correspondence between A and $f(A)$. The latter set is a subset of $\mathbb{N}$.
(3) $\Rightarrow$ (1) by Proposition 15.9. □

Corollary 15.12. *A subset of a countable set is countable.*

Proof. Let A be a subset of a countable set B. By Proposition 15.10, there is a 1-1 function $f : B \to \mathbb{N}$. Its restriction to A is a 1-1 function from A to $\mathbb{N}$. Hence, by Proposition 15.10, A is countable. □

Remark 15.13. *Let f be the function sending*

$$1, 2, 3, 4, 5, 6, 7, 8 \ldots \ \textit{to} \ \ 0, -1, 1, -2, 2, -3, 3, -4 \ldots$$

Then $f$is a 1-1 correspondence between $\mathbb{N}$ and $\mathbb{Z}$.

The statement above may look surprising since there seems to be "many more" integers than natural numbers. Here is an even more surprising result:

Proposition 15.14. $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$ *(i.e. $\mathbb{N} \times \mathbb{N}$ is infinite countable).*

Proof. requires a picture — in class. □

More generally, we have

Theorem 15.15. *If $A_1, A_2, ..., A_n$ are countable then $A_1 \times ... \times A_n$ is countable.*

Proof. By Proposition 15.10, there are 1-1 functions $f_1 : A_1 \to \mathbb{N}$, ..., $f_n : A_n \to \mathbb{N}$. By the same proposition, it is enough to prove that there is a 1-1 function $f : A_1 \times ... \times A_n \to \mathbb{N}$. We define it as follows: Let $p_1 = 2, p_2 = 3, p_3 = 5, ...$ be the sequence of all primes. For $(a_1, a_2, ..., a_n) \in A_1 \times ... \times A_n$ we define

$$f(a_1, a_2, ..., a_n) = p_1^{f_1(a_1)} ... p_n^{f_n(a_n)} \in \mathbb{N}.$$

We claim that f is 1-1. Indeed, if $(a_1, a_2, ..., a_n) \neq (b_1, b_2, ..., b_n)$ then $a_i \neq b_i$ for at least one i. Then $f_i(a_i) \neq f_i(b_i)$ (since f_i is 1-1) and, consequently, the numbers $f(a_1, a_2, ..., a_n)$ and $f(b_1, b_2, ..., b_n)$ have different prime factorizations. By uniqueness of prime factorization (Theorem 11.8), $f(a_1, a_2, ..., a_n) \neq f(b_1, b_2, ..., b_n)$. □

Corollary 15.16. *The set $\mathbb{Q}$ of rational numbers is countable.*

Proof. For every $x \in \mathbb{Q}$, $x \neq 0$, there is unique $p \in \mathbb{Z}$ and $q \in \mathbb{N}$ such that $x = p/q$, $p \neq 0$ and p, q are relatively prime. (Note that the sign of p coincides with the sign of x). Consider the function $f : \mathbb{Q} \to \mathbb{Z} \times \mathbb{N}$ sending x to (p, q) defined above, and sending 0 to $(0, 1)$. This function is 1-1, since $f(x) = (p, q) = f(x')$ implies $x = p/q = x'$. By Remark 15.13 and Theorem 15.15, $\mathbb{Z} \times \mathbb{N}$ is countable and, therefore, by Corollary 15.12, $\mathbb{Q}$ is countable as well. □

Further properties of countable sets:

Proposition 15.17. *(1) If A and B are countable sets, then $A \cup B$ is countable.*
(2) Furthermore, if $A_1, A_2, A_3, ...$ are countable, then $\bigcup_{i=1}^{\infty} A_i$ is countable as well.

Proof. By Proposition 15.10, there is a 1-1 function $f_1 : A \to \mathbb{N}$. Since $B - A$ is a subset of B, it is countable, by Corollary 15.12. Therefore there is a 1-1 function $f_2 : B - A \to \mathbb{N}$. Hence we have a function $g : A \cup B \to \mathbb{N} \times \{1, 2\}$ defined by $g(a) = (f_1(a), 1)$ for $a \in A$ and $g(b) = (f_2(b), 2)$ for $a \in B - A$. It is easy to see that this function is 1-1. Since $\mathbb{N} \times \{1, 2\}$ is countable (by Thm 15.15), Im $g \subseteq \mathbb{N} \times \{1, 2\}$ is countable, where Im g is the image of g. Since g is a 1-1 correspondence from $A \cup B$ onto Im g, $A \cup B$ is countable. □

We are going to prove next that the interval $(0, 1)$ is uncountable. For this purpose we are going to use the fact that each real number has a decimal expansion

$$d_n d_{n-1} ... d_0 . d_{-1} d_{-2} ...$$

which denotes

$$x = \sum_{i=-\infty}^{n} d_i \cdot 10^i = \lim_{k \to -\infty} \sum_{i=k}^{n} d_i \cdot 10^i.$$

Therefore, the decimal expansion defines x uniquely. Note however that x does not necessarily have a *unique* expansion. For example $0.\bar{9} = 0.9999.... = 1$. Similarly, $2.1799999... = 2.18$. However, one can prove that every real number has a unique decimal expansion without infinitely repeating nines at the end.

Theorem 15.18. *The interval* $(0,1)$ *is uncountable.*

Proof. Consider an arbitrary function $f : \mathbb{N} \to (0,1)$. We are going to prove that f cannot be onto. By the comments above, every number in $(0,1)$ has a unique decimal expansion $0.a_1a_2...$ without ending with infinitely repeating nines.

For each n, $n \geq 1$, let d_n be the n-th digit of the decimal expansion of $f(n) \in (0,1)$. We want to construct a number $x = 0.b_1b_2.... \in (0,1)$ such that $b_n \neq d_n$ for all n. This would imply that $x \neq f(n)$ for all n. (Indeed, these two numbers disagree on the n-th digit.) Therefore, x does not belong to the image of f in $(0,1)$ and f is not onto. This is Cantor's famous "diagonal argument".

There are lots of ways to construct x, but here is a simple one: let $b_n = 8$ if $d_n \neq 8$ and let $b_n = 7$ if $d_n = 8$. Note that the decimal expansion of x has only 7's and 8's, so $0 < x < 1$ (and x does not end with repeating 9's).

This shows that no f from $\mathbb{N}$ to $(0,1)$ is onto, so $(0,1)$ cannot be countable. □

Proposition 15.19. *(1)* $f(x) = x/(1-x^2)$ *is a* 1-1 *correspondence between* $(-1,1)$ *and* $\mathbb{R}$.
(2) There is a 1-1 *correspondence between* $(0,1)$ *and* $(-1,1)$. *Therefore,* $(0,1)$, $(-1,1)$, *and* $\mathbb{R}$ *are all equivalent.*

Proof. (1) Since f is differentiable and $f'(x) > 0$ for all x, f is increasing. Therefore, f is 1-1.
Proof that f is onto: Let $y \in \mathbb{R}$. We need to show that there is $x \in (-1,1)$ such that $f(x) = y$. Observe that

$$lim_{x \to -1} f(x) = -\infty, \quad \text{and} \quad lim_{x \to 1} f(x) = \infty.$$

Therefore f takes arbitrarily large and small values. In particular, $f(x_0) < y$ and $f(x_1) > y$ for some $x_0, x_1 \in (-1,1)$. Since f is continuous, by the Intermediate Value Theorem (of Calculus), f takes all values between $f(x_0)$ and $f(x_1)$, i.e. $f(x) = y$ for some x.
(2) left as HW — see HW 15.2. □

Corollary 15.20. $\mathbb{R}$ *is uncountable.*

Corollary 15.21. *The set of irrational numbers is uncountable.*

Proof. Left as HW. □

PROBLEMS 15.

Problem 15.1. *Prove Proposition 15.4.*

Problem 15.2. *Prove that the following sets have the same cardinality:*

(1) The open intervals $(0,1)$ *and* $(-1,1)$*.*
(2) Any two open intervals (a,b) *and* (c,d) *where* $a<b$*,* $c<d$ *and* a,b,c,d *are all (finite) real numbers.*

Problem 15.3. *Prove that if* $f:A\to B$ *is a* 1-1 *function and* B *is countable, then* A *is countable.*

Problem 15.4. *Describe a* 1-1 *correspondence* f *between* $\mathbb{N}$ *and* $\mathbb{N}\times\mathbb{N}$*. Write down the values of* $f(1),...,f(10)$*. Hint: Such a* 1-1 *correspondence was discussed in class, c.f. Proposition 15.14.*

Problem 15.5. *Is it true that* $A_1\times B\sim A_2\times B$ *for sets* A_1,A_2,B *implies that* $A_1\sim A_2$*?*

Problem 15.6. *Prove that* $[0,1]$ *is uncountable.*

Problem 15.7. *Prove Corollary 15.21.*

Problem 15.8. *(a) Find a* 1-1 *function* $f:(0,1)\times(0,1)\to(0,1)$*.* Hint: *use decimal expansions of numbers in* $(0,1)$*.*
(b) Is your f *onto? Justify your answer*
Motivation: *We will prove later that* $(0,1)\times(0,1)\sim(0,1)$*. However, it is not easy to find an explicit* 1-1 *correspondence between these sets.*

Problem 15.9. *Use the statement of the previous problem to show that* $\mathbb{R}\times\mathbb{R}\sim\mathbb{R}$*.*

Problem 15.10. *Find a* 1-1 *correspondence between* $\mathbb{R}$ *and* $\mathbb{Z}\times[0,1)$*.*

Problem 15.11. *Prove that the intervals* $(0,1)$ *and* $[0,1]$ *are equivalent.* Hint: *Let* $B_1=\{1/2,1/3,1/4,\ldots\}$*. Let* $A_1=A_2=(0,1)-B_1$*. Let* $B_2=\{0,1\}\cup B_1$*. Check that* $(0,1)=A_1\cup B_1$ *and that* $[0,1]=A_2\cup B_2$*. Construct a* 1-1 *correspondence between* $(0,1)$ *and* $[0,1]$ *sending* A_1 *to* A_2 *and* B_1 *to* B_2*.*

Problem 15.12. *Prove that the set of all* 2*-element subsets of* $\mathbb{N}$ *is countable.*

Problem 15.13. *Prove that if* A *and* B *are equivalent then their power sets* 2^A *and* 2^B *are equivalent too.*

Problem 15.14. *(a) Let* A *be a set of mutually disjoint open intervals in* $[0,1]$*. Prove that* A *is countable.*
(b) Let A *be a set of mutually disjoint open intervals in* $\mathbb{R}$*. Prove that* A *is countable.*

16. Cardinal Numbers

“Math Proofs” Ch. 10.4-5, “How to Prove It” Ch. 7.3

For each set A one defines its cardinality, denoted by $|A|$. For example, if A is a set of n elements, we write $|A| = n$ and we write $|\emptyset| = 0$. If A is infinite countable, we write $|A| = \aleph_0$. (“Aleph”, $\aleph$, is the first letter of Hebrew alphabet.) We denote the cardinality of $\mathbb{R}$ by $|\mathbb{R}| = \mathfrak{c}$. This Gothic “c” stands for “continuum”.

Since the proper definition of cardinality is bit involved, we will not formulate it here. Imprecisely speaking, $|A|$ is the equivalence class of all sets equivalent to A. Hence we write $|A| = |B|$ iff A and B are equivalent.

Definition. *$|A| \leq |B|$ if A is equivalent to a subset of B.*

Theorem 16.1 (Schröder-Bernstein)**.** *The following are equivalent:*
- $|A| = |B|$
- $|A| \leq |B|$ *and* $|B| \leq |A|$.

Proof. $\Rightarrow$ obvious.
$\Leftarrow$ skipped. (Fairly difficult.) □

We say that A is of smaller cardinality than B and B has larger cardinality than A if $|A| \leq |B|$ and $|A| \neq |B|$. We write $|A| < |B|$ then.

Proposition 16.2. *The following are equivalent:*
(1) $|A| \leq |B|$
(2) there is a 1-1 *function* $f : A \to B$
(3) there is an onto function $g : B \to A$

Proof. in class or HW. □

Theorem 16.3 (Trichotomy Law For Cardinal Numbers)**.**
For every sets A, B exactly one of the following three conditions happens: $|A| < |B|$ or $|A| = |B|$ or $|A| > |B|$.

Proof. At most one of these conditions happens — proof in class.
At least one of these conditions happens — proof skipped — difficult. □

By Corollary 15.20, $\aleph_0 \neq \mathfrak{c}$. Furthermore, we have

Corollary 16.4. $\aleph_0 < \mathfrak{c}$.

Proof. in class. □

Recall that 2^A denotes the set of all subsets of A.

Theorem 16.5. $|2^{\mathbb{N}}| = \mathfrak{c}$.

Proof. in class. □

In 1877, Georg Cantor stated the following famous

Conjecture 16.6 (Continuum Hypothesis (CH))**.** *There is no set A such that $\aleph_0 < |A| < \mathfrak{c}$.*

David Hilbert stated it as the first problem in his famous list of 23 problems for the 20th century in the international mathematics congress in Paris in 1900.

Kurt Gödel showed that CH cannot be disproved on the basis of Peano Axioms. Paul Cohen showed that CH cannot be proven from these axioms either! Therefore, we can assume that CH holds or that it does not hold without any contradiction. For that reason we say that the system of Peano Axioms is incomplete. One could resolve that conundrum by adding the statement of Continuum Hypothesis (or its negation) to Peano axioms. However, that systems of axioms will be incomplete as well:

Theorem 16.7 (Gödel Incompleteness Theorem)**.** *No finite system of axioms is capable of proving all facts about the natural numbers.*

Figure 10. George Cantor and Kurt Gödel

It is natural to ask whether there are sets of cardinality higher than $\mathfrak{c}$.

Theorem 16.8. *For every set A, 2^A has higher cardinality than A.*

Note that this statement is obvious for finite but not for infinite sets.

Proof. Since $f : A \to 2^A$ sending any $a \in A$ to the one element subset $\{a\}$ is 1-1, the cardinality of 2^A is either larger or equal to the cardinality of A. Therefore, it is enough to prove that $|A| \neq |2^A|$. We are going to prove that by showing that there is no onto function $f : A \to 2^A$.

Proof by contradiction. Suppose that $f : A \to 2^A$ is onto. We will say for the sake of the proof, that $a \in A$ is "self-included under f" if

$a \in f(a)$. E.g. If $A = \{1, 2, 3\}$ and $f(1) = \emptyset$, $f(2) = \{2, 3\}$, $f(3) = \{3\}$ then 2 and 3 are self-included. Let

$$S = \{a \in A \mid a \text{ not self-included under } f\}.$$

Since $S \in 2^A$ and $f : A \to 2^A$ is onto, $S = f(a)$ for some $a \in A$. Does a belong to S? If it does, then $a \in f(a) = S$. Hence a is self-included and $a \notin S$. Contradiction. If a doesn't belong to S, then $a \notin f(a)$ and, hence, a is not self-included. Therefore $a \in S$. Also a contradiction. □

Theorem 16.8 implies that there are infinitely many types of infinity. Indeed, for every set A there is another one (2^A) of strictly greater cardinality!

PROBLEMS 16.

Problem 16.1. *Prove Proposition 16.2.*

Problem 16.2. *Prove that* $(0, 1) \sim (0, 1) \times (0, 1)$. *Hint: Use Theorem 16.1, the* 1-1 *function* $f : (0, 1) \times (0, 1) \to (0, 1)$ *which you found in Problem 15.8, and some* 1-1 *function* $f : (0, 1) \to (0, 1) \times (0, 1)$.

Problem 16.3. *Prove that* $\mathbb{R} \sim \mathbb{R} \times \mathbb{R}$ *(or, equivalently, that* $\mathbb{R} \sim \mathbb{C}$*).*

Problem 16.4. *Let* $F(\mathbb{R}, \mathbb{R})$ *be the set of all functions from* $\mathbb{R}$ *to* $\mathbb{R}$. *Prove that* $|F(\mathbb{R}, \mathbb{R})| \geq |2^{\mathbb{R}}|$. Hint: *Find a* 1-1 *function* $f : 2^{\mathbb{R}} \to F(\mathbb{R}, \mathbb{R})$.

Problem 16.5. *Let* $X_1 = \mathbb{R}$ *and let* X_n *for* $n > 1$ *be defined recursively by* $X_{n+1} = 2^{X_n}$. *Prove that there exists a set* Y *such that* $|Y| > |X_n|$ *for every* n.

Problem 16.6. *Prove that* $(0, 1) \sim [0, 1]$. Hint: *Show that* $|(0, 1)| \leq |[0, 1]|$ *and that* $|(0, 1)| \geq |[0, 1]|$. *(This is a different proof of Problem 15.11)*

Problem 16.7. *Suppose that* $|X| \leq |Y|$. *Prove that* $|X \cup Y| = |Y|$.

Problem 16.8. *Does there exist a set* Ω *such that* $|A| \leq |\Omega|$ *for every set* A.

Problem 16.9. *Let* $f : A \to 2^A$ *be a function. We say that* x *in* A *is 'self-included' if* $x \in f(x)$.

Let $A = \{1, \ldots, 20\}$. *Define* $f : A \to 2^A$ *by*

$$f(n) = \{m^2 \mid m \in \mathbf{N}, m^2 \in A, m \text{ divides } n \text{ and } m \neq 1, n\}.$$

Find $S = \{x \in A \mid x \text{ is self included}\}$.

Problem 16.10. *Prove that for any* $X \subset \mathbb{R}$, $|X \times \mathbb{R}| = |R|$.

17. Rings and Fields

The operation of addition associates with any two rational numbers, x, y, their sum, $x + y$. Therefore, addition can be thought as a function defined on the set of all pairs of rational numbers, $\mathbb{Q} \times \mathbb{Q}$, with values in $\mathbb{Q}$. Any such function is called a binary operation. ("Binary" refers to the two numbers, x, y in the input. "Operation" means that the output is in $\mathbb{Q}$, unlike in a relation, xRy, where the output is either True or False.) Clearly, multiplication is a binary operation as well.

We make a formal definition.

Definition 17.1 (binary operation, operation)**.** *Let A be a set. A binary operation on A is a function $A \times A \to A$. A binary operation is called binary because it takes two inputs.*

We often refer to binary operations simply as "operations," since we rarely encounter any others.

The cross product $\mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3$ is another binary operation. Is a subtraction a binary operation on $\mathbb{N}$?
Is division a binary operation on $\mathbb{Q}$?

We say that a set R is a ring if

(1) there are two binary operations defined on R :
addition: $+ : R \times R \to R$ and multiplication: $\cdot : R \times R \to R$.

(2) these operations are associative, i.e.
$$(a + b) + c = a + (b + c) \text{ and } (a \cdot b) \cdot c = a \cdot (b \cdot c),$$
for all $a, b, c \in R$.

(3) addition is commutative, $a + b = b + a$.

(4) multiplication is distributive over addition, i.e.
$$(a + b) \cdot c = a \cdot c + b \cdot c \text{ and } c \cdot (a + b) = c \cdot a + c \cdot b$$
for all $a, b, c \in R$.

(5) There are two different distinguished elements $0, 1 \in R$ such that
$$0 + a = a \text{ and } 1 \cdot a = a \cdot 1 = a \text{ for all } a.$$
0 and 1 are called the additive and the multiplicative identity, respectively. 1 is also sometimes called "unity". (Sometimes the existence of 1 is not required.)

(6) Every $a \in R$ has its additive inverse in R i.e. an element $b \in R$ such that $a + b = 0$. (such b is denoted by $-a$).

Examples: $\mathbb{Z}$ and $\mathbb{Q}$, are rings. In this section we will also consider real numbers, $\mathbb{R}$, which we formally didn't introduce yet. They form a ring too. Since $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$, we say that $\mathbb{Z}$ is a subring of $\mathbb{Q}$ and

$\mathbb{Q}$ is subring of $\mathbb{R}$. On the other hand, $\mathbb{N}$ is not a ring, since its elements do not have additive inverses. The reason for introducing the notion of a ring is that it encompasses properties of many important algebraic objects in mathematics. We describe below several important and interesting rings which you encountered already.

Example 17.2. *Recall from Section 11, that $\mathbb{Z}[\sqrt{d}]$ denotes the set of all numbers of the form $a+b\sqrt{d}$, where $a, b \in \mathbb{Z}$. By Proposition 12.25, $\mathbb{Z}[\sqrt{d}]$ satisfies property (1). Properties (2)-(6) are easy to verify as well. Therefore, $\mathbb{Z}[\sqrt{d}]$ is a ring.*

Recall from Sec. 13, that for any $n \in \mathbb{N}$, $\mathbb{Z}/n$ denotes the quotient of $\mathbb{Z}$ by the equivalence relation $mod\, n$. ($\mathbb{Z}/n$ is also often denoted by $\mathbb{Z}_n$.) For example, $\mathbb{Z}/3$ has three elements:

$$[0] = \{..., -6, -3, 0, 3, 6, ...\},\ [1] = \{..., -5, -2, 1, 4, 7, ...\},\ [2] = \{..., -4, -1, 2, 5, ...\}.$$

Of course, $[0] = [3] = [6] = ...$, $[1] = [4] = [7] = ...$

Proposition 17.3. *$\mathbb{Z}/n$ is a ring with addition and multiplication defined as follows:*

- *if $x = [a]$, $y = [b]$, then $x + y = [a + b]$ and $x \cdot y = [ab]$.*
- *$[0]$ and $[1]$ is the additive and the multiplicative identity in this ring.*

Proof. We need to prove first that the above addition and multiplication is "well defined". That is that for any given $x, y \in \mathbb{Z}/n$, $[a+b] \in \mathbb{Z}/n$ and $[a\cdot b] \in \mathbb{Z}/n$ do not depend on the choice of $a \in x$ and $b \in y$. (Recall that we faced an analogous problem when defining addition and multiplication of rational numbers in Sec. 14.) In order words we need to prove that if $a, a' \in x$ and $b, b' \in y$ then $[a+b] = [a'+b']$ and $[a \cdot b] = [a' \cdot b']$. Our assumptions imply that $a = a' \mod n$ and $b = b' \mod n$. These congruences imply that $a - a'$ and $b - b'$ are divisible by n. Since $a - a' + b - b'$ is divisible by n, we have $a + b = a' + b' \mod n$. Hence $[a + b] = [a' + b']$.

The proof of $[a\cdot b] = [a'\cdot b']$ is similar: We need to prove that $a\cdot b - a'\cdot b'$ is divisible by n. Since $a \cdot b - a' \cdot b' = a \cdot (b - b') + (a - a') \cdot b'$, the claim follows from the fact that $b - b'$ and $a - a'$ are divisible by n.

Now that we established the definition of addition and multiplication we need to verify all ring conditions (associativity of these operations, distributivity of addition over multiplication, etc.) – these are straightforward to check. □

Mathematicians often write "$2+4 = 1$ in $\mathbb{Z}/5$", skipping brackets for simplicity, understanding that that $2, 4$ and 1 really mean $[2], [4]$ and $[1]$.

Example 17.4. *Let X be a set and let $F(X)$ denote the set of all functions $f : X \to \mathbb{R}$. We can add and multiply functions together. If f, g are functions from X to $\mathbb{R}$ then $f + g, f \cdot g : X \to \mathbb{R}$ are functions such that*

$$(f+g)(x) = f(x) + g(x) \in \mathbb{R}, \quad (f \cdot g)(x) = f(x) \cdot g(x) \in \mathbb{R}.$$

It is not difficult to verify conditions (1)-(6) above and, hence, to see that $F(X)$ is a ring.

Example 17.5. *Let $C(\mathbb{R})$ be the set of continuous functions $f : \mathbb{R} \to \mathbb{R}$. Since the set of continuous functions is closed under addition and multiplication and the conditions (1)-(6) hold, $C(\mathbb{R})$ is a ring. It is a subring of $F(\mathbb{R})$.*

Example 17.6. *A polynomial is a function of the form*

$$f(x) = a_n x^n + ... + a_1 x + a_0.$$

$a_0, ..., a_n$ are called coefficients of f. We denote the set of polynomials with coefficients in $\mathbb{R}$ by $\mathbb{R}[x]$. This set is closed under addition and multiplication. Furthermore the constant functions 0 and 1 are the zero and the identity in $\mathbb{R}[x]$. Since $\mathbb{R}[x]$ satisfies conditions (1)-(6) above, it is a ring as well. Since every polynomial is continuous, $\mathbb{R}[x]$ is a subring of $C(\mathbb{R})$.

We say that $a \in R$, $a \neq 0$, is a zero divisor if there exists $b \in R$, $b \neq 0$ such that $a \cdot b = 0$. We know that $\mathbb{Z}, \mathbb{Q}$, or $\mathbb{R}$ are rings with no zero divisors. However, the rings $\mathbb{Z}/n$ have zero divisors for some n's. For example $2, 3 \neq 0$ in $\mathbb{Z}/6$ but $2 \cdot 3 = 0$ in $\mathbb{Z}/6$.

Proposition 17.7. *$\mathbb{Z}/n$ does not have zero divisors iff n is prime.*

Proof. in class. □

The ring with commutative multiplication ($\forall_{x,y \in R}\ x \cdot y = y \cdot x$) is called a commutative ring. Hence $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{Z}[\sqrt{d}], \mathbb{Z}/n$ are examples of commutative rings. However, there are interesting examples of rings with non-commutative multiplication.

Example 17.8. *The set $M_n(\mathbb{R})$ of all $n \times n$ matrices is a non-commutative ring for $n \geq 2$. For $n = 2$ the addition and multiplication are defined as follows:*

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} \\ a_{21}+b_{21} & a_{22}+b_{22} \end{pmatrix},$$

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11}+a_{12}b_{21} & a_{11}b_{12}+a_{12}b_{22} \\ a_{21}b_{11}+a_{22}b_{21} & a_{21}b_{12}+a_{22}b_{22} \end{pmatrix}.$$

Fields. We say that a commutative ring R is a <u>field</u> if every nonzero element of R has a multiplicative inverse, i.e.

$$\forall_{a\in R,\, a\neq 0}\, \exists_{b\in R}\; a\cdot b = 1.$$

As usual, the multiplicative inverse of $a \neq 0$ is denoted by $1/a$ or a^{-1}. Note that an immediate consequence of this definition is that for any $b \in R$ the division a/b is defined and belongs to R.

For example, $\mathbb{Q}$ and $\mathbb{R}$ are fields. On the other hand $\mathbb{Z}$ is not a field since 2 has no multiplicative inverse. Similarly $\mathbb{Z}/6$ is not a field, since $2 \cdot b \neq 1$ for every $b \in \mathbb{Z}/6$.

Lemma 17.9. *If a is a zero divisor in a commutative ring R then a does not have a multiplicative inverse in R.*

Proof. Since a is a zero divisor, $a \cdot b = 0$ for some $b \neq 0$, $b \in R$. If a has a multiplicative inverse $c \in R$ then $a \cdot c = 1$. Hence

$$0 = (a\cdot b)\cdot c = a\cdot(b\cdot c) = a\cdot(c\cdot b) = (a\cdot c)\cdot b = b.$$

Contradiction. □

Theorem 17.10. *A finite ring is a field iff it has no zero divisors.*

Proof in class. □

(There are however infinite rings without zero divisors, which are not fields. You should know an example!)

Combining Proposition 17.7 and Theorem 17.10 we obtain:

Corollary 17.11. *The ring $\mathbb{Z}/n$ is a field iff n is prime.*

For example $\mathbb{Z}/7$ is a field and one can perform all arithmetic arithmetic operations in it. For example $1/3 = 5$ and $-1/3 = 2$ in $\mathbb{Z}/7$. However the sum of 7 ones in $\mathbb{Z}/7$ is zero!

PROBLEMS 17.

Problem 17.1. *Is the following a ring? $R = \{True, False\}$ with the addition $\vee$, multiplication $\wedge$, False being 0 and Truth being 1.*

Problem 17.2. *Consider the set S of all functions $f : \mathbb{R} \to \mathbb{R}$ with the usual addition and with the "multiplication" being composition of functions, i.e. the "product" of f and g is a function fg sending x to $f(g(x))$ for every $x \in \mathbb{R}$. Show that this product does not left distribute over addition, i.e. $f(g+h) \neq fg + fh$ in general. (Therefore, S is not a ring.)*

Problem 17.3. *Is the set $\{a + b\sqrt[3]{2} : a, b \in \mathbb{Z}\}$ a ring (with respect to the usual operations of addition and multiplication)? Justify your answer.*

Problem 17.4. *A person defined a function $f : \mathbb{Z}/5 \to \mathbb{Z}/10$ by declaring that $f([n]) = [n] \in \mathbb{Z}/10$, for every $[n] \in \mathbb{Z}/5$ (where the first bracket is the equivalence class of n with respect to congruence mod 5 and the second bracket is the equivalence class of n with respect to congruence mod 10.) Is this operation well defined? (See the discussion of the notion of being "well-defined" in the proof of Prop. 17.3.)*

Problem 17.5. *Give an example of a zero divisor in $M_2(\mathbb{R})$.*

Problem 17.6. *(a) What $f \in C(X)$ is the multiplicative identity in Example 17.5?*
(b) Find a zero divisor in $C(\mathbb{R})$ or prove that they do not exist.

Problem 17.7. *(a) If $x = \pm 1$ then x is its own multiplicative inverse in $\mathbb{Z}[\sqrt{2}]$. Find an element $x \neq \pm 1$ in $\mathbb{Z}[\sqrt{2}]$ which has a multiplicative inverse in $\mathbb{Z}[\sqrt{2}]$.*
(b) Find an element $x \neq 0$ in $\mathbb{Z}[\sqrt{2}]$ which does not have a multiplicative inverse in $\mathbb{Z}[\sqrt{2}]$.
(c) Is $\mathbb{Z}[\sqrt{2}]$ a field?

Problem 17.8. *Let $\mathbb{Q}[\sqrt{d}]$ denote the set of numbers $x + y \cdot \sqrt{d}$, where $x, y \in \mathbb{Q}$ for some $d \in \mathbb{Z}$. As with $\mathbb{Z}[\sqrt{d}]$, it is easy to check that $\mathbb{Q}[\sqrt{d}]$ is a ring. (You don't need to do it.) Prove that $\mathbb{Q}[\sqrt{d}]$ is a field. There are two cases to consider: (a) $\sqrt{d} \in \mathbb{Q}$ (What set $\mathbb{Q}[\sqrt{d}]$ is then?) (b) $\sqrt{d} \notin \mathbb{Q}$.*

18. Orderings, least upper bounds

Definition 18.1 ((Linear) Order)**.** *A linear order on a set S is a transitive relation $<$ such that for every $x, y \in S$, exactly one of the following conditions holds $x < y$ or $y < x$ or $x = y$. We shall also refer to a linear order as simply an "order".*

Definition 18.2 (Ordered Set)**.** *An ordered set is a pair $(S, <)$ such that S is a set and $<$ is an order on S.*

We may also described an ordered set as "a set that is equipped with an order." Notice that this does not mean quite the same thing as "a set S such that there exists an order on S." Indeed, as we shall see below every set has an order on it, and most sets have many different orders on them. When we say a set is "equipped with an order" we mean not only that one or more orders exist, but also that we have picked one.

Example 18.3. *(1) The standard order $<$ on $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$.*
(2) Any set whose elements are written in a sequence is ordered: $x < y$ if x is ahead of y in the sequence. E.g. the set of the 26 English letters $L = \{a, b, c, ..., z\}$ has a standard ordering $a < b < c < ... < z$.
(3) The set of all words in the English dictionary is written (and, hence, ordered) in "lexicographic" order.

Orderings will be often used in this course. They are also useful in "real life", as in the the dictionary example above, and in computer science. For example, in order to save all cars registered in NY state in the DMV database, they need to be ordered somehow, preferably in a meaningful way. (That makes locating a car registration easier.)

The following generalizes Example 18.3(3):

Theorem 18.4. *For any ordered sets $(S_1, <_1)$, $(S_2, <_2)$, the Cartesian product $S_1 \times S_2$ can be ordered by the relation $<$ defined as follows:*

$$(s_1, s_2) < (s_1', s_2') \text{ iff either } s_1 <_1 s_1' \text{ or } (s_1 = s_1', \text{ and } s_2 <_2 s_2').$$

Proof: in class. □

The above order on $S_1 \times S_2$ is called lexicographic. It allows us to order all points in the plane, $\mathbb{R} \times \mathbb{R}$, even though it is hard to put all these points in a single line.

Note that lexicographic order means somewhat different things in Example 18.3(3) and in Theorem 18.4. (Why?)

Opposite orders, and a few points about notation and jargon. We have noted above that the relation $<$ ("less than") defined on $\mathbb{N}$ in

Definition 7.8 is an example of a linear order as defined in Definition 18.1. But note that the relation $>$ ("greater than"), also defined in Definition 7.8 is also an example of a linear order as defined in Definition 18.1. Indeed, it turns out that *every* linear order can be reversed to produce another linear order called the opposite order.

Lemma 18.5. *Let A be a set and $\prec$ is an order on A. Then $\{(b,a) : (a,b) \in \prec\}$ is also a linear order on A.*

The proof may be given as homework.

Definition 18.6. *If A is a set and $\prec$ an order on A, then the order $\{(b,a) : (a,b) \in \prec\}$ is called the opposite order of $\prec$.*

Mathematicians usually denote an order with either $<$ or a symbol which looks somewhat like $<$ such as $\prec$ or $\ll$. The opposite order is then denoted with the mirror-image symbol ($>$, $\succ$, $\gg$, etc). Adding a line produces the notation for the corresponding "or equal to" relation. That is, if A is a set and $\prec$ is a relation on A, then $a \preceq b$ means $(a \prec b) \vee (a = b)$ and $a \succeq b$ means $(b \prec a) \vee (b = a)$.

The choice of a symbol that looks like $<$ also influences the choice of terminology that is used: "smallest element," "minimum," "lower bound", etc. (See below.)

Minima and Maxima. Consider an ordered set $(S, <)$. We say that $m \in S$ is the minimum or the smallest element of S if $\forall_{s \in S}\, m \leq s$. (We talked of this, for example, in the context of the Well Ordering Principle.) Similarly, $M \in S$ is the maximum or the largest element of S if $\forall_{s \in S}\, s \leq M$. A set may have no maximum and/or no minimum. For example, $\mathbb{Z}, \mathbb{Q}$ and $\mathbb{R}$ have neither.

Every finite ordered set has a unique smallest element and a unique largest element. An infinite ordered set may or may not have a smallest element and a largest element.

Question 18.7. *What is the smallest and the largest element of $S = \{(n,m) : 1 < n+m < 5\}$ in $\mathbb{N} \times \mathbb{N}$ with lexicographic order.*

In Calculus you studied minima and maxima of functions defined on intervals or on all real numbers, so for example, you should be able to answer the following:

Problem 18.8. *Find the minima and the maxima of the following sets (if they exist):*

$$S_1 = \{x^3 - 3x + 1 : x \in [-1, 2]\} \subseteq \mathbb{R},$$

$$S_2 = \{x^3 - 3x + 1 : x \in (-3, 2]\} \subseteq \mathbb{R},$$

We say that a set S well-ordered by $<$ if every non-empty subset of S has a smallest element. Recall that one of the fundamental properties of $\mathbb{N}$ is that it is well-ordered.

Theorem 18.9. *Every set can be well ordered.*

This is a very surprising theorem. Rationals and reals are definitely not well ordered as neither of them nor many of their subsets do not have their minimums. However, according to this theorem there is some (strange) ordering $<'$ of all real numbers such that $\mathbb{R}$ and every subset of $\mathbb{R}$ has a smallest element.

Least Upper Bounds. A related notion to minimum and maximum is that of lower and upper bound.

Definition 18.10 (Upper bound, lower bound, bounded above, bounded below)**.** *Let $(X, <)$ be an ordered set and S a subset of X. As in Definition 11.17, we say that $l \in X$ is a lower bound of S in X if $l \leq s$ for all $s \in S$. We say that S is bounded from below if such an l exists. Similarly, $u \in X$ is an upper bound of S in X if $s \leq u$ for all $s \in S$. We say that S is bounded from above if such a u exists.*

Notice that a minimum or least element of S must be an element of S, while a lower bound of S only has to be an element of X. Thus, every minimum is a lower bound, but not every lower bound is a minimum. A set which has no minimum might still have a lower bound. Can you think of an example? The situation with upper bounds and maxima is similar.

Example 18.11. • *Every rational number $l \leq 1$ is a lower bound for he set $\{1, 2, 3\}$ in $\mathbb{Q}$ and every rational number $u \geq 3$ is an upper bound for this set in $\mathbb{Q}$.*
• *Give examples of upper and lower bounds for $S = \{1/n : n \in \mathbb{N}\}$ in $\mathbb{Q}$.*
• *Find a lower and an upper bound for S_1 above without using calculus.*

Definition 18.12 (Least upper bound, lub, supremum, sup)**.** *Let $(X, <)$ be an ordered set, and let S be a subset of X. We say that $u \in X$ is a least upper bound for S if u is the smallest upper bound for S. That is, u is an upper bound of S and $u \leq v$ for every upper bound v of S. Equivalently u is the smallest element of the set of upper bounds for S. "Least upper bound" is often abbreviated "l.u.b." or "lub." A least upper bound is also called a "supremum"; this word is abbreviated "sup."*

Note that $U = \{v : v \text{ is an upper bound for } S\}$ might not have a smallest element, even when U is nonempty. Can you think of an example where it doesn't? Can you think of an example where it does?

We define the greatest lower bound analogously. This may be abbreviated "glb". Another word for the same thing is "infimum" which is abbreviated "inf."

Remark 18.13. *If S has a smallest element then this element is its greatest lower bound. Similarly, if S has a largest element then this element is its least upper bound.*

What is the least upper bound and the greatest lower bound for $S = \{1/n : n \in \mathbb{N}\}$ in $\mathbb{Q}$?

Proposition 18.14. *If the least upper bound exists then it is unique.*

Proof. Suppose that $u_1 \neq u_2$ are least upper bounds for S. Then either $u_1 < u_2$ and u_2 is not the smallest upper bound or $u_1 > u_2$ and, then, u_1 is not the least upper bound. □

A least upper bound and a greatest lower bound might not exist. We will consider an example of such a situation in the next section.

Ordered Rings. We say that a commutative ring R is an ordered ring with order $<$ iff for every $x < y$ in R:

- $x + z < y + z$ for every $z \in R$.
- $x \cdot z < y \cdot z$ for every $z > 0$, $z \in R$.

For example $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and all their subrings are ordered rings. Is there an ordering on $\mathbb{Z}/5$ making it an ordered ring? (This is a HW problem.)

PROBLEMS 18.

Problem 18.1. *What is the minimum and the maximum of $\{(n, m) \in \mathbb{Z} \times \mathbb{Z} : 2|n| + |m| \leq 3\}$ with respect to lexicographic order on $\mathbb{Z} \times \mathbb{Z}$.*

Problem 18.2. *Let $S = \{(-1)^n \frac{n}{n+1} : n \in \mathbb{N}\} \subseteq \mathbb{Q}$.*
(a) Does S have a minimum?
(b) Does S have a maximum?
(c) Find a lower and an upper bound for S in $\mathbb{Q}$.
(d) Does S have a least upper bound and a greatest lower bound in $\mathbb{Q}$?

Problem 18.3. *Determine the minima and maxima of the following sets (if they exist) and the greatest lower bounds and the least upper bounds in $\mathbb{R}$:*
(a) $S_a = \{x^3 - 6x + 1 : x \in [-1, 3]\} \subseteq \mathbb{R}$,
(b) $S_b = \{x^3 - 3x + 1 : x \in (-1, 3)\} \subseteq \mathbb{R}$,
(c) $S_c = \{x^3 - 3x + 1 : x \in (-2.5, 2.5)\} \subseteq \mathbb{R}$.

Problem 18.4. *Determine the minima and the maxima of the following sets in $\mathbb{R}^2$:*
(a) $\{x+y : (0 \leq x, y \leq 1) \wedge (xy = 1\})$
(b) $\{x+y : x^2+y^2 = 1\}$.

Problem 18.5. *Find a lower and an upper bound for* $\{x^4 - 4x^3 + x^2 + 4x + 1 : x \in [-1,3]\}$ *in* $\mathbb{R}$*, without using calculus or relying on a computer generated graph of this function. Justify your answer.*

Problem 18.6. *Prove that there is no ordering on* $\mathbb{Z}/5$ *making it an ordered ring.*

19. The Least Upper Bound Property, Real Numbers

The following theorem justifies the need for real numbers.

Proposition 19.1. *(due possibly to Hippasus.)*
There is no positive rational number x such that $x^2 = 2$. (Hence, assuming our knowledge of real numbers, $\sqrt{2}$ is a real number which is not rational, a.k.a. "irrational.")

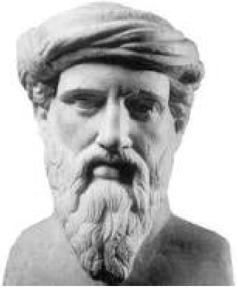

Figure 11. Hippasus, 5 century BC.

Proof by contradiction: Suppose that $(\frac{m}{n})^2 = 2$ for some $m, n \in \mathbb{Z}$, $n \neq 0$. By dividing m and n by $gcd(m, n)$ if necessary, we can assume that m and n are relatively prime. We have $m^2 = 2n^2$ and, therefore, $2 \mid m \cdot m$. By Euclid's Lemma (Corollary 12.9), 2 divides m. Hence $m = 2k$ for some integer k. But $m^2 = 2n^2$ implies that $2k^2 = n^2$. Hence n is divisible by 2. Therefore m and n are both even, contradicting relative primality. □

But how do we define real numbers? The challenge is to do it in a way which involves only notions defined rigorously already. There are two ways to do it: (1) through Dedekind "cuts" and sets, explained in Sec. C, and (2) by "Cauchy sequences". The approach of the second method is based on the fact that every real number is a limit of an infinite sequence of rational numbers. For example, one can prove that the sequence $a_1 = 1$, $a_{n+1} = 1 + 1/a_n$, converges to the golden ratio, $L = \frac{1+\sqrt{5}}{2}$. Hence, one might want to define $\frac{1+\sqrt{5}}{2}$ as the limit of that sequence. (However, one problem with this approach is that different sequences of rationals may have the same limit). We will not go into the details of the definitions of real numbers. Instead, for simplicity, we will define real numbers by the means of the following property:

Definition 19.2. *An ordered set X satisfies the "Least Upper Bound Property" if every non-empty subset S of X that is bounded from above has a least upper bound in X.*

An ordered set satisfying the Least Upper Bound Property is also called “Dedekind complete”.

As an example, consider

$$S = \{x \in \mathbb{Q} : |x| < \sqrt{2}\} = \{x \in \mathbb{Q} : x^2 < 2\} \subseteq \mathbb{Q}.$$

As a subset of $\mathbb{R}$, the least upper bound of S is $\sqrt{2}$. As a subset of $\mathbb{Q}$, the set S is bounded from above but it does not have a least upper bound. Indeed, every rational number x greater than $\sqrt{2}$ is an upper bound for S and for any such number there is a smaller rational number greater than $\sqrt{2}$. Therefore, $\mathbb{Q}$ does not satisfy the Least Upper Bound property — that is the crucial difference between $\mathbb{Q}$ and $\mathbb{R}$. That property has powerful implications for calculus. For example, we can use it to formally define $\sqrt{2}$, as the least upper bound of $\{x \in \mathbb{Q} : x^2 < 2\}$. One can then prove that $(\sqrt{2})^2 = 2$. (Note that we cannot simply declare that $\sqrt{2}$ is a number such that $(\sqrt{2})^2 = 2$ since we don’t know if such a number exists.)

Now we are ready to formally introduce real numbers through the following theorem (whose proof we skip):

Theorem 19.3. *(1) There is a unique ordered field satisfying the Least Upper Bound property. We denote that field by $\mathbb{R}$. Its elements are called the real numbers.*
(2) $\mathbb{R}$ contains $\mathbb{Q}$.

The first statement is usually understood as saying that *up to isomorphism*, there is only one ordered field which satisfies the least upper bound property. One then defines $\mathbb{R}$ to be this unique ordered field which satisfies the least upper bound property. Technically, thus does not tell us whether any given object is or is not an element of $\mathbb{R}$. But this is more of a feature than a bug. It expresses our understanding that what makes $\mathbb{R}$ $\mathbb{R}$ is the structure that it has, not the names of its elements. The above result is a very deep. It says that everything we know about the real numbers (including all of Calculus) is a consequence of two facts: (a) they form an ordered field and (b) they satisfy the Least Upper Bound property. Nevertheless, we have grown up thinking of $\mathbb{Q}$ as a subset of $\mathbb{R}$. How should we integrate this with our new way of thinking about $\mathbb{R}$? The answer lies in the second part of the theorem, which tells us that $\mathbb{R}$ contains an isomorphic copy of $\mathbb{Q}$. Since we are thinking of $\mathbb{R}$ “up to isomorphism” we may, if we like, replace each element of this isomorphic copy by the corresponding element of $\mathbb{Q}$, so that $\mathbb{Q}$ actually sits inside of $\mathbb{R}$ as a subfield.

Definition 19.4. *We say that an ordered set X satisfies the Greatest Lower Bound property iff every non-empty subset S of X that is bounded from below has a greatest lower bound in X.*

Proposition 19.5. *Let R be ordered ring. R satisfies the Least Upper Bound property iff R satisfies the Greatest Lower Bound property.*

Proof. in class or HW. □

For a non-empty set $S \subseteq \mathbb{R}$ we define sup S (from the word "supremum") as follows: If S is bounded from above then sup S denotes its least upper bound (which exists by the theorem above.) If S is not bounded from above then we set sup $S = \infty$.

Similarly, for a non-empty set $S \subseteq \mathbb{R}$ we define inf S (from the word "infimum") as follows: If S is bounded from below then inf S denotes its greatest lower bound (which exists by the theorem above.) If S is not bounded from below then we set inf $S = -\infty$.

Archimedean Principle, ceiling and floor functions.

As a consequence of the Least Upper Bound Principle we obtain

Theorem 19.6 (Archimedean Property)**.** *For any $x, y > 0$ in $\mathbb{R}$ there is $n \in \mathbb{N}$ such that $xn > y$.*

Proof by contradiction: Assume that for some $x, y > 0$, $xn < y$ for all $n \in N$. Then the set $A = \{xn : n \in \mathbb{N}\}$ is bounded from above by y and by the Least Upper Bound Principle it has the least upper bound u. Now take any $n \in \mathbb{N}$. Since $x(n+1) \in A$, we have $x(n+1) \leq u$ and, consequently, $xn \leq u - x$. Since that inequality holds for all n, $u - x$ is an upper bound for A and, hence, u is not the least upper bound for A — contradiction. □

Corollary 19.7. *For every positive $\varepsilon \in \mathbb{R}$, there exists $n \in \mathbb{N}$ such that $\frac{1}{n} < \varepsilon$.*

Proof is left as HW.

Remark 19.8. *Loosely speaking the Greek epsilon, ε, means a "very small" quantity. More precisely, ε can be an arbitrary real number, but the statement containing ε is interesting only if ε is very small. Corollary 19.7 is an example.*

Definition 19.9. *For every real number x,*
(1) $\lfloor x \rfloor$ is the greatest integer not greater than x.
(2) $\lceil x \rceil$ is the smallest integer not less than x.

$\lfloor x \rfloor$ is sometimes called the greatest integer in x. For example,

$$\lfloor 2 \rfloor = \lceil 2 \rceil = 2, \quad \lfloor -2 \rfloor = \lceil -2 \rceil = -2,$$

$$\lfloor \sqrt{10} \rfloor = 3, \quad \lceil \sqrt{10} \rceil = 4, \quad \lfloor -\sqrt{10} \rfloor = -4, \quad \lceil -\sqrt{10} \rceil = -3.$$

Proposition 19.10. *For every $x \in \mathbb{R}$, $\lceil x \rceil$ and $\lfloor x \rfloor$ exist.*

Proof. (1) Let $A \subseteq \mathbb{Z}$ be the set of all integers larger than or equal to x. We claim that $A \neq \emptyset$. Indeed, if $x < 0$ then $1 \in A$. If $x > 0$ then by the Archimedean property for x and 1, we have $1 \cdot n > x$ for some $n \in \mathbb{N}$ and hence $n \in A$.

Since $A \neq \emptyset$, then by the Well Ordering Principle, there exists a smallest element in A. It is $\lceil x \rceil$.
(2) The proof is similar. (We skip the details.) □

The functions $\lfloor \cdot \rfloor, \lceil \cdot \rceil : \mathbb{R} \to \mathbb{Z}$ are called the floor and ceiling functions, respectively.

Remark 19.11. *(1) If $x \in \mathbb{Z}$ then $\lceil x \rceil = \lfloor x \rfloor = x$.*
(2) If $x \notin \mathbb{Z}$ then $\lceil x \rceil = \lfloor x \rfloor + 1$.

Dense subsets of $\mathbb{R}$.

Definition 19.12. *We say that a set $S \subseteq \mathbb{R}$ is dense in $\mathbb{R}$ if for all real numbers $x_1 < x_2$ there exists $s \in S$ such that $x_1 < s < x_2$.*

Clearly, $\mathbb{R}$ is dense in $\mathbb{R}$ but $(0,1) \subseteq \mathbb{R}$ is not. (There are no elements of $(0,1)$ between $x_1 = 2$ and $x_2 = 3$.)

Proposition 19.13. *$\mathbb{Q}$ is a dense subset of $\mathbb{R}$*

Here is what it means: Imagine an infinite line representing all real numbers, with ..., $-2, -1, 0, 1, 2,$ ... marked. Mark two points x_1 and x_2 on this line as close to each other as you can. The statement says that there must be a rational number between them. To see that, assume first that x_1 and x_2 represent rational numbers. Can you name another rational number in between them?

When one or both of the numbers x_1, x_2 are irrational, finding a rational one in-between is harder.

Proof of Proposition 19.13: For any $x_1 < x_2$ we will find a rational number between them by the following idea: Let $q \in \mathbb{N}$ be large enough so that $1/q$ is smaller than $x_2 - x_1$ (the length of the interval $[x_1, x_2]$). Such a q exists by Corollary 19.7. Then one of the multiples of $1/q$, i.e. $1/q, 2/q, 3/q, ...$ must fall in between x_1 and x_2. Which one? Note that

$\lfloor qx_1 \rfloor / q < qx_1/q = x_1$ is the last multiple of $1/q$ before x_1. Therefore, p/q, for $p = \lfloor qx_1 \rfloor + 1$, is a rational number larger than x_1.

Furthermore, we also claim that $p/q < x_2$ and, therefore, it is a rational number that we are looking for. To see that $p/q < x_2$, observe that otherwise, we would have

$$\frac{\lfloor qx_1 \rfloor}{q} < x_1 < x_2 < \frac{\lfloor qx_1 \rfloor + 1}{q}$$

implying that $1/q > x_2 - x_1$, which contradicts our choice of q above. □

Irrational numbers are dense in $\mathbb{R}$ as well. To see this observe the following:

Lemma 19.14. *(1) The set $\sqrt{2} \cdot \mathbb{Q} = \{\sqrt{2} \cdot x : x \in \mathbb{Q}\}$ contains no nonzero rational numbers.*
(2) $\sqrt{2} \cdot \mathbb{Q} - \{0\}$ is dense in $\mathbb{R}$.

Proof. (1) by contradiction: Assume that $\sqrt{2} \cdot \frac{p}{q}$ is rational for some $p, q \in \mathbb{Z}$ and, hence, equal to a/b for some $a, b \in \mathbb{Z}$. Then $\sqrt{2} = \frac{aq}{bp}$, contradicting the irrationality of $\sqrt{2}$.

(2) We need to show that for every real numbers $x_1 < x_2$ there is an element of $\sqrt{2} \cdot \mathbb{Q}$ in between them. But that follows from the fact that there is a rational number p/q between $x_1/\sqrt{2}$ and $x_2/\sqrt{2}$ (since rationals are dense in $\mathbb{R}$). □

PROBLEMS 19.

Problem 19.1. *Find* inf X *and* sup X, *in $\mathbb{Q}$ for $X = \{1/n : n \in \mathbb{N}\}$. Prove your answers.*

Problem 19.2. *Prove Proposition 19.5.*

Problem 19.3. *Prove Corollary 19.7.*

Problem 19.4. *(1) Prove that if a non-empty set $X \subseteq \mathbb{R}$ is bounded from above and below then* $\inf X \leq \sup X$.
(2) What is the simplest characterization of sets $X \subseteq \mathbb{R}$ such that $\inf X = \sup X$*?*

Problem 19.5. *Let x and y denote real numbers. In terms of the greatest integer:*

a) Show that $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor$.

b) Give an example where $\lfloor x \rfloor + \lfloor y \rfloor < \lfloor x + y \rfloor$.

c) Show that $x + y < \lfloor x \rfloor + \lfloor y \rfloor + 2$.

d) Give an example where $x + y = \lfloor x \rfloor + \lfloor y \rfloor + 1.99$.

Problem 19.6. *(1) Can a set bounded from below be dense in $\mathbb{R}$?*
(2) Find an example of a subset of $\mathbb{R}$ which is unbounded from below and from above and which is not dense.

Problem 19.7. *Prove that if $S \subseteq \mathbb{R}$ is dense then for all $x < y$ in $\mathbb{R}$ there are infinitely many elements $s \in S$ such that $x < s < y$.* Hint: *Suppose that there are finitely many of them only. Label them $s_1, ..., s_n$ in an increasing order. Derive a contradiction.*

Problem 19.8. *Prove that $\mathbb{Z}[\sqrt{2}]$ is dense in $\mathbb{R}$.*

20. The Monotone Sequence Property

An infinite sequence (of real numbers) is a function $f : \mathbb{N} \to \mathbb{R}$, often denoted by $f(1), f(2), \ldots$ or by $\{f(n)\}_{n=1}^{\infty}$. For example, $f(n) = 1/n$ is often written as $1, 1/2, 1/3, \ldots$ or $\{1/n\}_{n=1}^{\infty}$. Hence, $\{a_n\}_{n=1}^{\infty}$ denotes the function $f(n) = a_n$.

A sequence $\{a_n\}_{n=1}^{\infty}$ is bounded from above (or below) if the set $\{a_n : n \in \mathbb{N}\}$ is bounded from above (or below).

Definition 20.1. *$\{a_n\}_{n=1}^{\infty}$ converges to a real number L, denoted by $\lim_{n\to\infty} a_n = L$, if for every $\varepsilon > 0$ there exists $N \in \mathbb{N}$ such that $|a_n - L| < \varepsilon$ for all $n > N$.*

We say that a property $P(n)$, where $n \in \mathbb{N}$, holds for large n if there is $N \in \mathbb{N}$ such that $P(n)$ holds for all $n > N$. Hence, $\lim_{n\to\infty} a_n = L$, if for every $\varepsilon > 0$, $|a_n - L| < \varepsilon$ for large n.

Example 20.2. *$\{1/n\}_{n=1}^{\infty}$ converges to* 0.

Proof. in class. □

Note that the limit of a sequence $\{a_n\}$ makes sense for n going to infinity only. In other words, unlike $\lim_{x\to c} f(x)$ which make sense and can exist for various c, $\lim_{n\to c} a_n$ make sense for $c = \infty$ only. Therefore, instead of $\lim_{n\to\infty} a_n$ one can write $\lim a_n$.

Proposition 20.3. *A convergent sequence is bounded.*

Proof. in class or HW. □

Definition 20.4. *A sequence $\{a_n\}_{n=1}^{\infty}$ is non-decreasing if $a_{n+1} \geq a_n$ for all $n \in \mathbb{N}$ and increasing if $a_{n+1} > a_n$ for all $n \in \mathbb{N}$. Similarly, the sequence is non-increasing if $a_{n+1} \leq a_n$ for all $n \in \mathbb{N}$ and decreasing if $a_{n+1} < a_n$ for all $n \in \mathbb{N}$. A sequence is monotone if either it is non-increasing or non-decreasing.*

For example, the sequence $1, 1, 2, 2, 3, 3, 4, 4, 5, \ldots$ is non-decreasing (but not increasing).

Proposition 20.5 (The Monotone Sequence Property)**.**
(1) Every non-decreasing sequence bounded from above converges to its least upper bound (in $\mathbb{R}$).
(2) Every non-increasing sequence that is bounded from below converges to its greatest lower bound (in $\mathbb{R}$).

Proof. in class □

We discussed the golden ratio in Section 10. We claim that the following sequence converges to it.

Theorem 20.6. *Let x_1 be any number in $[-1, \frac{1+\sqrt{5}}{2}]$ and let $x_2, x_3, ...$ be defined recursively by $x_{n+1} = \sqrt{1 + x_n}$ for $n \geq 2$. Then x_n converges to the golden ratio, $\phi = \frac{1+\sqrt{5}}{2}$.*

For example, for $x_1 = 1$, $x_2 = \sqrt{2} \simeq 1.41$, $x_3 = \sqrt{1 + \sqrt{2}} \simeq 1.55$, $x_4 = \sqrt{1 + \sqrt{1 + \sqrt{2}}} \simeq 1.60$, $x_5 \simeq 1.61$, while the Golden Ration is $\frac{1+\sqrt{5}}{2} \simeq 1.62$.

Proof of Theorem 20.6: By high-school algebra (or the graph below),

$$x \leq \sqrt{x+1} \leq \phi$$

for $x \in [-1, \theta]$.

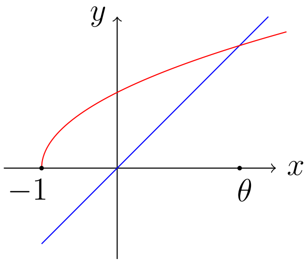

FIGURE 12. $y = x$ is below $y = \sqrt{x+1}$ for $-1 \leq x < \theta$

Therefore, $x_n < x_{n+1} < \frac{1+\sqrt{5}}{2}$ for every n and, consequently, $\{x_n\}_{n=1}^{\infty}$ is convergent by the Monotone Sequence Property. Let us denote $\lim_{n\to\infty} x_n$ by L. Then $L = \frac{1+\sqrt{5}}{2}$. Why? □

Here is another application of the Monotone Sequence Property: The area under the hyperbola $y = 1/x$ for $1 \leq x \leq n$, is

$$\int_1^n 1/x\,dx = \ln x\,|_1^n = \ln(n) - \ln(1) = \ln(n).$$

The picture below shows that this area is less than the harmonic sum $\sum_{i=1}^{n-1} 1/i$.

Denote the difference $\sum_{i=1}^{n-1} 1/i - \ln(n)$ by d_n.

Lemma 20.7. *The sequence $d_1, d_2, d_3, ...$ is increasing and bounded from above.*

(Proof left to HW).

Therefore, by the Monotone Sequence Property, $\lim_{n\to\infty} d_n$ exists. It is called Euler's Constant (or the Euler-Mascheroni Constant) and is denoted by γ. Its value is approximately 0.5772157. (Not to be

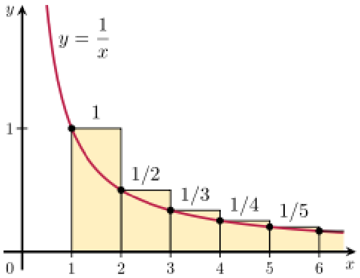

Figure 13. Approximation of the area below $y = 1/x$, $1 \le x \le n$ by the harmonic sum

confused with Euler's constant $e \simeq 2.718$.) There is no closed formula known for it. Since Euler's time, mathematicians have conjectured that γ is irrational, but no proof of it has been found.

PROBLEMS 20.

Problem 20.1. *Using the definition of a limit, prove that* $\lim_{n\to\infty} \frac{1}{n^2} = 0$.

Problem 20.2. *Prove Proposition 20.3.*

Problem 20.3. *Prove Proposition 20.6 for* $x_1 \in (0, \frac{1+\sqrt{5}}{2})$,

Problem 20.4. *Prove Lemma 20.7. Hint: To prove that* $\{d_n\}_{n=1}^{\infty}$ *is bounded from above consider an approximation of* $\ln n = \int_1^n \frac{1}{x} dx$ *by rectangles under the curve.*

21. Complex Numbers

The most intuitive way of introducing complex numbers is by declaring existence of a "number" i such that $i^2 = -1$. Then every complex number is of the form $a + bi$, for some $a, b \in \mathbb{R}$.

But we cannot just declare that i exists without a proof. The only statements assumed without proof in mathematics are its axioms. We could introduce a new axiom declaring the existence of i, but we wouldn't know if that new axiom doesn't contradict the existing axioms.

Here is a formal construction of complex numbers based on the already established definition of reals. It relies on the fact that every complex number $a + bi$ is determined by two reals a, b. Hence, for now we can think of complex numbers as elements of $\mathbb{R}^2$.

Consider $\mathbb{R}^2$ with the addition operation,

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2) \tag{23}$$

and multiplication operation

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1a_2 - b_1b_2, a_1b_2 + a_2b_1). \tag{24}$$

Clearly, the addition is additive, associative and $(0, 0)$ is the zero element.

Lemma 21.1. *This multiplication is commutative, associative, and distributive over addition. Furthermore,* $(1, 0)$ *is the identity element.*

Proof. (1) The multiplication is commutative, since

$$(a_2, b_2)\cdot(a_1, b_1) = (a_2a_1 - b_2b_1, a_2b_1 + a_1b_2) = (a_1a_2 - b_1b_2, a_1b_2 + a_2b_1) = \\ = (a_1, b_1) \cdot (a_2, b_2).$$

(2) Proof of associativity is left as HW.
(3) Proof of distributivity is skipped.
(4) Proof of $(1, 0)$ being the identity element is left as HW. □

Since $(-a, -b)$ the additive inverse of (a, b), $\mathbb{R}^2$ with addition and multiplication defined above is a ring!

Proposition 21.2. *For every* $(a, b) \neq (0, 0)$, $\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right)$ *is the multiplicative inverse of* (a, b).

Proof. $(a, b)\cdot\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right) = \left(a \cdot \frac{a}{a^2+b^2} - b \cdot \frac{-b}{a^2+b^2}, a \cdot \frac{-b}{a^2+b^2} + b \cdot \frac{a}{a^2+b^2}\right) = (1, 0)$. □

Hence, we have proved that $\mathbb{R}^2$ (with the above addition and multiplication) is a field! We call it the field of complex numbers and denote it by $\mathbb{C}$. With each real number r we can associate an element $(r, 0) \in \mathbb{C}$.

Note that these elements add and multiply as real numbers do, i.e. $(r,0)+(s,0)=(r+s,0)$ and $(r,0)\cdot(s,0)=(rs,0)$. Hence we can identify an element of the form $(r,0)$ in $\mathbb{C}$ with the real number $r\in\mathbb{R}$. As we have observed already, $0=(0,0)$ is the zero in $\mathbb{C}$ and $1=(1,0)$ is the identity in $\mathbb{C}$. Denote $(0,1)$ by i. Then

$$i^2=(0,1)\cdot(0,1)=(0\cdot 0-1\cdot 1, 0\cdot 1+1\cdot 0)=(-1,0)=-1.$$

Lemma 21.3. *For every $a,b\in\mathbb{R}$, $(a,b)=(a,0)+(0,b)=a+i\cdot b$*

Proof. $i\cdot b=(0,1)\cdot(b,0)=(0,b)$ □

Therefore, every complex number is of the form $a+bi$, for some $a,b\in\mathbb{R}$. You do not need to use the equation (24) to multiply complex numbers, as long as you remember that $i^2=-1$. For example, $(1+2i)(-1+3i)=\ldots$

If $z=x+yi$ then $\overline{z}=x-yi$ is called the conjugate of z. Note that $z\cdot\overline{z}=a^2+b^2$. This is always a non-negative real number and its square root, $\sqrt{a^2+b^2}$, is called the norm or modulus of z and it is denoted by $|z|$. Geometrically, every complex number represents a point on the xy-plane and $|z|$ is the distance of this point to the origin.

Theorem 21.4 (Triangle Inequality)**.** $|x+y|\le|x|+|y|$ *for all complex numbers x,y.*

The points $0,z_1,z_1+z_2$ form a triangle in the complex plane, with sides of length $l(0,z_1)=|z_1|$, $l(z_1,z_1+z_2)=|z_2|$ and $l(z_1+z_2,0)=|z_1+z_2|$. Hence, geometrically, the triangle inequality says that a side of a triangle is no longer than the sum of lengths of the two other sides. That is the motivation for its name. You may be asked for a rigorous proof of that inequality in HW.

Since $z\overline{z}=|z|^2$, we have $z^{-1}=\frac{\overline{z}}{|z|^2}$ for $z\neq 0$. Note that this formula coincides with the one of Proposition 21.2.

For a non-zero $z\in\mathbb{C}$, the argument of z, denoted by $arg\, z$ is an angle between the positive real axis and the vector representing z. To remove any ambiguity, the angle is positive and measured counterclockwise. Hence $arg\, z\in[0,2\pi)$ (although some mathematicians define it as an element in $(-\pi,\pi]$).

More formally, $arg\, z$ is equal $\phi\in[0,2\pi)$ such that

$$z=|z|(\cos\phi+i\cdot\sin\phi).$$

One can easily prove that ϕ exists and, since we assume that $z\neq 0$, that it is unique.

Theorem 21.5 (Fundamental Theorem of Algebra)**.** *Every polynomial with complex coefficients and degree ≥ 1 has a complex root, i.e. for* *every* $c_0, c_1, ..., c_n \in \mathbb{C}$*,* $n \geq 1$*, with* $c_n \neq 0$*, there is a* $z \in \mathbb{C}$ *such that* $c_n z^n + ... + c_1 z + c_0 = 0$.

The proof is difficult. (In fact, this is the first Theorem in this course, whose proof is too difficult to be discussed here.) Note that an analogous theorem does not hold for real numbers. For example, $x^2 + 1 = 0$ has no roots.

Theorem 21.6 (An alternative version of Fundamental Theorem of Algebra)**.** *Every polynomial with complex coefficients is a product of linear factors. More specifically, for every* $c_0, ..., c_n \in \mathbb{C}$ *there exist* $z_1, ..., z_n \in \mathbb{C}$ *such that*

$$c_n z^n + ... + c_1 z + c_0 = c_n (z - z_1) \cdot ... \cdot (z - z_n)$$

for all $z \in \mathbb{C}$*.*

Clearly the statement above implies Theorem 21.5. One can prove the opposite implication as well by induction on n.

PROBLEMS 21.

Problem 21.1. *Prove the Triangle Inequality, Thm 21.4. Hint: Represent* x *and* y *by* $a_1 + b_1 i$ *and* $a_2 + b_2 i$*, respectively and then prove the corresponding inequality involving real numbers* a_1, b_1, a_2, b_2*.*

Problem 21.2. *Prove that* $|x - y| \geq |x| - |y|$ *for arbitrary complex numbers* x, y*.*

Problem 21.3. *Write a formula expressing* $arg\, z_1 z_2$ *in terms of* $arg\, z_1$ *and* $arg\, z_2$*, for any complex numbers* z_1, z_2*.*

Problem 21.4. *(1) We say that* $x \in \mathbb{C}$ *is a square root of* $z \in \mathbb{C}$ *if* $x^2 = z$*. Does every complex number have a square root? How many? (Notice that unlike for* z *real we cannot not require that the square root is non-negative.)*
(2) Write a formula expressing $arg \sqrt{z}$ *in terms of* $arg\, z$*.*
(3) Find square roots of i *and of* $1 + i$*.*

Appendix A. Applications of Number Theory to Cryptography

Cryptography is the practice and study of techniques for secure communication between two parties, usually referred to as "Alice" and "Bob", in the presence of third parties. One of the most famous encryption algorithms was implemented in the German "Enigma" machine. It was first "cracked" by Polish mathematicians and then, building on their work, Alan Turing cracked an improved model of Enigma, as depicted in the movie "The Imitation Game".

One of the most important types of modern encryption is Public Key Cryptography, in which one of the parties, say Bob, disseminates a "public key". Anyone can plug Bob's public key into a publicly known algorithm to start sending secret messages to Bob. ("Bob" can be a bank, for example. Knowing the the bank's public key, its clients may communicate with the bank securely.)

One can find the public key of an internet server with the Linux command ssh-keyscan.

The most famous public key encryption algorithm, RSA, was developed by mathematicians Rivest, Shamir, Adleman. It is based on the fact that no efficient integer factorization algorithms are known for large numbers. For example, it is quite easy to multiply two 100 digit numbers on a computer. The result will have 200 digits. However, even with a very fast computer, it is believed to take hundreds of years to factor a 200 digit number into prime factors.

Here is how the RSA encryption works: Bob chooses

- two distinct prime numbers, p and q, and
- natural numbers c and d such that $c \cdot d = 1 \bmod (p-1)(q-1)$.

For example, $p = 23$, $q = 41$, $c = 7$, $d = 503$ will work. (In practice, p and q should have close to 100 digits.)

Proposition A.1. *Under the assumptions above $n^{c \cdot d} = n \bmod pq$ for any $n \in \mathbb{Z}$.*

Proof. By assumption, $c \cdot d = k(p-1)(q-1)+1$ for some k. We claim that $p \mid n^{cd} - n$. Since this is certainly the case if $p \mid n$, assume that $p \nmid n$. By Corollary 12.23, $p \mid n^{p-1} - 1$. Hence, $n^{p-1} = 1 \bmod p$ and

$$n^{c \cdot d} = n^{k(p-1)(q-1)+1} = n^{k(p-1)(q-1)} \cdot n = (n^{p-1})^{k(q-1)} \cdot n = 1^{k(q-1)} \cdot n = n \bmod p.$$

Hence, we proved that $p \mid n^{cd} - n$. We prove that $q \mid n^{cd} - n$ the same way. Now, by Problem 12.5, $pq \mid n^{cd} - n$. □

In RSA encryption scheme, $p \cdot q$ and c form the public key of Bob. (But p, q and d are kept secret!) Any information Alice wants to send to Bob can be encrypted as sequence of numbers. Then Alice encrypts a number n between 1 and $pq-1$ by raising it to the power c and taking its remainder r mod pq. Bob decrypts r by raising it to the power d and taking its remainder r' mod pq.

Note that

$$r = n^c \bmod pq \quad \text{and } r' = r^d \bmod pq.$$

Hence,

$$r' = (n^c)^d = n \bmod pq$$

by the proposition above. Hence, Bob has figured out Alice's number n!

The RSA encryption method is based on the following (not obvious) facts:

- taking powers of numbers mod pq is fast
- it is computationally impossible to figure out n, knowing just c and n^c mod pq for large pq (without knowing d).
- it is impossible to figure out d without knowing p and q.
- finding the prime factors of a product pq is computationally impossible for large p, and q.

Appendix B. Constructing the Integers

This section is an alternative approach to that of Section 8 for constructing the integers and the operations on them. The definition of integer presented here is more abstract than that of Section 8, while the proof that the operations work as they should is more conceptual than that of Section 8. There is a tradeoff here, and students would benefit from reading both approaches.

Historically, negative integers were used to describe debts. (See `https://nrich.maths.org/5961` for a history of negative numbers.) Following that idea, will think of an integer as a pair of natural numbers (m, n), where m represents total assets and n represents liabilities of a person, business, country, etc.

Two integers (m, n) and (k, l) are equivalent, if the net worths are the same. That is, if

$$“m - n = k - l''.$$

The problem is, this equation has no meaning if n is bigger than m and if we don't have negative numbers yet. Fortunately, we can rearrange that formula so that it is expressed only in terms of positive integers:

$$m + l = k + n.$$

Now we are ready to model the construction of the integers on the construction of the rational numbers.

Definition B.1. *Let $\sim$ be a relation on $\mathbb{N} \times \mathbb{N}$ such that*

$$(a, b) \sim (c, d) \textit{ iff } a + d = b + c.$$

Proposition B.2. *The relation $\sim$ is an equivalence relation on $\mathbb{N} \times \mathbb{N}$.*

Proof of this proposition is assigned as HW.

The equivalence class of $(2, 5)$ with respect to this relation is $[(2, 5)] = \{(1, 4), (2, 5), (3, 6), (4, 7), ...$ Equivalently,

$$[(2, 5)] = \{(a, b) \in \mathbb{N} \times \mathbb{N} : 2 + b = 5 + a\}.$$

Now we are ready for the formal definition of an integer, alternative of that of Sec. 8.

Definition B.3. *An integer or whole number is an equivalence class of the relation $\sim$ (defined in Def. B.1) on $\mathbb{N} \times \mathbb{N}$. We think of the equivalence class $[(m, n)]$ as $m - n$.*

So for example, we define 0 by

$$0 = [(1, 1)] \quad (= [(2, 2)], \text{ etc.})$$

For $n \in \mathbb{N}$, we identify n with $[(n+1,1)]$ (why not $[(n,0)]$?) and we identify $-n$ with $[(1,n+1)]$.

Hence, the set of integers is the quotient set

$$\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/\sim$$

(using here the notion of quotient introduced in Definition 13.9.)

Now we need to define addition and multiplication of integers.

If we can define addition and multiplication so that they are commutative and associative then it ought to be true that

$$\begin{aligned}(m-n)+(k-l) &= (m+k)-(n+l)\\ (m-n)\cdot(k-l) &= (mk+nl)-(nk+ml).\end{aligned}$$

So we *define* addition and multiplication so that it has these properties.

Definition B.4. *If $x = [(a,b)]$ and $y = [(c,d)]$ then we define $x+y$ and $x \cdot y$ by*

$$x + y = [(a+c, b+d)] \quad \textit{and} \quad x \cdot y = [(ac+bd, ad+bc)].$$

For example, -2 is the equivalence class of $(1,3)$ and -1 is the equivalence class of $(1,2)$. Hence,

$$-2 + -1 = [(1,3)] + [(1,2)] = [(2,5)] = -3 \text{ and}$$
$$-2 \cdot (-1) = [(1,3)] \cdot [(1,2)] = [(1\cdot 1 + 3 \cdot 2, 1 \cdot 2 + 3 \cdot 1)] = [(7,5)] = 2.$$

So the definition above works as expected.

As with rational numbers, we need to show that addition and multiplication are well-defined.

Proposition B.5. *The definition above of $x+y$ does not depend on the choice of a representative (a,b) of x and the choice of a representative (c,d) of y.*

Proof. We need to prove that if $[(a,b)] = [(a',b')]$ and $[(c,d)] = [(c',d')]$ then

$$[(a+c, b+d)] = [(a'+c', b'+d')].$$

The premise of this implication says that $(a,b) \sim (a',b')$ and $(c,d) \sim (c',d')$. The conclusion says

$$((a+c, b+d) \sim (a'+c', b'+d').$$

We leave the details of the proof to the reader. □

Proposition B.6. *The definition above of $x \cdot y$ does not depend on the choice of a representative (a,b) of x and the choice of a representative (c,d) of y.*

The proof of this proposition turns out to be harder than that of Proposition B.5. (See Mazzochi, Foundations of Analysis: Landau Revisited.)

Proof. We need to prove that if $[(a,b)] = [(a',b')]$ and $[(c,d)] = [(c',d')]$ then

$$(ac + bd, ad + bc) \sim (a'c' + b'd', a'd' + b'c').$$

The premise of this implication says that $(a,b) \sim (a',b')$ and $(c,d) \sim (c',d')$. That is,

$$a + b' = a' + bc + d' \quad = c' + d$$

The conclusion says

$$(ac + bd, ad + bc) \sim (a'c' + b'd', a'd' + b'c').$$

We do this in two stages:

1) We show $[(a,b)] \cdot [(c,d)] = [(a',b')] \cdot [(c,d)]$, that is

$$(ac + bd, ad + bc) \sim (a'c + b'd, a'd + b'c)$$

By definition, this means that $ac+bd+a'd+b'c = ad+bc+a'c+b'd$. Now both sides of this equation have a factor of $c + d$: the equation is true if and only if

$$(a + b')c + (a' + b)d = (a + b')d + (a' + b)c$$

But $a + b' = a' + b$, so this last equation is true if and only if

$$(a + b')c + (a + b')d = (a + b')d + (a + b')c$$

That is, if and only if

$$(a + b')(c + d) = (a + b')(d + c)$$

So we are done with part 1).

2) We show $[(a',b')] \cdot [(c,d)] = [(a',b')] \cdot [(c',d')]$, that is

$$(a'c + b'd, a'd + b'c) \sim (a'c' + b'd', a'd' + b'c')$$

which is true if and only if

$$a'c + b'd + a'd' + b'c' = a'd + b'c + a'c' + b'd'$$

The proof of this is similar to the proof of 1), but uses that $c+d' = c'+d$ and is left to the reader.

Parts 1) and 2) together give the result we want by transitivity. □

Now we are ready to state the fundamental arithmetic properties of integers.

Theorem B.7. *Arithmetic Properties of Integers*

(1) *addition of integers is commutative and associative,*
(2) $\forall_{x\in\mathbb{Z}}\ x+0=x$ *(i.e.* $0=[(1,1)]$ *is the "additive identity"),*
(3) *multiplication of integers is commutative and associative,*
(4) $\forall_{x\in\mathbb{Z}}\ x\cdot 1=x$ *(i.e.* $1=[(2,1)]$ *is the "multiplicative identity"),*
(5) $\forall_{x,y,z\in\mathbb{Z}}\ (x+y)z=xz+yz$ *(i.e. multiplication is distributive over addition).*

Proof. In class. □

Definition B.8. *Let* $x=[(a,b)]$ *and* $y=[(c,d)]$*. We define* $x<y$ *iff* $a+d<b+c$*.*

Note that this is not a self-referential definition, since the right side of the "iff" above involves an inequality relation among natural numbers only, which was defined in Section 7.

As usual, $y>x$ is equivalent to $x<y$ and $x\le y$ means $x<y$ or $x=y$.

Proposition B.9. *The following properties hold for integers:*

(1) *For every* $x,y\in\mathbb{Z}$*, exactly one of the following cases holds:* $x=y$*,* $x>y$*, or* $y>x$*.*
(2) *The relation* $<$ *is transitive on* $\mathbb{Z}$*,*
(3) *For all* $x,y,z\in\mathbb{Z}$*,* $x<y\Rightarrow x+z<y+z$*,*
(4) *For all* $x,y,z\in\mathbb{Z}$*, if* $z>0$ *and* $x<y$ *then* $x\cdot z<y\cdot z$*.*

PROBLEMS B.

Problem B.1. *Complete the proof of Proposition B.2.*

Problem B.2. *Complete the proof of Proposition B.5.*

Problem B.3. *Complete part 2) of the proof of Proposition B.6.*

Problem B.4. *Which of the following are true? Justify your answer.*

(1) *An integer is an element of* $\mathbb{N}\times\mathbb{N}$*.*
(2) *An integer is an infinite set.*
(3) *Every infinite subset of* $\mathbb{N}\times\mathbb{N}$ *is an integer.*

Problem B.5. *Prove that if integers* x *and* y *are not equal to zero, then* $x\cdot y\neq 0$*.*

Appendix C. Construction of the Real Numbers

We will define real numbers by approximating them by rational ones.

Let us start with the following informal definition: A "Dedekind cut" is a pair of sets

$$A=\mathbb{Q}\cap(-\infty,\alpha),\quad B=\mathbb{Q}\cap[\alpha,\infty), \tag{25}$$

for some real (rational or irrational number) α. The motivation for this construction is that a Dedekind cut describes a real number in terms of rational ones — it divides all rational numbers into those which lie below α and those which lie above it. This is the reason for the term "cut".

The set A is called a Dedekind set. Since $B = \mathbb{Q} - A$, the Dedekind cut (A, B) is determined by the Dedekind set A. Every Dedekind set A has the following properties:

(1) $A \subseteq \mathbb{Q}$ is non-empty and not equal to $\mathbb{Q}$,
(2) For every $x \in A$ and every $y \in \mathbb{Q} - A$, $x < y$.
(3) A does not contain a greatest element.

Definition C.1 (Formal definition of a Dedekind set and cut)**.** *A Dedekind set is subset of $\mathbb{Q}$ satisfying properties (1), (2), and (3). A Dedekind cut is a pair (A, B) where A is a Dedekind set and $B = \mathbb{Q} - A$.*

Remark C.2. *Condition (2) implies that if x belongs to a Dedekind set A, then for every $y \in \mathbb{Q}$ with $y < x$, then we have $y \in A$ as well. (Indeed, if $y \in \mathbb{Q} - A$ then $y > x$ by condition (2) above.)*

Lemma C.3. including Definition *For every $\alpha \in \mathbb{Q}$, $\{x \in \mathbb{Q} : x < \alpha\}$ is a Dedekind set. We denote it by $\underline{\alpha}$.*

The statement follows from the discussion above. Here is a formal proof: Condition (1) holds since $\alpha - 1 \in \underline{\alpha}$ and $\alpha + 1 \notin \underline{\alpha}$.
If $a \in \underline{\alpha}$ and $b \in \mathbb{Q} - \underline{\alpha}$ then $a < \alpha \leq b$ — hence condition (2) holds as well.
To prove condition (3), we need to show that for every element $a \in \underline{\alpha}$ there is an element $a' \in \underline{\alpha}$ larger than a. We claim that $a' = \frac{a+\alpha}{2} \in \underline{\alpha}$ is such an element. Indeed a' is the arithmetic mean of a and α. Hence it is always between a and α. Here is a formal version of this argument: $a < \alpha \Rightarrow a + \alpha < 2\alpha \Rightarrow \frac{a+\alpha}{2} < \alpha$. Hence $a' \in \underline{\alpha}$. On the other hand, $a < \alpha \Rightarrow 2a < \alpha + a \Rightarrow a < \frac{a+\alpha}{2} = a'$. □

Remark C.4. *Assuming a knowledge of real numbers, observe that furthermore $\underline{\alpha}$ is a well-defined subset of $\mathbb{Q}$ for all real numbers α. This will motivate us to define real numbers as Dedekind sets (or, equivalently, Dedekind cuts)!*

Intuitively, we would like to identify $\sqrt{2}$ with the Dedekind set

$$\{x \in \mathbb{Q} : x < \sqrt{2}\},$$

but of course such definition would be self-referential, since this expression involves $\sqrt{2}$. However, we can rewrite this set as

$$\{x \in \mathbb{Q} : (x^2 < 2) \vee (x < 0)\}.$$

Let us denote this set by $\underline{\sqrt{2}}$. Note that the part "$x < 0$" of the condition is important, since $x^2 < 2$ means $x \in (-\sqrt{2}, \sqrt{2})$ and we need $(-\infty, \sqrt{2})$. Here is a formal verification of the fact that this is a Dedekind set:

Lemma C.5. $\underline{\sqrt{2}} = \{x \in \mathbb{Q} : x^2 < 2 \text{ or } x < 0\}$ *is a Dedekind set.*

Proof. Condition (1) holds since $1 \in A$ and $2 \notin A$.
Proof of condition (2): Let $x \in A$ and $y \in \mathbb{Q} - A$. Then $y^2 \geq 2$ and $y \geq 0$. There are two possibilities: (a) $x < 0$ or (b) $x \geq 0$ and $x^2 < 2$. The first one implies $x < 0 < y$ and the second one implies $y^2 > x^2$. In other words, $y^2 - x^2 = (y - x)(y + x) > 0$. Since $y + x > 0$, then $y - x > 0$. Therefore, we proved that in both cases, (a) and (b), $y > x$.
Proof of condition (3): Let $x \in \underline{\sqrt{2}}$. We need to find an element of $\underline{\sqrt{2}}$ which is larger than x. If $x < 0$ then 1 is such an element. Therefore assume that $x \geq 0$ and $x^2 < 2$. We are going to complete the proof by showing that there exists a natural number n such that

$$x + \frac{1}{n} \in \underline{\sqrt{2}}.$$

This inequality can be rewritten as

$$x^2 + 2x\frac{1}{n} + \frac{1}{n^2} < 2,$$

or as

$$(2 - x^2)n^2 - 2xn - 1 > 0.$$

Since x is constant, the left side is a quadratic function in n with positive leading coefficient. Hence indeed the expression above is positive for sufficiently large n. □

Linear Ordering of Dedekind sets.

Proposition C.6. *For Dedekind sets A and B, either $A \subseteq B$ or $B \subseteq A$.*

Proof. Suppose that $A \not\subseteq B$. Then there is $a \in A$ such that $a \notin B$. By condition (2) of the definition of a Dedekind set, since $a \notin B$, then $\forall_{b \in B}\ b < a$. By Remark C.2, all $b \in B$ belong to A. Hence $B \subseteq A$. □

Definition C.7. *For Dedekind sets A and B we write $A \leq B$ iff $A \subseteq B$ and we write $A < B$ iff $A \subsetneq B$.*

The proposition above implies that for all Dedekind sets A, B precisely one condition holds: $A < B$ or $A = B$ or $B < A$.

Addition of Dedekind sets.

Definition C.8. *If $A, B \subseteq \mathbb{Q}$ are Dedekind sets, then define a subset $A + B$ of $\mathbb{Q}$ by*

$$A + B = \{x + y : x \in A, y \in B\} \subseteq \mathbb{Q}.$$

For example, we claim that

$$\underline{1/2} + \underline{1} = \underline{3/2}.$$

To see that, we need to prove two inclusions. Proof of $\underline{1/2} + \underline{1} \subseteq \underline{3/2}$: Every element of $\underline{1/2} + \underline{1}$ is of the form $x + y$ where $x < 1/2$ and $y < 1$. Since $x + y$ is rational number lower than $3/2$, it belongs to $\underline{3/2}$.

Proof of $\underline{1/2} + \underline{1} \supseteq \underline{3/2}$: Every element z of $\underline{3/2}$ can be written as $z/3 + 2z/3$. Since these summands are rational and $z/3 < 1/2$, $2z/3 < 1$, then $z/3 \in \underline{1/2}$ and $2z/3 \in \underline{1}$. Hence, $z \in \underline{1/2} + \underline{1}$. □

The following is a generalization of the example above:

Proposition C.9. *If A and B are Dedekind sets, then $A + B$ is a Dedekind set as well.*

Proof. Proof of condition (1): Since A, B are non-empty, $A + B$ is non-empty as well. By condition (1) of Dedekind sets, there are $x \in \mathbb{Q} - A$, $y \in\in \mathbb{Q} - B$. We are going to complete the proof of condition (1) for $A+B$ by showing that $x+y \notin A+B$. Proof: Suppose that $x+y \in A+B$. Then $x+y = a+b$ for some $a \in A$, $b \in B$ and $(x-a)+(y-b) = 0$. Hence either $x - a \leq 0$ or $y - b \leq 0$ (since $x - a > 0$ and $y - b > 0$ would mean $(x - a) + (y - b) > 0$). In the first case, $x \leq a$, implying that $x \in A$, by Remark C.2, and hence contradicting the fact that $x \in \mathbb{Q} - A$. In the second case, $y \leq b$ implying that $y \in B$ and contradicting the fact that $y \in \mathbb{Q} - B$.

Proof of Condition (2): Let $c \in A + B$ and $d \in \mathbb{Q} - (A + B)$. We need to show that $c < d$. By definition of $A + B$, $c = a + b$ for some $a \in A$ and $b \in B$. Note that $d - a \notin B$, since if $d - a = b' \in B$ then $d = a + b' \in A + B$. Hence by condition (2) applied to B, $b < d - a$. Therefore $c = a + b < d$.

Proof of condition (3): left as HW. □

Recall that $\underline{0} = \{x \in \mathbb{Q} : x < 0\}$.

Theorem C.10. *(1) For all Dedekind sets A, $\underline{0} + A = A$ (i.e. $\underline{0}$ is the additive identity)*
(2) For all Dedekind sets A, B, then $A + B = B + A$ (i.e. addition is commutative)
(3) For all Dedekind sets A, B, C, then $(A + B) + C = A + (B + C)$

(i.e. addition is associative)
(4) For every Dedekind set A there is a Dedekind set denoted by $-A$, such that
$A + (-A) = \underline{0}$ *(i.e. every Dedekind set has an additive inverse).*
(5) If $A < B$ then $A + C < B + C$. for all Dedekind sets C
(6) For every $x, y \in \mathbb{Q}$, $\underline{x} + \underline{y} = \underline{x + y}$.

Proof. This result is technical.

□

Multiplication of Dedekind sets. Now are are going to define multiplication of Dedekind sets. The informal idea is as follows: by Remark C.4, every Dedekind set is of the form $\underline{\alpha} = \{a \in \mathbb{Q} : a < \alpha\}$ for some real α. We want to define a multiplication of $\underline{\alpha}$ with $\underline{\beta} = \{b \in \mathbb{Q} : b < \beta\}$, so that

$$\underline{\alpha} \cdot \underline{\beta} = \underline{\alpha \cdot \beta} = \{c \in \mathbb{Q} : c < \alpha \cdot \beta\}.$$

Unfortunately, we cannot use this as a formal definition, since we didn't define real numbers yet, and we cannot use Remark C.4.

The definition of addition of Dedekind sets suggests that we should define $A \cdot B$ as $\{a \cdot b : a \in A, b \in B\}$. Indeed, if $a \in \underline{x}$ and $b \in \underline{y}$ and $a > 0$ or $b > 0$ then $ab \in \underline{xy}$. Unfortunately this definition does not work if $a, b < 0$. E.g. $-10 \in \underline{2}$, $-10 \in \underline{3}$ but $(-10)(-10) \notin \underline{6}$. Therefore, the definition of multiplication needs to take into account the signs of a and b. Hence for all Dedekind sets $A, B \subseteq \mathbb{Q}$, we define

$$A \cdot B = \begin{cases} \{x \cdot y : x \in A, x > 0, y \in B\} & \text{if } A > \underline{0} \\ \{x \cdot y : x \in A, y \in B, y > 0\} & \text{if } B > \underline{0} \end{cases}$$

and $A \cdot B = (-A) \cdot (-B)$ for $A \leq \underline{0}$ and $B \leq \underline{0}$.

Theorem C.11. *If A, B are Dedekind sets then so is $A \cdot B$.*

Theorem C.12. *For all Dedekind sets A, B, C*
(1) $A \cdot \underline{1} = A$
(2) $A \cdot B = B \cdot A$
(3) $A \cdot (B \cdot C) = (A \cdot B) \cdot C$.
(4) $A(B + C) = AB + AC$.
(5) If $A < B$ and $C > 0$ then $A \cdot C < B \cdot C$.

For any Dedekind sets $A, B > \underline{0}$ we define

$$A/B = \{a/b \in \mathbb{Q} : a \in A, b \in \mathbb{Q} - B\}.$$

Proposition C.13. *For all Dedekind sets $A, B > \underline{0}$,*
(1) A/B is a Dedekind set.
(2) $A/B \cdot B = A$.

We've already defined A/B where $A$and B are both > 0. We now define A/B in the remaining cases. For all Dedekind sets A and B, where $B \neq \underline{0}$, define A/B as follows:

$$A/B = \begin{cases} \underline{0} & \text{if } A = \underline{0} \\ -((-A)/B) & \text{if } A < \underline{0},\ B > \underline{0} \\ -(A/(-B)) & \text{if } A > \underline{0},\ B < \underline{0} \\ (-A)/(-B) & \text{if } A < \underline{0},\ B < \underline{0}. \end{cases}$$

The point of this definition is that the quotients on the right side involve positive Dedekind sets only and, hence, are defined by Proposition C.13. Therefore, A/B is a Dedekind set for all Dedekind sets A and $B \neq \underline{0}$. Furthermore, we have the following generalization of Proposition C.13:

Proposition C.14. *For all Dedekind sets A and $B \neq \underline{0}$ we have $A/B \cdot B = A$.*

Summarizing the discussion above, we see that
(1) every rational number defines a Dedekind set
(2) our intuition about irrational real numbers tells us that each of them defines a Dedekind set as well
(3) Dedekind sets can be added, multiplied, and divided, and that these operations satisfy the properties of addition, multiplication and division of real numbers.
(4) one can define inequalities $A < B$ between Dedekind sets.

Therefore, applying the principle:
"if it looks like a duck, swims like a duck and quacks like a duck, then it is a duck"
we define real numbers as Dedekind sets.

Definition C.15. *A real number is a Dedekind set. We denote the set of all real numbers by $\mathbb{R}$. Real numbers of the form $\underline{x}$ for $x \in \mathbb{Q}$ are called rational real numbers. The real numbers which are not rational are called irrational.*

By our earlier definition,

$$\underline{\sqrt{2}} = \{x \in \mathbb{Q} : (x^2 < 2) \vee (x < 0)\}$$

Indeed, one can prove that

$$\underline{\sqrt{2}} \cdot \underline{\sqrt{2}} = \underline{2} \text{ and } \underline{\sqrt{2}} > \underline{0}. \tag{26}$$

Therefore, denoting the above set by $\underline{\sqrt{2}}$ is fully justified. By Proposition 19.1, $\underline{\sqrt{2}}$ is an irrational real number.

Definition C.16. *For every positive $x \in \mathbb{R}$ and for every $n \in \mathbb{Z}$ let*

$$\sqrt[n]{x} = \{a \in \mathbb{Q} : (a \leq 0) \vee (a^n < x)\}.$$

It is called the n-th root of x.

Theorem C.17. *For every positive $x \in \mathbb{R}$ and for every $n \in \mathbb{N}$,*
(1) $\sqrt[n]{x}$ is a Dedekind set.
(2) $\sqrt[n]{x}$ is the unique positive real number such that $(\sqrt[n]{x})^n = x$.

Sketch of Proof:
We leave part (1) as HW.
We prove (2) by contradiction. Suppose that $A \neq \sqrt[n]{x}$ and $A^n = x$, $A > 0$. If $A < \sqrt[n]{x}$, then by Proposition C.12,

$$A < \sqrt[n]{x} \Rightarrow A^2 < A \cdot \sqrt[n]{x} < (\sqrt[n]{x})^2 \Rightarrow ... \Rightarrow A^n < (\sqrt[n]{x})^n,$$

by an inductive argument (similar to that of the proof of Proposition 9.5(4)), leading to a contradiction. If $\sqrt[n]{x} < A$ then the proof is analogous. □

Given real numbers $x < y$, we define

$$\begin{aligned}(x, y) &= \{z \in \mathbb{R} : x < z < y\}\\ [x, y) &= \{z \in \mathbb{R} : x \leq z < y\}\\ (x, y] &= \{z \in \mathbb{R} : x < z \leq y\}\\ [x, y] &= \{z \in \mathbb{R} : x \leq z \leq y\}.\end{aligned}$$

Therefore (a, b) may mean either an ordered pair, $\{a, \{b\}\}$, or an open interval from a to b. Usually the specific meaning of (a, b) is obvious from the context, but if not then one can specify whether one means an ordered pair or an open interval.

Although $\pm\infty$ is not a number, it is useful and natural to expand the above notation to

$$(x, \infty) = \{z \in \mathbb{R} : x < z\},\ [x, \infty) = \{z \in \mathbb{R} : x \leq z\},$$

$$(-\infty, y) = \{z \in \mathbb{R} : z < y\},\ (-\infty, y] = \{z \in \mathbb{R} : z \leq y\},\ (-\infty, \infty) = \mathbb{R}.$$

PROBLEMS C.

Problem C.1. *(1) How would you define $\underline{-\sqrt{2}}$?*
(2) Proof that your definition satisfies conditions (1) and (2) of Dedekind sets.

Problem C.2. *Complete the remaining part of the proof of Proposition C.9. That is, if A, B are Dedekind sets then $A + B$ satisfies condition (3) of Dedekind sets.*

Problem C.3. *Proof of Theorem C.10(1).* Hint: *Prove two inclusions:* $A + \underline{0} \subseteq A$ *(easy) and* $A + \underline{0} \supset A$ *(harder). To prove the second inclusion, use the fact that for every* $a \in A$ *there is an* $a' \in A$ *larger than* a.

Problem C.4. *Let* $\underline{\sqrt{2}} = \{x \in \mathbb{Q} : (x^2 < 2) \vee (x < 0)\}$. *Prove that*
(a) $\underline{\sqrt{2}} > \underline{1}$
(b) $\underline{\sqrt{2}} \cdot \underline{\sqrt{2}} \leq \underline{2}$. *(In fact, we have* $\underline{\sqrt{2}} \cdot \underline{\sqrt{2}} = \underline{2}$, *c.f. eq. (26), but to make things simpler for you, I do not ask you to prove it.)*

Problem C.5. *Prove* $\underline{1}/\underline{2} = \underline{1/2}$ *using the definition of* A/B *(without referring to Proposition C.13).*

Problem C.6. *Let* $x > 0$ *and* $n \in \mathbb{N}$. *Prove a piece of Theorem C.17(1) by showing that* $\sqrt[n]{x}$ *satisfies the following properties of Dedekind sets:*
(1) $\sqrt[n]{x} \neq \emptyset$ *and* $\sqrt[n]{x} \neq \mathbb{Q}$.
(2) if $a \in \sqrt[n]{x}$ *and* $b \in \mathbb{Q} - \sqrt[n]{x}$ *then* $a < b$.

Problem C.7. *Find irrational real numbers* x, y *such that* $x + y$ *is rational. (*Hint*: You can take* $x = \sqrt{2}$, *which is irrational by Proposition 19.1. You need to prove that your* y *is irrational.)*

Problem C.8. *Using your calculus knowledge, show that* $\{x \in \mathbb{Q} : x^3 + 3x < 1\}$ *is a Dedekind set.*

Appendix D. Series and Decimal Expansions

Informally speaking, an infinite series is a sum of terms of an infinite sequence, $\sum_{n=1}^{\infty} a_n = a_1 + a_2 + ...$ (We often abbreviate infinite series to "series".) To make this definition formal we need to use a notion of a limit. $S_N = \sum_{n=1}^{N} a_n$ is called N-th partial sum. We say that $\sum_{n=1}^{\infty} a_n$ converges to S if $S = lim_{N\to\infty} S_N$, where S is finite. We say that $\sum_{n=1}^{\infty} a_n$ diverges to ∞ if $lim_{N\to\infty} S_N = \infty$.

Example D.1. *(1) For the geometric series,* $a_n = aq^{n-1}$,

$$S_N = a(1 + q + ... + q^{N-1}) = a\frac{1-q^N}{1-q}.$$

Hence the infinite series converges to $lim_{N\to\infty} S_N = a\frac{1}{1-q}$ *if* $|q| < 1$.
(2) The p-series, $\sum_{n=1}^{\infty} 1/n^p$, *converges for* $p > 1$ *and diverges to* ∞ *for* $p \leq 1$.
(3) The infinite series $1 - 1 + 1 - 1...$ *neither converges to diverges to* ∞.

Numbers $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$ are called digits.

Lemma D.2. *For any sequence of digits* $a_1, a_2, ...$, *the infinite series* $a_1 \cdot 10^{-1} + a_2 \cdot 10^{-2} + a_3 \cdot 10^{-3}...$ *converges.*

Proof. Since the terms are non-negative, the sequence of partial sums S_N is non-decreasing. Furthermore, $S_N < (a_1 + 1) \cdot 10^{-1}$. (That can be proved by induction on N.) Now the statement follows from the Monotone Sequence Property. □

A decimal numeral system is a method of denoting real numbers as sequences of digits. A sequence

$$\pm b_m...b_0.a_1a_2a_3...$$

denotes the sum

$$x = \pm(b_m \cdot 10^m + ... + b_1 \cdot 10 + b_0 + a_1 \cdot 10^{-1} + a_2 \cdot 10^{-2} + a_3 \cdot 10^{-3}...) \tag{27}$$

There are finitely many b's (in front of the decimal point) but there may be a finite or infinite number of a's. By the lemma above x is always a finite number. The right side of (27) is called a decimal expansion or decimal representation of x.

Remark D.3. *If* $a_k = 0$ *for all* $k > n$ *then* $b_m...b_0.a_1a_2a_3...$ *(infinite decimal expansion) is equal to and identified with* $b_m...b_0.a_1a_2a_3...a_n$ *(finite expansion).*

Lemma D.4. *For every* $x \in \mathbb{R}$ *there is the greatest* $m \in \mathbb{Z}$ *such that* $x \geq 10^m$

Proof. in class □

If $x > 0$ then such expansion of x can be constructed as follows:
- Let m be the greatest integer such that $x \geq 10^m$. Its existence is implied by Lemma D.4
- Let $b_m = \lfloor x/10^m \rfloor$, $b_{m-1} = \lfloor (x - b_m \cdot 10^m)/10^{m-1} \rfloor$, $b_{m-2} = \lfloor (x - b_m \cdot 10^m - b_{m-1} \cdot 10^{m-1})/10^{m-2} \rfloor$, and so on. Finally, let
- $b_0 = \lfloor x - (b_m \cdot 10^m + b_{m-1} \cdot 10^{m-1} + ... + b_1 \cdot 10) \rfloor$.

Let $x_0 = x - b_m \cdot 10^m - b_{m-1} \cdot 10^{m-1} - ... - b_1 \cdot 10 - b_0$. Note that $0 \leq x_0 < 1$ and that $x - x_0 \in \mathbb{Z}$. Therefore $x_0 = x - \lfloor x \rfloor$.

Now we define $a_1, a_2, ...$ inductively:
- $a_1 = \lfloor x_0 \cdot 10 \rfloor$, $a_2 = \lfloor x_0 \cdot 10^2 - a_1 \cdot 10 \rfloor$.

Suppose that $a_1, ..., a_n$ are defined. Then
- $a_{n+1} = \lfloor (x_0 \cdot 10^{n+1} - (a_1 \cdot 10^n + ... + a_{n-1} \cdot 10 + a_n \cdot 10)) \rfloor$.

If x has a decimal expansion $b_m...b_0.a_1a_2a_3...$ then we declare the decimal expansion of $-x$ to be $-b_m...b_0.a_1a_2a_3...$ Hence every real number has a decimal expansion.

A decimal expansion is finite iff $a_n = 0$ for large n. (Recall from Sec. 20 that it means that there is N such that $a_n = 0$ for all $n \geq N$.) Such zeros are usually omitted in the notation.

We say that a decimal expansion $b_m...b_0.a_1a_2a_3...$ is repeating or recurring of period $p \in \mathbb{N}$ if $a_{n+p} = a_n$ for large n. We denote such decimal expansion by $b_m...b_0.a_1a_2a_3...a_n\overline{a_{n+1}...a_{n+p}}$. For example $1/3 = 0.\overline{3}, 1/7 = 0.\overline{142857}, 1/12 = 0.08\overline{3}$.

Remark D.5. *Some real numbers have more than one decimal expansion. Recall that the infinite geometric series* $a + aq + aq^2 + ...$ *converges iff* $|q| < 1$ *and, in this case, its sum is* $\frac{a}{1-q}$. *Therefore* $0.\overline{9} = 0.9 \cdot (1 + 10^{-1} + 10^{-2} + ...)$ *is a converging infinite geometric series and its sum is* $0.9 \cdot \frac{1}{1-10^{-1}} = 1$. *Hence* $0.\overline{9} = 1$ *!*

Theorem D.6. *Every real number* x *has a unique decimal expansion without terminal repeating* 9.

Theorem D.7. *Every real number with repeating decimal expansion is rational.*

Proof. Assume first that $x = 0.\overline{a_1...a_p}$. Then

$$x = 0.a_1...a_p + 0.a_1...a_p \cdot 10^{-p} + ... = 0.a_1...a_p(1 + 10^{-p} + 10^{-2p} + ...)$$

is a converging geometric series whose sum is

$$x = 0.a_1...a_p \cdot \frac{1}{1 - 10^{-p}} = \frac{a_1...a_p}{10^p(1 - 10^{-p})} = \frac{a_1...a_p}{10^p - 1}.$$

It is a rational number.

Suppose now that $x = b_m ... b_0.a_1 ... a_n\overline{a_{n+1} ... a_{n+p}}$. Clearly,

$$x_0 = b_m ... b_0.a_1 ... a_n = b_m \cdot 10^m + ... + b_0 + a_1 \cdot 10^{-1} + ... + a_n \cdot 10^{-n}$$

is a finite sum of rational numbers and, hence, a rational number itself. We have also proved above already that $0.\overline{a_{n+1} ... a_{n+p}}$ is rational. Therefore, $10^{-n} \cdot 0.\overline{a_{n+1} ... a_{n+p}}$ is also rational and, hence, $x = x_0 + 10^{-n} \cdot 0.\overline{a_{n+1} ... a_{n+p}}$ is rational as well. □

Theorem D.8. *Every rational number has either finite or a repeating expansion.*

For example, the period of the expansion $1/7 = 0.\overline{142857}$ is 6.

Proof. in class. Consider any rational number. Without loss of generality we can assume that it is positive. Hence it can be written as $n + p/q$, where $n = 0, 1, ...$ and $0 \le p/q < 1$.

• First case: Assume first that q is indivisible by 2 and by 5.
By "Fermat's Little Theorem" (Theorem 12.22), $q | 10(10^{q-1} - 1)$. I.e. $qa = 10^{q-1} - 1$ for some $a \in \mathbb{N}$ and

$$\frac{p}{q} = \frac{pa}{qa} = \frac{pa}{10^{q-1}-1} = \frac{1}{10^{q-1}} \frac{pa}{1-10^{1-q}} = 10^{-q+1} pa(1+10^{-(q-1)}+10^{-2(q-1)}+....).$$

Since $pa < 10^{q-1}$, it has at most $q-1$ digits. These $q-1$ digits are recurring in the decimal expansion of p/q.

• Second case: $q = 2^c 5^d q'$ where $c, d \in \mathbb{N}$ and q' is not divisible by 2 nor 5. Then by multiplying both p and q by $5^c 2^d$ we get $p/q = 5^c 2^d p/10^{c+d} q'$. Since division by 10^{c+d} simply shifts the decimal point, it is enough to prove that $5^c 2^d p/q'$ has a repeating decimal expansion. Since $5^c 2^d p/q' = \lfloor 5^c 2^d p/q' \rfloor + p'/q'$, where $0 \ge p'/q' < 1$, the statement follows from the case above.

□

Corollary D.9. *A real number is rational if and only if it has a finite or repeating decimal expansion.*

PROBLEMS D.

Problem D.1. *Find the rational presentation, p/q of the number* $0.\overline{123}$.

Problem D.2. *Give an actual, explicit example of a non-repeating (non-terminating) decimal. Your answer should be such that you could determine without a computer what the thousandth decimal place would be. 'The decimal expansion of π or of $\sqrt{2}$' is not an answer, since you can't describe these decimal expansions explicitly (what is the thousandth decimal place of $\sqrt{2}$?).*

Problem D.3. *How would you characterize numbers q (in terms of their divisors) such that p/q has a finite decimal expansion for every p?*

Proof. Let $0 \leq a_n \leq 1/2^n$ for every n. Prove that $\sum_{i=1}^{\infty} a_n$ is converging. □

Index